

JOeSandbox Cloud BASIC



ID: 605429

Sample Name: ll.exe

Cookbook: default.jbs

Time: 10:00:35

Date: 08/04/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report II.exe	5
Overview	5
General Information	5
Detection	5
Signatures	5
Classification	5
Process Tree	5
Malware Configuration	5
Yara Signatures	5
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	6
AV Detection	6
Exploits	6
Spreading	6
Spam, unwanted Advertisements and Ransom Demands	6
Persistence and Installation Behavior	6
Mitre Att&ck Matrix	6
Behavior Graph	7
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	9
URLs	9
Domains and IPs	9
Contacted Domains	9
World Map of Contacted IPs	9
Public IPs	9
Private	9
General Information	11
Warnings	12
Simulations	12
Behavior and APIs	12
Joe Sandbox View / Context	12
IPs	12
Domains	12
ASNs	12
JA3 Fingerprints	12
Dropped Files	12
Created / dropped Files	12
C:\MSOCache\All Users\R3ADM3.txt	12
C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\OWOW64WW.cab	13
C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\OWOW64WW.cab.NB65 (copy)	13
C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\Office64WW.xml	13
C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\Office64WW.xml.NB65 (copy)	14
C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\ProPlusWW.xml	14
C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\ProPlusWW.xml.NB65 (copy)	14
C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\ProPsWW.cab	15
C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\ProPsWW.cab.NB65 (copy)	15
C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\ProPsWW2.cab	15
C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\ProPsWW2.cab.NB65 (copy)	16
C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\R3ADM3.txt	16
C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\Setup.xml	16
C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\Setup.xml.NB65 (copy)	17
C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\pkeyconfig-office.xrm-ms	17
C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\pkeyconfig-office.xrm-ms.NB65 (copy)	17
C:\MSOCache\All Users\{90160000-0016-0409-0000-00000000FF1CE}-C\ExcelLR.cab	18
C:\MSOCache\All Users\{90160000-0016-0409-0000-00000000FF1CE}-C\ExcelLR.cab.NB65 (copy)	18
C:\MSOCache\All Users\{90160000-0016-0409-0000-00000000FF1CE}-C\ExcelMUI.xml	18
C:\MSOCache\All Users\{90160000-0016-0409-0000-00000000FF1CE}-C\ExcelMUI.xml.NB65 (copy)	19
C:\MSOCache\All Users\{90160000-0016-0409-0000-00000000FF1CE}-C\R3ADM3.txt	19
C:\MSOCache\All Users\{90160000-0016-0409-0000-00000000FF1CE}-C\Setup.xml	19
C:\MSOCache\All Users\{90160000-0016-0409-0000-00000000FF1CE}-C\Setup.xml.NB65 (copy)	20
C:\MSOCache\All Users\{90160000-0018-0409-0000-00000000FF1CE}-C\PowerPointMUI.xml	20
C:\MSOCache\All Users\{90160000-0018-0409-0000-00000000FF1CE}-C\PowerPointMUI.xml.NB65 (copy)	20
C:\MSOCache\All Users\{90160000-0018-0409-0000-00000000FF1CE}-C\PptLR.cab	21
C:\MSOCache\All Users\{90160000-0018-0409-0000-00000000FF1CE}-C\PptLR.cab.NB65 (copy)	21
C:\MSOCache\All Users\{90160000-0018-0409-0000-00000000FF1CE}-C\R3ADM3.txt	21
C:\MSOCache\All Users\{90160000-0018-0409-0000-00000000FF1CE}-C\Setup.xml	22
C:\MSOCache\All Users\{90160000-0018-0409-0000-00000000FF1CE}-C\Setup.xml.NB65 (copy)	22

C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PubLR.cab	22
C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PubLR.cab.NB65 (copy)	23
C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PublisherMUI.xml	23
C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PublisherMUI.xml.NB65 (copy)	23
C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\R3ADM3.txt	24
C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\Setup.xml	24
C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\Setup.xml.NB65 (copy)	24
C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlkLR.cab	24
C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlkLR.cab.NB65 (copy)	25
C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlookMUI.xml	25
C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlookMUI.xml.NB65 (copy)	25
C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\R3ADM3.txt	26
C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\Setup.xml	26
C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\Setup.xml.NB65 (copy)	26
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\R3ADM3.txt	27
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\Setup.xml	27
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\Setup.xml.NB65 (copy)	27
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordLR.cab	28
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordLR.cab.NB65 (copy)	28
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordMUI.xml	28
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordMUI.xml.NB65 (copy)	29
C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proofing.xml	29
C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proofing.xml.NB65 (copy)	29
C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\R3ADM3.txt	29
C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Setup.xml	30
C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Setup.xml.NB65 (copy)	30
C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfLR.cab	30
C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfLR.cab.NB65 (copy)	31
C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.xml	31
C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.xml.NB65 (copy)	31
C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\R3ADM3.txt	32
C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\Setup.xml	32
C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\Setup.xml.NB65 (copy)	32
C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.cab	33
C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.cab.NB65 (copy)	33
C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.xml	33
C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.xml.NB65 (copy)	34
C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\R3ADM3.txt	34
C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\Setup.xml	34
C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\Setup.xml.NB65 (copy)	35
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.xml	35
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.xml.NB65 (copy)	35
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OnoteLR.cab	35
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OnoteLR.cab.NB65 (copy)	36
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\R3ADM3.txt	36
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\Setup.xml	36
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\Setup.xml.NB65 (copy)	37
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveLR.cab	37
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveLR.cab.NB65 (copy)	37
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveMUI.xml	38
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveMUI.xml.NB65 (copy)	38
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\R3ADM3.txt	38
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\Setup.xml	39
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\Setup.xml.NB65 (copy)	39
C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.cab	39
C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.cab.NB65 (copy)	40
C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.xml	40
C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.xml.NB65 (copy)	40
C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\R3ADM3.txt	41
C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\Setup.xml	41
C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\Setup.xml.NB65 (copy)	41
C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\OSMUXMUI.cab	41
C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\OSMUXMUI.cab.NB65 (copy)	42
C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\OSMUXMUI.xml	42
C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\OSMUXMUI.xml.NB65 (copy)	42
C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\R3ADM3.txt	43
C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\Setup.xml	43
C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\Setup.xml.NB65 (copy)	43
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OffSetLR.cab	44
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OffSetLR.cab.NB65 (copy)	44

Static File Info	44
General	44
File Icon	45
Static PE Info	45
General	45
Entrypoint Preview	45
Rich Headers	46
Data Directories	47
Sections	47
Resources	47
Imports	47
Possible Origin	47

Network Behavior	48
Snort IDS Alerts	48
TCP Packets	48
UDP Packets	50
ICMP Packets	50
HTTP Request Dependency Graph	50
HTTPS Proxied Packets	50
Statistics	181
System Behavior	181
Analysis Process: ll.exePID: 7164, Parent PID: 5608	181
General	181
File Activities	182
File Created	182
File Moved	188
File Written	197
File Read	341
Registry Activities	347
Disassembly	347

Windows Analysis Report

ll.exe

Overview

General Information

Sample Name:

ll.exe

Analysis ID:

605429

MD5:

f746ea39c0c5ff9...

SHA1:

dac28369f5a443..

SHA256:

7f6dbd9fa0cb7ba..

Infos:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Score:

76

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Multi AV Scanner detection for subm...

Antivirus / Scanner detection for sub...

Infected executable files (exe, dll, sy...

Machine Learning detection for sam...

Writes many files with high entropy

Connects to many different private I...

Connects to many different private I...

Uses 32bit PE files

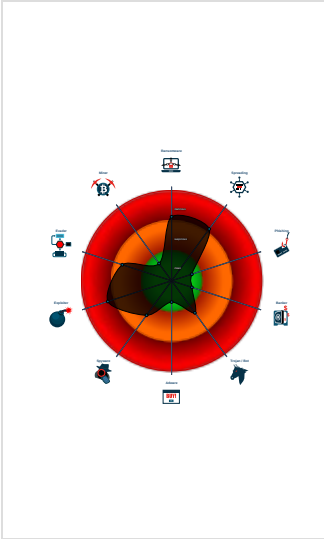
Queries the volume information (nam...

Contains functionality to check if a d...

May sleep (evasive loops) to hinder...

Uses code obfuscation techniques (...)

Classification



Process Tree

System is w10x64

ll.exe (PID: 7164 cmdline: "C:\Users\user\Desktop\ll.exe" MD5: F746EA39C0C5FF9D0A1F2D250170AD80)

cleanup

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ICMP Destination Unreachable Port Unreachable - Source IP: 192.168.2.1 - Destination IP: 192.168.2.3

Timestamp:	04/08/22-10:01:39.199823
SID:	402
Protocol:	ICMP
Classtype:	Misc activity

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

Exploits



Connects to many different private IPs (likely to spread or exploit)

Connects to many different private IPs via SMB (likely to spread or exploit)

Spreading



Infects executable files (exe, dll, sys, html)

Spam, unwanted Advertisements and Ransom Demands



Writes many files with high entropy

Persistence and Installation Behavior



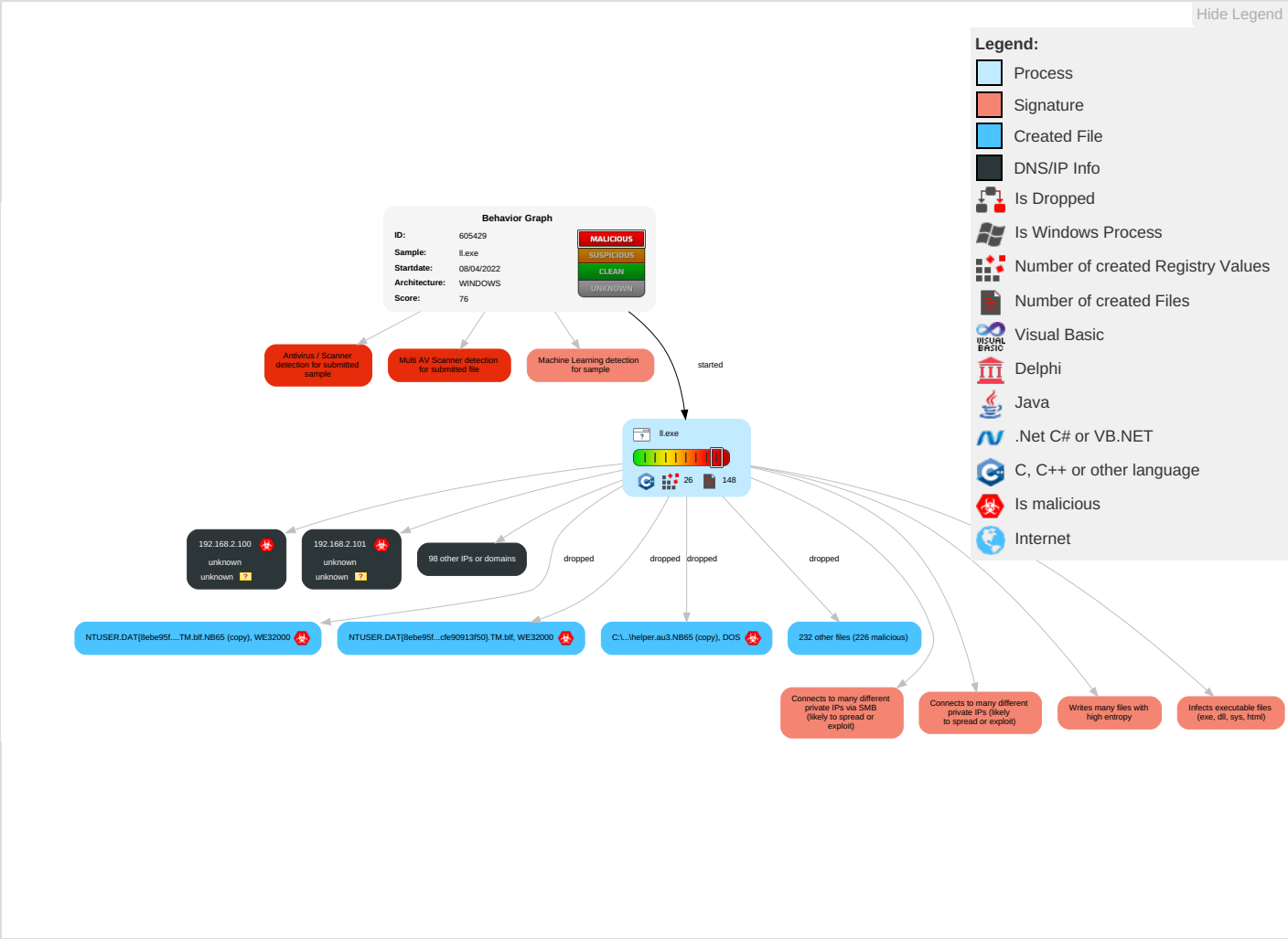
Infects executable files (exe, dll, sys, html)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	Path Interception	Path Interception	3 Masquerading	1 Input Capture	1 Network Share Discovery	1 Taint Shared Content	1 Input Capture	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Virtualization/Sandbox Evasion	LSASS Memory	1 System Time Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	2 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	4 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	2 3 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

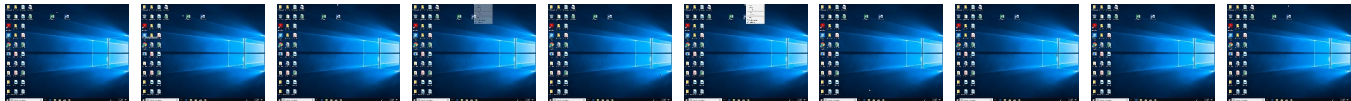
Behavior Graph

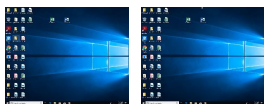


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ll.exe	57%	Virustotal		Browse
ll.exe	73%	ReversingLabs	Win32.Ransomwar e.Conti	
ll.exe	100%	Avira	HEUR/AGEN.1213 270	
ll.exe	100%	Joe Sandbox ML		

Dropped Files

 No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.ll.exe.f20000.0.unpack	100%	Avira	HEUR/AGEN.12 13270		Download File

Source	Detection	Scanner	Label	Link	Download
1.0.11.exe.f20000.0.unpack	100%	Avira	HEUR/AGEN.12 13270		Download File

Domains

 No Antivirus matches
--

URLs

 No Antivirus matches
--

Domains and IPs

Contacted Domains

 No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
----	--------	---------	------	-----	----------	-----------

Private

IP
192.168.2.148
192.168.2.149
192.168.2.146
192.168.2.147
192.168.2.140
192.168.2.141
192.168.2.144
192.168.2.145

IP
192.168.2.142
192.168.2.143
192.168.2.159
192.168.2.157
192.168.2.158
192.168.2.151
192.168.2.152
192.168.2.150
192.168.2.155
192.168.2.156
192.168.2.153
192.168.2.154
192.168.2.126
192.168.2.247
192.168.2.127
192.168.2.248
192.168.2.124
192.168.2.245
192.168.2.125
192.168.2.246
192.168.2.128
192.168.2.249
192.168.2.129
192.168.2.240
192.168.2.122
192.168.2.243
192.168.2.123
192.168.2.244
192.168.2.120
192.168.2.241
192.168.2.121
192.168.2.242
192.168.2.97
192.168.2.137
192.168.2.96
192.168.2.138
192.168.2.99
192.168.2.135
192.168.2.98
192.168.2.136
192.168.2.139
192.168.2.250
192.168.2.130
192.168.2.251
192.168.2.91
192.168.2.90
192.168.2.93
192.168.2.133
192.168.2.254
192.168.2.92
192.168.2.134
192.168.2.95
192.168.2.131
192.168.2.252
192.168.2.94
192.168.2.132
192.168.2.253
192.168.2.104
192.168.2.225

IP
192.168.2.105
192.168.2.226
192.168.2.102
192.168.2.223
192.168.2.103
192.168.2.224
192.168.2.108
192.168.2.229
192.168.2.109
192.168.2.106
192.168.2.227
192.168.2.107
192.168.2.228
192.168.2.100
192.168.2.221
192.168.2.101
192.168.2.222
192.168.2.220
192.168.2.115
192.168.2.236
192.168.2.116
192.168.2.237
192.168.2.113
192.168.2.234
192.168.2.114
192.168.2.235
192.168.2.119
192.168.2.117
192.168.2.238
192.168.2.118
192.168.2.239
192.168.2.111
192.168.2.232

General Information	
Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	605429
Start date and time:	2022-04-08 08:00:35 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ll.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal76.rans.spre.expl.winEXE@1/746@0/100
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.2% (good quality ratio 92.6%) • Quality average: 75.4% • Quality standard deviation: 28.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, VSSVC.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 93.184.221.240, 23.10.249.49
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteFile calls found.

Simulations

Behavior and APIs

 No simulations

Joe Sandbox View / Context

IPs

 No context

Domains

 No context

ASNs

 No context

JA3 Fingerprints

 No context

Dropped Files

 No context

Created / dropped Files

C:\MSOCache\All Users\R3ADM3.txt

Process:	C:\Users\user\Desktop\l.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	1290
Entropy (8bit):	4.607071403570347
Encrypted:	false
SSDEEP:	24:jtVCRJFxFtmyib6WAn/O4i5hFmJZED2GbuiRGDFZcfSO+7DzGbn2vJKsXFFINNF:jtVCLxzsbxqUbuiRGDKqO+bGb2vJKht
MD5:	FADB0F250D20EF2F614C4AB5D5D3AB0F
SHA1:	41E8255C91A40A8E832A8AC05747C9A579F55D07
SHA-256:	2CD73F11DA515955B62A930CA4DEFDE9CCB5230B8F5809E3C304EF854604EDA3
SHA-512:	E97F4B069ACB91C332BDDCA5C4314CBE6CC79C37E93CBB3F4D8B37544B49C2868E23B603FE4563A8961616F137CF646153A82F387D9C55CF8191108E86CF136
Malicious:	false
Reputation:	low
Preview:	_____ .\ \ _ _ V _ _ _ . \ / / _ _ _ \ . . ` _ _ \ _ \ \ \ . \ / / \ / \ _ / . \ \ \ ^ _ ^ _ _ / ...By now it's probably painfully apparent that your environment has..been infected with ransomware. You can thank Conti for that.....We've modified the code in a way that will prevent you from decrypting..it with their decryptor.....We've exfiltrated a significant amount of data including private emails,..financial information, contacts, etc.....Now, if you wish to contact us in order to save your files from permanent..encryption you can do so by emailing network_battalion_0065@riseup.net.....You have 3 days to establish contact. Failing to do so will result in..that data remaining permanently encrypted.....While we have very little sympathy for the situation you find yourselves..in right now, we will honor our agreement to restore your files across..the affected environment once contact is established and payment is made

C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\OWOW64WW.cab	
Process:	C:\Users\user1\Desktop\ll.exe
File Type:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	30592722
Entropy (8bit):	7.999968945971768
Encrypted:	true
SSDEEP:	786432:omK8OSSRxbgW01vsFz5dvWqwAWYJeY8kKxkQC6y3hGiZMpC1muTeN:jKCSRqH0TFRwAtEkKxhvy3h/MsTeN
MD5:	A087182116F101A533FACFDC1963F7F0
SHA1:	9D8951A23DA853AE1516826CC5048F99B5313D3D
SHA-256:	6DA06EBE21D68EFE88886AB3C45226BE6D57E0C9FEE46E689E4F61D7323A3998
SHA-512:	7E7A4AE699125D53B9103BF46EEEA2BF3441E5A5232F4AA519D12488EBA387BA705796C490C146CAA5F17551CAA96E4A04F8D110D2EA4AAC6D4FE6AB08A72AD3
Malicious:	true
Reputation:	low
Preview:	.3...IW...v.b..Tp\..r...k.a...A.?z...Y.....%j.....ig.t..6...8...a(Tl.../..j....O..]B9k.z.Yf....(s.+..h.(.....RGo..0.m.30.....L.9..?N.....p...[.L..'...U...((f....._..b.i.y... .G."...:~I.E..+..A...[C8.....#...>3.WJ.84z..x.y.m...^.*T.a.....mz1.\$2k...nK=-..A\!fm.^?r.@...\$O%Z....).H.9..._..j..q.^2w..Na.....W#\$hyQH....+.....@.D.-.....g...).7K(WK. q...w...3...&.ExC.yy=..../*.....Lt.7....n.M.B7..[.1.p...^.]YADy...[.]yA.#...\$.K.....{w.@&w.i-...?..&@..(W.KN{%.J.k<aD_l.GT5Z...\$....L.....!..l..t.<.<.y...4*.....XzS.. .C.+P=...3..k.G.4.....=j-...'.u.S....(.....!o"X...f...uz'.jgOj..58A.....q..F..%r....d.W[.]..."m."5%...[.]...pK....[yR[.2....n.Z....l.....p'.L..3.A...O..>wT.....o>!...l.....J. 9Sj.Z....5.....1e.\$.....v.?.....T:9..\`...6.[R.T...f.g.!...d#.D200q....~"/!&kt..t.uA...x.....7...zq.W....?&.....o.....D.x....8...[.].wxH0..

C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\OWOW64WW.cab.NB65 (copy)  	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	30592722
Entropy (8bit):	7.999968945971768
Encrypted:	true
SSDEEP:	786432:omK8OSSRxbgw01lvsFzf5dvWqwAWYJeY8kKxkQC6y3hGiZMpC1muTeN;jKCSRqH0TFRwAtEkKxhvy3h/MsTeN
MD5:	A087182116F101A533FACFDC1963F7F0
SHA1:	9D8951A23DA853AE1516826CC5048F99B5313D3D
SHA-256:	6DA06EBE21D68EFE88886AB3C45226BE6D57E0C9FEE46E689E4F61D7323A3998
SHA-512:	7E7A4AE699125D53B9103BF46EEEA2BF3441E5A5232F4AA519D12488EBA387BA705796C490C146CAA5F17551CAA96E4A04F8D110D2EA4AAC6D4FE6AB08A72AD3
Malicious:	true
Reputation:	low
Preview:	.3...IW...v.b..Tp\l.r...r.k.a...A...?z...Y...%j.....ig.t..6...8...a(Tl.../...j....O...J]B9k.z.Yf....(s.+..h.(....RGo..0..m.30.....L.9..?..N.....p...[...L...U...((f....._b..i.y... .G..."LE..+A... C8.....#...>3.WJ.84z..x.y.m.^*T.a.....mz1.\$2k...nK=..A\fm.^?r.@...\$O%Z....).H.9..._j..q.^2w..Na.....W#\$hyQH...+.....@.D.....g...).7K(WK. q...w...3...&ExC.yy=.../*.....Lt.7....n.M.B7.. .1.p...^..]YADy... .yA.#...\$.K.....{w.@&w.i-...?..&@..(W.KN{%.J.k<aD_\l.GT5Z..\$....L...!..l..t.<.<.y_...4*....,XzS.. C.+P=.../3...k.G.4....=j-'.u.S....(.....lo"X...f..uz'.jgOj..58A.....q.F..%r....d.W[.]..."m."5%...]-pK... yR[.2....n.Z....~l....p'.L..3.A...O..>wT.....o>!...l....J. 9S Z.....5.....1e.\$....v.?.....T:9..\`...6.{R.T...f.g.l!...d#.D200q...~"/!.&kt...T.uA...x....7...zq.W....?.&.....o.....D.x....8....}.w.xH0..

C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\Office64WW.xml

Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	5526
Entropy (8bit):	7.961897719722573
Encrypted:	false
SSDEEP:	96:Knkl+ArPi58nYVVvOsD4XTCsnffSwW6PaueZ/dlCCrhqahhDzOjX:HYABYVVMXTCsffSwWEEhOdHDCjX
MD5:	AF1636E008E21429F9199E8BBAD3A70F
SHA1:	069043128B71046A350A5E55ECC191E5EEDA0563
SHA-256:	3881498BA8CC12A26CC03F988D9219E534A41564BC499684A1A43F5E5ACD9ACC
SHA-512:	CEF39BE815338E781DB58B2973804AE5E9CBEC81C9BF43A62A184D7D1D62D6A185EF1E4DE88E045E79ABE40E8546188F171E78F0D4E9BB22F9986EF6AD3E8624
Malicious:	false
Reputation:	low
Preview:	;.T.J.E.\.l.\....4.J].+.....M....l.H..p-.js....Y..V?4S....N.....+v.Qn..`#5..'.yP2...=.#......(8..g..1z/.....F\$......a....[t...d9.N.....b.....f..9.....D K.e.aR...`v....mv.s...i.V.j...q.h....p..7..Y\G.vme.Fh.Ce...Q..Ry?.x...S.....wq0..r.\.`k?9.. .a.C.Vh.^m.....m*z..\$......f.!jU..G.n.j...S.....*...)M..u@.x[.....tt...\$....X....jc.....B...7....Ql.+q.e..z.?.....@\$.<[V....T.1..Ut.....0^W....%;<0...A..T...F.jH....55..C..F....k....-K.s.NQ....i....G....O...SU...:E..O...k.G..'.t8..[...0>.b..).9....<...c.....A..6W3E....(#p..)....R..M2.hn{.}....: .j.&\$.>..R^..8..\$.6J.,.....[1...,Z..st.j].Tlu....."....{.;m../R.%a.:=.G....2MR....).1..&..X..N....wF..tc9z.0dy_U..-?.S...VW.,E.....O..o.5]w.2.K>..p.lv.r)J.-....AH."...&..E@.H.{_&....f.:U..{L5..}).\3Y...Sf.o...z..MA.....f..8.....`o.B.....e...]+~:....6....S....x.e...h`_.:....(."n"

C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\Office64WW.xml.NB65 (copy)	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	5526
Entropy (8bit):	7.961897719722573
Encrypted:	false
SSDEEP:	96:Knkl+ArPi58nYVVvOsD4XTCsnffSwW6PaueZ/dlCCrhqahhDzOjX:HYABYVVMXTCsffSwWEEhOdHDCjX
MD5:	AF1636E008E21429F9199E8BBAD3A70F
SHA1:	069043128B71046A350A5E55ECC191E5EEDA0563
SHA-256:	3881498BA8CC12A26CC03F988D9219E534A41564BC499684A1A43F5E5ACD9ACC
SHA-512:	CEF39BE815338E781DB58B2973804AE5E9CBEC81C9BF43A62A184D7D1D62D6A185EF1E4DE88E045E79ABE40E8546188F171E78F0D4E9BB22F9986EF6AD3E8624
Malicious:	false
Reputation:	low
Preview:	;.T.J.E.\.l.\....4.J].+.....M....l.H..p-.js....Y..V?4S....N.....+v.Qn..`#5..'.yP2...=.#......(8..g..1z/.....F\$......a....[t...d9.N.....b.....f..9.....D K.e.aR...`v....mv.s...i.V.j...q.h....p..7..Y\G.vme.Fh.Ce...Q..Ry?.x...S.....wq0..r.\.`k?9.. .a.C.Vh.^m.....m*z..\$......f.!jU..G.n.j...S.....*...)M..u@.x[.....tt...\$....X....jc.....B...7....Ql.+q.e..z.?.....@\$.<[V....T.1..Ut.....0^W....%;<0...A..T...F.jH....55..C..F....k....-K.s.NQ....i....G....O...SU...:E..O...k.G..'.t8..[...0>.b..).9....<...c.....A..6W3E....(#p..)....R..M2.hn{.}....: .j.&\$.>..R^..8..\$.6J.,.....[1...,Z..st.j].Tlu....."....{.;m../R.%a.:=.G....2MR....).1..&..X..N....wF..tc9z.0dy_U..-?.S...VW.,E.....O..o.5]w.2.K>..p.lv.r)J.-....AH."...&..E@.H.{_&....f.:U..{L5..}).\3Y...Sf.o...z..MA.....f..8.....`o.B.....e...]+~:....6....S....x.e...h`_.:....(."n"

C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\ProPlusWW.xml	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	17642
Entropy (8bit):	7.989019596489402
Encrypted:	false
SSDEEP:	384:oj8Jm3t9JUaPwLMu5kYPPURCBp+fdBGYXvk/pinmbYNXUiO9mqRuXEKqL:ojwcJUaPwLKYEgP+JKpiZaY8jbl
MD5:	4FD1596403016C87FC0FD06346833131
SHA1:	E17859E07EADD22F08489FFC158A5221C60F131
SHA-256:	665D38285CA084AE5D9EF128461B936A59D523F7031B8CAF066C24FA8A622FF3
SHA-512:	45F0341228D7EBB1BBF232D7E239207DE47DEE382FEA5A1DEA168A6AA9B731ABEA4DD8667DDB36748454D1000D7D017E465EF5C13610C32C1771BBC8FFD1AAA
Malicious:	false
Reputation:	low
Preview:	8.5..";.....)6...Hj;...@O.K#`J....f...A+.73...R.....+.Qw.>..L...+L*..P..._-\. .....[Z=f.h..H..9.....y*.."n"...<.p&d.d1.l/#[Q....C..'-~...-...[x.V{uj;...."rG.....&...Jev...L....=C...t...v v.... .l.6S.....0..{.L...:"F....."9..t.Hou.....x.....&v.2..OJ#.....A.ca.r-..&H7,Y.r.\$).@..bT"Y.T.mQE.).D`..!.. .)~-.4XhEj.Y...sU..('iQ.....H="X.0.Gu...y..~...m...2.....lnV.....[...<...l.3.?3N..3.9&)N.1....;Z).rkM...z.....t....?Q.P.(H.....)`][Q..J...F....z.w.P.....8o-...-TA=b`...;vr.A.vR...@.j....m.l..M.....O.]v..O#.2G..Ug.>.t.ka0...7..-...[...qM.H.O..-B.L.x.....8.ue\$N.Kn..o.O).!^Q>.....yn.v..{....m.W.qN.K....c..[...Z...A....(Wv..U@q..d.w....P.:S.....A\O....Fay..s.k..l.....~..o...DN..b...N.-.S.....*; \$Wh..[Q.P....D....9v.t....5A...~-. [...D.v\Z.Z>[4lZ3/<W...uQy.....3.....6.....j2).s.k.14..D.n.Vx.\....CB<.DTE..d...`]...."gU9.....;4....9t..O.t....3.s.R~..tt.Y.[..@cf.P..u....C

C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\ProPlusWW.xml.NB65 (copy)
--

Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	17642
Entropy (8bit):	7.989019596489402
Encrypted:	false
SSDEEP:	384:oj8JmJt9JUaPwLMu5kYPPURCBp+fdBGYxvk/pinmbYNXUiO9mqRuXEKqL:ojwcJUaPwLKYEgp+JKpiZaY8jbl
MD5:	4FD1596403016C87FC0FD06346833131
SHA1:	E17859E07EADDF22F08489FFC158A5221C60F131
SHA-256:	665D38285CA084AE5D9EF128461B936A59D523F7031B8CAF066C24FA8A622FF3
SHA-512:	45F0341228D7EBB1BBF232D7E239207DE47DEE382FEA5A1DEA168A6AA9B731ABEA4DDD8667DDB36748454D1000D7D017E465EF5C13610C32C1771BBC8FFD1AAA
Malicious:	false
Reputation:	low
Preview:	8.5..";.....)6...H;...@O.K#"J....f...A+.73...R.....+'.Qw>..L_+L_*..P..._-..[.....[Z=f.h..H..9.....y*.. "n'<.p&d.d1.1#/[Q.....C..'~...~...-...[x.V{.uj....."....rG.....&...Jev...L....=C...t...v v.....]!.6S.....0..[.L..:"F....."9..t.Hou.....x.....&v.2..OJ#.....A.ca.r-..&H7.Y.r.\$)..@..bt"Y.T..mQE.).D'..!..\\.)~..4XhE.j. Y...sU..('iQ.....H="X.0.Gu...y..~...m...2.....InV.....[.... <...!..3.?3N..3.9&)N.1.....[Z].rkM...z.....t...?Q.P.(H.....)`][Q..J.....F.....z.w.P..._....8o...-....TA.=b'...;vr.A.vR..@..j....m..\\..M....O.]v..O#.2G..Ug..>.t.ka0...7.[-.qM.H.O..- B.L.x.....8.ue\$N.Kn..o.O)..\'Q>.....yn.v..{....m.W.qN.K....c..[.z...A....(Wv..U@q..d.w....P..5.....A\\O....Fay..s.k..!.....~..o..DN..b...N..-..S.....*;\$Wh..[Q.P....D....9v.t....5A...~.. [...D.\\iz.Z>[4Iz3/.<W....uQy.....3.....6.....j2).s.k..14...D.n..Vx\\.CB<. DTE..d...`].'"gU9.....;4.....9t..O.t....3.s.R~..tt.Y.[..@cf.P.. ..u....C

C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\ProPsWW.cab  	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	323579508
Entropy (8bit):	7.999959516157797
Encrypted:	true
SSDEEP:	6291456:f8tD3MCBIfHVSJRJou3fOgZ6XLXQ0q8taUjosDaCrZ58ppW5Zjc6l9cY1G5:UaSRJ73wQ0q8XjosD1Z58pp4uoa8
MD5:	17449E00A3586FAAC19EF2CE2FBC61AA
SHA1:	D9807A1EAEC484B8C24EE8D8EC666A90BCCEE2C3
SHA-256:	FB68F6889348183166C3EA52394E8322550E1BDC7AC9DC60AAABD30CE0EB75B6
SHA-512:	7808D0A31F5D48AF0581562515DF6554BE42E56167F74E242C17347BA94839176509AB2747FC5B834D62D12F086871DA4F003CBF91FD5FC7899F7EEACC42DC55
Malicious:	true
Reputation:	low
Preview:	J..R.....a.^.....UEC..6...=...V2...~v.+..5?i3`K.#...""...NF.....J.j.=...~vy...T.%hV[5..ZiK.[',,(...../.bAw..9...h.....qN....R.*... x3...z...:l.o7ux.Y...@.D....."]....7.4DP?&.....P. ./.....V..l.....mP..4Z....F..z94....1..&..U7Z[.V.V.....+....[C..Cg:.x.sQ....~.....E.. .5\\.....B.SV..z.w*.X09..+#+9.....L.bP_u.^..Jm..l.....E..6T5...q.U#..L...J..L'Pg.....?&_..-#. .U.F.....`(.A.fA.).6%(3..).+.8=...W.....H..8D.]...0t./[(DdXV.z~F.8..PS#kO...>N..l.....b.brm.....y*oiA.....>d...;.K01n...7Y...[.R...#.p..QuJW.mHY...)~\$.Q~. >...=.gwZ...xo...K.u.1h...#.\\.^..q..c_.fpG)..m5[.kS..~].fjXv...fe=...E..?X.M..!\$..b.O...j.V'.....G...8q./...;U+. .f...?D~.....r.z5Ej.p..c.m].q.m.T..U.S..k..#'.w.&.....<T_4.\$; .z..\\.)...\$S.B9M..Yr/...c...0.....(r.G.....3.....0.....xH..>.zk,.3Dv...1.9b.....,.....{.....4J....b...C.....Ri.)c/....X...+...;+Z.f..0....m.7.j.rM.pR...07.v/..C.N..'

C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\ProPsWW.cab.NB65 (copy)  	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	323579508
Entropy (8bit):	7.999959516157797
Encrypted:	true
SSDEEP:	6291456:f8tD3MCBIfHVSJRJou3fOgZ6XLXQ0q8taUjosDaCrZ58ppW5Zjc6l9cY1G5:UaSRJ73wQ0q8XjosD1Z58pp4uoa8
MD5:	17449E00A3586FAAC19EF2CE2FBC61AA
SHA1:	D9807A1EAEC484B8C24EE8D8EC666A90BCCEE2C3
SHA-256:	FB68F6889348183166C3EA52394E8322550E1BDC7AC9DC60AAABD30CE0EB75B6
SHA-512:	7808D0A31F5D48AF0581562515DF6554BE42E56167F74E242C17347BA94839176509AB2747FC5B834D62D12F086871DA4F003CBF91FD5FC7899F7EEACC42DC55
Malicious:	true
Reputation:	low
Preview:	J..R.....a.^.....UEC..6...=...V2...~v.+..5?i3`K.#...""...NF.....J.j.=...~vy...T.%hV[5..ZiK.[',,(...../.bAw..9...h.....qN....R.*... x3...z...:l.o7ux.Y...@.D....."]....7.4DP?&.....P. ./.....V..l.....mP..4Z....F..z94....1..&..U7Z[.V.V.....+....[C..Cg:.x.sQ....~.....E.. .5\\.....B.SV..z.w*.X09..+#+9.....L.bP_u.^..Jm..l.....E..6T5...q.U#..L...J..L'Pg.....?&_..-#. .U.F.....`(.A.fA.).6%(3..).+.8=...W.....H..8D.]...0t./[(DdXV.z~F.8..PS#kO...>N..l.....b.brm.....y*oiA.....>d...;.K01n...7Y...[.R...#.p..QuJW.mHY...)~\$.Q~. >...=.gwZ...xo...K.u.1h...#.\\.^..q..c_.fpG)..m5[.kS..~].fjXv...fe=...E..?X.M..!\$..b.O...j.V'.....G...8q./...;U+. .f...?D~.....r.z5Ej.p..c.m].q.m.T..U.S..k..#'.w.&.....<T_4.\$; .z..\\.)...\$S.B9M..Yr/...c...0.....(r.G.....3.....0.....xH..>.zk,.3Dv...1.9b.....,.....{.....4J....b...C.....Ri.)c/....X...+...;+Z.f..0....m.7.j.rM.pR...07.v/..C.N..'

C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\ProPsWW2.cab  	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data

File Type:	data
Category:	dropped
Size (bytes):	28316
Entropy (8bit):	7.994390327127431
Encrypted:	true
SSDEEP:	
MD5:	36D6CEF7F7DC9FF081840E2DE5D534EF
SHA1:	4BBDD33D1D36472D180F2F0516C4385F015194CC
SHA-256:	69431E39EB386DC40BBB7B6A24F72DB2D7A7900AE1BE1293B1659F50925F0443
SHA-512:	0F71BDE192C90797FBAA41E7487AC8C40AFDE21691B0527963B2CE930CD7EFF5DEC0967571F4A13FFB243FB2A8DCB5C44AFA774F1B4C898CD25371FAA5B3C16
Malicious:	true
Reputation:	low
Preview:	D...{.C...(.s4...=.b...{lw.....F.....Z...x...v~.3.W...C...}...%.h.vu.SlZ>\$.p...((.....+..."O...F.Fc.Y.^..2..}.c...@c.\$L...q..s..265.^..r...N.C.....o..).P.+t...h-:.....]5..N.^y..w.].ioJ...e.....a.CP~..Kv...x..T...X&.....wW...{.*....'W.....@`..P...@...?lnV~...p.]'U4.a....X...s...;3.b...p.w.....&..2w.3.....s".g-..[]..K.l.....V...[\$.YBp...F...h....un.p..0.P.)a{B..%C.....6.....\$Pz!..(&).dd.k.s..."t5)#J.j.....r..j...P..k%:[...'+.....]i...1.B.."Y^@...^U.....qnJ...1.x.l.-_Z_@X...8...q..l...{.....}...W....Kw!.)T.'...x.E....N..VV*...o.4_uTC.r../Ox...{.?e..+{.}.hbv..'n.....R.a...D.{.D.]{J#...x%.R...P{..Zl.3...Tz...5lm.A....R..... _/_..9.<..1Al =n...'w.l.....:9fhjo.*C...h...R.4nk~-[.....W\ &f.&: .hY+.4.....c<.>....cl..0.....?['.! n...k..J.t.C..P ...r.c.....lAn..DR....H..y.....<K.\$..\$......t..JlR.NU....\B.....:J...Ul.x.VP.i.g.X.....

C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Setup.xml.NB65 (copy)

Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	28316
Entropy (8bit):	7.994390327127431
Encrypted:	true
SSDEEP:	
MD5:	36D6CEF7F7DC9FF081840E2DE5D534EF
SHA1:	4BBDD33D1D36472D180F2F0516C4385F015194CC
SHA-256:	69431E39EB386DC40BBB7B6A24F72DB2D7A7900AE1BE1293B1659F50925F0443
SHA-512:	0F71BDE192C90797FBAA41E7487AC8C40AFDE21691B0527963B2CE930CD7EFF5DEC0967571F4A13FFB243FB2A8DCB5C44AFA774F1B4C898CD25371FAA5B3C16
Malicious:	true
Reputation:	low
Preview:	D...{.C...(.s4...=.b...{lw.....F.....Z...x...v~.3.W...C...}...%.h.vu.SlZ>\$.p...((.....+..."O...F.Fc.Y.^..2..}.c...@c.\$L...q..s..265.^..r...N.C.....o..).P.+t...h-:.....]5..N.^y..w.].ioJ...e.....a.CP~..Kv...x..T...X&.....wW...{.*....'W.....@`..P...@...?lnV~...p.]'U4.a....X...s...;3.b...p.w.....&..2w.3.....s".g-..[]..K.l.....V...[\$.YBp...F...h....un.p..0.P.)a{B..%C.....6.....\$Pz!..(&).dd.k.s..."t5)#J.j.....r..j...P..k%:[...'+.....]i...1.B.."Y^@...^U.....qnJ...1.x.l.-_Z_@X...8...q..l...{.....}...W....Kw!.)T.'...x.E....N..VV*...o.4_uTC.r../Ox...{.?e..+{.}.hbv..'n.....R.a...D.{.D.]{J#...x%.R...P{..Zl.3...Tz...5lm.A....R..... _/_..9.<..1Al =n...'w.l.....:9fhjo.*C...h...R.4nk~-[.....W\ &f.&: .hY+.4.....c<.>....cl..0.....?['.! n...k..J.t.C..P ...r.c.....lAn..DR....H..y.....<K.\$..\$......t..JlR.NU....\B.....:J...Ul.x.VP.i.g.X.....

C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\pkeyconfig-office.xrm-ms

Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	591057
Entropy (8bit):	7.999728911043132
Encrypted:	true
SSDEEP:	
MD5:	772F40525F5D8DCE24845850CA7D7307
SHA1:	57DD5DA04E034BC5F72E50DF2B911FD49C514444
SHA-256:	3BF31F16F9A6B4EB2CAB0603FD4ACD1E02B5F33854298156B77D0843B542AFCEB
SHA-512:	9CB0CF995F2D9D5A2E6A51C1797ECBDEF6E9FB3C9C1D1427EF27F9813F2332ACB265D7692321F6D1CDF33FE39CE1D70636D4F0477C6C1BF683F7092B4DD1DF7
Malicious:	true
Reputation:	low
Preview:	}.....\$).<#.*b.\[.a.I.X..O..N....Enxs.....lq...~i(h."i{b.W...F.....3.\$:s;u.Gd1?.@!c.5v...Yv...D.=..z/_..r..2..xz..T....>U.(.1..9.P..l{n...y<3.y...!..u..d..zv..LWyr...^..~..1..Y.M...1..L..>+...H/.T.....@.....]F."&..Z..m.FZ...X.....6.....]z....o.t0..A..F.....^.....@x..t..j..._-=.@!Uu.i..l...j)Bv.A..^..E....i-..s.9.D.]A.N...L.....:(h.o.K3.T...f..3s..'.g'&/>~-.l%i1.9X.h.S_).\$.#"...{..w.l..._oP.....B+..P...?=-.*4.z%f."h.....D4.'...'n..l6.....dl....Y.wC...Q...^..arR.Y....h..q.n.....B.'>_Qd.\$.....7.._X...k./G...v&]l...1....\$.x>F..1e...3%{.....).V.K...~f.gc.\...6...QES.....*l...+].L.P.B....B....@....l.{..CF'..@.E.d.+>p.>.m.#k\ld.m.Moc.v.v.E.?Y..S.B...xr.m.X.q.<..H...8....}<W...%{w!'...^g.T.?...@tUXd.Q.e.D.{...;...T.x.N.q.....?hu.?.....m..fX~...S.....<W..o.H.. U]...%Y...z-w.L....V.l.l.J.}....a.SW.-.

C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\pkeyconfig-office.xrm-ms.NB65 (copy)

Process:	C:\Users\user\Desktop\ll.exe
----------	------------------------------

File Type:	data
Category:	dropped
Size (bytes):	591057
Entropy (8bit):	7.999728911043132
Encrypted:	true
SSDEEP:	
MD5:	772F40525F5D8DCE24845850CA7D7307
SHA1:	57DD5DA04E034BC5F72E50DF2B911FD49C514444
SHA-256:	3BF3F16F9A6B4EB2CAB0603FD4ACD1E02B5F33854298156B77D0843B542AFCEB
SHA-512:	9CB0CF995F2D9D5A2E6A51C1797ECBDEF6E9FB3C9C1D1427EF27F9813F2332ACB265D7692321F6D1CDF33FE39CE1D70636D4F0477C6C1BF683F7092B4DD1D7F7
Malicious:	true
Preview:	}.....\$).<#*b.\[a.I.X..O..N....Enxs.....lq..~i.(h.. "i[b.W...F.....3\$.s;u.Gd1?.@!c.5v...Yv...D=..z/_...r.2..xz..T....>U.(.1..9.P...l{[n...y<3.y...!..u..d..zv..LWyr...^..~..1..Y.M.. ..1..L..>+...H/.T.....@.....]F."&..Z..m.FZ...X....6.....]Z....0.t0..A..F.....^.....@x..t..j..._-@.!Uu.i..l...j)Bv.A..^..E....i-..s.9.D..]A.N...L.....:(h.o.K3.T...f..3s.. 'g'....&/>~..l.%i1.9X.h.S_).\$.#"..{.w.l..._oP.....B+.P...?*=.4.z%f.. "h.....D4.. '...'n..l6.....dl.....Y.wC...Q...^..arR.Y....h..q.n.....B.'>_Qd.\$.....7_..X...k.. /G... .v&j]..l...1....\$.x.>F..1e....3%{.....).V.K...~f.gc.\....6...QES.....*!l...+.]...L.P.B....,B...@.....l{..CF'..@.E.d.+>.p..>.m.#.k[\d..m.Moc.v.v.E.?Y..S.B...xr.m.X.q.-<..H...8.....} <W...%{w.'...^g .T.?...@tUXd.Q.e.D..{...;...T.xN.q.....?hu.?.....,m..fX~...S.....<W..o.H.. U]...%Y....z-w.L.....V.l.l.J.}....a.SW.-.

C:\MSOCache\All Users\{90160000-0016-0409-0000-00000000FF1CE}-C\ExcelLR.cab  	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	5770100
Entropy (8bit):	7.999780664070838
Encrypted:	true
SSDEEP:	
MD5:	12CF959DDA15DE08F731FA3F2D63D5A6
SHA1:	B9E680B7D4E33D53AB36D5693897BAE1FF3ADF43
SHA-256:	43048971C91CDB9350B13030531C395B48BEB4FFE9D93F3E199B79D1410F42A3
SHA-512:	912B1F352EAA888771FF7BB04BE80D1DD1CAAD7305D66D1E13CB8BDEEF71075656C1ED1A4217EB69FCB1E5B27E6809CC063470FC82DE4C0F833AEF8CEEBD73
Malicious:	true
Preview:	x..jh..)e..EQli..FX.e.CyJ.\.>.....\$.x.b.L.....~.....k ...RlE?...v..U5<.K{....2r..}.U...].#.....Ck9w..._..._./Q...k.....8.....L..X^..K.Z.YR..G.-2..u./l...U...o.j}#....Tz....U..... ..yV...;.....+...V...0.....8..\$......1[.....>...8.G&s...!^ado5C7P..u.Y.....*...Z...1.uU.....a.....h.sno.....-c.....4....4....x!.....'Y.....`c..~.6y...W..._E.....r... <1E.../z.pr D=...O..U..~h.H...[3...;d@..&i....>".C'.4i.D...{%;n.n.q)A..e.....t.t.\$...@m.P..T...q..m.u...r...k.J.7..k.i...w<..9m)i.G.t...1./C.D.!7VFo.....j..ld)><.....qd.....!..SRv ..s.'w.z..7...!...B.Q..[>8...-/..._J.@O].C.....O...~w.@...b..D..d.....Y...,(B^.....8.....o.]..._L*.tj.km..V~...{ .A(..J...[...v..wC.>..e.....1&(j::P.c...A..~.C-#.....E.lg^ ..a..k.2...f[l8...ne.)o*...a/5...^>.....S....lqJ..%).\$...l.Q\$.S...^o...t.'5g.ud...O\$.~!'......8.l;q:@.....g&2U..rGWI1_..C/B...!.....e.6.y.T...

C:\MSOCache\All Users\{90160000-0016-0409-0000-00000000FF1CE}-C\ExcelLR.cab.NB65 (copy)  	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	5770100
Entropy (8bit):	7.999780664070838
Encrypted:	true
SSDEEP:	
MD5:	12CF959DDA15DE08F731FA3F2D63D5A6
SHA1:	B9E680B7D4E33D53AB36D5693897BAE1FF3ADF43
SHA-256:	43048971C91CDB9350B13030531C395B48BEB4FFE9D93F3E199B79D1410F42A3
SHA-512:	912B1F352EAA888771FF7BB04BE80D1DD1CAAD7305D66D1E13CB8BDEEF71075656C1ED1A4217EB69FCB1E5B27E6809CC063470FC82DE4C0F833AEF8CEEBD73
Malicious:	true
Preview:	x..jh..)e..EQli..FX.e.CyJ.\.>.....\$.x.b.L.....~.....k ...RlE?...v..U5<.K{....2r..}.U...].#.....Ck9w..._..._./Q...k.....8.....L..X^..K.Z.YR..G.-2..u./l...U...o.j}#....Tz....U..... ..yV...;.....+...V...0.....8..\$......1[.....>...8.G&s...!^ado5C7P..u.Y.....*...Z...1.uU.....a.....h.sno.....-c.....4....4....x!.....'Y.....`c..~.6y...W..._E.....r... <1E.../z.pr D=...O..U..~h.H...[3...;d@..&i....>".C'.4i.D...{%;n.n.q)A..e.....t.t.\$...@m.P..T...q..m.u...r...k.J.7..k.i...w<..9m)i.G.t...1./C.D.!7VFo.....j..ld)><.....qd.....!..SRv ..s.'w.z..7...!...B.Q..[>8...-/..._J.@O].C.....O...~w.@...b..D..d.....Y...,(B^.....8.....o.]..._L*.tj.km..V~...{ .A(..J...[...v..wC.>..e.....1&(j::P.c...A..~.C-#.....E.lg^ ..a..k.2...f[l8...ne.)o*...a/5...^>.....S....lqJ..%).\$...l.Q\$.S...^o...t.'5g.ud...O\$.~!'......8.l;q:@.....g&2U..rGWI1_..C/B...!.....e.6.y.T...

C:\MSOCache\All Users\{90160000-0016-0409-0000-00000000FF1CE}-C\ExcelMUI.xml	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	2314

Entropy (8bit):	7.912806350278128
Encrypted:	false
SSDEEP:	
MD5:	AF617EDE8AC85FF8E132F93807D9E143
SHA1:	3D9B495A42103E7236A9A27A0407A37E36B046AE
SHA-256:	AF236A62B8CA499C2E841C93D4BDF87BE6F6B63EB13C6C5D915BA3C45B0B073B
SHA-512:	57707010BC3A0D2A1EF7500E0E4C287C1BF7BF52EA770DFBE4F8F381D185CA1C20FF15E4F5A44DC5A3FE77F23B1CECD87F386316092A6E035213B7D2AFEBDEAE
Malicious:	false
Preview:	9..l..W.8.!N..h..m9L2^..\....`..D.`.4R1.PwJ.n.9...?F{c...y2....kF..[.2.2.i.....].tu.6....W..Z. ...`...u....`...&w.....X.y._.*.t?...kA1;G...#t..v....l...H...;C\$.W...t..[Y.T..z..P.3?..>PV...7..m.....{.}.jl...Hw.P.h.Y....B.n....O=7...lw..\..g....~e.`.K...\H..u.D.<F.H....q).....%.>.@?.l..WN.\$N.u,...'.A.".....C.d.....h..ji.....U....^..y.z...zZ..4..q...ya...a.h.6X.9u...r.5.?].2XA.G..1.....Qh.z>.5..+L..<k...kl.l.=_....P...Vj....O...dek.v\$.LE....fXK.."/t~1b...V.?>!.{.M.%.m.7_.....d..K.H.d.....7....m.+0`z9.k.3.....4_Rd...%J.l!".fp.....l.c.tC...[.u.;R..N.j....o...f.x.O.Jl.i.E7....J.g.h...L..u/.q.F0(8.R...S.....w.....m.....*7E..j(m.&}.WE...=j...ST.p+....C..@D".K..g_2...;..kz...!kMQ^..K..*..B..["..W.O....E.....MBCd.J.{.3y..}#S[.T.....p@!.....H..mF.....Y..q...1....w....p...\$.D.....@...yi...f.....0....q[.m..K....<6.*.y....c...!.(#[..

C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelMUI.xml.NB65 (copy)	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	2314
Entropy (8bit):	7.912806350278128
Encrypted:	false
SSDEEP:	
MD5:	AF617EDE8AC85FF8E132F93807D9E143
SHA1:	3D9B495A42103E7236A9A27A0407A37E36B046AE
SHA-256:	AF236A62B8CA499C2E841C93D4BDF87BE6F6B63EB13C6C5D915BA3C45B0B073B
SHA-512:	57707010BC3A0D2A1EF7500E0E4C287C1BF7BF52EA770DFBE4F8F381D185CA1C20FF15E4F5A44DC5A3FE77F23B1CECD87F386316092A6E035213B7D2AFEBDEAE
Malicious:	false
Preview:	9..l..W.8.!N..h..m9L2^..\....`..D.`.4R1.PwJ.n.9...?F{c...y2....kF..[.2.2.i.....].tu.6....W..Z. ...`...u....`...&w.....X.y._.*.t?...kA1;G...#t..v....l...H...;C\$.W...t..[Y.T..z..P.3?..>PV...7..m.....{.}.jl...Hw.P.h.Y....B.n....O=7...lw..\..g....~e.`.K...\H..u.D.<F.H....q).....%.>.@?.l..WN.\$N.u,...'.A.".....C.d.....h..ji.....U....^..y.z...zZ..4..q...ya...a.h.6X.9u...r.5.?].2XA.G..1.....Qh.z>.5..+L..<k...kl.l.=_....P...Vj....O...dek.v\$.LE....fXK.."/t~1b...V.?>!.{.M.%.m.7_.....d..K.H.d.....7....m.+0`z9.k.3.....4_Rd...%J.l!".fp.....l.c.tC...[.u.;R..N.j....o...f.x.O.Jl.i.E7....J.g.h...L..u/.q.F0(8.R...S.....w.....m.....*7E..j(m.&}.WE...=j...ST.p+....C..@D".K..g_2...;..kz...!kMQ^..K..*..B..["..W.O....E.....MBCd.J.{.3y..}#S[.T.....p@!.....H..mF.....Y..q...1....w....p...\$.D.....@...yi...f.....0....q[.m..K....<6.*.y....c...!.(#[..

C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\R3ADM3.txt	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	1290
Entropy (8bit):	4.607071403570347
Encrypted:	false
SSDEEP:	
MD5:	FADB0F250D20EF2F614C4AB5D5D3AB0F
SHA1:	41E8255C91A40A8E832A8AC05747C9A579F55D07
SHA-256:	2CD73F11DA515955B62A930CA4DEFDE9CCB5230B8F5809E3C304EF854604EDA3
SHA-512:	E97F4B069ACB91C332BDDCA5C4314CBE6CC79C37E93CBB3F4D8B37544B49C2868E23B603FE4563A8961616F137CF646153A82F387D9C55FC8191108E86CF136
Malicious:	false
Preview:	_ _ _ _ _ . \ _ _ V _ _ _ . \ / / / _ _ _ \ . . ` _ _ \ _ _ \ \ \ . \ / / / / \ _ / \ _ \ _ _ \ _ _ / ...By now it's probably painfully apparent that your environment has..been infected with ransomware. You can thank Conti for that....We've modified the code in a way that will prevent you from decrypting..it with their decryptor.....We've exfiltrated a significant amount of data including private emails,..financial information, contacts, etc.....Now, if you wish to conta ct us in order to save your files from permanent..encryption you can do so by emailing network_battalion_0065@riseup.net.....You have 3 days to establish contact. Failing to do so will result in..that data remaining permanently encrypted.....While we have very little sympathy for the situation you find yourselves..in right now, we will ho nor our agreement to restore your files across..the affected environment once contact is established and payment is made

C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\Setup.xml	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	3016
Entropy (8bit):	7.928172453033418
Encrypted:	false
SSDEEP:	

MD5:	0C8B9D07909BAE3D77E9D12BFFFF98EF
SHA1:	203DBD7D6100018A598A5A05FE60F978E8D41917
SHA-256:	36FACAF9577D14697A24BDE6E939241AB9B9CB9666CAEA826C5A757829EBF82A
SHA-512:	28C0B4F373F51E4CEEFF16CC34B110012A8062D68AEB91C8EBE8C061E86DC000BFBC3FFBD94E9FEE5BDE1E8BC251BC8E26DA2D47D712C7FD467782C9CB9AE20F7
Malicious:	false
Preview:	.0..">..?..[.=P..<{..a6g.h...../'3,c,O....SM4R.q..J.s.`.-\A..jU;.) T...#.....! "t_ _F_{~O.Q.C...s..V.U.U.U<m*..@..KF...9B Y,8.G...D_ _L.hU3.....X8 ..K..?m.....9v2...Z...f....Mb'...7.d...NW...8.M.5~.X..1-.....&.V.u.]]!L.W.H_.....4.K%.....;...Qz.x...[.e...P.w.....k.v.\$..z^.. i.ce.=.v..l..A.&d...x....g3....P....&+v.7.....K.rL.Y..."..q..}..2 3%...." _v.&.*9?.a.U.&[1%zu.G.....E..k...j.l.].J....W....l.].}A.Fg.RT."7.T...u.O...+6_ _s.w....?....F.s..WrB.#W..M9..k.y. ..2..F[c..tm.[eO....TK...K.@cD.j.VQ.C#..}.N%!4:.YP(...{RR...F...;...-7C. ..M...aqI4E.O8v...Mq.+@[.^,.....n...W;..BM..(qt...p3.w.qT!X3z.p.s>k^L..... X. J9.Z...."6.T9..._c.Z.a.P.Bf.e.*X.W%+d...../.....9.q.. P.C]....g.lpO.Y.O..%VE[...Y..Z....r.d^t.BSu..Xo..%.....cq...o...3(`{!R.y+#.&.....8...E.a.M.k.....e-.Pp...o..H.q...G.....~ ,....{y.....k....#mQo%.L.A.....U]'...A...q!;t.k...

C:\MSOCache\All Users\{90160000-0016-0409-0000-00000000FF1CE}-C\Setup.xml.NB65 (copy)	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	3016
Entropy (8bit):	7.928172453033418
Encrypted:	false
SSDEEP:	
MD5:	0C8B9D07909BAE3D77E9D12BFFFF98EF
SHA1:	203DBD7D6100018A598A5A05FE60F978E8D41917
SHA-256:	36FACAF9577D14697A24BDE6E939241AB9B9CB9666CAEA826C5A757829EBF82A
SHA-512:	28C0B4F373F51E4CEEFF16CC34B110012A8062D68AEB91C8EBE8C061E86DC000BFBC3FFBD94E9FEE5BDE1E8BC251BC8E26DA2D47D712C7FD467782C9CB9AE20F7
Malicious:	false
Preview:	.0..">..?..[.=P..<{..a6g.h...../'3,c,O....SM4R.q..J.s.`.-\A..jU;.) T...#.....! "t_ _F_{~O.Q.C...s..V.U.U.U<m*..@..KF...9B Y,8.G...D_ _L.hU3.....X8 ..K..?m.....9v2...Z...f....Mb'...7.d...NW...8.M.5~.X..1-.....&.V.u.]]!L.W.H_.....4.K%.....;...Qz.x...[.e...P.w.....k.v.\$..z^.. i.ce.=.v..l..A.&d...x....g3....P....&+v.7.....K.rL.Y..."..q..}..2 3%...." _v.&.*9?.a.U.&[1%zu.G.....E..k...j.l.].J....W....l.].}A.Fg.RT."7.T...u.O...+6_ _s.w....?....F.s..WrB.#W..M9..k.y. ..2..F[c..tm.[eO....TK...K.@cD.j.VQ.C#..}.N%!4:.YP(...{RR...F...;...-7C. ..M...aqI4E.O8v...Mq.+@[.^,.....n...W;..BM..(qt...p3.w.qT!X3z.p.s>k^L..... X. J9.Z...."6.T9..._c.Z.a.P.Bf.e.*X.W%+d...../.....9.q.. P.C]....g.lpO.Y.O..%VE[...Y..Z....r.d^t.BSu..Xo..%.....cq...o...3(`{!R.y+#.&.....8...E.a.M.k.....e-.Pp...o..H.q...G.....~ ,....{y.....k....#mQo%.L.A.....U]'...A...q!;t.k...

C:\MSOCache\All Users\{90160000-0018-0409-0000-00000000FF1CE}-C\PowerPointMUI.xml	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	2195
Entropy (8bit):	7.899572808020685
Encrypted:	false
SSDEEP:	
MD5:	87BFAC272B91F0E5A0F0EFF99DB5CED6
SHA1:	498AB27D3104DD1CD0F93D32F04ABCA8DC732D8E
SHA-256:	9DCBE0F552357FF7566641BF4E1AEC879CAE2FC068913E9111F97D6B2DDD90B3
SHA-512:	E76B26E6E743B5FEBADDEBA3298A858FB38C763F5E5DA56E97EE499F43DCA314386A0C92902101329C812398F6CDFE271F67761DA4AD074D4F5B9AD9505A8CD
Malicious:	false
Preview:	9...~M..!Y.Y.E6..c..R.....NN\G..v ..qm.&z.M.-.#I.C_../.)...M.Mf.t.....E.<.....'.Wf.Gr@.....3'.4@.....aqhoho.7.b[#&3...M1x"A...2....^...P..Q".p...]...Y..^..l...3...q.3@w. ...~...x~..m.....l].....[Y ..`..8V..[.(<M..b...[o.F.....6..ygnV%.....V>...KE.D...g...<.h.....@...[.n.l.1.Y...N.^.....d.?E.....+ ..Q....[j...#g...#B.d.g..l....\$~.9.....M...Cy.z...*oO .O...\.2K(\$....P.7...5.H.ou..7..z.<"2Z.y].+...6SG...;..Q...t...Un.1W+...W.....9.i...Qj..'.5.l...OX^wL... ..mk...T.T.....{/ _h..\$ZH1.h=...v.{.....h;..F&a.....8n....(=.C...0..".r*Z]....s o...Pt7..".0.W.lj)\$.....a...lr.Angr..i5K4..6/v/z.y.%%E.%c.[y7.MA.."N. e.F.....ES@W.D....H....QvftR.6.....d..P.,>...)``z....&O.t.'.=.m..gE...y(%..BaJ8...wN.([P..j..P^. ..9fF..6..\.!.....c....)5A'~VAm..Rr.~.0..H{...l...E>.7.u....Y.=w.A..pw...v.&k...[.~'w.A....F.t\$t...{aY.(j...T*=..YL.....3...s>..73.7.]P...0z.6....c8d_\$N..#.....s..F.v.l.n. ;...N.

C:\MSOCache\All Users\{90160000-0018-0409-0000-00000000FF1CE}-C\PowerPointMUI.xml.NB65 (copy)	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	2195
Entropy (8bit):	7.899572808020685
Encrypted:	false
SSDEEP:	
MD5:	87BFAC272B91F0E5A0F0EFF99DB5CED6
SHA1:	498AB27D3104DD1CD0F93D32F04ABCA8DC732D8E
SHA-256:	9DCBE0F552357FF7566641BF4E1AEC879CAE2FC068913E9111F97D6B2DDD90B3

SHA-512:	E76B26E6E743B5FEBADDEBA3298A858FB38C763F5E5DA56E97EE499F43DCA314386A0C92902101329C812398F6CDFE271F67761DA4AD074D4F5B9AD9505A8CD
Malicious:	false
Preview:	9...~M..!Y.Y.E6..c...R.....NN\G..v..qm.&z.M.-#l.C.../.)...M.Mf.t.....E.<.....'.Wf.Gr@.....3'.4@...aqhofo.7.b[...M1x"A...2....^...P..Q..".p...].Y..^..l...3...q.3@w. ..-...x~..m....l]..... Y..`..8V..{..<M..b...[o.F.....6..ygnV..%.....V>...KE..D...g...<..h.....@...[.n.l.1.Y...N.^.....d.?E.....+...Q....[j...#g...#B.d.g..l....\$~.9.....M...Cy.z...*oO O...\.2K(\$...P.7...5.H.ou..7..z.<"2Z.y].+...6SG...;..Q...t...Un.1W+...W.....9.i...Qj..'.5.l...0X^wL...mk...T.T.....{/_h..\$ZH1.h=...v.{.....h;..F&a.....8n....(=.C...0..".r*Z]....s o...Pt.7..".0.W.l]\$.....a...lr.Angr..i5K4..6/v/z.y.%%.E.%c.[.y7.MA.."N\ e.F.....ES@W.D....H....QvftR.6....d..P..>...").`z....&O..t'.=..m..gE....y(%..BaJ8...wN.([P..j..P^ .9fF..6..^..*...l.....c....)5A~VAm..Rr..~0..H{...l...E>.7....Y..=w.A..pw...v.&k... .'.w..A....F.t.\$t...{aY.()T*=..YL.....3...s>..73.7. P...0z.6....c8d_\$N.#.....s..F.v.l.n.;...N.

C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PptLR.cab  	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	6310660
Entropy (8bit):	7.999936242488887
Encrypted:	true
SSDEEP:	
MD5:	10DD39DE37D487BE6C0831326BC837A9
SHA1:	2D5E656B007569DF1A10C63257234789D4D22720
SHA-256:	E72A7412BE7DFCA0A1A30671CE339D8A075F6069985A3AFCD3BF614CE3C7335CB
SHA-512:	16307F4329C05DE1D5761EC11D13332DE9A12EC2B14C79DB0FB875A9D18B35830C0B471A053B8D65357F7A41C4226F5565124AEC39E59C891787DC04E38364C
Malicious:	true
Preview:	P...1+.."7H1..{....=E.y.)...K.(.+SO...~"). g....V.....X.D....#=#...3.p.pQ5....b....~.....Xv..OE<..T.....nA...7..i.;(s.....&..<...N.)x..5.Y.!Du.....O...fQ...) .0.Z..K#T..e0.... ..m{k.k.b..t...G..a.r.....0...v4.....Gi.....m.D..2.?1.E.j...^.....}.P-q.i...../.....\$.lr....\$.R.g.&F....K.`b..!8hM.e.L9^M...K.g.....p...Wi.3..ld...C..D...A..E7...@.R.r.7..TU....4L...`.....+ \$...CmJ.sNU.x...2.....g...4.....J...u.2"w.B.(.....t.7.>F..).RB....MIQ..=.Y....K.D.r.6/....%.[.n.#2..^y.T0.mY.G..._K..c.W...E...S.A..A.H.U.....f"...-gsJY.....!.....G.6.Bu.. _.....X...&v..U.y.u...3tH2.../.....v.-cm...t!.o9S..W....v9.7gD..s.k....cW.....l)D.2..jd.....N.q...\$.Q..X.+#v..=B.k\..xayB...ie.,9U.R.x...VFQ.9.%..._r.P.8..O..X..Dy.#.\....U ..gx.v.....4.....Z...V.....).s....G.))U.... .i..6...TsOnr:...{W.L.....m.JY...._2f.?v..V..;/;2.....=-.G..hx.Q.DvL...-....0.g.'.Y.....c..Z..y..z.R1U.....9..(h&q.n).

C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PptLR.cab.NB65 (copy)  	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	6310660
Entropy (8bit):	7.999936242488887
Encrypted:	true
SSDEEP:	
MD5:	10DD39DE37D487BE6C0831326BC837A9
SHA1:	2D5E656B007569DF1A10C63257234789D4D22720
SHA-256:	E72A7412BE7DFCA0A1A30671CE339D8A075F6069985A3AFCD3BF614CE3C7335CB
SHA-512:	16307F4329C05DE1D5761EC11D13332DE9A12EC2B14C79DB0FB875A9D18B35830C0B471A053B8D65357F7A41C4226F5565124AEC39E59C891787DC04E38364C
Malicious:	true
Preview:	P...1+.."7H1..{....=E.y.)...K.(.+SO...~"). g....V.....X.D....#=#...3.p.pQ5....b....~.....Xv..OE<..T.....nA...7..i.;(s.....&..<...N.)x..5.Y.!Du.....O...fQ...) .0.Z..K#T..e0.... ..m{k.k.b..t...G..a.r.....0...v4.....Gi.....m.D..2.?1.E.j...^.....}.P-q.i...../.....\$.lr....\$.R.g.&F....K.`b..!8hM.e.L9^M...K.g.....p...Wi.3..ld...C..D...A..E7...@.R.r.7..TU....4L...`.....+ \$...CmJ.sNU.x...2.....g...4.....J...u.2"w.B.(.....t.7.>F..).RB....MIQ..=.Y....K.D.r.6/....%.[.n.#2..^y.T0.mY.G..._K..c.W...E...S.A..A.H.U.....f"...-gsJY.....!.....G.6.Bu.. _.....X...&v..U.y.u...3tH2.../.....v.-cm...t!.o9S..W....v9.7gD..s.k....cW.....l)D.2..jd.....N.q...\$.Q..X.+#v..=B.k\..xayB...ie.,9U.R.x...VFQ.9.%..._r.P.8..O..X..Dy.#.\....U ..gx.v.....4.....Z...V.....).s....G.))U.... .i..6...TsOnr:...{W.L.....m.JY...._2f.?v..V..;/;2.....=-.G..hx.Q.DvL...-....0.g.'.Y.....c..Z..y..z.R1U.....9..(h&q.n).

C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\R3ADM3.txt	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	1290
Entropy (8bit):	4.607071403570347
Encrypted:	false
SSDEEP:	
MD5:	FADB0F250D20EF2F614C4AB5D5D3AB0F
SHA1:	41E8255C91A40A8E832A8AC05747C9A579F55D07
SHA-256:	2CD73F11DA515955B62A930CA4DEFDE9CCB5230B8F5809E3C304EF854604EDA3
SHA-512:	E97F4B069ACB91C332BDDCA5C4314CBE6CC79C37E93CBB3F4D8B37544B49C2868E23B603FE4563A8961616F137CF646153A82F387D9C55FC8191108E86CF136
Malicious:	false

Preview:	..g....%.."^.....@P*M.^?.ed.L..@......8ZN.....4.....y.`D.[x.3..D!..T6].A..t.%E'&....Q.....~54L.....+y..3FP.+.....-G.m.'@..]".l..l.....g.m..y.J~.....<@N..Z...N....{^..B..#b....o..[.....]....L.....~\$y.....f..1.i\$B...V....}Z.v.cV./zL.G.....TyT8..(..z.Kq..!>)..7G0...3f..+9h.m.T0^&_x.....y...&_x.[\..=.....1..r^...H.....3.2_].C.9l.Y...a-s:..)?..VI.Ka.i.J..2p..Z...!.....`v;;h..p...&@..`(..8...3..u.y.Kd..4..m....bW...R.\$..Ot.....U.....6.l"G..%G....E.....9t*fq...&....q.uS]r..?....#...[r.&Y...i.YT.....*..[.s"C*~.^...^..E..(..S?V...8..R...Q..yP.)..[.....f..r..1.2:G...(\$....).4@...~x....}yzB....G....q.F.i/..N.L_[r.{.>#bQG.....O....?&..H....9].....i`.2.{.sY..B.....`\$...U.4L.3q...Xl...'P?0...SDe!8&...<!&...C....3....K)?1*@...!E`...4...g..v4.mE-..&..y..U-!vG...q....3@!N.`e...7..(.....1.z2....#M_/_/..e.b.3..V.w..F..dC/P..Y..2...V...<.9J
----------	---

C:\MSOCache\All Users\{90160000-0019-0409-0000-00000000FF1CE}-C\PubLR.cab.NB65 (copy)  	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	3562181
Entropy (8bit):	7.999378478377738
Encrypted:	true
SSDEEP:	
MD5:	1BD64E78490D3E51C922D3E3087C82D3
SHA1:	B498C6D45FE50C59D601700EC6EB8FCD2546AB20
SHA-256:	466B35C1084F8D6A315543D2BCCA32B6F9CCEB5EA5E12C32968F565E9D8B549D
SHA-512:	1EF1B05720A95D958F0EC51828D8348A98954C137FE3FE8B6809DBA501CCAEBBBB99AC353AA2244188757E9A32D69FBD655234F05271E3C606ADB66A64A193A8
Malicious:	true
Preview:	..g....%.."^.....@P*M.^?.ed.L..@......8ZN.....4.....y.`D.[x.3..D!..T6].A..t.%E'&....Q.....~54L.....+y..3FP.+.....-G.m.'@..]".l..l.....g.m..y.J~.....<@N..Z...N....{^..B..#b....o..[.....]....L.....~\$y.....f..1.i\$B...V....}Z.v.cV./zL.G.....TyT8..(..z.Kq..!>)..7G0...3f..+9h.m.T0^&_x.....y...&_x.[\..=.....1..r^...H.....3.2_].C.9l.Y...a-s:..)?..VI.Ka.i.J..2p..Z...!.....`v;;h..p...&@..`(..8...3..u.y.Kd..4..m....bW...R.\$..Ot.....U.....6.l"G..%G....E.....9t*fq...&....q.uS]r..?....#...[r.&Y...i.YT.....*..[.s"C*~.^...^..E..(..S?V...8..R...Q..yP.)..[.....f..r..1.2:G...(\$....).4@...~x....}yzB....G....q.F.i/..N.L_[r.{.>#bQG.....O....?&..H....9].....i`.2.{.sY..B.....`\$...U.4L.3q...Xl...'P?0...SDe!8&...<!&...C....3....K)?1*@...!E`...4...g..v4.mE-..&..y..U-!vG...q....3@!N.`e...7..(.....1.z2....#M_/_/..e.b.3..V.w..F..dC/P..Y..2...V...<.9J

C:\MSOCache\All Users\{90160000-0019-0409-0000-00000000FF1CE}-C\PublisherMUI.xml	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	2196
Entropy (8bit):	7.907341904973455
Encrypted:	false
SSDEEP:	
MD5:	9E4267006FC8F7CD0ECB315B9A85B3F3
SHA1:	44EFC1322721949EA9E12501A79321F5E8421EE9
SHA-256:	703F0A80EA9B859B9A2266756841E61BCBDB1E56BB0B0DD778E71B449EE74BD
SHA-512:	7E47CA20545F44C5DFDE6F72BD9D778D576F81C38ED877E21788BAF61AB1653474D674064C3530C5243FDE002775A7F3C4C4EA5C01E31E343006DA50D0089CE
Malicious:	false
Preview:	..2.O....&.*.....~.8.AuR.....0.R.....m.f.Jd..f....Y...F.Z..M.iE..%.....h.@...C..m.E].....z.....b....r..+..(u.bU..g(..q....L.Q.?7...o..M..wHO....2....*...6.a6e..>.K/~..R....4..Wh.n.h.-a)..o.t.w.]]}~;@>G."A7he....+..s.`l..0O..xK.....e....*yV:...f.HD.&.o....)x.f..M....l..&3.3.Pp..\$.C..D(p.]....h*.f.&w...X..#...<...Wc.R..G^`^V_a..'......3....k.../..l...j..Uas..Q.._M.s...kn.K.k.j.....p. l:..M.x.....~h.....H.J}.P-'..W5..'..d.l..c....o.... ...L5..../.E.2..W/....7?x.*OVh.y.#.r...O..O.j.a..w..".GP.....=%bs..#...o.`5D.U.S.....Z..5.[..\$P.q.wO[x??.*...l..K.....7..w....~r.9.....s!.`?EA].p....M..f%\$...3.Ky.DVE.rQ....W%..f....*....BG...y9..t....4p..V..W..]&`_%.%...3.8.R....Z..aN...Q..&....g....+4)..#...._wm.B.5s.A.7]...jx#w_w_l.W...M.3Wl.....n.....y..e.n..>i..5...@...S...x..._8>...T...x..l.x...7v..P.+S.....w([...~.B4..Rm.Z.][y...P....b..0>

C:\MSOCache\All Users\{90160000-0019-0409-0000-00000000FF1CE}-C\PublisherMUI.xml.NB65 (copy)	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	2196
Entropy (8bit):	7.907341904973455
Encrypted:	false
SSDEEP:	
MD5:	9E4267006FC8F7CD0ECB315B9A85B3F3
SHA1:	44EFC1322721949EA9E12501A79321F5E8421EE9
SHA-256:	703F0A80EA9B859B9A2266756841E61BCBDB1E56BB0B0DD778E71B449EE74BD
SHA-512:	7E47CA20545F44C5DFDE6F72BD9D778D576F81C38ED877E21788BAF61AB1653474D674064C3530C5243FDE002775A7F3C4C4EA5C01E31E343006DA50D0089CE
Malicious:	false
Preview:	..2.O....&.*.....~.8.AuR.....0.R.....m.f.Jd..f....Y...F.Z..M.iE..%.....h.@...C..m.E].....z.....b....r..+..(u.bU..g(..q....L.Q.?7...o..M..wHO....2....*...6.a6e..>.K/~..R....4..Wh.n.h.-a)..o.t.w.]]}~;@>G."A7he....+..s.`l..0O..xK.....e....*yV:...f.HD.&.o....)x.f..M....l..&3.3.Pp..\$.C..D(p.]....h*.f.&w...X..#...<...Wc.R..G^`^V_a..'......3....k.../..l...j..Uas..Q.._M.s...kn.K.k.j.....p. l:..M.x.....~h.....H.J}.P-'..W5..'..d.l..c....o.... ...L5..../.E.2..W/....7?x.*OVh.y.#.r...O..O.j.a..w..".GP.....=%bs..#...o.`5D.U.S.....Z..5.[..\$P.q.wO[x??.*...l..K.....7..w....~r.9.....s!.`?EA].p....M..f%\$...3.Ky.DVE.rQ....W%..f....*....BG...y9..t....4p..V..W..]&`_%.%...3.8.R....Z..aN...Q..&....g....+4)..#...._wm.B.5s.A.7]...jx#w_w_l.W...M.3Wl.....n.....y..e.n..>i..5...@...S...x..._8>...T...x..l.x...7v..P.+S.....w([...~.B4..Rm.Z.][y...P....b..0>

C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FFICE}-C\R3ADM3.txt	
Process:	C:\Users\luser\Desktop\ll.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	1290
Entropy (8bit):	4.607071403570347
Encrypted:	false
SSDEEP:	
MD5:	FADB0F250D20EF2F614C4AB5D5D3AB0F
SHA1:	41E8255C91A40A8E832A8AC05747C9A579F55D07
SHA-256:	2CD73F11DA515955B62A930CA4DEFDE9CCB5230B8F5809E3C304EF854604EDA3
SHA-512:	E97F4B069ACB91C332BDACA5C4314CBE6CC79C37E93CBB3F4D8B37544B49C2868E23B603FE4563A8961616F137CF646153A82F387D9C55CF8191108E86CF136
Malicious:	false
Preview:	-- ____ _ . \ __ V __ __ . \ / / ___ \. .` __ __ \ \\. \ // \ / _//.._\ \^ ^ ^ ^ ^ ^ ^ ^ ..By now it's probably painfully apparent that your environment has..been infected with ransomware. You can thank Conti for that....We've modified the code in a way that will prevent you from decrypting..it with their decryptor.....We've exfiltrated a significant amount of data including private emails,..financial information, contacts, etc.....Now, if you wish to conta ct us in order to save your files from permanent..encryption you can do so by emailing network_battalion_0065@riseup.net.....You have 3 days to establish contact. Failing to do so will result in..that data remaining permanently encrypted.....While we have very little sympathy for the situation you find yourselves..in right now, we will ho nor our agreement to restore your files across..the affected environment once contact is established and payment is made

C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\Setup.xml	
Process:	C:\Users\user1\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	2329
Entropy (8bit):	7.907397051258632
Encrypted:	false
SSDEEP:	
MD5:	15AD3801D0DEFCFF43C61847842935CB
SHA1:	2E7C9E0167CCCE9E80BF2D755666F22142F55C34
SHA-256:	DA57BE9739F221664DE120209C30F4CFDE6AC67319341CF570AF38D0D8131744
SHA-512:	4BD6B35BA4AAD24CF79CECEDC71F5AB2271AB65690BEE201B810C24AE605830DA60B0A9A07D1A03DE09BC8557B6B3CAA2AD0F732E6ECD373029375B9D94B A3C2
Malicious:	false
Preview:	-...}=R...%9..T..zX"...[...]'4d'-[-].....N....F..@O.....N..Y.t3.J..[n..].E.Xh..Rzb..Ne....Z...N..)[f.9.h8'.y4.\$%..[-.0J..].h.....p.....8.....R}.....8d5...lh..DU...X..c.....s...'G'.....H.xk.....[.*.....AK..v.W..#Jv.Ux.....e.(..Z.....lzHo.....-.....w..C*.#.w/D.)&.>.....g..y...T.3..i..\$.o.....g....yJ..SuP-0d.X.4...#.t0..L..\nPhtq..6t...X.[..).D.e\.....9(..... {..YN.....)j-.e{N.....e.....3.v...[.....4_1=%d.....][[.t..w.xp.M.....>...q.-l....)/...Sk.....6.f....>N.....X.....Tmo.K..[.(.NM.j-1.'n%.l.....f.....X..q.x.E1...Ot.u).o.....(.O 6...tD.hf).....f.4Q.l.T.....N..W;...Q..'c.e.....=H-.....?..C.....Qg.l.&...jD.=q=9...[X.....@..[.=u{c.t8...hl.Tv^..n..R.>o.....\X..&s.6hx.K(..H.x...'?..V.l.b.S..\....4_...d<..U.9... &b...7.R...'.e.4'..4...9M?&[...;[Sc.....E.#Vc.[.. =.....<..9.e.b...8DUT;l...&0C..\$.=...'.B.2..E.Drcm..Q...w.0....._jv...W..zM.+!.....Q

C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\Setup.xml.NB65 (copy)	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	2329
Entropy (8bit):	7.907397051258632
Encrypted:	false
SSDEEP:	
MD5:	15AD3801D0DEFCFF43C61847842935CB
SHA1:	2E7C9E0167CCCE9E80BF2D755666F22142F55C34
SHA-256:	DA57BE9739F221664DE120209C30F4CFDE6AC67319341CF570AF38D0D8131744
SHA-512:	4BD6B35BA4AAD24CF79CECEDC71F5AB2271AB65690BEE201B810C24AE605830DA60B0A9A07D1A03DE09BC8557B6B3CAA2AD0F732E6ECD373029375B9D94B A3C2
Malicious:	false
Preview:	}=R...%9..T..zX"...[.....'4d'.~[.....N.....F..@O.....N..Y.t3.J..n..]E.Xh..Rzb..Ne....Z...N..)[f.9.h8'.y4.\$%.. .0J.. ..h.....p.....8.....R}.....8d5...!h..DU...X..c.....s.....G".....H.xk.....].*.....AK...v.W..#Jv.Ux.....e.(..Z.....lZHo.....w..C*.#.w/D.)&.>.....g..y...T.3..i..\$.o.....g....yJ..SuP~0d.X.4..#.t0..L..\nPhT.q.6t...X.)..D..e.\.....9(.....{..yN.....)}j~.e[Q.....e.....3.v...[.....4_1=%d.....][.t.w.xp.M.....>...q.-l.....)/...Sk.....6.f....>N.....X.....Tmo.K..[.(.NM.j-1.'n%.l.....f.....X..q.x.E1...Ot.u}.o.....(.O6...tD.hf).....f.4Q.l.T.....N..W;...Q..'c.e.....=H~.....?.C.....Qg.l.&.....jD.=q=9...[X.....@.:.f.=.u{.c.t8...h!.Tv^..n..R.>o.....\X..&s.6hx.K(.H.x.....'?..V.l.b.S..\...4_<d<..U.9...&b...7.R...e.e.4"...4...9M?&[...; Sc.....E.#Vc[.]=.....<..9.e.b...8DUT;l...&0C..\$.=...B.2...E.Drcm..Q...w.0.....jv...W..zM.+!.....Q

C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlkLR.cab  	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data

Category:	dropped
Size (bytes):	4009719
Entropy (8bit):	7.999800682530956
Encrypted:	true
SSDEEP:	
MD5:	66CA5D08DB8423E52645A3F492FA61AB
SHA1:	68917C18C3B6B4E07C1BBAD26865216844791D3B
SHA-256:	A605E852A76889D336A09645F4631996DB52EC09F5BD4912846A7128433832C7
SHA-512:	61608624158B52CF4763E623FE4C1C38866FE24A732BB1E59FD62673B7B4D7F9213D89481E427858C429C318D51C21A419CF2061B171E79A26D00DF6CE40CCE1
Malicious:	true
Preview:	- ...&...r\...O.qnn...0.Q.G.@(.N.a...{.C....v.W.1.....Lk.j...W....9.e.d.i...&8.J.....g..G9.@...=_?>3i*lpf.....o..."..BF{[_T{...lj.g..F.`5...;.P...\\...\\B.\$.....O.....3^1..l.ypc..n m.~.J.j..Slq^Rm.....[.T...2...g.p.U.e.....N...sa.<i.Q.wJ4rA.....Fo.;Q..u..Rp.*....^#)..B:.....t.*Q..LdD.....8.s.og.y8.....OA..y...[...M.h..Z.x..%F.9.(...1....3F...q..{*s.UI...kl.(U.....s...h.%....)*.Q.w..L..@.8t...%3.....U...>?K...B....3..c[...E.>\\...&n....@.K.).R.?IPK...C..AeVv...w".....#G,NE)fN...>.Ti.v=AN(q...HMk...4.E..h.r.O.d1x.....\\>e...K E[...\\.\$}Yr%n...+.\\a.....Q.. .Z....!.jK...j.W..# .c.Z..m3k..2n....B.\$V..(j..aA..#Y..j.R...Dl=z..Yb...g.....\$.2. &.Un.c=..>=...CN.Y.0.,*...[.1.E...1..t..S...@.x.....\$....(U...))...%YnPe.)...af7..U...M#(....X.C&..V.....a..p1....Wl&.._i&Y..^X..UgE..]A.go.V....^..k.W.\\>R..h..[G.h(;.AuG.6..H.....n..w.F.!B..Y...jM..f.XQ<4

C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlkLR.cab.NB65 (copy)  	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	4009719
Entropy (8bit):	7.999800682530956
Encrypted:	true
SSDEEP:	
MD5:	66CA5D08DB8423E52645A3F492FA61AB
SHA1:	68917C18C3B6B4E07C1BBAD26865216844791D3B
SHA-256:	A605E852A76889D336A09645F4631996DB52EC09F5BD4912846A7128433832C7
SHA-512:	61608624158B52CF4763E623FE4C1C38866FE24A732BB1E59FD62673B7B4D7F9213D89481E427858C429C318D51C21A419CF2061B171E79A26D00DF6CE40CCE1
Malicious:	true
Preview:	- ...&...r\...O.qnn...0.Q.G.@(.N.a...{.C....v.W.1.....Lk.j...W....9.e.d.i...&8.J.....g..G9.@...=_?>3i*lpf.....o..."..BF{[_T{...lj.g..F.`5...;.P...\\...\\B.\$.....O.....3^1..l.ypc..n m.~.J.j..Slq^Rm.....[.T...2...g.p.U.e.....N...sa.<i.Q.wJ4rA.....Fo.;Q..u..Rp.*....^#)..B:.....t.*Q..LdD.....8.s.og.y8.....OA..y...[...M.h..Z.x..%F.9.(...1....3F...q..{*s.UI...kl.(U.....s...h.%....)*.Q.w..L..@.8t...%3.....U...>?K...B....3..c[...E.>\\...&n....@.K.).R.?IPK...C..AeVv...w".....#G,NE)fN...>.Ti.v=AN(q...HMk...4.E..h.r.O.d1x.....\\>e...K E[...\\.\$}Yr%n...+.\\a.....Q.. .Z....!.jK...j.W..# .c.Z..m3k..2n....B.\$V..(j..aA..#Y..j.R...Dl=z..Yb...g.....\$.2. &.Un.c=..>=...CN.Y.0.,*...[.1.E...1..t..S...@.x.....\$....(U...))...%YnPe.)...af7..U...M#(....X.C&..V.....a..p1....Wl&.._i&Y..^X..UgE..]A.go.V....^..k.W.\\>R..h..[G.h(;.AuG.6..H.....n..w.F.!B..Y...jM..f.XQ<4

C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlookMUI.xml	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	3371
Entropy (8bit):	7.944261601820058
Encrypted:	false
SSDEEP:	
MD5:	DA317A1239F1167F74D0ACD2957D706B
SHA1:	7512CEA8DDD6BE849EBB7DDF163CBD7D77FB7580
SHA-256:	C02CFB1CFB74ED52FA4E1D5F919578D3B7D32EEB7438631FA00B6B7664250881
SHA-512:	00764F0BA9C59D6834E5BE8AF5B11EFA87E639E42243D555722635FEA9BF219E7E2EEA30F0061F329185DC58CF78CE137224287A237A596DF0F1DB4BC8ABC40B
Malicious:	false
Preview:	..!..>pS<j...G....=1W..&.W.s{...m.= BC...U.a\O...[0 V.>J....".T...g.....-b...Nz...w ...]./.%.d..VR.)lr.j...Z....@IY.....oX*+...Xt".#K\....NP.....)-.c...;A.L....L.. :.....=q.M.....&....8..t.4...=s...A.K..9..p..B .E?A...m.G...v^.(.l...G.O.XU.....'W..{.'Yc.V...p%r..W...o.y.=.J....[[h..g.ec.Zr]-0\99.G...nk.....+^z..-..#..(....7.0*.. J.t@...;J.k....*D3K.y..y...`["C].m.....[...#. .L.yD.....[.7u..5C..+W.^6.o...4..i)j.X.& pz...F..<9#.nS.E.+<..j].pW..%&....H..GE'a.K..mK..c. .s.....W./....c.9.....?Zn;O.....\..l...hB#.4.*.#A.6....d.J...STe.'rA..i..4...^o.9.....%i..E..\\..u..[M.....H.E."q...\\.....^d..x..1W....l..&1....Z...~.9....M..v..\$.&....Z.h...v.e.....D'A....(sQ[...L.l.gC'.....4....%.0...M...O..TF...G.dS+7.../Kg.....A4oU...i...(^aV...6t....5...!..i..j.=nZ...^...9"...o6...))j...Jb.6j.R....^.....6.6A.OLa..

C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlookMUI.xml.NB65 (copy)	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	3371
Entropy (8bit):	7.944261601820058
Encrypted:	false

Preview:	.r.....^}.R/P.!.#N.....O5)Q...W...k..4:).H`~p.r....C.YZ.=b...l.....~.aS...p....v.o.....s.A...Z..a.M..).D%.Vs.S+ .C...K...wJ. @.....R.z.....5...6\$2.d.....'.....J.qQ....zr!...'Z2}.\$d."...p....RS.....(.....^H.(.fv..6..al.d3....".....#.E..Z.3.....&_Q...L...<.....KG.lgoe.....1.i.a'ke.?.!..O..S.....>..l.....R..8..O@>..v^.....1...t.x!..i.a.....G..`...h.4.a...t..nB.V....li^....?..l.SJX.^....q.qUD>....V.....LG.%(.....E.1Qs.;.Y.:Q..J.....d...))..J.....{...i..l."5.C...O.;4A<..v.....P..q.....l.l1K...T....?a...:D%O.....y..l.+).t.S.....).q.u.A.'\.*.Le.\$..V.l..N...JE.....fuv.x.%.....}.{@:Fx..X3^...../y9..L<...}.v#q..1^....0.e~gE...U.<.....A.H,3...kh.....5...y..S...nE9...=.cn.M.w.... ..._T...c...JGK..t+X....{*.UO..2MJ..l.9...^.....a.k.....3..../3u.KR.....V.....-F.\$.;."V .?.C..k.A! .}{m.X..LU9.A)/.s.Z .Gw....K%.p-*......7w.cX.S..
----------	--

C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordLR.cab  	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	10080267
Entropy (8bit):	7.999387105562405
Encrypted:	true
SSDEEP:	
MD5:	FA040C89B33F8970B9C8FE4F0DF2B27F
SHA1:	A03332F7BF387CB32E67283B5E094980832A5995
SHA-256:	A75C890ECAE48A4873E674C972714FD16896591429D0595BE9561CFBB8C06A59
SHA-512:	1489F69F755D47E0F1080F029613EACBE462B45CF0A3BEE7DF04527B9F66A07E933AD04C653D5CC46B226176FD01E4368B7BC5B622BB5F81FF5BDE91891A136
Malicious:	true
Preview:	I...!F.k..9;.....}".....V...fR..ZO...z?a.) ..-/./l...C.k.6j...C..A.4.&.C...~Q.5...+.N.D.....@..n[...`.....!Z.s..".....C.gD.)#.AMWB.....+...;mT...v..e #_JF.n..'.O.....+.. 5.....4J.Z#.jr.S....u .'.....s.)@...1..5..P<[9V....`b.YO.n...b./....Y. .=.j....A. 7..l.)).b"wy".Bw.....L... \.p(Yp.&...%.....i...5...R.l..M.....>B~e6.m.k.).j.._u.+...hZ..~>.RV...yD..u.UHqr.*.=iXN..^...9m.6J>.@...E.....LH.l(....tN.9.=s3=...&...'2`.9.\$...6..'YlC..4 7oC..].<Y.K.r.oS.....%V.d>/...l...g.5.Y+e....R...d.T@.Q.J.g@...3...7.....c7'm..kH..m....y..<h.mtl.bA...'...._V<S..b..g.. '.>M..E.q..wxz@m.....TZ.f.]...sh8F..k..D.l.YH.P.p.?FRi.j..S...us.y8.=8.{.....1.0.o.(k#s....by.....b.G..l..J-^..pYM..1.1.v)..a...j&..T@.E...Z..HRj.F...C...lO.+W..._u.e...}'^Co.N.`.....8k.....rq..w.D.9...../..3.....<....._.=<...CKL_T<...4 m].....-s.....^..[ij]?... ;-.%(){..o..Ed...p.....O'q....

C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordLR.cab.NB65 (copy)  	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	10080267
Entropy (8bit):	7.999387105562405
Encrypted:	true
SSDEEP:	
MD5:	FA040C89B33F8970B9C8FE4F0DF2B27F
SHA1:	A03332F7BF387CB32E67283B5E094980832A5995
SHA-256:	A75C890ECAE48A4873E674C972714FD16896591429D0595BE9561CFBB8C06A59
SHA-512:	1489F69F755D47E0F1080F029613EACBE462B45CF0A3BEE7DF04527B9F66A07E933AD04C653D5CC46B226176FD01E4368B7BC5B622BB5F81FF5BDE91891A136
Malicious:	true
Preview:	I...!F.k..9;.....}".....V...fR..ZO...z?a.) ..-/./l...C.k.6j...C..A.4.&.C...~Q.5...+.N.D.....@..n[...`.....!Z.s..".....C.gD.)#.AMWB.....+...;mT...v..e #_JF.n..'.O.....+.. 5.....4J.Z#.jr.S....u .'.....s.)@...1..5..P<[9V....`b.YO.n...b./....Y. .=.j....A. 7..l.)).b"wy".Bw.....L... \.p(Yp.&...%.....i...5...R.l..M.....>B~e6.m.k.).j.._u.+...hZ..~>.RV...yD..u.UHqr.*.=iXN..^...9m.6J>.@...E.....LH.l(....tN.9.=s3=...&...'2`.9.\$...6..'YlC..4 7oC..].<Y.K.r.oS.....%V.d>/...l...g.5.Y+e....R...d.T@.Q.J.g@...3...7.....c7'm..kH..m....y..<h.mtl.bA...'...._V<S..b..g.. '.>M..E.q..wxz@m...TZ.f.]...sh8F..k..D.l.YH.P.p.?FRi.j..S...us.y8.=8.{.....1.0.o.(k#s....by.....b.G..l..J-^..pYM..1.1.v)..a...j&..T@.E...Z..HRj.F...C...lO.+W..._u.e...}'^Co.N.`.....8k.....rq..w.D.9...../..3.....<....._.=<...CKL_T<...4 m].....-s.....^..[ij]?... ;-.%(){..o..Ed...p.....O'q....

C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordMUI.xml	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	2642
Entropy (8bit):	7.916808350850443
Encrypted:	false
SSDEEP:	
MD5:	11F391EB38662EE52FACCA9E1297037A4
SHA1:	63B28D659EC974551109658AFF9C23195CA88F70
SHA-256:	9FA4ABCA4ED658008EE8E00F982D8BAFEACCE878F809B96CAD47D13675B19656
SHA-512:	B7D7C83F78CD9752A4DECA0171DF5FBABE5B3E60E5569FCA70B4E4315475C821B72DC7CB694FEDF1899010748D2920A7A5EBAC4D10BAC386A358215DCEE74008
Malicious:	false
Preview:	.2..a.^.*.5....).WE.....VzP.B..Q.....%.B.=!*".....t... ^G...k.....d... 2.i.~.....'u...=.@[;D..e.\S.z..mp.7:aK..q/..Ew.Z.....a.T....V%...*0Rg@..pZ.qkd..s...'U....l.Z.s.<B&e.H...fG7...^..S(?F.....0.1....d'+.QW....%\$.K..F..n....z]zc...P...B..rk..D.Pw...yy.v.....!=[{...k.....l&G.n.....{...> ...5.3..O..&jj.L?.....AT.+Gvnm..J..+;.=...>...k9b...*D..f.w... .P.....C..D^B.....&P..~e...J).....'7=A&.....#.....P..uE"...V@.H.n....G~...f.+p6..@..0...n.. A...2Omx.)...8.....O...^c:...U..Z}...l..q.*!...(s...e1c.#...Z.....E.....\$3...+z .R.fi...&.....Z-r.)YVO.v..Jd.R3({.....M:.'l.* **(..l..._4...t.../.....s>.2...w...K..{..}.w...z..7g...).8.MnN"...s!:=..fU..{7.K&..w.N...8..md./P.. }....(.e.RFf.q...Y.<).n.F_2.S.K..p.Uz..[SLGg.OD....Z.hs. >@G.t.wW.....R.tr..~(JH...P..0.....{...?D<[...s.....Pl..n)...l.).....qz.sO....O..g...J..Q..l.DQg..h.. >..

C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordMUI.xml.NB65 (copy)	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	2642
Entropy (8bit):	7.916808350850443
Encrypted:	false
SSDEEP:	
MD5:	11F391EB38662EE52FACC9E1297037A4
SHA1:	63B28D659EC974551109658AFF9C23195CA88F70
SHA-256:	9FA4ABCA4ED658008EE8E00F982D8BAFEACCE878F809B96CAD47D13675B19656
SHA-512:	B7D7C83F78CD9752A4DECA0171DF5FBABE5B3E60E5569FCA70B4E4315475C821B72DC7CB694FEDF1899010748D2920A7A5EBAC4D10BAC386A358215DCEE74008
Malicious:	false
Preview:	.2..a.^*.5....).WE.:.....VzP.B..Q.....%......B.=!*.....t... ^G....k.....d... 2.i~:.....'u....=@[.;D..e.lS.z..mp.7:aK..q/..Ew.Z..... ...a.T....V%...*0Rg@..pZ.qkd.s...'.U...l..Z.s.<B&e.H....fG7...^.S(?F.....0.1....d'+.QW....%\$.K..F..n...z zc...P...B..rk..D.Pw...yy.v.....!= [...k.....l&G.n.....{.:>. ,..S.3..O...&jj.L?...AT.+Gvnm..J..+.:.=...>...k9b...*D..f.w,..P.....C..D.^B....&P.~.e...J).....'7=A&.....#.....P..uE"...V@.H.n....G~...f.+p6..@..0...n.. A...2Omx)...8.....O...^c:...U.Z]..!..q..!..!(s.....e1c.#...Z......E.....\$\$3...+z ..R.fi....&.....Z-r.)YVO.v..Jd.R3(.....M!:`l.* **...(l..._4...t.../.....s>2...w....K..[.]..w...z..7g...].8.MnN"...s.!=..fU..{7.K&..w.N...8..md./P.\]....(..e.RFf.q...Y.<].n.F_2.S.K..p.Uz..[SLGg.OD....Z.hs. >.@G.t.wW.....R.tr.~(JH...P..0.....{...?D<[...s.....Pl.n)...)......qz.sO,...O..g...J..Q..\..DQg..h.]>..

C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proofing.xml	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	1558
Entropy (8bit):	7.854442633868881
Encrypted:	false
SSDEEP:	
MD5:	B3D1F8F8D5442556967661706D8058DA
SHA1:	EBD674070D8101BBC8B66D70CB6FEC44587D416E
SHA-256:	AA82BB4A1B37D9156508CE3A86BD27D96E3E544086544A9B3334E066779BB6C2
SHA-512:	74B44A631AAB40E1BDDA02CE05AB9B24BDA8385ECBA2F100203DA7CAC10AD96268760D663FD0587B8CF3EEED95938C436FDB658CAAB4A479E290E6AF7F0661CF
Malicious:	false
Preview:	.Y.....u8.O.;!t.t.H...@.z..M.T.D.)o...Y.6..+....Q.?.....Zo...6...y.X.....-&.....2~V7:~'....C..N..d..B.g+...2p.y..~7.....5.....Q.Dh.{v}.<.. Y...5a.#.....&.tGD.C.*8[[..>}.D...lc...0.....l.@..sE."j"..-..p..[h..qxUw.....z..wz.....r..s>.o..!z...u...+....w.....fG.QSNjk+^..H.j..C...^ChV&.....{.R.L...8#{..uh.i.....>}.w.l.X.^5....%N%....v.x..o.Cw3...2^#..a...[cR.]b]>^..t..(.].....1.....)rAl...l5.....EO...].0U.'X...[...3f.;x..!2...C...1..T....nD.....=M..l...{7@.=...b..h....N...r..T..-f...X...r.(...lKY.ue.y...E.S9etk=c....4.R..J...!lK.~-.#...Q;\$....).K].5.'.u..l..oo"K.Z..T.r1...u[R..3....(l.%.&...8.W..OJ*8....)X..@..l.....E....b.waec.....{8A...q..eb...V.....\$.l.im,SH.:%#<...k.AJ...R=-."f..B....q.c...t....Ae[.....x.*8...H...l..c.....s.^eV*.....{..n..wC.....1.x..M.....le.z..*^>..)K....)%{...u...\$.1....P.;8..m.B...k)..r..Y.2j.&+

C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proofing.xml.NB65 (copy)	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	1558
Entropy (8bit):	7.854442633868881
Encrypted:	false
SSDEEP:	
MD5:	B3D1F8F8D5442556967661706D8058DA
SHA1:	EBD674070D8101BBC8B66D70CB6FEC44587D416E
SHA-256:	AA82BB4A1B37D9156508CE3A86BD27D96E3E544086544A9B3334E066779BB6C2
SHA-512:	74B44A631AAB40E1BDDA02CE05AB9B24BDA8385ECBA2F100203DA7CAC10AD96268760D663FD0587B8CF3EEED95938C436FDB658CAAB4A479E290E6AF7F0661CF
Malicious:	false
Preview:	.Y.....u8.O.;!t.t.H...@.z..M.T.D.)o...Y.6..+....Q.?.....Zo...6...y.X.....-&.....2~V7:~'....C..N..d..B.g+...2p.y..~7.....5.....Q.Dh.{v}.<.. Y...5a.#.....&.tGD.C.*8[[..>}.D...lc...0.....l.@..sE."j"..-..p..[h..qxUw.....z..wz.....r..s>.o..!z...u...+....w.....fG.QSNjk+^..H.j..C...^ChV&.....{.R.L...8#{..uh.i.....>}.w.l.X.^5....%N%....v.x..o.Cw3...2^#..a...[cR.]b]>^..t..(.].....1.....)rAl...l5.....EO...].0U.'X...[...3f.;x..!2...C...1..T....nD.....=M..l...{7@.=...b..h....N...r..T..-f...X...r.(...lKY.ue.y...E.S9etk=c....4.R..J...!lK.~-.#...Q;\$....).K].5.'.u..l..oo"K.Z..T.r1...u[R..3....(l.%.&...8.W..OJ*8....)X..@..l.....E....b.waec.....{8A...q..eb...V.....\$.l.im,SH.:%#<...k.AJ...R=-."f..B....q.c...t....Ae[.....x.*8...H...l..c.....s.^eV*.....{..n..wC.....1.x..M.....le.z..*^>..)K....)%{...u...\$.1....P.;8..m.B...k)..r..Y.2j.&+

C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\R3ADM3.txt	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	ASCII text, with CRLF, LF line terminators

Category:	dropped
Size (bytes):	1290
Entropy (8bit):	4.607071403570347
Encrypted:	false
SSDEEP:	
MD5:	FADB0F250D20EF2F614C4AB5D5D3AB0F
SHA1:	41E8255C91A40A8E832A8AC05747C9A579F55D07
SHA-256:	2CD73F11DA515955B62A930CA4DEFDE9CCB5230B8F5809E3C304EF854604EDA3
SHA-512:	E97F4B069ACB91C332BDDCA5C4314CBE6CC79C37E93CBB3F4D8B37544B49C2868E23B603FE4563A8961616F137CF646153A82F387D9C55CF8191108E86CF136
Malicious:	false
Preview:	_ ____ _ _____. __ V __ _ . \ // __ _ \. .` __ \ _ \ \ \. \ / / \ / \ / \. \. \ / \ ^ ^ ____ ^ ____ /...By now it's probably painfully apparent that your environment has..been infected with ransomware. You can thank Conti for that.....We've modified the code in a way that will prevent you from decrypting..it with their decryptor.....We've exfiltrated a significant amount of data including private emails,..financial information, contacts, etc.....Now, if you wish to conta ct us in order to save your files from permanent..encryption you can do so by emailing network_battalion_0065@riseup.net.....You have 3 days to establish contact. Failing to do so will result in..that data remaining permanently encrypted.....While we have very little sympathy for the situation you find yourselves..in right now, we will ho nor our agreement to restore your files across..the affected environment once contact is established and payment is made

C:\MSOCache\All Users\{90160000-002C-0409-0000-00000000FFICE}-C\Setup.xml	
Process:	C:\Users\user1\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	6601
Entropy (8bit):	7.971571818282002
Encrypted:	false
SSDEEP:	
MD5:	5CECAE7160C6FDE13C0925DAB3735E50
SHA1:	25D0D6A3109280FE4D4FA6C070D3A33249924C7B
SHA-256:	C7538C4B257482E3AC6306E6018961A4A59CD01B240C36102FCEB574B68CFE9A
SHA-512:	3532F797B084D0FC3C6A2BB6454DF74DBBB205DEB4AD3690EDB8A3BD37A8A90920D535EFFBA695CFFEF553DB94393461D67836CB51CCC1D19C1592E0AF358DF
Malicious:	false
Preview:	.q.ymz.....Vzm2...E.T.....NB.....X..o..O..W..T..%.....^..gS`z...~g.<.....R(t...Q.....Q..WzL2..^...o..0.l.n.....l.k(6.....@Nv...h`...V...^.....PR.Q.x.....k~..b.4...'.sh..(ft.6U.r.<..y\$LF.f- ... \..l.#..(. "U V.L.L+R.oR).....07#...4.Y.8TxP...O...S9...3;...J...m.{...!..Y..(G...J.....S"-..HJ...oiVej_..a.7..D...U...W.g.Q...&.0.3iU....i...~.fJR.?J..T./.....P..D'..(N..M.....(C.....GK..U.B#..y.M.....4!50.F.JD...'.j.*.][...S...\$A....?..+...+.....Y... ..p....._84.....@c]..+0_8.N!>.gh8...X...Z.....tl..>..J.@2...aF9`'....@i...0.....CM..l.d.e%.....".....&).Nr.0...j.d.'d'.....S.J...jdBv>0Z..Ms.oj."..a...V:v...D...O.q...0P..D...Os)5.%..D.3b`v...g..W.d...J.....EH...G2.8..}.q..q...gQ.{...TL...{!..`.....L...!..H..X...aS..C%.*-.....N...U.n.....O.....d...@C\$......2.....U).~'!..K..J.T..5Fz.4.F..8jG.G.9..@..1elU.....\$.aL.....H.`C9.....DX..wk`....b.....m.....'0`"f.l..

C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Setup.xml.NB65 (copy)	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	6601
Entropy (8bit):	7.971571818282002
Encrypted:	false
SSDEEP:	
MD5:	5CECAE7160C6FDE13C0925DAB3735E50
SHA1:	25D0D6A3109280FE4D4FA6C070D3A33249924C7B
SHA-256:	C7538C4B257482E3AC6306E6018961A4A59CD01B240C36102FCEB574B68CFE9A
SHA-512:	3532F797B084D0FC3C6A2BB6454DF74DBBB205DEB4AD3690EDB8A3BD37A8A90920D535EFFBA695CFFEF553DB94393461D67836CB51CCC1D19C1592E0AF358DF
Malicious:	false
Preview:	.q.ymz.....Vzm2...E.T.....NB.....X..o .O..W..T..%....^..gS`z...~g.<.....R(t..Q.....Q..WzL2..^...o..0.l.n.....l.k(6.....@Nv....h`...V...^.....PR.Q.x.....k~...b.4....'...sh..(ft.6U.r.<..y\$LF.- ...;\..l.#..(. "U V.L.L+R.oR).....07#...4.Y.8TxP...O...S9...3;.....J.....m.{ _!..Y..(G...J.....S`"-..HJ...oiVej_...a.7..D..U...W.g.Q...&.0.3iU...i...~.fJR.?J..T./.....P..D'.(N..M.....(C.....GK...U.B#..y.M.....4!50.F.JD...'.j.*.]{...S...\$A....?+...+.....Y. ....p....._84.....@c].+0_8.N!>.gh8...X...Z.....tl..>..J.@2...aF9`'@i...0.....CM..l.d.e%..." :(&.).Nr..0...].d'.....S.J..jdBv>0Z..Ms.oj." :a..V:v...D...O.q...0P...D...Os].5.%..D.3b`.v...g.W.d...J.....EH..\.G2.8.}.q.q....gQ.{...TL....{[. `.....L...!..H..X..a.e.S.C%*.....N.....U.n.....O.....d...@C\$.2.....U).~'...K .J.T..5Fz.4.F..8jG.G.9.@.1elU.....\$.aL.....H.'C9.....DX.wk`....b.....m.....'0 "`f.l..

C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfLR.cab  	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	3912184

Entropy (8bit):	7.999836747541346
Encrypted:	true
SSDEEP:	
MD5:	107F922011729A2EA63FDB0FCA313981
SHA1:	DE63DDA3C0DA70F7076A95CE82CE33235A691988
SHA-256:	7BF42F7FE4790977309A16EF9C832ECF9E4AA422FDF9CCCE4EDF4380C6056188
SHA-512:	B218229A073347F244D56316D752C80FDD158BB2CE24564761BDE23801E4472881F7D3BA04E2815AC2AA1DCCCC887C3F0FE50CD8A8F8E6B08FA110125A4AE64D
Malicious:	true
Preview:	e".".T.G...P.- 0U...p`.H^{.'&h...Q.d\l.)......`2@w...G...D.....).....\$.+...e...p.(4..T.8#.....:1..]3.h.....L/.....k~>..B.{~.._Lf...W6...)0.'.....U#.IP.y.0..@t.#.%..V...r.....2_9..B.S \$p.....D*f...p.....O...m.h...tM77J.Q....._b/.U.?...YT..."j1x...].8s.d.?h..(..V6.i>..4.....4.J.....i0...XG.....;g3... ..J...+.....{...y.l.....rVkf.Gr.#.D'.Hw,Y...1..m.3.,2. %......k-.K..0.#..".%.&72..P.5.hZ.z..s...r;.&C.;...B....NG`..).6. B...s.])...RM...W.P.Q...d.m..9JQG<.....).....H...V.xU.8.`&..bL\WH.1CxD+B'..IR.y..T..?.e!...o..].n.k..@. B.....u'.?Mq.....#Z!.....5.aT;N.Xx..k.%ZM. .5. ...2... ..Y.jl.e@.j.*...b]... ...-.....hO.Eq...;s.....HO..3.P...Z.....y!...)....L!.XQ...i.o...Xc..6.Q.di[n.Y.,S.1....3.. .3...O...h...`9..0...c.q.r....c.>!.....z\..C-.sm...5.....%.....+K.ux.....tXk[N.cv...b.2...f..'.8\B.OI.+..\$.N...E.....l.....+..7e. ..].1g.....:^.u.#.....

C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfLR.cab.NB65 (copy)  	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	3912184
Entropy (8bit):	7.999836747541346
Encrypted:	true
SSDEEP:	
MD5:	107F922011729A2EA63FDB0FCA313981
SHA1:	DE63DDA3C0DA70F7076A95CE82CE33235A691988
SHA-256:	7BF42F7FE4790977309A16EF9C832ECF9E4AA422FDF9CCCE4EDF4380C6056188
SHA-512:	B218229A073347F244D56316D752C80FDD158BB2CE24564761BDE23801E4472881F7D3BA04E2815AC2AA1DCCCC887C3F0FE50CD8A8F8E6B08FA110125A4AE64D
Malicious:	true
Preview:	e".".T.G...P.- 0U...p`.H^{.'&h...Q.d\l.)......`2@w...G...D.....).....\$.+...e...p.(4..T.8#.....:1..]3.h.....L/.....k~>..B.{~.._Lf...W6...)0.'.....U#.IP.y.0..@t.#.%..V...r.....2_9..B.S \$p.....D*f...p.....O...m.h...tM77J.Q....._b/.U.?...YT..."j1x...].8s.d.?h..(..V6.i>..4.....4.J.....i0...XG.....;g3... ..J...+.....{...y.l.....rVkf.Gr.#.D'.Hw,Y...1..m.3.,2. %......k-.K..0.#..".%.&72..P.5.hZ.z..s...r;.&C.;...B....NG`..).6. B...s.])...RM...W.P.Q...d.m..9JQG<.....).....H...V.xU.8.`&..bL\WH.1CxD+B'..IR.y..T..?.e!...o..].n.k..@. B.....u'.?Mq.....#Z!.....5.aT;N.Xx..k.%ZM. .5. ...2... ..Y.jl.e@.j.*...b]... ...-.....hO.Eq...;s.....HO..3.P...Z.....y!...)....L!.XQ...i.o...Xc..6.Q.di[n.Y.,S.1....3.. .3...O...h...`9..0...c.q.r....c.>!.....z\..C-.sm...5.....%.....+K.ux.....tXk[N.cv...b.2...f..'.8\B.OI.+..\$.N...E.....l.....+..7e. ..].1g.....:^.u.#.....

C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.xml	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	1764
Entropy (8bit):	7.868275604518784
Encrypted:	false
SSDEEP:	
MD5:	366BD7B64331D37D0D145CFF0A1CEF07
SHA1:	189DC1009670CDE4D61499D465DC77CE2C83FEB8
SHA-256:	C5FD767E7004ACF19F1E528F89D0C5D87B5DEF03563704B1C68F1DB9BB6E2D5B
SHA-512:	5199CE835ED089F8F53B54656370853608E90B0C48EB16B52D18DB700D174FCE0AEF6E8CA3BE8FF4604149675944D10F4919A8F87F9DE5897F3BBDE0AF08FABD
Malicious:	false
Preview:	%Z8f89.....&.*E.5.T.*].Pg0VT:"^.....&/.).3.+.../.....#Z^..z....Eh.1..7.Gu:\$r.[...omJ.kE..p.0.^...U?X.....Jg...D7..."Y..{lmq\$....K.&?.9.m(.3.`....bb...'@...ym.KM...." .....Sq.Y.&e`.1\$Rc..70....#.....ZYR.o..S][i@f.....o.Q.G.\$j#.....P.\$.....h2~...A.....N...\$G% ^h..35...u.KG..Se+..C\$&..k.U9yu..d].....;#..k..L...4.....Hl...h..G.U.Z.#.].\$a...r6. ..B...y5.....5.x.g.<..._A.l.....o.v...y.%.....b..E.8.Z[...sc..t.z.q..S...5.b.....>X.z...^Q....fW...'.L.E4:l.+s.H*q{L.....}.pW...lX.....bM..._...#N..QLG.D.q.j2.C%.=..._\$.h... ^yH.F.....B..l5.l.....N.a...l.wNo.WRh7M...5.-...Fl.^.....l.....Z...^..qkZ..K...~.....e1...4J.9.P.Xm.W.^...C..N...@N.....pG.....p~}.S&/0...>..V+.\...@2.&..'i.7....w..cz.\..n../B.OB...i4....TwV...:x.o.""9...eE..v.t...fa)..\$.C.<{/.^*1.D...c*#}).r.....l.l!'.....&... \V..D.G.4..>M.8...x!l.K.l.n.^....@~.lv..m@...d>y...@-.....b..

C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.xml.NB65 (copy)	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	1764
Entropy (8bit):	7.868275604518784
Encrypted:	false
SSDEEP:	

SHA-512:	4E95F3AEA8FB820B269B671F010387CD7C67B4DA8D331AA0EED31151C945DD59DD0F9F091CB208272564BDD6B230C70FE492B016528783E4A62010C85D47BE11
Malicious:	false
Preview:	..X.@.v.JF.r../.}.z.}......0.O.....)F.....TP0.\^1...*...j..f g...c.j.C....r....X.^%....D.fx....2.....H.....Z.iZx...W2.D..Fb..X.;%=.iX....^8CN.....{...zO.c/O`).l.qM...Yc.,P....,4i.O...f.a>.V.p.~..`Sz`.*.Tc..7;X.q).O.....Q?...L.f...=T..s..x:....0.)n.n.Q./j/.gs#...q....='<c.l.;.....BN.0...N.t.cz.bl!..z.. W.X.d.*.....b".w....>.._X...P.M...c.d5..t./...az...2..H 'x'Q+p9....+....(.....00...q/.....O8 PpF&\$siTu3s;}Ht...b..f...o.6..c.`....Ao.q..s..WH....\..7=-.a.bC..Z_...9.9/1W.x.9...M...Z.LnM..p.....#....:0.;.H..E1.6..4..-..... (.1kt.]k..&;'.w.]...n...H...~.n*.y..F0....7.i.s...H&,...M<8..({.u&q.prV.-xt..5.....{>.e2..hM'.N.~.p...>.d&.h.K..k.sZ..@G3 X.g..h...q.]...t0...=r..].N.!}.~.".PE..*\$.....8g.Y...m.D....L.Y../N..+..k(....N.9.9.T'.....9..8.<.a.j.Sx.....v..C.h...L..N....fo3.....a.Ke...;Yy..s.>TD4.....7.K.^K..'sE.....j...b...D...k....J2_....'...2.+x.b..=OD.c\@._@.z.b R.R;`.4_.\$.*.

C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.cab  	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	642124
Entropy (8bit):	7.999658671442192
Encrypted:	true
SSDEEP:	
MD5:	750A3737095024F053DB9D1180CF0BF1
SHA1:	9D49EF9C51BC36F2257036914102392321900586
SHA-256:	4B10E1BF0B6315085472B33E9B9EFD393CACC4DCCFD1F666FA6D166D8C99081
SHA-512:	FDA9EB34F47008F48C93790201CA5C8A79356136A226FE642C78C969D5381353A30C556A9B0914E2BF97B4490E9CA12BA38AB0E8DE464FCEC0FAE0A6D15E8D42
Malicious:	true
Preview:	...;w....4.=95.F.E.{ GZIX.D....u.qr.....#.....6.....Wn.iR.tJ..K..c?...^N.6....g.M s..Y.....y....iOQ.%mN....2?Azb.IV..._(a..X...CJ..._.....g_u.M.TD<<.Kr..i..(4.k...{7V,p>.[Zbj6{;U=.....ds.vv\....9\...".:C.L...gq.1..]M+...H..#...Z.{UA.P...cFPt.1M'U...M.....p..Rp....!...l9&Wy..../n. 6..f;.....efS.oK...i.t.4...Z..z.Q...6...uT.y.j&Y.K..B....X..C.....z...^G.C\$:.M:9..q..&\.....h.....e.....G{...+...`J...O.WeZ<O.....9 'l.Hp..c`...S..j.....s@..F.?.N+g.../..`".B.....f.w....`.....!...6y. ...x..d.....Q(5..T...VR.I>.....}g..-~*.....e.c_q.9^O...`..7u8.k.Q...[.C.9..JC~...%..-9//@*!....b...*3.*..Lu.1/c.<QQ..)......r\p.j..h..~.&2>(a.&#.....D..d.X].7..\..).....R.....o...R.z(..).B0K_<]....D~....!n..*.?#.....M.[[.....qz..&v..je.....@....F....1...3i.q.j.R....U....5...i.4....e0.>bd..*&...>Y.J..Q.. u...>y.G8.7.-\3M+..!./P.fv...O.a....Yac.k.W@f.L...8%<.. o.IG6..`..H.v..E.{.....\..

C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.cab.NB65 (copy)  	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	642124
Entropy (8bit):	7.999658671442192
Encrypted:	true
SSDEEP:	
MD5:	750A3737095024F053DB9D1180CF0BF1
SHA1:	9D49EF9C51BC36F2257036914102392321900586
SHA-256:	4B10E1BF0B6315085472B33E9B9EFD393CACC4DCCFD1F666FA6D166D8C99081
SHA-512:	FDA9EB34F47008F48C93790201CA5C8A79356136A226FE642C78C969D5381353A30C556A9B0914E2BF97B4490E9CA12BA38AB0E8DE464FCEC0FAE0A6D15E8D42
Malicious:	true
Preview:	...;w....4.=95.F.E.{ GZIX.D....u.qr.....#.....6.....Wn.iR.tJ..K..c?...^N.6....g.M s..Y.....y....iOQ.%mN....2?Azb.IV..._(a..X...CJ..._.....g_u.M.TD<<.Kr..i..(4.k...{7V,p>.[Zbj6{;U=.....ds.vv\....9\...".:C.L...gq.1..]M+...H..#...Z.{UA.P...cFPt.1M'U...M.....p..Rp....!...l9&Wy..../n. 6..f;.....efS.oK...i.t.4...Z..z.Q...6...uT.y.j&Y.K..B....X..C.....z...^G.C\$:.M:9..q..&\.....h.....e.....G{...+...`J...O.WeZ<O.....9 'l.Hp..c`...S..j.....s@..F.?.N+g.../..`".B.....f.w....`.....!...6y. ...x..d.....Q(5..T...VR.I>.....}g..-~*.....e.c_q.9^O...`..7u8.k.Q...[.C.9..JC~...%..-9//@*!....b...*3.*..Lu.1/c.<QQ..)......r\p.j..h..~.&2>(a.&#.....D..d.X].7..\..).....R.....o...R.z(..).B0K_<]....D~....!n..*.?#.....M.[[.....qz..&v..je.....@....F....1...3i.q.j.R....U....5...i.4....e0.>bd..*&...>Y.J..Q.. u...>y.G8.7.-\3M+..!./P.fv...O.a....Yac.k.W@f.L...8%<.. o.IG6..`..H.v..E.{.....\..

C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.xml	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	1749
Entropy (8bit):	7.865372462150396
Encrypted:	false
SSDEEP:	
MD5:	332A955D28624D7B7465F4EA37A3C814
SHA1:	7E7CBD25B90ABD47A67CE7E265FFA4D6D011F793
SHA-256:	A7E428BEFABD5F4560EC3F3496ABED70014F4C043FF5E5F96220D27180662428
SHA-512:	C7030D5054071652EBC146796138EA24B6EFEADA31B8DA1D1814C4289ACEAC32D05917526D64BE91EEA0FD6E8DF6CEAA4D963C12C92A0772D491AFD3EF98851
Malicious:	false

C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\Setup.xml.NB65 (copy)	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	2342
Entropy (8bit):	7.901406619084725
Encrypted:	false
SSDEEP:	
MD5:	BA6E6BFC213F1D2FAF527CD43531C3E4
SHA1:	2B4A2FD02CF8C1BB2FEDBF69B7740212F3E750C1
SHA-256:	2A6A15DAD8218B0990794C7C154FF0463F7E23C8F9CFD01EA3316EBB558FBF72
SHA-512:	946B1E1CF25923872FE0F781C63FB93BABA259BBAC1549C269DD5FE8F57451C2B693297D82307BD759CE673AE61DCC399D0C370D978B641E0ACA15A97C8C041
Malicious:	false
Preview:	*.\$./_...W'.....Z ..p.....p+bN..E...Q;.....<.f.V..j..s...&L...6[w.....i..m#.....2 ..z..W....k.v.....I-R...=o.Y..CM....5...6.M..... .k....\ .=fBj.> q_..._Ngv.....Nb..7..a.[q.s.<..L.p.....) ..=..Z..3..q7...O...Plq...r.Y...Uh.p.'\]Hu.'?'...L...x.b..k...E.U...c*0.d.....o.]VV..*0[<.....G?lyX.R...>...J....."(r.0He..W.....~..0...j.y..~...s.Cs.M.}...U.Pw...Apz.IE.[7.....7....P..W.'4..'86.....S....Z.eZ\I? ..'.....P...\$...?c.....\$&=4.....C...B.'...'R...i.W.->.P....NIO]....B..3.q.p.9.st..{LQ.).....gx .f.-.]\$.%ijnkz..hWn../.s".....R.3^.....F.+...f/.U..S..M..*k...E{[...?5.....7.j..NiO..U.....O...N.<GR..bm.l.....gi..Y../Fs#.b..o2.t.=...^3mDs.9)cJ...&a.....Z^.....5@...~2.O..4...G.....vt[e_...!bF... =.....{3.G..._g.N)...H...p.mCd... ..}.....&s.....g...#7.U~...m.....b[U...u.`..1..1..w.....S.+z..EDmC. 2..4...].Hx.&*y~..u....X....%/x7&...2..B[[R_x.....=.i.q'@.....<ZK..

C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.xml	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	2351
Entropy (8bit):	7.9010019667958415
Encrypted:	false
SSDEEP:	
MD5:	CEB3EFB51911FC07CB86D9062DF9FDE9
SHA1:	18F1027D4DB529074B3DD719A0D1DABB06EC5CD1
SHA-256:	A6AB0BCC1759ADD40BDBA614236D5C144BB2961D176FC56945EA10E0807B203F
SHA-512:	972FBFC3DE9F6A81EF652929E32DFDA23A467752FC38232C5886BD05E5F8726F43079FC5A271FACC316EED0971E58CCC1DD0E06640E9711FCCBD16FB53BE3CAC
Malicious:	false
Preview:	.Y.Jf.;.;#8..8.0~..z...Y..fM.^..U.....b...k.....#5..7.F:'.....2 .QA..T .n.....Zh>4n#..J>_...b.4.g=.....SO..v..[.^).....f.M...k.?..sS..8 _ln..i.Ro....(,A=...D.v.~ .. V..."z.....U..XK..t.&{q.....Z..3...2..E.....4.....3.m.l#..n?..Y.U=0+....h.....<P...*6c...B.M)\$~...XK.s.P....u]%)... .6.....~...*.....G...;@...?..kJ\$JJ.&V...+!D.xQa x...Z..&..l..l..."~...tQ&~...N7.'0.L=bL.B\$.s.9"..Fl'..W.r...3'.l.....s...}.i...@.+!...~5(...Fhg.YzM..."ns.C\...H-o.^@X...{S...u.H..x...^>.....R7r.CV*p.....4....."^.J...3...j\$&.O.. X.].....B.v.CLog...pk.....F.s?"...b...P.&..Lx...^.....l.....= ...y...a...#...%*c^..J'.....sE."}.&..~...(...2m.w.s"...:[9..7.F..H..U.(.uk..y....+...a \.%(IR.....aZ.....2..0'.0.q...!7d.n;..gf=y.O..J...M..."..W.4.oY&r..n...S.. ...Q..ur...~..p.sr.cx...K.}wm.N4!.#+.^_W_...8"...[.l....fb...../nk%...Qe..7y..s+]V6.....}.j.u.C.w..4.8.m.)Gp.2C.f.vF...O...w.=

C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.xml.NB65 (copy)	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	2351
Entropy (8bit):	7.9010019667958415
Encrypted:	false
SSDEEP:	
MD5:	CEB3EFB51911FC07CB86D9062DF9FDE9
SHA1:	18F1027D4DB529074B3DD719A0D1DABB06EC5CD1
SHA-256:	A6AB0BCC1759ADD40BDBA614236D5C144BB2961D176FC56945EA10E0807B203F
SHA-512:	972FBFC3DE9F6A81EF652929E32DFDA23A467752FC38232C5886BD05E5F8726F43079FC5A271FACC316EED0971E58CCC1DD0E06640E9711FCCBD16FB53BE3CAC
Malicious:	false
Preview:	.Y.Jf.;.;#8..8.0~..z...Y..fM.^..U.....b...k.....#5..7.F:'.....2 .QA..T .n.....Zh>4n#..J>_...b.4.g=.....SO..v..[.^).....f.M...k.?..sS..8 _ln..i.Ro....(,A=...D.v.~ .. V..."z.....U..XK..t.&{q.....Z..3...2..E.....4.....3.m.l#..n?..Y.U=0+....h.....<P...*6c...B.M)\$~...XK.s.P....u]%)... .6.....~...*.....G...;@...?..kJ\$JJ.&V...+!D.xQa x...Z..&..l..l..."~...tQ&~...N7.'0.L=bL.B\$.s.9"..Fl'..W.r...3'.l.....s...}.i...@.+!...~5(...Fhg.YzM..."ns.C\...H-o.^@X...{S...u.H..x...^>.....R7r.CV*p.....4....."^.J...3...j\$&.O.. X.].....B.v.CLog...pk.....F.s?"...b...P.&..Lx...^.....l.....= ...y...a...#...%*c^..J'.....sE."}.&..~...(...2m.w.s"...:[9..7.F..H..U.(.uk..y....+...a \.%(IR.....aZ.....2..0'.0.q...!7d.n;..gf=y.O..J...M..."..W.4.oY&r..n...S.. ...Q..ur...~..p.sr.cx...K.}wm.N4!.#+.^_W_...8"...[.l....fb...../nk%...Qe..7y..s+]V6.....}.j.u.C.w..4.8.m.)Gp.2C.f.vF...O...w.=

C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OnoteLR.cab  	
Process:	C:\Users\user\Desktop\ll.exe

File Type:	data
Category:	dropped
Size (bytes):	13355306
Entropy (8bit):	7.999924814406783
Encrypted:	true
SSDEEP:	
MD5:	A8E73ECAC60EB1DA614DFD2D627943FE
SHA1:	AC6A6361D27D7ADD260FFE43690CB3FD01F63138
SHA-256:	4250DAF835338C696D877DCDE8D04267DF2B8158AAF2ECF8CCD912D52C2D3B6E
SHA-512:	F8D8D8E57F0D7A5ECCAFD639984FB93DF37584D9DD4BC811DB88DA8F5C45258E22547BD44B787AFAFFA00B7C4AD8488C3D3CA195B41CA9539A125226609543F5
Malicious:	true
Preview:	J..QKJlg.V9N.k>....x.z...<R..A...o.s..2}.m.}.f.3.:{;.....d.....7Y}.kG.)4.....A..b.....c.)..L.~.....O..._(q6..b.p.0.W..Ji....@....8.....~^...vD.(&..g.A.<E...M.m.e).....t...e...hDb0.....t.M..fn..J..k.o.d.2~6.....x..}.K.....gk.[.Uhx.....QH..M...F}.a.z..G..X.+?...e....._1(DE..u!..hUyl..D....*....). >..}.8.....^ h..W.l....R.3....x....R..=(5..1.....O....7..X.))p.i...x..}9%..cac.....wWC..2#.i.p%Jpx.T.j>.....o.il...09..e}.Ti6Lgo.^...Q..F.....&.5...i>R..\$.Bl..M...%-C)...%.(.({.....a)9b.is.7..q.Z} ..b.B..a1..>A+.....g.rR^?.pN[...E3.qm.m.?.....-s0<.rr?9>.....}.62:}.m.g2 Oy..t.0P)..U.....}.@.MQ.....e.Q.G.'6..z.{.....S..K..... #.....V...D'bp..G..9S:.....Q.sk...+(...h:0...}.=..Z.....4..L..s....x.f....Y..>8.oV..}J5l..f.to.....;u(6.n.&.51,70.n.Z!)..n.y..m.5Z.r.3b..F.E..u.Jk.FW.^{.....6.#.L.....CTQ...'RW..u..r.W.+h.y.^C.)}%.....O..dR.gi<C>.. .}....Z..O

C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OnoteLR.cab.NB65 (copy)  	
Process:	C:\Users\user1\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	13355306
Entropy (8bit):	7.999924814406783
Encrypted:	true
SSDEEP:	
MD5:	A8E73ECAC60EB1DA614DFD2D627943FE
SHA1:	AC6A6361D27D7ADD260FFE43690CB3FD01F63138
SHA-256:	4250DAF835338C696D877DCDE8D04267DF2B8158AAF2ECF8CCD912D52C2D3B6E
SHA-512:	F8D8D8E57F0D7A5ECCAFD639984FB93DF37584D9DD4BC811DB88DA8F5C45258E22547BD44B787AAFFA00B7C4AD8488C3D3CA195B41CA9539A125226609543F5
Malicious:	true
Preview:	J..QKJlg\..V9N.k>....z....<R..A...o.s..2].m.\.}.f.3..{;.....d.....7Y].kG.)4.....A..b....c)...L~.....O_...{q6...b.p.O.W..}i....@....8.....~^...vD.(&..g.A.<E...M.m.e\.....t...e..hDb0.....t.m..fn..J..k.o.d.2~-6.....x...\.K.....gk.[UhX.....QH..M...F}.a.z..G..X.+?...e..._1(DE.u\..hUyl..D....*.... .i.>..}8.....^ h..W.l.....R.3....x....R..=(5..1.....O...7.X.))p.i...x...l%\.cac.....wWC..2#..i.p%Jpx.T.j>.....o.il!...09...e\..Tl6Lgo.^...Q..F.....&5....i>R..\$.Bl..M...%-C)...%.(.{.....a)9[b.is.7...q.q.Z]...b.B..a1..>A.+.....g.rR^?.pN[]...E3.qm.m.?.....-s0<.rr?9>.....\..62.:M.g2\Oy..t.0P).U.....}.@.MQ.....e.Q.G.'6..z.{.....S..K..... #....V....D'bp.G.9S:.....Q.sk...+(...h:0...\..=-.Z.....4..L.s....x.f....Y..>8.oV..]J5l..F.to.....;u[6.n.&51.70.n.Zl)..n.y.m.5Z.r.3b..F.E..u.Jk.FW.^{.....6.#.L.....CTQ...'RW..u.r.W.+h..y.^C..)%.....O..dR.gi<C...>..Z..O

C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FFICE}-C\R3ADM3.txt	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	1290
Entropy (8bit):	4.607071403570347
Encrypted:	false
SSDEEP:	
MD5:	FADB0F250D20EF2F614C4AB5D5D3AB0F
SHA1:	41E8255C91A40A8E832A8AC05747C9A579F55D07
SHA-256:	2CD73F11DA515955B62A930CA4DEFDE9CCB5230B8F5809E3C304EF854604EDA3
SHA-512:	E97F4B069ACB91C332BDACA5C4314CBE6CC79C37E93CBB3F4D8B37544B49C2868E23B603FE4563A8961616F137CF646153A82F387D9C55CF8191108E86CF136
Malicious:	false
Preview:	-- ____ _...-\ \ __ V__ __ . \ \ / _ _ _\ \. .` __ ___\ \\.. \ / /\ /_/_\ ^ ^____^_____/...By now it's probably painfully apparent that your environment has..been infected with ransomware. You can thank Conti for that.....We've modified the code in a way that will prevent you from decrypting..it with their decryptor.....We've exfiltrated a significant amount of data including private emails,..financial information, contacts, etc.....Now, if you wish to contact us in order to save your files from permanent..encryption you can do so by emailing network_battalion_0065@riseup.net.....You have 3 days to establish contact. Failing to do so will result in..that data remaining permanently encrypted.....While we have very little sympathy for the situation you find yourselves..in right now, we will honor our agreement to restore your files across..the affected environment once contact is established and payment is made

C:\MSOCache\All Users\{90160000-00A1-0409-0000-00000000FF1CE}-C\Setup.xml	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	2709

Entropy (8bit):	7.923958505514895
Encrypted:	false
SSDEEP:	
MD5:	21EC158FF4B21C5C47C58ACE0C54B0DB
SHA1:	3A67055C625D231EAADCA53D30DE635D88CBC9C2
SHA-256:	A5C412FF54D60A0D3C45804C8A281B221CC7A8F0A792A16C35D758808FB22D9C
SHA-512:	7F447D9818505E113AD92C2A2276FD6DBF25B27DE8316BBBD14CF7EFCDA22CA74EB1462B1336D95BB38669584677C5D4F7C96A740EE98B7D3C7AA7EB229EE9F1F
Malicious:	false
Preview:	D...w....+.]D..F.....X..v..o.....nk.w...#. {...S.....4.A.....S.{>...l..7...1.u.i...b#q.%...-.....W{<....C....Z.v.zi....@...e...u.....F.C.m.q.J./.....m....W..Q..6...<\$....L....".s.*. .u.B.....w.9...-q..j.Q.J.D_...>.,K.....i].T.-~:C.7.)...1a./&.[>j....f6..h.(. {.F._'z'...&e.M.YS.W.r.z.B..s.b.....E....j~j.....'k.f..._ \l.C.zm....T"7.X.L1.&.:6mU.;...5/=z.O.n..6O].t._e.oBQ.l&b...9...ae....Uu...{...P(.7Q...f.9.....yh..8.M.....31)...L.ai..F1.u^....7.p..8.+^.....%K.,G`...?%D.9.w:....v#.%P.`).mw.+`~.7.-.l.U.]...l.F..L.J.%j.fM.H....P&.@.n. *~<....<.n.+.[W.Y]...r.#....%t<....Q..G.L.Tc^]e....0.v.o.^f=...g.5...Q.....6..X.Mp.u...@!cn.@J...1.ytL\...Bf..gY.7.....2{.R.*.p..T.4Had..5(^.4.....5.F.].F.9....@..C.y.an fB...&t.Yi..8... :X3..q.....3...ym.....dG<...ze.....0.ws~..Qu.....<..Ki..W.BA_';Z.?.Gv..+.%..w..E...Lc.p.Z....g.%..?S(>....%...4..)]...(\....,

C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\Setup.xml.NB65 (copy)	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	2709
Entropy (8bit):	7.923958505514895
Encrypted:	false
SSDEEP:	
MD5:	21EC158FF4B21C5C47C58ACE0C54B0DB
SHA1:	3A67055C625D231EAADCA53D30DE635D88CBC9C2
SHA-256:	A5C412FF54D60A0D3C45804C8A281B221CC7A8F0A792A16C35D758808FB22D9C
SHA-512:	7F447D9818505E113AD92C2A2276FD6DBF25B27DE8316BBBD14CF7EFCDA22CA74EB1462B1336D95BB38669584677C5D4F7C96A740EE98B7D3C7AA7EB229EE9F1F
Malicious:	false
Preview:	D...w....+.]D..F.....X..v..o.....nk.w...#. {...S.....4.A.....S.{>...l..7...1.u.i...b#q.%...-.....W{<....C....Z.v.zi....@...e...u.....F.C.m.q.J./.....m....W..Q..6...<\$....L....".s.*. .u.B.....w.9...-q..j.Q.J.D_...>.,K.....i].T.-~:C.7.)...1a./&.[>j....f6..h.(. {.F._'z'...&e.M.YS.W.r.z.B..s.b.....E....j~j.....'k.f..._ \l.C.zm....T"7.X.L1.&.:6mU.;...5/=z.O.n..6O].t._e.oBQ.l&b...9...ae....Uu...{...P(.7Q...f.9.....yh..8.M.....31)...L.ai..F1.u^....7.p..8.+^.....%K.,G`...?%D.9.w:....v#.%P.`).mw.+`~.7.-.l.U.]...l.F..L.J.%j.fM.H....P&.@.n. *~<....<.n.+.[W.Y]...r.#....%t<....Q..G.L.Tc^]e....0.v.o.^f=...g.5...Q.....6..X.Mp.u...@!cn.@J...1.ytL\...Bf..gY.7.....2{.R.*.p..T.4Had..5(^.4.....5.F.].F.9....@..C.y.an fB...&t.Yi..8... :X3..q.....3...ym.....dG<...ze.....0.ws~..Qu.....<..Ki..W.BA_';Z.?.Gv..+.%..w..E...Lc.p.Z....g.%..?S(>....%...4..)]...(\....,

C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveLR.cab  	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	873496
Entropy (8bit):	7.999794902917263
Encrypted:	true
SSDEEP:	
MD5:	CD9A000352F8A3162F1F3D7F82103B22
SHA1:	E35FFE7C4C784FD009C349C296698423F3476674
SHA-256:	117F2CF2F4D50E1B1E730A9A8F066A681227D4BC7273ED668D1A2C03E608C0BE
SHA-512:	AFC03EBD3287452CE16130B8B6493B659FBC4654404E85FF59F2A0C808F5180BF6B660CDC3BEE5CE90DC3EB422C7C89EF475972316D50B8E74FFA9C5BAB54B67
Malicious:	true
Preview:	P..q...E...w%.A...^..s*...n].kw>.1W5...4...S6..G...7'[...]leo.*\$.i..}7...yae..K.l<.w..Z...F#.....F.!4.@.@D.....\$9...r.p?...].....Lfr.m....EVA.3.6.`6...~...a.S.or.A...T.. ..oJ.b.S.kld..k.....hV..P. l.e.t...]q(h...))...=m..D.....D.ZZ1H")\..u.....8Z.<=&..FFI{.....9..W.7 ?8.7.J\IOM.....).H....9... \S1.E.....nd...m..F...l...y.R.m....E.4K...o.4.....cA.... MA.[. ?ld..?.&.(v>.L.b...*R.r'.4}.w..#M`Y`v..K....}.4.<s.M.*...HT...q.;X..E..\$.K...Q.%o\n..~.."s).r.c..(&..r...7RS_\$.d.[D2.a.:J#q.umF.U.5...Ys...cp. [-~.(3..... ?R.....2....)b.C~e..")&.... oR....b..uF\..:..m.....&..~s..H.z.6J...8.a>.\8.*Kn..\$X.5.=.o.P.....gY..A#^.....LG.f.K...i/...6..G1.....,7....:L..&+j...CBC.....~u.Ct...L...L 3.B.p....XR...z%.y..C...3....2.V,'*~N.t.\$n..D*nYJ>...JH...y...ft.E9}...2\...@..`qu.....&#b.1m.%S...c.k...>b}.u.....b.....?!\N.N.....P..7...VD

C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveLR.cab.NB65 (copy)  	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	873496
Entropy (8bit):	7.999794902917263
Encrypted:	true
SSDEEP:	

MD5:	CD9A000352F8A3162F1F3D7F82103B22
SHA1:	E35FFE7C4C784FD009C349C296698423F3476674
SHA-256:	117F2CF2F4D50E1B1E730A9A8F066A681227D4BC7273ED668D1A2C03E608C0BE
SHA-512:	AFC03EBD328745C2E16130B8B6493B659FBC4654404E85FF59F2A0C808F5180BF6B660CDC3BEE5CE90DC3EB422C7C89EF475972316D50B8E74FFA9C5BAB54B67
Malicious:	true
Preview:	P..q....E...w%.A....^..s*.n[.kw>.1W5...4....S6..G...7'.[...leo.*\$.i..}7...yae..K.l.<w..Z...F#.....F.!4.@.@D.....\$9...r.p?..[.....Lfr.m....EVA.3.6.`6....~...a..S.or.A...T... ...o.j.b.S.k.l.d..k.....hV..P..I.e..t...j]q(h...))....=m..D.....D.ZZ1H")\..u.....8Z<=&..FFI{.....9..W.7`?8.7..J.\OM.....).H....9...\.S1.E.....nd...m..F...l...y.R.m....E.4K...o.4.....cA.... MA.[.?.?ld..?.&.(v>.L.b...*.R.r'.4].w..#M`Y"v..K.....).4.<s.M.*...HT....q.;X...E..\$.K..}Q.%o\n..~"..s).r..c...(&.r...7RS...\$.d.[D2.a.:J#..q..umF.U.5...Ys....cp.[~..(3..... ?.R.....2....)b.C~..e.."]&....oR....b..uF.\..:m.....&..~s..H.z.6J...8.a>.\8.*Kn..\$X.5..=.o.P.....gY..A#^.....LG.f.K...i/.6..G1.....7....:L..&+j...CBc.....~u.Ct...L...L 3.B..p....XR..z%.y..C...3....2.V..'*~N.t.\$n..D*nYJ>....]H....y...f.t.E9.}...2\....@..`.qu.....&#b.1m.%S...c.k...>b.}u.....b.....?!N.N_.....P..7...VD

C:\MSOCache\All Users\{90160000-00BA-0409-0000-00000000FF1CE}-C\GrooveMUI.xml	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	1660
Entropy (8bit):	7.8686410396141095
Encrypted:	false
SSDEEP:	
MD5:	FFB63AFA8B56FB40483F76608306C0CE
SHA1:	C000AC8898001138D6B9BFE51FD1440C7023F2EF
SHA-256:	64AA93B3CFAEEADDBE4A1B007650FEAC9DDE3B1AB1736EB9D9C1F00914C0873D
SHA-512:	538A8C590688E87B8AE61096436D1D92193F416E762AECB3D0D22E9555C279A979B3901BF29A15B6C79F1F39F6096677976C442CEB54FEE34F9D9568D155AF1F
Malicious:	false
Preview:	..s.....}.t;!.%P.....y).?.....&.88ad)4r.u.gmJ... "p.(U`X.r.....j0....Hq*..`....t9.../.....l.....+i.....A..O..D....A....Lx..W.....r.mj%.";=...}.X_N.v../.l...O..r.H.J;..V4.1.2.....u.....:.....G .Qk-..b.SZ.D9L.U..c.I7^z.z.....4..5y.....2L.K...2.u...dcn.z.'4A..5....A.{..`B...[....@was.Ok.....f.....+D.*r...Q..5..V.3....uoE..y.w.. 9 ..x...a2L...1...a.A.M`.....x.>.....% H.>..%.hV.4....du.....`"...f&t..B...F..Ll..A..LU.J.`k4mK.....[i.....%h...{w0H2^cK3.%B...V.F...S.3....o%G...v...cC..y....]&..OJ..1.o..{M./bL`!h.L['.}.#..#^...l...}W..9. ..r.^i.....RP.....'B.g.....f...m..a...^S...Y..3y4^.....[Q..'.l.P.....s....]X.Q...N.U.}'.....a.....K[b.\$!..T..6h...D3:f.#.S.....O..D8..q:...K.l....<.....!ly*%)D..l...g{T<...h.../..`{..aG i ...""E.cp....UiH.....&A[...&F..T..4..l..L.oa3}...hl.&.{.....H..TM...[R....A..l.R.X.....l.NPG....V]..K.QD...y`u.....)b...?V ..l.'!f.

C:\MSOCache\All Users\{90160000-00BA-0409-0000-00000000FF1CE}-C\GrooveMUI.xml.NB65 (copy)	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	1660
Entropy (8bit):	7.8686410396141095
Encrypted:	false
SSDEEP:	
MD5:	FFB63AFA8B56FB40483F76608306C0CE
SHA1:	C000AC8898001138D6B9BFE51FD1440C7023F2EF
SHA-256:	64AA93B3CFAEEADDBE4A1B007650FEAC9DDE3B1AB1736EB9D9C1F00914C0873D
SHA-512:	538A8C590688E87B8AE61096436D1D92193F416E762AECB3D0D22E9555C279A979B3901BF29A15B6C79F1F39F6096677976C442CEB54FEE34F9D9568D155AF1F
Malicious:	false
Preview:	..s.....}.t;!.%P.....y).?.....&.88ad)4r.u.gmJ... "p.(U`X.r.....j0....Hq*..`....t9.../.....l.....+i.....A..O..D....A....Lx..W.....r.mj%.";=...}.X_N.v../.l...O..r.H.J;..V4.1.2.....u.....:.....G .Qk-..b.SZ.D9L.U..c.I7^z.z.....4..5y.....2L.K...2.u...dcn.z.'4A..5....A.{..`B...[....@was.Ok.....f.....+D.*r...Q..5..V.3....uoE..y.w.. 9 ..x...a2L...1...a.A.M`.....x.>.....% H.>..%.hV.4....du.....`"...f&t..B...F..Ll..A..LU.J.`k4mK.....[i.....%h...{w0H2^cK3.%B...V.F...S.3....o%G...v...cC..y....]&..OJ..1.o..{M./bL`!h.L['.}.#..#^...l...}W..9. ..r.^i.....RP.....'B.g.....f...m..a...^S...Y..3y4^.....[Q..'.l.P.....s....]X.Q...N.U.}'.....a.....K[b.\$!..T..6h...D3:f.#.S.....O..D8..q:...K.l....<.....!ly*%)D..l...g{T<...h.../..`{..aG i ...""E.cp....UiH.....&A[...&F..T..4..l..L.oa3}...hl.&.{.....H..TM...[R....A..l.R.X.....l.NPG....V]..K.QD...y`u.....)b...?V ..l.'!f.

C:\MSOCache\All Users\{90160000-00BA-0409-0000-00000000FF1CE}-C\R3ADM3.txt	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	1290
Entropy (8bit):	4.607071403570347
Encrypted:	false
SSDEEP:	
MD5:	FADB0F250D20EF2F614C4AB5D5D3AB0F
SHA1:	41E8255C91A40A8E832A8AC05747C9A579F55D07
SHA-256:	2CD73F11DA515955B62A930CA4DEFDE9CCB5230B8F5809E3C304EF854604EDA3
SHA-512:	E97F4B069ACB91C332BDDCA5C4314CBE6CC79C37E93CBB3F4D8B37544B49C2868E23B603FE4563A8961616F137CF646153A82F387D9C35CF8191108E86CF136
Malicious:	false

Preview:	O.F5w..<...8.l...(@!'.....Flu6.;jL.....B.;6w ..a....F+....C.....%V..E.SQ^.....9..x ..;.:[:4.d.9....05Z]..7Zi....0.....q...N2...f_...*....13..S..B.X+.'vy..iX<+..`....j.1....YU.....;..R.O ...C..3.2G..5.....9.C?'..v8..2y..>W.X\$....._...L..*N..p?.%l `o(....rZ..Kr4R.pPz].....-...dd.Qm.q.Z../n.U....M&h."...U.c.A!..`T.....D.i...dmRGM`....).lu+.[.6.Y.'d.nn & ..vMO+..Ql'!...!A.....e...Am.yl.GUM.v.&...!P..j!`.....<...K.6t.vd2.B..\..EZ.8..Wp.\$.5# .p.....!..._O'ux.C.lw....`y0A..Xc.b'l<....d.1.m.M....Z.\%...0v..m.i.....U&K ..R =.....Ui".....U`.3.....].[-D~..5CF{.U..".\$.!..g....ZS*+;d(H@...F.....](l~T.{.W...lg..4tQ%z)....T.}.P.....%a....S...p.."..v.*.V(nwd...n.>9:R#.L..p..f[{.....sl...lY4....._jo. [/....7".CX\$.Qq...G.O.....D.....1L..O..fs ..P..a.j....5.j.Uk?..3C.'J.- .\$.!....K0...TsnNP.g(.hJ.B~xi..Y..?.....\$.....x.[./..\$.u".p..j.@...w.(-/)...E.....4.....
----------	---

C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.cab.NB65 (copy)	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	17347
Entropy (8bit):	7.988558992209177
Encrypted:	false
SSDEEP:	
MD5:	ADA0A2ECD73B386805EC9773EF6E825F
SHA1:	C1B2D627064E7976A247C3F57BE65F8DE2C847EB
SHA-256:	CEBFCAB1CBAA09708515A3887CAC6E8B7D41BDFC0CDAF8A58A32AE53C9890EC5
SHA-512:	24C907E8027333EBDD44A59E6175B543C8B1CB5CD103A545E4ED38F4C55490D1FE6ABF990A043B99BEEC201B0B3E2DE9058A0D45DA34EF057AC0315D0051C53A
Malicious:	false
Preview:	O.F5w..<...8.l...(@!'.....Flu6.;jL.....B.;6w ..a....F+....C.....%V..E.SQ^.....9..x ..;.:[:4.d.9....05Z]..7Zi....0.....q...N2...f_...*....13..S..B.X+.'vy..iX<+..`....j.1....YU.....;..R.O ...C..3.2G..5.....9.C?'..v8..2y..>W.X\$....._...L..*N..p?.%l `o(....rZ..Kr4R.pPz].....-...dd.Qm.q.Z../n.U....M&h."...U.c.A!..`T.....D.i...dmRGM`....).lu+.[.6.Y.'d.nn & ..vMO+..Ql'!...!A.....e...Am.yl.GUM.v.&...!P..j!`.....<...K.6t.vd2.B..\..EZ.8..Wp.\$.5# .p.....!..._O'ux.C.lw....`y0A..Xc.b'l<....d.1.m.M....Z.\%...0v..m.i.....U&K ..R =.....Ui".....U`.3.....].[-D~..5CF{.U..".\$.!..g....ZS*+;d(H@...F.....](l~T.{.W...lg..4tQ%z)....T.}.P.....%a....S...p.."..v.*.V(nwd...n.>9:R#.L..p..f[{.....sl...lY4....._jo. [/....7".CX\$.Qq...G.O.....D.....1L..O..fs ..P..a.j....5.j.Uk?..3C.'J.- .\$.!....K0...TsnNP.g(.hJ.B~xi..Y..?.....\$.....x.[./..\$.u".p..j.@...w.(-/)...E.....4.....

C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.xml	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	1657
Entropy (8bit):	7.879862466180648
Encrypted:	false
SSDEEP:	
MD5:	B3544BBA02865C2FC03EBE0447A17318
SHA1:	41E36F4D79FFFE33740495D23BDF4A47DAAF8E7F
SHA-256:	FA50CA5681334F56BAB447FCA50745C5A22044275F79997956FD56E4130F99E1
SHA-512:	326E91F3577BB134DA763B6B59DA6D98B776EE55DAECBD748E91D76C028202DC473826FF77BE1A6B16919031669141B8DD5311A9E029AE2074FAD9EBD4E3E2E
Malicious:	false
Preview:	...ut...@..."P...w..v.2]"~v..O..y....Cx-V..i@.S...r.zV..%.W..l.;...L.J..L...>..W.8}ZPkO.6N'.....Op;E.....j.i=ox`4.(.SQ.\$o..`2KK.3..r...z.yA0.p.]-2^?..2.....d....+M...F...j.y..... u..o....0E"P.dY*.uj.... j\..X...^..i.....4.....}.H.....Z.AD0N.....G...U...[mw.d.nH..wk.5"....%....._...l..39.&s.....;s.wz.{.....Z...";P..j.}....3..#..>.....R\$.o\$.l...- ..s#WC..Y.....@....cl....{....t.....hr9^..h}b.D{.....7....j..\...~).U.C2.bg.....+...ri...9.v...+....V.j.BP.w.m.\Gt.....!pgS.....6..._Jnk:...V~...1h"}...f...E....ob.wL. !?.[e...^R.3.kd#...2...pV..S.#.p.Jl.w5.b<..^p.q..W #...?....m..C.7:nu!(....z.(...Z...re:q)P..p...q..Gl...1.. "f..~....4bZ6A.o(F.5s!8Z...\$.2...[1DE0.E..P.T....).d....9.%.....E. ..q..... q<..DM.L+M....r.S.+G.Ql!...!& p.....U.....C.p.....w.6.....7..krr.j.lw....q:..]&7.-~v..2.....7.]k.f.&(gk\.....D....@ S..r....0.`q.Y.....

C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.xml.NB65 (copy)	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	1657
Entropy (8bit):	7.879862466180648
Encrypted:	false
SSDEEP:	
MD5:	B3544BBA02865C2FC03EBE0447A17318
SHA1:	41E36F4D79FFFE33740495D23BDF4A47DAAF8E7F
SHA-256:	FA50CA5681334F56BAB447FCA50745C5A22044275F79997956FD56E4130F99E1
SHA-512:	326E91F3577BB134DA763B6B59DA6D98B776EE55DAECBD748E91D76C028202DC473826FF77BE1A6B16919031669141B8DD5311A9E029AE2074FAD9EBD4E3E2E
Malicious:	false
Preview:	...ut...@..."P...w..v.2]"~v..O..y....Cx-V..i@.S...r.zV..%.W..l.;...L.J..L...>..W.8}ZPkO.6N'.....Op;E.....j.i=ox`4.(.SQ.\$o..`2KK.3..r...z.yA0.p.]-2^?..2.....d....+M...F...j.y..... u..o....0E"P.dY*.uj.... j\..X...^..i.....4.....}.H.....Z.AD0N.....G...U...[mw.d.nH..wk.5"....%....._...l..39.&s.....;s.wz.{.....Z...";P..j.}....3..#..>.....R\$.o\$.l...- ..s#WC..Y.....@....cl....{....t.....hr9^..h}b.D{.....7....j..\...~).U.C2.bg.....+...ri...9.v...+....V.j.BP.w.m.\Gt.....!pgS.....6..._Jnk:...V~...1h"}...f...E....ob.wL. !?.[e...^R.3.kd#...2...pV..S.#.p.Jl.w5.b<..^p.q..W #...?....m..C.7:nu!(....z.(...Z...re:q)P..p...q..Gl...1.. "f..~....4bZ6A.o(F.5s!8Z...\$.2...[1DE0.E..P.T....).d....9.%.....E. ..q..... q<..DM.L+M....r.S.+G.Ql!...!& p.....U.....C.p.....w.6.....7..krr.j.lw....q:..]&7.-~v..2.....7.]k.f.&(gk\.....D....@ S..r....0.`q.Y.....

File Type:	data
Category:	dropped
Size (bytes):	4231235
Entropy (8bit):	7.999826754548407
Encrypted:	true
SSDEEP:	
MD5:	BAA0593644D9F2A5746EAFACAC919F3B9
SHA1:	B84BCF58384435EA963AE31932FD6B138A16E6DF
SHA-256:	D4E00263910AAB588871DA9F5CB186F73FD1B4C1B0FD782A81C1C90583B09BBA
SHA-512:	54EDA0111B6496B53ED613BE5A8A60EA64374BE00F764512ED182067C595208922F34942D7106DBDB6BEF4E4CBC0122D04C4CC29E6D1E7D970FDC3284E277563
Malicious:	true
Preview:	.JMG=.....pJ.,*....uH...p.f3C...[h.....e...wE.NY=~.F.:A...~.oEu7...K...(-...m4.....u.4.y..X.2.4.....B.M@w.5..2.#W~...@.pF...>.7.<.G..S..\$.y.{.8..~.m..5.IC.....m.w....f.w.....{c..l....}.o.&.....'.l...+.n...E..c....i...O/-..p..{S....S/..:E.....}GC...q...w].....<.....?..p.i.O..w..M.g..cAn.X[.L...<.0Fr7.j+E../L..g....nU..J=0.c4....P....W...:..@{.L..R.G...e.l...~hc...k{.}'...!-5..P...(D{.j6....}.A&+c.2R.f.b+yQ.....j\.:@.....6.%i.Z.7.c...b.l.7.X]...YAN.....[L...A/'J..yp'.A..fl.9e5CU.L...!7.L..A@.W'.G.o.`.@<.../'.....Y..l.+6...@.J.#..V.....{...#.D..%Y)...\$.!..Uly..c..g...\.\\..1S..}...0.`a...y.H..pX....n..G..j\$.h...\\..NY..d.9.t\.....F...Q...&[...p.]...f>...{.....}.....k..lS.....PH3.O.%...Y..v.<..gQKS..KUzQ_-'.....<.....C..v...n<.l.l...9=...F..c..DM4..d..6.CNN.....5."..\\C&h...Z.....{...c...[...A?....{...{E.V..b.(D.....wj...y..w].0.W....1.>.\$k...lc..2.

C:\MSOCache\All Users\{90160000-00E2-0409-0000-00000000FF1CE}-C\OSMUXMUI.cab.NB65 (copy)  	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	4231235
Entropy (8bit):	7.999826754548407
Encrypted:	true
SSDEEP:	
MD5:	BAA0593644D9F2A5746EAFACAC919F3B9
SHA1:	B84BCF58384435EA963AE31932FD6B138A16E6DF
SHA-256:	D4E00263910AAB588871DA9F5CB186F73FD1B4C1B0FD782A81C1C90583B09BBA
SHA-512:	54EDA0111B6496B53ED613BE5A8A60EA64374BE00F764512ED182067C595208922F34942D7106DBDB6BEF4E4CBC0122D04C4CC29E6D1E7D970FDC3284E277563
Malicious:	true
Preview:	.JMG=.....pJ.,*....uH...p.f3C...[h.....e...wE.NY=~.F.:A...~.oEu7...K...(-...m4.....u.4.y..X.2.4.....B.M@w.5..2.#W~...@.pF...>.7.<.G..S..\$.y.{.8..~.m..5.IC.....m.w....f.w.....{c..l....}.o.&.....'.l...+.n...E..c....i...O/-..p..{S....S/..:E.....}GC...q...w].....<.....?..p.i.O..w..M.g..cAn.X[.L...<.0Fr7.j+E../L..g....nU..J=0.c4....P....W...:..@{.L..R.G...e.l...~hc...k{.}'...!-5..P...(D{.j6....}.A&+c.2R.f.b+yQ.....j\.:@.....6.%i.Z.7.c...b.l.7.X]...YAN.....[L...A/'J..yp'.A..fl.9e5CU.L...!7.L..A@.W'.G.o.`.@<.../'.....Y..l.+6...@.J.#..V.....{...#.D..%Y)...\$.!..Uly..c..g...\.\\..1S..}...0.`a...y.H..pX....n..G..j\$.h...\\..NY..d.9.t\.....F...Q...&[...p.]...f>...{.....}.....k..lS.....PH3.O.%...Y..v.<..gQKS..KUzQ_-'.....<.....C..v...n<.l.l...9=...F..c..DM4..d..6.CNN.....5."..\\C&h...Z.....{...c...[...A?....{...{E.V..b.(D.....wj...y..w].0.W....1.>.\$k...lc..2.

C:\MSOCache\All Users\{90160000-00E2-0409-0000-00000000FF1CE}-C\OSMUXMUI.xml	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	1992
Entropy (8bit):	7.888862886515418
Encrypted:	false
SSDEEP:	
MD5:	9E4252BD25F91499994D1904828C490C
SHA1:	5817121A5D3AAD3B2E96634A23D32A6C51371E1C
SHA-256:	5D13C705856CE830879881366BA5076BAEC5795BD1102ECCF19B8EBF490D8A29
SHA-512:	82731F3BC317006147FCC89916B70B0A884AE757CDAA5B14F46AA600602D32FE474964CFF40B25710533BCE8C5FBBE4B97A6030CEF1E3007B87CD3CF658BC8CE
Malicious:	false
Preview:	>.E..(?..~.W..OX...K...-.....W.u.....x.7.R..K{q....U.....E...;~...p?.T.U.t.f'y....z.L...dTl]-w.....G..P.3.2de..m..g<L...B&\...wo....N.l.j.].....wL...V.M*.u.6.f4@.....l?la;.....<.2.-.H'\$..^R.K*Q.....#....X....8(M"=.R.Y.;Vw.....B..2....k'.).tT".....T.jj?J..F.[...X.@...e..oG;p.4.'O..f.F"'.~.jH.e....3.J..\$.e....e....U.....p.....%[FH>9.....*y>N..8...rTf{G[.R.iOK../.....[Y..s].....u.o.o..b....u.....1..wi.K.V.'.jQm\...h)..xFZsM.Z9T..V..lW.M-.....g....z&=(...k.j.j.fG...Lv.P.Z.M.f.9.....-.....s.....;Kb..M.A#..t.>.E....X'..e...+s..98..+A(.T9HWb@%V'.X...P>..u;O V.o...y..f.\.V..6.Z...L..i@.)u..j..b?././jj.3].jJ.v#j....[{:..y.lv.M..7.....}.~...['.Hl..xTn1P_?..-\..9.Y..").}...o..~dlK.sn.....s?..u.A...;...j*..VH0..05.[.....9-C....._Y.....".....AdS.....L.....qhA...+...]..8.W..P..q...y..Z.....r.C....p.@...b/..M.;...3#A.F\..9o.....

C:\MSOCache\All Users\{90160000-00E2-0409-0000-00000000FF1CE}-C\OSMUXMUI.xml.NB65 (copy)	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	1992

MD5:	F2694EF4F98F2ADE49723A8E2EE43307
SHA1:	A0464DD3A1984C41BE74469245A4DF03AEC77EEC
SHA-256:	A5E6C237F1CB48CC574F7F20359CEF9F7068FD1DA9361E4E44A412E7520D6969
SHA-512:	D8405866235D062F448E7D42A96F68A9E5C37B03EA3E6F5B84A1AA0B29CBB5390F3B9F08A180ED96A69DA6E12CF7597A6EDB7AEA6E5D64DE5DE94D4934EBDD2
Malicious:	false
Preview:	..E...v.P.s.9...ts.... D....AjE3..v...-x/....p..g....H.O\p.QH.I....rr[,e....9H...p...u.V... ..K.. As...8"... :1{.....@...-A.?.)/.*q.a.. R Y\, ["<...^..W52.b.M...@...p.WR...=..~< .sU,(.j5Ws...S.....DeL.....i..x... ...Nwhqd...\$.QaA.....e.O<p/...YE..f7...Y...rE...=9./D.)e\$.V[.*...<z...]!PRt.q.....(....yS...e..0.....~b..3./VG.....U\$....?. p..mp}...7... oV.W<.T.V....\$.O.1.QNC:!.m.....{.f.....S...Nl..p{.6...?.T}P....=[.g.l0...t5.]s.A.-n.....V_n~.lu.....*<X..r%...X.'j9.....J+...ww..y..L..Qg.R..7\$8ESb.....0..H.b..y.h.pw..E\3/...-.Q.M....p..DD.....3x,q . .Bi.=rO...S.....?bN.t.0.....D; t[.].@..!.....ji< n.Y&...x\$.....\,2.?.h..1T..}v.Gh1.D[M.?r;.....i....Gr..pNh.N.'....b.u2..^.....'.WJ.f....E.(.k.'.....d.5b..aKo(./)%}Jj[.....*N...}.\$.N...@.S.o.P..A..i{+...Hg...~q..U... SX.....&...r..G.o}5.8.'i5.(4.b.H....u/....+.H4W..j..9.....M!oD.A/A'.p.(.83x%5.3x'....

C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OffSetLR.cab	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	16242
Entropy (8bit):	7.98948678203108
Encrypted:	false
SSDEEP:	
MD5:	36317E63FD21D02B92EA4FBF730AECAD
SHA1:	2DD39C3BF2EE546D5DC6829D1B497E03853D4EEE
SHA-256:	8C6DC6F82CBA977A24C1BE5D694E5DCC91F45A4074991B0FDC38746506B4EB16
SHA-512:	7136B6D9F7ECFFD5508A3FD544DF85B0416798867CFBE69DD9747552145633DCA1C170CDD0EBEDD7B857F4ACFE1650DF6EC0F19E5C512DCA98B8278E009535C1
Malicious:	false
Preview:	^m.J...0-I.KY.Z.%.....T...~..pD.L.m.9..0}.AvAt..Kj'..{.....d...q.n.\$...-.. '..g3.l.5.tq...D\...r\$.KN!R.S..w.y....ftZ...ku.yl.i...T...N...-GU?.in...R.K.....P.x9.QXB.x3.....3.....<.Y.....[.W.j.XIMWA{.fzf.6...G&>...KL`U..z..9..3.s...r.C...k.l..K">.n...Y;..N+....~sF(B....Cv..t..R....`.....c..f.F*V0.r:mG.l....*.h!....9.....j@.Nn...<...'.a.d..J..5...B.2....[...&.....X...w.....<.V.HiB.@...?.].M_..h..D.....}.?.C.M..A....}.rg...rZra.....c.k.*PK.N7S#.Z=..ks..7[1...s2u....[.& .e..... .W4..W....R..o.E...!.....?.....*{x.lj.Q*.o.B.Gl...[.y]i.."d\...#.9.....9.p /R.p..r..4..oj.gN.....*X...R.....dq..r}.*S.l.k..[a.+AEF..YG=..vzN..?.....H..1E;.7.>...=h5.L...4.*.V1...._z..#1T..b/.i{.iF{.Ba...Q.7...4..%-~.?./j\$.~0.^F:.....3..\$.m([...].%....v.....S.).~".B.8tR,...Z.sZT.\$...&.d.e.. U.Y.....h.n_bbVLT..0V..F.<.Sk...yU'....d...@..@.....].>.....s.....<.90.l.MJ..F...ns

C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OffSetLR.cab.NB65 (copy)	
Process:	C:\Users\user\Desktop\ll.exe
File Type:	data
Category:	dropped
Size (bytes):	16242
Entropy (8bit):	7.98948678203108
Encrypted:	false
SSDEEP:	
MD5:	36317E63FD21D02B92EA4FBF730AECAD
SHA1:	2DD39C3BF2EE546D5DC6829D1B497E03853D4EEE
SHA-256:	8C6DC6F82CBA977A24C1BE5D694E5DCC91F45A4074991B0FDC38746506B4EB16
SHA-512:	7136B6D9F7ECFFD5508A3FD544DF85B0416798867CFBE69DD9747552145633DCA1C170CDD0EBEDD7B857F4ACFE1650DF6EC0F19E5C512DCA98B8278E009535C1
Malicious:	false
Preview:	^m.J...0-I.KY.Z.%.....T...~..pD.L.m.9..0}.AvAt..Kj'..{.....d...q.n.\$...-.. '..g3.l.5.tq...D\...r\$.KN!R.S..w.y....ftZ...ku.yl.i...T...N...-GU?.in...R.K.....P.x9.QXB.x3.....3.....<.Y.....[.W.j.XIMWA{.fzf.6...G&>...KL`U..z..9..3.s...r.C...k.l..K">.n...Y;..N+....~sF(B....Cv..t..R....`.....c..f.F*V0.r:mG.l....*.h!....9.....j@.Nn...<...'.a.d..J..5...B.2....[...&.....X...w.....<.V.HiB.@...?.].M_..h..D.....}.?.C.M..A....}.rg...rZra.....c.k.*PK.N7S#.Z=..ks..7[1...s2u....[.& .e..... .W4..W....R..o.E...!.....?.....*{x.lj.Q*.o.B.Gl...[.y]i.."d\...#.9.....9.p /R.p..r..4..oj.gN.....*X...R.....dq..r}.*S.l.k..[a.+AEF..YG=..vzN..?.....H..1E;.7.>...=h5.L...4.*.V1...._z..#1T..b/.i{.iF{.Ba...Q.7...4..%-~.?./j\$.~0.^F:.....3..\$.m([...].%....v.....S.).~".B.8tR,...Z.sZT.\$...&.d.e.. U.Y.....h.n_bbVLT..0V..F.<.Sk...yU'....d...@..@.....].>.....s.....<.90.l.MJ..F...ns

Static File Info	
General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.457201413540288
TrID:	- Win32 Executable (generic) a (10002005/4) 99.96% - Generic Win/DOS Executable (2004/3) 0.02% - DOS Executable Generic (2002/1) 0.02% - Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	ll.exe

File size:	179712
MD5:	f746ea39c0c5ff9d0a1f2d250170ad80
SHA1:	dac28369f5a4436b2556f9b4f875e78d5c233edb
SHA256:	7f6dbd9fa0cb7ba2487464c824b6d7e16ace9d4cd15e4452df4c9a9fd6bd1907
SHA512:	dffb4eaa4119df790eb6b85ae341ee2ba4438d7983d0023320f19a4f2df201a3fc3d4d3cc4f1a67c6d1cad4809ac1b914bdad584da7df1b500354386f07fbc30
SSDEEP:	3072:QQKp8PavONh7mJ1XGK68AL8BBW8MpYZEmn4klVw5tBdGuUjuXssPMSwxFCyyNZR:B+DmTfk68AKW8uYHBZ5Qeshd0m/Y
TLSH:	B0045B05B20E5379F16B687426E9697256A8EC34539F88FBB7C28B5415309E23230FB7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode...\$......g...g.....g.....g.....g.....g...f...g...d...g...c...g...b...g.?..n...g.:.....g.?..e...g.Rich..g.....

File Icon	
	
Icon Hash:	00828e8e8686b000

Static PE Info	
General	
Entrypoint:	0x417efe
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6247EB6E [Sat Apr 2 06:21:34 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	f5346a7d2508fd5976d3449f3afc971d

Entrypoint Preview
Instruction
call 00007F90051AABAFh
jmp 00007F90051AA713h
push ebp
mov ebp, esp
test byte ptr [ebp+08h], 00000001h
push esi
mov esi, ecx
mov dword ptr [esi], 004241ECh
je 00007F90051AA88Ch
push 0000000Ch
push esi
call 00007F90051AA62Dh
pop ecx
pop ecx
mov eax, esi
pop esi
pop ebp
retn 0004h
push ebp
mov ebp, esp
push esi

Instruction
push dword ptr [ebp+08h]
mov esi, ecx
call 00007F90051AA27Ah
mov dword ptr [esi], 004241F4h
mov eax, esi
pop esi
pop ebp
retn 0004h
and dword ptr [ecx+04h], 00000000h
mov eax, ecx
and dword ptr [ecx+08h], 00000000h
mov dword ptr [ecx+04h], 004241FCh
mov dword ptr [ecx], 004241F4h
ret
push ebp
mov ebp, esp
push esi
mov esi, ecx
lea eax, dword ptr [esi+04h]
mov dword ptr [esi], 00424184h
push eax
call 00007F90051AB649h
test byte ptr [ebp+08h], 00000001h
pop ecx
je 00007F90051AA88Ch
push 0000000Ch
push esi
call 00007F90051AA5CDh
pop ecx
pop ecx
mov eax, esi
pop esi
pop ebp
retn 0004h
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007F90051AA202h
push 00429374h
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007F90051AB634h
int3
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007F90051AA815h
push 0042947Ch
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007F90051AB617h
int3

Rich Headers	
Programming Language:	• [RES] VS2015 UPD3 build 24213 • [LNK] VS2015 UPD3.1 build 24215 • [C] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x29944	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2e000	0x1e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2f000	0x155c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x28cd0	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x28d08	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x24000	0x130	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections								
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x224c6	0x22600	False	0.513799715909	data	6.52239880644	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x24000	0x5fee	0x6000	False	0.423583984375	data	4.91330913111	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2a000	0x2428	0x1a00	False	0.276742788462	data	3.31123175346	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.gfids	0x2d000	0x11c	0x200	False	0.365234375	data	2.28831765042	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2e000	0x1e0	0x200	False	0.53125	data	4.71767883295	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2f000	0x155c	0x1600	False	0.797940340909	data	6.54865418743	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources					
Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x2e060	0x17d	XML 1.0 document text	English	United States

Imports	
DLL	Import
USER32.dll	wsprintfW
WS2_32.dll	WSAGetLastError, htons, inet_ntoa
KERNEL32.dll	WideCharToMultiByte, DecodePointer, EncodePointer, WriteConsoleW, SetFilePointerEx, GetConsoleMode, LoadLibraryA, GetProcAddress, CloseHandle, GetLocalTime, CreateToolhelp32Snapshot, Process32NextW, Process32FirstW, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, IsProcessorFeaturePresent, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, IsDebuggerPresent, GetStartupInfoW, GetModuleHandleW, RaiseException, RtlUnwind, GetLastError, SetLastError, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, LoadLibraryExW, GetStdHandle, WriteFile, GetModuleFileNameA, MultiByteToWideChar, CreateFileW, ExitProcess, GetModuleHandleExW, GetACP, HeapFree, HeapAlloc, FindClose, FindFirstFileExA, FindNextFileA, IsValidCodePage, GetOEMCP, GetCPInfo, GetCommandLineA, GetCommandLineW, GetEnvironmentStringsW, FreeEnvironmentStringsW, LCMapStringW, SetStdHandle, GetFileType, GetStringTypeW, GetProcessHeap, HeapSize, HeapReAlloc, FlushFileBuffers, GetConsoleCP

Possible Origin		
Language of compilation system	Country where language is spoken	Map

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/22-10:01:39.199823	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.1	192.168.2.3

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2022 10:01:30.339246988 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.351450920 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.351550102 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.351596117 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.351639986 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.351679087 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.351721048 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.351732016 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.351761103 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.351764917 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.351771116 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.351775885 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.351779938 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.351784945 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.351805925 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.351815939 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.351850033 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.351862907 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.351890087 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.351903915 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.351932049 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.351941109 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.351973057 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.351986885 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.352005005 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.352025986 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.352063894 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.352483034 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.352524996 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.352555037 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.352567911 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.352607012 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.352610111 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.352647066 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.352652073 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.352664948 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.352689028 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.352708101 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.352721930 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.352746964 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.352778912 CEST	49719	443	192.168.2.3	23.54.113.53

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2022 10:01:30.353399038 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.353442907 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.353468895 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.353483915 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.353523970 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.353524923 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.353534937 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.353566885 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.353578091 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.353606939 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.353622913 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.353651047 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.353667021 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.353723049 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.354274035 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.354331970 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.354345083 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.354376078 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.354392052 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.354408026 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.354435921 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.354481936 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.379918098 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.392113924 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.392167091 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.392206907 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.392251015 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.392292976 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.392333031 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.392373085 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.392415047 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.392456055 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.392462969 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.392467976 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.392472982 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.392477036 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.392482042 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.392505884 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.392549992 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.392589092 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.392631054 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.392652035 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.392661095 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.392669916 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.392682076 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.392704010 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.392748117 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.392776966 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.393243074 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.393281937 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.393321991 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.393335104 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.393358946 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.393363953 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.393371105 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.393403053 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.393416882 CEST	49719	443	192.168.2.3	23.54.113.53
Apr 8, 2022 10:01:30.393445969 CEST	443	49719	23.54.113.53	192.168.2.3
Apr 8, 2022 10:01:30.393457890 CEST	49719	443	192.168.2.3	23.54.113.53

UDP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2022 10:01:30.886255980 CEST	137	137	192.168.2.3	192.168.2.255
Apr 8, 2022 10:01:31.636706114 CEST	137	137	192.168.2.3	192.168.2.255
Apr 8, 2022 10:01:32.402405024 CEST	137	137	192.168.2.3	192.168.2.255
Apr 8, 2022 10:01:33.168015003 CEST	137	137	192.168.2.3	192.168.2.255
Apr 8, 2022 10:01:33.918370962 CEST	137	137	192.168.2.3	192.168.2.255
Apr 8, 2022 10:01:39.199748039 CEST	49874	274	192.168.2.3	192.168.2.1
Apr 8, 2022 10:03:34.873001099 CEST	138	138	192.168.2.3	192.168.2.255

ICMP Packets						
Timestamp	Source IP	Dest IP	Checksum	Code	Type	
Apr 8, 2022 10:01:39.199822903 CEST	192.168.2.1	192.168.2.3	8300	(Port unreachable)	Destination Unreachable	

HTTP Request Dependency Graph
- login.live.com - fs.microsoft.com - arc.msn.com - img-prod-cms-rt-microsoft-com.akamaized.net - sls.update.microsoft.com - ris.api.iris.microsoft.com - displaycatalog.mp.microsoft.com - https: - www.bing.com

HTTPS Proxied Packets					
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49975	20.190.160.67	443	C:\Users\user\l\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:14 UTC	0	OUT	POST /RST2.srf HTTP/1.0 Connection: Keep-Alive Content-Type: application/soap+xml Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 10.0; Win64; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; IDCRL 18.10.0.17134.0.0; IDCRL-cfg 16.000.29158.8; App svchost.exe, 1 0.0.17134.1, {DF60E2DF-88AD-4526-AE21-83D130EF0F68}) Content-Length: 4796 Host: login.live.com
2022-04-08 08:02:14 UTC	0	OUT	Data Raw: 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 73 3a 45 6e 76 65 6c 6f 70 65 20 78 6d 6c 6e 73 3a 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 33 2f 30 35 2f 73 6f 61 70 2d 65 6e 76 65 6c 6f 70 65 22 20 78 6d 6c 6e 73 3a 70 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 50 61 73 73 70 6f 72 74 2f 53 6f 61 70 53 65 72 76 69 63 65 73 2f 50 50 43 52 4c 22 20 78 6d 6c 6e 73 3a 77 73 73 65 3d 22 68 74 74 70 3a 2f 2f 64 6f 63 73 2e 6f 61 73 69 73 2d 6f 70 65 6e 2e 6f 72 67 2f 77 73 73 2f 32 30 30 34 2f 30 31 2f 6f 61 73 69 73 2d 32 30 30 34 30 31 2d 77 73 73 2d 77 73 73 65 63 75 72 69 74 79 2d 73 65 63 65 78 74 2d 31 Data Ascii: <?xml version="1.0" encoding="UTF-8"?><s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:ps="http://schemas.microsoft.com/Passport/SoapServices/PPCRL" xmlns:wsse="http://docs.oasis-open.org/ws/2004/01/oasis-200401-wss-wssecurity-secext-1

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:14 UTC	5	IN	HTTP/1.1 200 OK Cache-Control: no-store, no-cache Pragma: no-cache Content-Type: application/soap+xml; charset=utf-8 Expires: Fri, 08 Apr 2022 08:01:14 GMT P3P: CP="DSP CUR OTPi IND OTRi ONL FIN" Referrer-Policy: strict-origin-when-cross-origin x-ms-route-info: R3_BL2 x-ms-request-id: 94ee6905-7819-4dc6-aa81-1c38db909401 PPServer: PPV: 30 H: BL02EPF0000670C V: 0 X-Content-Type-Options: nosniff Strict-Transport-Security: max-age=31536000 X-XSS-Protection: 1; mode=block Date: Fri, 08 Apr 2022 08:02:14 GMT Connection: close Content-Length: 11093
2022-04-08 08:02:14 UTC	5	IN	Data Raw: 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 20 3f 3e 3c 53 3a 45 6e 76 65 6c 6f 70 65 20 78 6d 6c 6e 73 3a 53 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 33 2f 30 35 2f 73 6f 61 70 2d 65 6e 76 65 6c 6f 70 65 22 20 78 6d 6c 6e 73 3a 77 73 65 3d 22 68 74 74 70 3a 2f 2f 64 6f 63 73 2e 6f 61 73 69 73 2d 6f 70 65 6e 2e 6f 72 67 2f 77 73 73 2f 32 30 30 34 2f 30 31 2f 6f 61 73 69 73 2d 32 30 30 34 30 31 2d 77 73 73 2d 77 73 73 65 63 75 72 69 74 79 2d 73 65 63 65 78 74 2d 31 2e 30 2e 78 73 64 22 20 78 6d 6c 6e 73 3a 77 73 75 3d 22 68 74 74 70 3a 2f 2f 64 6f 63 73 2e 6f 61 73 69 73 2d 6f 70 65 6e 2e 6f 72 67 2f 77 73 73 2f 32 30 30 34 2f 30 31 2f 6f 61 73 69 73 2d 32 30 30 Data Ascii: <?xml version="1.0" encoding="utf-8" ?><S:Envelope xmlns:S="http://www.w3.org/2003/05/soap-envelope" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49980	23.35.236.56	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:19 UTC	16	OUT	HEAD /fs/windows/config.json HTTP/1.1 Connection: Keep-Alive Accept: */* Accept-Encoding: identity User-Agent: Microsoft BITS/7.8 Host: fs.microsoft.com
2022-04-08 08:02:19 UTC	16	IN	HTTP/1.1 200 OK Content-Length: 55 Content-Type: application/octet-stream Last-Modified: Thu, 20 Apr 2017 16:10:39 GMT Accept-Ranges: bytes ETag: "f9c874a7f0b9d21:0" Server: Microsoft-IIS/10.0 Content-Disposition: attachment; filename=config.json X-Powered-By: ASP.NET Cache-Control: public, max-age=222127 Date: Fri, 08 Apr 2022 08:02:19 GMT Connection: close X-CID: 2

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49989	20.82.210.154	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:32 UTC	73	OUT	GET /v3/Delivery/Placement?pubid=da63df93-3dbc-42ae-a505-b34988683ac7&pid=280815&adm=2&w=1&h=1&wpx=1&hpx=1&fmt=json&cltp=app&dim=le&rafb=0&nct=1&pm=1&cfmt=text,image,poly&sft=jpeg,png,gif&topt=1&poptin=0&localid=w:472DC600-FEAB-E7F8-720D-1E33F00FD1E7&ctry=US&time=20220408T170231Z&lc=en-US&pl=en-US&idtp=mid&uid=4388269c-b420-4134-ac19-bc7ca8a19ac1&aid=00000000-0000-0000-0000-000000000000&ua=WindowsShellClient%2F9.0.40929.0%20%28Windows%29&asid=18d6cf97b83f4ce195194e5e6aa953a0&ctmode=MultiSession&arch=x64&cdm=1&cdmver=10.0.17134.1&devfam=Windows.Desktop&devform=Unknown&devosver=10.0.17134.1&disphorzzres=1280&dispsize=17.1&dispvrtres=1024&isu=0&lo=1463022&metered=false&nettype=ethernet&npid=sc-280815&oemName=hsehht%2C%20Inc.&oemid=hsehht%2C%20Inc.&ossku=Professional&smBiosDm=hsehht7%2C1&tl=2&tsu=1463022&waasBldFlt=1&waasCfgExp=1&waasCfgSet=1&waasRetail=1&waasRing= HTTP/1.1 Accept-Encoding: gzip, deflate X-SDK-CACHE: cid=128000000001627409&chs=0&imp=0&chf=0&ds=50583&fs=32319&sc=6 X-SDK-HW-TOKEN: t=EwDYAppeBAAUIAKXDAoFTQM+n+MaRVFKzH/ehWgAAdVW0iu23GlXjRyUBGA+V5LMoU/IMaTj obBnQosoTe6w30OZEf3HulBKeYXog3CqxSfjOHeF/J4iLS/gKyhq/ZV/xtrYHZ35PhcBmS2qzlwNBiXp0+l4efq5ns DEEEESQ06VT9dPxHYgWIFLG65LRysydA1IM9dDPzftFvDLM/ickJDFevqkA3hG2mKV46lqHL4CT7eP4Hk0/MORp8JB 5tewfjl7o25TIEcXI9Ohbx1KlwUuqQcpj0nfDAUZEjkQqVS2z/wQaH+/fdlFO/AoxQI3Cbc0TeaCp3XlesBJX0bxVN zc22qQqCPfGWQ/Sb52rGvkgBRvdW8DFg8ToMjfQpYDZgAAcE3mODPOPAwVqAFPV53gZZc0aOkGu+JWn w46hEU9aCKlpEDkH6SywZSQt+Z6lyumM/ZCz1/Exb6MZih9PGVRFV0dS4rZOFTTSEXw5x6gJoWeqkJZJquL/LQNZp daM/TGNQWWhUnnbhyzuL3J52vftsZzAtC6HDHUtfcP567luQfNJw1zOBQG/Pho8+d+FIHWtcPKMXaDH+X7PpflRpHT m7bd+I+rsPvLvdstjafDCGAADV0pkaM4oU0n35rzdzjoAWTcazcHXkrs0Gr34gDLPkE96nUwLpeDlXN3LOntP44gHn gftJAavz4io7zKxVkmOUwHoTarQK7POiXKiwa8x1QRMWrij0xK5k34eIR6SWW4uOhaTkCvknjxlUvc2iz/sxwS6ZoJu zJ60lCbcq6ptimZGdy/yulx2CKNYcUG/nBNXbdKf3Kz0nMb3Ry9n0QIm/ncP9d68+s4WIRlc+RuW5MPI3aHMGGt2s nchu87pA34+QQKDXqPJVZnC+RaoA8mYS8BGPqZ//PidcqGGmwz2vccoT1N6pSAD7mXPym9QONX68BD3 4uYAk1VCPPhRpsKh41QE=&p= Cache-Control: no-cache MS-CV: BYqskdYKuUKf7ZeJ.0 User-Agent: WindowsShellClient/9.0.40929.0 (Windows) X-SDK-HWF: tch0,m301,m751,mA01,mT01 Host: arc.msn.com Connection: Keep-Alive
2022-04-08 08:02:32 UTC	75	IN	HTTP/1.1 200 OK Cache-Control: no-store, no-cache Pragma: no-cache Content-Length: 3067 Content-Type: application/json; charset=utf-8 Expires: Mon, 01 Jan 0001 00:00:00 GMT Server: Microsoft-IIS/10.0 ARC-RSP-DBG: [{"RADIDS":"","1,P425116123-T700333390-C128000000001627409+B+P20+S1"},{"OPTOUTST ATE":"","256"}] X-ARC-SIG: rTF2rjGWtenDA3aEUCcn2eaUHQMP13nKy5fwur8c8fE5X0qwlYtDm2nyyF4ISAZpKACb8zuMF6PvT PLvY+g8gqOZZkaVKHdD/TspsTuThl3ICqIWC7qNvc5f6SEdAfGCzZ4n36zvg1kSTdZ6LxFiUhBhDkBS5+X4HJ8K9A d5LezYqzSCoXFILAcrwBmHqCNwDJEraoGlix1mkx+2ci/Ym/CTTPi3jhqAUlvQimqHyWg7YDTSMQIPWv6hus5T7cDN RDIBkzohTsN98T0KAfglWEVapY+NGBlNvW/hXV1N5wBE0X9VYXZQ5+3VfUjnyqLMkGqDQDuVAqYHps36tow== Accept-CH: UA, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform, UA-Platform-Version X-AspNet-Version: 4.0.30319 X-Powered-By: ASP.NET Strict-Transport-Security: max-age=31536000; includeSubDomains Date: Fri, 08 Apr 2022 08:02:32 GMT Connection: close
2022-04-08 08:02:32 UTC	76	IN	Data Raw: 7b 22 62 61 74 63 68 72 73 70 22 3a 7b 22 76 65 72 22 3a 22 31 2e 30 22 2c 22 69 74 65 6d 73 22 3a 5b 7b 22 69 74 65 6d 22 3a 22 7b 5c 22 66 5c 22 3a 5c 22 72 61 66 5c 22 2c 5c 22 76 5c 22 3a 5c 22 31 2e 30 5c 22 2c 5c 22 72 64 72 5c 22 3a 5b 7b 5c 22 63 5c 22 3a 5c 22 43 44 4d 5c 22 2c 5c 22 75 5c 22 3a 5c 22 53 75 62 73 63 72 69 62 65 6 4 43 6f 6e 74 65 6e 74 5c 22 7d 5d 2c 5c 22 61 64 5c 22 3a 7b 5c 22 63 6c 61 73 73 5c 22 3a 5c 22 63 6f 6e 74 65 6e 74 5c 22 2c 5c 22 63 6f 6c 6c 65 63 74 69 6f 6e 73 5c 22 3a 5b 5d 2c 5c 22 69 74 65 6d 50 72 6f 70 65 72 74 79 4d 61 6e 69 66 65 73 74 5c 22 3a 7b 5c 22 6e 6f 4f 70 5c 22 3a 7b 5c 22 74 79 70 65 5c 22 64 5c 22 61 74 69 6f 6e 5c 22 7d 7d 2c 5c 22 69 74 65 6d 73 5c 22 3a 5b 7b 5c 22 70 72 6f 70 65 72 74 69 Data Ascii: {"batchrsp":{"ver":"","1.0","items":[{"item":{"f":"rafl","v":"","1.0"},"rdrt":{"l":"CDMI","u":"","SubscribedCont entl"}}, {"ad":{"class":"","content","collections":"","itemPropertyManifest":{"noOp":{"type":"","action"},"items":{"property

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49990	20.199.120.85	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:33 UTC	79	OUT	Data Raw: 43 4e 54 20 31 20 43 4f 4e 20 32 34 36 0d 0a 43 6f 6e 74 65 78 74 3a 20 36 65 34 64 35 61 32 64 61 39 33 62 33 36 34 61 0d 0a 0d 0a Data Ascii: CNT 1 CON 246Context: 6e4d5a2da93b364a
2022-04-08 08:02:33 UTC	79	OUT	Data Raw: 3c 63 6f 6e 6e 65 63 74 3e 3c 76 65 72 3e 32 3c 2f 76 65 72 3e 3c 61 67 65 6e 74 3e 3c 6f 73 3e 57 69 6e 64 6f 77 73 3c 2f 6f 73 3e 3c 6f 73 56 65 72 3e 31 30 2e 30 2e 30 2e 31 37 31 33 34 3c 2f 6f 73 56 65 72 3e 3c 70 72 6f 63 3e 78 36 34 3c 2f 70 72 6f 63 3e 3c 6c 63 69 64 3e 65 6e 2d 55 53 3c 2f 6c 63 69 64 3e 3c 67 65 6f 49 64 3e 32 34 34 3c 2f 67 65 6f 49 64 3e 3c 61 6f 61 63 3e 30 3c 2f 61 6f 61 63 3e 3c 64 65 76 69 63 65 54 79 70 65 3e 31 3c 2f 64 65 76 69 63 65 54 79 70 65 3e 3c 64 65 76 69 63 65 4e 61 6d 65 3e 56 4d 77 61 72 65 37 2c 31 3c 2f 64 65 76 69 63 65 4e 61 6d 65 3e 3c 2f 61 67 65 6e 74 3e 3c 2f 63 6f 6e 6e 65 63 74 3e Data Ascii: <connect><ver>2</ver><agent><os>Windows</os><osVer>10.0.0.0.17134</osVer><proc>x64</proc> <clid>en-US</clid><geold>244</geold><aoac>0</aoac><deviceType>1</deviceType><deviceName>VMware7.1</ deviceName></agent></connect>

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:33 UTC	79	OUT	Data Raw: 41 54 48 20 32 20 43 4f 4e 5c 44 45 56 49 43 45 20 31 30 31 34 0d 0a 43 6f 6e 74 65 78 74 3a 20 36 65 34 64 35 61 32 64 61 39 33 62 33 36 34 61 0d 0a 0d 0a 3c 64 65 76 69 63 65 3e 3c 63 6f 6d 70 61 63 74 2d 74 69 63 6b 65 74 3e 74 3d 45 77 43 6f 41 75 70 49 42 41 41 55 31 62 44 47 66 64 61 7a 69 44 66 58 70 6a 4e 35 4e 36 63 59 68 54 31 77 62 6d 51 41 41 51 77 65 75 52 78 64 54 45 52 58 49 34 58 73 61 55 64 61 66 67 57 47 68 6d 46 42 32 63 6a 51 30 2b 6c 52 4d 56 52 66 4d 58 33 46 77 79 4e 35 6e 68 5a 42 49 69 50 59 61 52 4e 51 2f 64 77 71 38 33 2f 58 59 37 5a 42 55 72 6d 54 65 77 44 66 6a 2f 57 6d 4f 6e 51 35 6b 4e 32 56 76 44 35 75 46 4d 37 47 6a 4c 78 56 73 37 55 78 36 70 69 69 71 41 6d 6c 4d 6d 4e 7a 57 34 6d 36 7a 78 2f 52 66 32 38 74 48 6b 4a 46 73 Data Ascii: ATH 2 CON\DEVICE 1014Context: 6e4d5a2da93b364a<device><compact-ticket>t=EwCoAupIBAAU1bDGfdaziDfXpjN5N6cYhT1wbmQAAQweuRxdTERXI4XsaUdafgWGhmFB2cjQ0+HRMVRfMX3FwyN5nhZBliPYaRNQ/dwq83/XY7ZBUrmTewDfj/WmOnQ5kN2VvD5uFM7GjLxVs7Ux6piiQAmIMmNzW4m6zx/Rf28tHkJFs
2022-04-08 08:02:33 UTC	80	OUT	Data Raw: 42 4e 44 20 33 20 43 4f 4e 5c 51 4f 53 20 32 39 0d 0a 43 6f 6e 74 65 78 74 3a 20 36 65 34 64 35 61 32 64 61 39 33 62 33 36 34 61 0d 0a 0d 0a Data Ascii: BND 3 CON\QOS 29Context: 6e4d5a2da93b364a
2022-04-08 08:02:33 UTC	80	IN	Data Raw: 32 30 32 20 31 20 43 4f 4e 20 35 38 0d 0a Data Ascii: 202 1 CON 58
2022-04-08 08:02:33 UTC	80	IN	Data Raw: 4d 53 2d 43 56 3a 20 73 69 44 6c 52 64 58 4e 59 30 32 36 5a 5a 37 44 6c 72 37 63 69 67 2e 30 0d 0a 0d 0a 50 61 79 6c 6f 61 64 20 70 61 72 73 69 6e 67 20 66 61 69 6c 65 64 2e Data Ascii: MS-CV: siDIRdXNY026ZZ7Dlr7cig.0Payload parsing failed.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49991	20.199.120.151	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:41 UTC	80	OUT	Data Raw: 43 4e 54 20 31 20 43 4f 4e 20 32 34 36 0d 0a 43 6f 6e 74 65 78 74 3a 20 37 62 30 64 66 37 39 34 39 61 64 62 32 63 35 62 0d 0a 0d 0a Data Ascii: CNT 1 CON 246Context: 7b0df7949adb2c5b
2022-04-08 08:02:41 UTC	80	OUT	Data Raw: 3c 63 6f 6e 6e 65 63 74 3e 3c 76 65 72 3e 32 3c 2f 76 65 72 3e 3c 61 67 65 6e 74 3e 3c 6f 73 3e 57 69 6e 64 6f 77 73 3c 2f 6f 73 3e 3c 6f 73 56 65 72 3e 31 30 2e 30 2e 30 2e 31 37 31 33 34 3c 2f 6f 73 56 65 72 3e 3c 70 72 6f 63 3e 78 36 34 3c 2f 70 72 6f 63 3e 3c 6c 63 69 64 3e 65 6e 2d 55 53 3c 2f 6c 63 69 64 3e 3c 67 65 6f 49 64 3e 32 34 34 3c 2f 67 65 6f 49 64 3e 3c 61 6f 61 63 3e 30 3c 2f 61 6f 61 63 3e 3c 64 65 76 69 63 65 54 79 70 65 3e 31 3c 2f 64 65 76 69 63 65 54 79 70 65 3e 3c 64 65 76 69 63 65 4e 61 6d 65 3e 56 4d 77 61 72 65 37 2c 31 3c 2f 64 65 76 69 63 65 4e 61 6d 65 3e 3c 2f 61 67 65 6e 74 3e 3c 2f 63 6f 6e 6e 65 63 74 3e Data Ascii: <connect><ver>2</ver><agent><os>Windows</os><osVer>10.0.0.0.17134</osVer><proc>x64</proc><lcid>en-US</lcid><geold>244</geold><aoac>0</aoac><deviceType>1</deviceType><deviceName>VMware7,1</deviceName></agent></connect>
2022-04-08 08:02:41 UTC	80	OUT	Data Raw: 41 54 48 20 32 20 43 4f 4e 5c 44 45 56 49 43 45 20 31 30 31 34 0d 0a 43 6f 6e 74 65 78 74 3a 20 37 62 30 64 66 37 39 34 39 61 64 62 32 63 35 62 0d 0a 0d 0a 3c 64 65 76 69 63 65 3e 3c 63 6f 6d 70 61 63 74 2d 74 69 63 6b 65 74 3e 74 3d 45 77 43 6f 41 75 70 49 42 41 41 55 31 62 44 47 66 64 61 7a 69 44 66 58 70 6a 4e 35 4e 36 63 59 68 54 31 77 62 6d 51 41 41 51 77 65 75 52 78 64 54 45 52 58 49 34 58 73 61 55 64 61 66 67 57 47 68 6d 46 42 32 63 6a 51 30 2b 6c 52 4d 56 52 66 4d 58 33 46 77 79 4e 35 6e 68 5a 42 49 69 50 59 61 52 4e 51 2f 64 77 71 38 33 2f 58 59 37 5a 42 55 72 6d 54 65 77 44 66 6a 2f 57 6d 4f 6e 51 35 6b 4e 32 56 76 44 35 75 46 4d 37 47 6a 4c 78 56 73 37 55 78 36 70 69 69 71 41 6d 6c 4d 6d 4e 7a 57 34 6d 36 7a 78 2f 52 66 32 38 74 48 6b 4a 46 73 Data Ascii: ATH 2 CON\DEVICE 1014Context: 7b0df7949adb2c5b<device><compact-ticket>t=EwCoAupIBAAU1bDGfdaziDfXpjN5N6cYhT1wbmQAAQweuRxdTERXI4XsaUdafgWGhmFB2cjQ0+HRMVRfMX3FwyN5nhZBliPYaRNQ/dwq83/XY7ZBUrmTewDfj/WmOnQ5kN2VvD5uFM7GjLxVs7Ux6piiQAmIMmNzW4m6zx/Rf28tHkJFs
2022-04-08 08:02:41 UTC	81	OUT	Data Raw: 42 4e 44 20 33 20 43 4f 4e 5c 51 4f 53 20 32 39 0d 0a 43 6f 6e 74 65 78 74 3a 20 37 62 30 64 66 37 39 34 39 61 64 62 32 63 35 62 0d 0a 0d 0a Data Ascii: BND 3 CON\QOS 29Context: 7b0df7949adb2c5b
2022-04-08 08:02:41 UTC	81	IN	Data Raw: 32 30 32 20 31 20 43 4f 4e 20 35 38 0d 0a Data Ascii: 202 1 CON 58
2022-04-08 08:02:41 UTC	81	IN	Data Raw: 4d 53 2d 43 56 3a 20 2f 48 45 54 6a 4e 34 72 36 30 4f 32 51 75 79 4c 4b 5a 4d 66 54 51 2e 30 0d 0a 0d 0a 50 61 79 6c 6f 61 64 20 70 61 72 73 69 6e 67 20 66 61 69 6c 65 64 2e Data Ascii: MS-CV: /HETjN4r60O2QuyLKZMITQ.0Payload parsing failed.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49994	23.10.249.43	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	81	OUT	GET /cms/api/am/imageFileData/RE4CJ3o?ver=76ff HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate, br User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134 Host: img-prod-cms-rt-microsoft-com.akamaized.net Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	2880	IN	Data Raw: 00 4c 5f 2b 6f 96 d6 8c c7 b9 ea 07 ad 4b 67 ac 5c 58 c9 73 a7 9b c5 8a df 76 d8 d9 7e fa fd 07 51 8a f3 fd 3f 52 ba d6 24 82 3f b3 2c 52 59 fc ad b7 73 34 cd f5 cd 5c d5 ef e1 21 b7 8a f1 3e 59 d7 f7 6d bb ef 32 d6 cf 0b 79 5a 6e f7 0e 55 7b 1a 77 5a c5 c7 86 ef af b4 b4 69 2e 52 56 fb d3 fc ed b4 f2 08 f4 cd 73 9e 2a b3 91 35 2d 91 ed dd 3a 89 36 c7 f7 57 d4 1a d8 7d 41 24 b1 82 ea e7 f7 b2 dc e1 77 2e 19 95 97 a7 d0 56 be ab a1 d8 49 a3 c7 77 13 37 da 3c bd cd f2 ee 5d de df fd 7a de 32 54 9a 6d 6f a7 cc a6 79 9d c6 8e ff 00 6a 64 f3 55 5b f8 69 63 67 b5 8d 51 3e 5f e1 dd fe 15 a1 78 b1 c7 26 cf 99 67 6f bc cd f2 ed 5a af 34 26 e1 7e 46 db 17 f7 b6 fc d5 e9 5d b5 a8 cc cb a8 c4 7f 3c 8b b9 5b e6 db 59 b7 17 db ba 2e d6 5f 97 e5 ad 4b eb 8f b1 b7 95 24 Data Ascii: L_+oKglXsv-Q?R\$?.RYS4!>Ym2yZnU{wZi.RVs*5-:6W)A\$w.Vlw7<j2TmoyjdU[icgQ>_x&goZ4&-F]<[_Y_K\$
2022-04-08 08:02:42 UTC	2896	IN	Data Raw: df 2e e6 6a ca b9 fb 3a ae c8 36 b0 dd b9 97 f4 aa e9 1d c5 9c d9 ff 00 54 ad fd df ee d1 ca 9a b9 66 a4 d1 a6 d6 8f fe 04 ab 50 36 9f 6f 75 f3 47 f0 af cc d5 2d ad f3 b4 39 8f e6 97 ee fc df 7a ad c7 7e 23 8f ec ed 16 e5 91 be 65 5a 9b b4 22 08 6f ec d5 62 49 77 6e e3 76 d6 db f2 d4 5a c4 36 f1 c2 cf 16 df de b7 cb e6 7d ed b5 8f a9 7d 9d 75 26 cb 7c bf 75 96 9f 75 a9 45 7f 24 70 6e db 0c 7f f8 f5 6a a9 ea a4 86 47 ad 5a 1b 65 82 44 6d c9 f7 7e ef dd aa 90 dc 4b 32 aa 15 f9 1b e5 dd fe cd 6c d8 20 b8 9b 63 af 98 8d f2 ab 56 85 ce 97 6f 61 1b 29 95 62 0a bf 79 97 e6 6f a5 5f b5 51 f7 5e e3 3b 4f 86 77 e9 73 6b 24 45 b6 ed fd dc 71 aa 96 6f 7c 57 a0 59 bd a4 36 ec f1 ee 81 dd 8f cb 27 f7 bd 71 5e 4b e0 9f 32 c6 f1 a4 3b bf 77 8f de 7f 0b 67 bd 7a 63 ad bc Data Ascii: .j:6TfP6uG-9z-#eZ"oblwnvZ6}}u& uuE\$pnjGZeDm~K2l cVoa)byo_Q^;Owsk\$Eqo WY6'q^K2;wgzc
2022-04-08 08:02:42 UTC	2903	IN	Data Raw: f3 25 2a c5 56 36 90 ed da 7a f3 eb 5f 8a 62 70 d2 a4 af 2d 0e ea 91 bd da 1f 73 ac 49 a8 69 eb 71 79 02 b4 f6 ac 62 fe c1 7c c6 f7 5a e5 3c 59 a7 e9 fe 28 d0 e7 b7 1a 64 71 34 b0 1d d1 b4 63 77 b1 19 ef f9 56 de ab 1d cf 82 e4 57 95 7c ff 00 3d b7 45 3c 8b e6 6d 5c 8e de bf 8d 51 b8 b0 ff 00 84 ba e2 cf 54 49 e5 81 d5 7c b8 da 36 db f3 56 54 6d 46 4a a2 76 57 d1 9e 7c ae 7c bf a7 c1 6f a2 dc 4b 02 cb b6 78 e4 2a d1 b7 ca cb 83 de ac 6a d7 cf a8 69 f7 96 f0 2c 97 2f bb 72 fd 9b ee ae 07 70 3d ab 3b c6 ab 16 8b e2 ed 5e 07 69 27 95 65 75 69 12 b6 b6 e0 7b d7 0d 36 b1 7f 0b 49 1d 9c f2 40 b2 2f cd b5 b6 ee 53 da bf 66 a1 4b db f2 d5 f2 4f f5 1a 64 91 ae db 85 db f2 b6 dd d5 ea df 07 7c 5b 25 8e a4 da 65 fd e2 c5 a7 4a a6 3f de 36 e5 dc 7f c6 bc 9a 3d 36 Data Ascii: %^V6z_bp-sliqyb Z<Y(dq4cwVW?=E<mQTI 6VTmFJvW joKx^ji./rp:~^i'euiv[6l/SfKOd [%eJ?6=6
2022-04-08 08:02:42 UTC	3563	IN	Data Raw: 3b fb 88 2d ee d5 96 f5 98 ee 93 f8 76 e3 8f cb ba 6f 12 5c 4e 8b 2c 90 5b 7f a2 aa ed 83 fe 99 f1 8e 71 ed 58 de 1f bc 8e e6 fa d9 2f 2c 56 e6 58 db cc 65 66 f9 64 4e fc d7 0d 17 cb 1e 74 8d 7d 9a 4e c6 32 78 04 5d 4c 84 ca b0 44 bf 75 59 b6 b3 57 ac fc 3f d1 2d bc 2f 79 e6 4f ff 00 1e a8 bf 2b 2f f1 3f 5c 54 fa d6 ab 61 e3 3f 0d e2 0b 68 2c ee 2c d8 2c 71 ae 15 99 7a 28 cf 7a e4 7c 3f 67 ae c9 ab 44 97 ea cd 06 d3 2c 6a ad fc bd 2b 8e ad 69 e2 e8 ca 15 1f 2f 46 8b 71 8c 36 d4 fa 2f 4b f1 75 85 e4 de 6e a2 bf 66 8a db 0b e4 2a 86 69 99 85 47 ad 7c 48 8a e3 fd 1a db 6d 9c 1f 7a 4d cb f2 f1 d8 01 5e 65 6b f1 33 c3 de 05 d3 e2 82 fd 7c dd 46 eb 7c 8d fc 5e 4e 7b 55 ed 2f 54 b3 f1 f3 6f 4b c5 82 cd be f3 46 bb 5b 68 f6 3e b5 f2 92 cb bd 9d e7 38 35 05 d7 a1 Data Ascii: ;-vo!N,[qX/VXefdNt}N2x LDuYW?-/yO+/?\Ta?h,,,qz(z ?gD.j+i/Fq6/Kunf*G Hmzm^ek3 F ^N{UoTKF h>85
2022-04-08 08:02:42 UTC	3579	IN	Data Raw: ec 2d 07 dd b9 f3 0d 70 4a 53 87 c4 97 2b dd f6 ec 29 59 2d 42 4b 67 b8 65 26 e7 f7 4b f7 b6 fd ea bf a9 59 db d9 fd 9a 58 20 fd d3 2e ed b0 31 65 e3 fa fa d5 2d 13 c2 71 e9 12 45 71 77 79 1b 5a cb 9d 8c ad b9 77 53 64 d0 ed 92 17 8e 4f b4 c1 60 cd fc 52 7f 0f a7 e3 59 f3 c5 cb 95 4b 45 e4 52 b2 13 c4 9a 85 a7 da 23 8a c2 39 17 52 91 7c c6 6f f9 64 ac 2b 9c ba d1 6f 2e 36 f9 bb a5 95 b2 d2 7c df 7b be 6b 42 6b 6b 6b 69 31 64 d2 34 5c ab 33 7f 0e 7d fd aa cb 2a 58 db ca 8f fb d9 55 59 a3 92 56 f5 f5 ae aa 72 fe 69 46 3f 8e e3 45 6d 27 45 bc d4 af bc 97 8a 45 81 70 de 62 ae f6 5c 7d 2a 7b 7d 02 f6 39 19 67 8a 7f 2a 49 37 48 d2 7d df 6f a5 56 93 c4 d7 1f 2c 96 d1 4f 04 31 2e df 2e 39 3e 5d d9 eb 57 21 f1 13 6a 51 ac 50 79 90 4e ec 77 33 7d e6 5f 7f ff 00 5d Data Ascii: -pJS+)Y-BKge&KYYX .1e-qEqwyZwSdO' RYKER#9R od+o.6 {kBkkki1d4\3}*XUYVnF?Em^Eepb\}*}9g*i7H }oV,O1..9> WijQPpNw3}_]
2022-04-08 08:02:42 UTC	3595	IN	Data Raw: 47 37 9b 62 81 95 5a 5f 95 ab 3e 52 b9 91 b3 36 ac 9a ac 9f 67 1f 37 96 bb b7 7f 7b f1 ac f9 ad c3 dc 79 50 6e da d8 66 fe f5 5e d2 74 99 2c 2d da 37 5d ed f7 77 2f f9 e2 b3 e1 be 93 45 d4 be 78 3c d7 8f e6 da d4 bd 07 6b 97 1f c5 47 4b 8d 6d a5 b6 dc bf 77 cf ff 00 67 bd 63 df e2 f2 4d e9 2e e4 6f bb bb f8 68 d7 75 47 d4 24 f3 1e 0f 2b cc fb ab fc 3b 6a e6 95 a0 cb 0d 8a ca f1 34 b0 48 df 79 7e f5 63 cb 1a 6b 9b 66 ca 6d cb 41 b6 b7 8d a2 c3 bf 6b 37 cb f2 ed f9 be 63 59 6f ae 6a 09 23 18 e7 6d cd f3 57 43 26 8f 02 c9 fb cb 95 81 37 6e 65 dc 37 7b d5 1b 9b 0b 39 b7 7d 8d fc f4 5f ba cd 44 5c 5b bb 57 31 d4 3c 33 34 6b a9 2b ea 92 b2 c5 27 de 93 de b7 2e bc 43 6f 1c b6 d1 32 cf 17 2a b2 2f f3 ac 88 ed ed a4 8d 8e ff 00 f8 0f f7 5a 9f 71 a6 e9 d0 c7 8f Data Ascii: G7bZ_>R6g7{yPnf^t,-7}wEx<kGKmwgcM.ohuG\$+;j4Hy-ckfmAk7Yoj#mWC&7ne7{9}_D {W1<34k+^Coo2* /Zq
2022-04-08 08:02:42 UTC	3603	IN	Data Raw: bd 44 36 31 47 34 f3 cf f3 0d a1 76 af f1 54 56 71 c9 1e d8 df 6b 6e ff 00 6a b4 ad 6d fc 95 51 77 b7 c8 91 8f 97 f8 56 35 25 64 52 57 23 b7 bc 4b 38 67 88 2e d7 91 82 c7 f2 d5 5d 59 a4 be da 88 db 9a 35 f9 56 af 6a 11 e9 df 65 69 22 97 fd 31 7f 87 f8 57 d7 35 95 04 c9 79 78 a0 7d f6 fe 1a ce 9d 9f bc 91 7d 2c 6e e9 76 72 ff 00 64 ac bb 55 b6 fc ad bb ef 7d 6b 3a e6 4b 88 63 fd dc 5f 3d 5b 91 ce 9b b4 16 59 51 be f2 ab 55 59 b5 48 ec fc a9 7e f7 f7 57 fd aa b8 c5 a0 65 17 69 2e 21 8b cc 66 55 dd f7 7f da ab ff 00 f0 8e c5 36 93 79 28 b9 8e 39 62 c7 ee 24 6f 9b 69 fe e9 aa 97 17 cf 7e bc 26 d6 fb db aa 17 9b 7a ed db f3 fd da 89 c6 5f 65 d8 8d 19 96 b6 ef 6d cb b6 ed bf 2f fb be d5 5a e6 37 76 67 db f7 bf bb 5b 8b 6f 15 bd ab 61 5b 77 0d f3 37 f1 66 a3 85 Data Ascii: D61G4vTVqknjmQwV5%dRW#K8g.]Y5Vjei"1W5yx}},nvrduJ}k:Kc_=[YQUYH-Wei.!fU6y(9b\$oi-&z_em/Z7vg[oa[w7f

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49996	23.10.249.43	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	82	OUT	GET /cms/api/am/imageFileData/RWMW3O?ver=5b92 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate, br User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134 Host: img-prod-cms-rt-microsoft-com.akamaized.net Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	99	IN	HTTP/1.1 200 OK Last-Modified: Mon, 04 Apr 2022 07:41:51 GMT Access-Control-Allow-Origin: * X-Datcenter: northeu X-ActivityId: 6dc0ab63-03d3-400b-a7a1-7eef7d986f66 Timing-Allow-Origin: * X-Frame-Options: deny X-ResizerVersion: 1.0 Content-Type: image/jpeg Content-Location: https://image.prod.cms.rt.microsoft.com/cms/api/am/imageFileData/RWMW3O?ver=5b92 X-Source-Length: 1605408 Content-Length: 1605408 Cache-Control: public, max-age=85170 Expires: Sat, 09 Apr 2022 07:42:12 GMT Date: Fri, 08 Apr 2022 08:02:42 GMT Connection: close
2022-04-08 08:02:42 UTC	100	IN	Data Raw: ff d8 ff e1 18 04 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 07 01 12 00 03 00 00 00 01 00 01 00 00 01 1a 00 05 00 00 00 01 00 00 00 62 01 1b 00 05 00 00 00 01 00 00 00 6a 01 28 00 03 00 00 00 01 00 02 00 00 01 31 00 02 00 00 00 1f 00 00 00 72 01 32 00 02 00 00 00 14 00 00 00 91 87 69 00 04 00 00 00 01 00 00 00 a8 00 00 00 d4 00 0e a6 00 00 00 27 10 00 0e a6 00 00 00 27 10 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 32 31 2e 31 20 28 57 69 6e 64 6f 77 73 29 00 32 30 32 31 3a 30 38 3a 30 35 20 31 33 3a 35 39 3a 32 39 00 00 00 00 00 00 03 a0 01 00 03 00 00 00 01 ff ff 00 00 a0 02 00 04 00 00 00 01 00 00 04 38 a0 03 00 04 00 00 00 01 00 00 07 80 00 00 00 00 00 00 00 06 01 03 00 03 00 00 00 01 00 06 00 00 01 1a 00 05 00 00 00 01 00 00 01 22 01 1b 00 05 00 Data Ascii: ExifMM*bj(1r2i"Adobe Photoshop 21.1 (Windows)2021:08:05 13:59:298"
2022-04-08 08:02:42 UTC	166	IN	Data Raw: db a5 ae 90 3d a3 6f d0 fe 46 e6 7b 14 33 3a 56 5e 39 1e a3 3d 46 b0 c8 7b 04 ba 7f aa 7f aa d5 54 5f d4 fd b4 34 c1 7c 90 e7 fb a5 a3 e9 4f a8 d1 66 d6 6d 7f d2 4f 86 ba c2 71 31 ec 7f 4f fc 54 1d 37 05 27 a3 59 ac f8 0f e7 00 d5 d1 00 fb e7 fc d5 4b 36 f7 07 7a 6d 76 ae f7 10 24 1e 76 ee 7f ef ff 00 6d 13 2f ab ef b8 d6 cd 85 ad 71 ad b6 47 b9 c6 3d fe 8f d3 da d6 6d ff 00 a6 b2 dc e6 db 6e fa fe 98 90 4b 8c c8 03 76 fd 3f 37 6f d3 4f 18 8c 8f 14 80 1a 5f fb eb 26 05 50 53 ed 12 da dc 76 06 43 9a 47 b9 db 87 e7 fe 3e d4 d6 bd c6 b3 ba 5f 68 69 91 a3 41 63 81 f7 c1 fa 4e dc 7f f3 04 db 5a 06 f7 1e 67 76 d1 b6 03 8e 92 df a4 84 6e da fd a3 f4 ac e5 c3 4d 74 3b b9 16 7f 59 4b 18 5d 50 ba ef f8 b0 f0 51 b0 c2 bb 1a 0c 1e 1d e1 e3 ab 74 51 0e 87 10 e3 ee 11 Data Ascii: =oF{3:V^9=F[T_4]OfmOq1GT7"YK6zmv\$vm/qG=mnKv?7oO_&PSvCG>_hiAcNZgvnMt;YK]PQTQ
2022-04-08 08:02:42 UTC	182	IN	Data Raw: 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 37 2d 32 36 54 31 30 3a 34 36 3a 34 33 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 45 64 67 65 5c 5f 43 72 6f 70 73 5c 45 64 67 65 2d 4c 69 66 65 73 74 79 6c 65 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 33 38 38 30 31 37 38 38 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 7 3 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 37 2d 32 36 54 31 30 3a 34 38 3a 35 37 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 45 64 67 65 5c 5f 43 72 6f 70 73 5c 45 64 67 65 2d 4c 69 66 65 73 74 79 6c 65 Data Ascii: 1080x1920.jpg saved
2016-07-26T10:46:43-07:00	File C:\Users\lv-lizagh\MSI\Windows10\Edge_Crops\Edge-Lifestyle_GettyImages-538801788_1080x1920.jpg saved
2016-07-26T10:48:57-07:00	File C:\Users\lv-lizagh\MSI\Windows10\Edge_Crops\Edge-Lifestyle
2022-04-08 08:02:42 UTC	215	IN	Data Raw: 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 45 64 67 65 5c 5f 43 72 6f 70 73 5c 45 64 67 65 2d 4c 69 66 65 73 74 79 6c 65 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 39 33 35 39 36 38 37 33 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 37 2d 32 36 54 31 31 3a 30 30 3a 32 35 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 45 64 67 65 5c 5f 43 72 6f 70 73 5c 45 64 67 65 2d 4c 69 66 65 73 74 79 6c 65 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 31 33 31 34 39 32 31 34 5f 31 30 38 30 7 8 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 Data Ascii: 	File C:\Users\lv-lizagh\MSI\Windows10\Edge_Crops\Edge-Lifestyle_GettyImages-593596873_1080x1920.jpg saved
2016-07-26T11:00:25-07:00	File C:\Users\lv-lizagh\MSI\Windows10\Edge_Crops\Edge-Lifestyle_GettyImages-113149214_1080x1920.jpg saved
20
2022-04-08 08:02:42 UTC	321	IN	Data Raw: 5c 53 75 72 66 61 63 65 5c 4a 75 61 6e 5c 53 75 72 66 61 63 65 50 65 6e 5c 43 72 6f 70 73 5c 53 55 52 31 35 5f 50 65 6e 5f 30 31 5f 42 4b 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 38 2d 33 31 54 31 33 3a 32 36 3a 34 34 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 53 75 72 66 61 63 65 5c 4a 75 61 6e 5c 53 75 72 66 61 63 65 50 65 6e 5c 43 72 6f 70 73 5c 53 55 52 5f 76 34 5f 50 65 6e 5f 46 61 6d 69 6c 79 5f 35 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 38 2d 33 31 54 31 33 3a 32 39 3a 31 37 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c Data Ascii: \Surface\Juan\SurfacePen\Crops\SUR15_Pen_01_BK_1080x1920.jpg saved
2016-08-31T13:26:44-07:00	File C:\Users\lv-lizagh\MSI\Windows10\Surface\Juan\SurfacePen\Crops\SUR_v4_Pen_Family_5_1080x1920.jpg saved
2016-08-31T13:29:17-07:00	File C:\Users\
2022-04-08 08:02:42 UTC	361	IN	Data Raw: 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 31 30 2d 31 37 54 30 38 3a 33 34 3a 35 36 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 6f 6d 65 6e 74 73 49 6e 54 69 6d 65 5c 48 6f 6c 69 64 61 79 53 68 6f 70 70 69 6e 67 5c 4d 49 54 2d 48 6f 6c 69 64 61 79 53 68 6f 70 70 69 6e 67 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 31 39 30 36 30 39 38 30 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 31 30 2d 31 37 54 30 38 3a 33 37 3a 31 30 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 Data Ascii: indows10\Lockscreen_1080x1920_Portrait.psd saved
2016-10-17T08:34:56-07:00	File C:\Users\lv-lizagh\MSI\Windows10\Moments\InTime\HolidayShopping\MIT-HolidayShopping_GettyImages-519060980_1080x1920.jpg saved
2016-10-17T08:37:10-07:00	File C:\Us
2022-04-08 08:02:42 UTC	420	IN	Data Raw: 64 20 6f 70 65 6e 65 64 26 23 78 41 3b 32 30 31 36 2d 31 31 2d 31 30 54 31 31 3a 34 35 3a 35 34 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 69 6e 67 5c 53 68 6f 70 70 69 6e 67 5c 5f 43 48 4f 53 45 4e 5c 4d 69 6e 67 5f 48 6f 6c 69 64 61 79 53 68 6f 70 70 69 6e 67 5f 47 65 74 74 79 2d 36 32 30 39 39 39 35 35 39 5f 31 30 38 30 78 31 39 32 30 5f 47 72 61 64 69 65 6e 74 4e 6f 57 6f 72 64 73 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 31 31 2d 31 30 54 31 31 3a 34 3 9 3a 30 38 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f Data Ascii: d opened
2016-11-10T11:45:54-08:00	File C:\Users\lv-lizagh\MSI\Windows10\Bing\Shop ping_CHOSEN\Bing_HolidayShopping_Getty-620999559_1080x1920_GradientNoWords.jpg saved
2016-11-10 T11:49:08-08:00	File C:\Users\lv-lizagh\MSI\Windows10\Lockscreen_

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	484	IN	Data Raw: 50 6f 72 74 72 61 69 74 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 31 2d 31 31 54 31 31 3a 30 36 3a 33 33 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 45 64 67 65 5c 50 72 6f 64 75 63 74 69 76 69 74 79 54 69 70 73 5c 5f 43 48 4f 53 45 4e 5c 45 64 67 65 2d 54 61 73 6b 56 69 65 77 5f 67 72 61 64 69 65 6e 74 5f 35 30 30 70 78 2d 31 32 31 31 39 3 0 33 39 35 5f 31 30 38 30 78 31 39 32 30 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 31 2d 31 31 54 31 31 3a 31 30 3a 32 33 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 45 64 67 65 5c 50 72 Data Ascii: Portrait.psd saved
2017-01-11T11:06:33-08:00	File C:\Userslv-lizagh\MS\Windows10\Edge\Prod uctivityTips\CHOSEN\Edge-TaskView_gradient_500px-121190395_1080x1920.psd saved
2017-01-11T11:10:23-08:00	File C:\Userslv-lizagh\MS\Windows10\Edge\Pr
2022-04-08 08:02:42 UTC	500	IN	Data Raw: 72 74 61 69 6e 6d 65 6e 74 5f 4d 61 72 63 68 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 39 31 38 36 39 39 35 33 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 32 2d 32 54 31 30 3a 35 34 3a 34 31 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 6f 6d 65 6e 74 73 49 6e 54 69 6d 65 5c 53 70 72 69 6e 67 45 6e 74 65 72 7 4 61 69 6e 6d 65 6e 74 5c 4d 61 72 63 68 5c 43 48 4f 53 45 4e 5c 4d 49 54 2d 53 70 72 69 6e 67 45 6e 74 65 72 74 61 69 6e 6d 65 6e 74 5f 4d 61 72 63 68 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 36 32 33 37 37 32 31 33 36 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 Data Ascii: rtainment_March_GettyImages-591869953_1080x1920.jpg saved
2017-02-22T10:54:41-08:00	File C:\Userslv-lizagh\MS\Windows10\MomentsInTime\SpringEntertainment\March\CHOSEN\MIT-SpringEntertainment _March_GettyImages-623772136_1080x1920.jpg saved
2017
2022-04-08 08:02:42 UTC	607	IN	Data Raw: 64 6f 77 73 31 30 5c 4d 69 63 72 6f 73 6f 66 74 5c 4d 61 6b 65 57 68 61 74 73 4e 65 78 74 5c 43 48 4f 53 45 4e 5c 4d 53 2d 4d 61 6b 65 57 68 61 74 73 4e 65 78 74 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 34 37 38 33 31 39 38 35 36 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 33 2d 30 37 54 31 31 3a 31 30 3a 35 37 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 69 63 72 6f 73 6f 66 74 5c 4d 61 6b 65 57 68 61 74 73 4e 65 78 74 5c 43 48 4f 53 45 4e 5c 4d 53 2d 4d 61 6b 65 57 68 61 74 73 4e 65 78 74 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 30 39 37 33 31 32 37 36 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 Data Ascii: dows10\Microsoft\MakeWhatsNext\CHOSEN\MS-MakeWhatsNext_GettyImages-478319856_1080x1920.jpg saved
2017-03-07T11:10:57-08:00	File C:\Userslv-lizagh\MS\Windows10\Microsoft\MakeWhatsNext\CHOSEN\ MS-MakeWhatsNext_GettyImages-509731276_1080x1920.jpg save
2022-04-08 08:02:42 UTC	659	IN	Data Raw: 33 37 32 36 33 37 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 34 2d 30 34 54 31 34 3a 31 34 3a 31 32 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 42 75 73 69 6e 65 73 73 2d 50 68 69 6c 61 6e 74 6 8 72 6f 70 69 65 73 5c 43 48 4f 53 45 4e 5c 50 68 69 6c 61 6e 74 68 72 6f 70 69 65 73 73 68 75 74 74 6f 6 3 6b 5f 37 32 39 30 35 32 38 34 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 34 2d 30 34 54 31 34 3a 31 35 3a 34 30 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 Data Ascii: 372637_1080x1920.jpg saved
2017-04-04T14:14:12-07:00	File C:\Userslv-lizagh\MS\Windows10\B usiness-Philanthropies\CHOSEN\Philanthropies_shutterstock_72905284_1080x1920.jpg saved
2017-04-0 4T14:15:40-07:00	File C:\Userslv-lizagh\AppData\Roami
2022-04-08 08:02:42 UTC	715	IN	Data Raw: 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 57 69 6e 64 6f 77 73 5c 43 72 65 61 74 6f 72 73 55 70 64 61 74 65 5c 43 48 4f 53 45 4e 5c 57 69 6e 2d 43 72 65 61 74 6f 72 73 55 70 64 61 74 65 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 36 30 35 31 38 34 35 33 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 35 2d 31 31 54 31 30 3a 34 36 3a 31 31 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 57 69 6e 64 6f 77 73 5c 43 72 65 61 74 6f 72 73 55 70 64 61 74 65 5c 43 48 4f 53 45 4e 5c 57 69 6e 2d 43 72 65 61 74 6f 72 73 55 70 64 61 74 65 5f 47 65 74 Data Ascii: 0	File C:\Userslv-lizagh\MS\Windows10\Windows\CreatorsUpdate\CHOSEN\Win-CreatorsUpda te_GettyImages-560518453_1080x1920.jpg saved
2017-05-11T10:46:11-07:00	File C:\Userslv-lizag h\MS\Windows10\Windows\CreatorsUpdate\CHOSEN\Win-CreatorsUpdate_Get
2022-04-08 08:02:42 UTC	754	IN	Data Raw: 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 41 64 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 37 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 57 69 6e 64 6f 77 73 49 6e 73 69 64 65 72 2d 52 53 33 2d 53 6c 6f 77 52 69 6e 67 5f 35 30 30 70 78 2d 31 30 32 36 31 37 30 37 5f 31 30 38 30 78 31 39 32 30 36 35 39 43 43 46 30 32 43 43 42 46 39 33 35 46 38 43 35 45 36 37 42 38 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 36 2d 30 37 54 31 30 3a 31 39 3a 35 36 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 57 Data Ascii: 00	File C:\Userslv-lizagh\AppData\Roaming\Adobe\Adobe Photoshop CC 2017\AutoRecover\ _WindowsIn sider-RS3-SlowRing_500px-10261707_1080x1920659CCF0BD5DCF602CCBF935F8C5E67B8.psb saved
2017-06-07T10:19:56-07:00	File C:\Userslv-lizagh\MS\Windows10\W
2022-04-08 08:02:42 UTC	786	IN	Data Raw: 70 73 5c 4d 61 6b 69 6e 67 41 44 69 66 66 65 72 65 6e 63 65 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 30 32 36 31 33 36 33 31 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 37 2d 30 33 54 32 31 3a 34 35 3a 33 32 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 41 64 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 37 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 3 0 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 46 30 31 39 34 34 45 44 31 42 37 43 33 38 42 38 44 46 35 33 38 45 43 44 33 39 43 34 43 43 46 43 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b Data Ascii: ps\MakingADifference_GettyImages-502613631_1080x1920.jpg saved
2017-07-03T21:45:32-0 7:00	File C:\Userslv-lizagh\AppData\Roaming\Adobe\Adobe Photoshop CC 2017\AutoRecover\ _Lockscre e_n_1080x1920_PortraitF01944ED1B7C38B8DF538ECD39C4CCFC.psb saved

2022-04-08 08:02:42 UTC	878	IN	Data Raw: 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 57 69 6e 64 6f 77 73 5c 4d 4d 58 5c 5f 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 57 69 6e 64 6f 77 73 4d 4d 58 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 36 33 36 30 32 31 39 33 34 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 37 2d 32 36 54 31 34 3a 31 35 3a 32 30 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 41 64 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 37 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 57 69 6e 64 6f 77 73 4d 4d 58 5f 47 65 Data Ascii: -07:00	File C:\Userslv-lizagh\MS\Windows10\Windows\MMX\CHOSEN\Crops\Windows\MMX_Gett yImages-636021934_1080x1920.jpg saved
2017-07-26T14:15:20-07:00	File C:\Userslv-lizagh\AppData\Roaming\Adobe\Adobe Photoshop CC 2017\AutoRecover\ _Windows\MMX_Ge

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	894	IN	Data Raw: 61 72 64 73 5c 57 65 6c 63 6f 6d 65 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4d 53 5d 57 65 6c 63 6f 6d 65 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 34 38 31 32 31 36 30 39 32 5f 31 30 38 30 78 31 39 32 30 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 39 2d 32 31 54 31 34 3a 35 34 3a 32 38 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 53 72 65 77 61 72 64 73 5c 57 65 6c 63 6f 6d 65 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4d 53 2d 57 65 6c 63 6f 6d 65 5f 47 65 74 79 49 6d 61 67 65 73 2d 34 38 31 32 31 36 30 39 32 5f 31 30 38 30 78 31 39 32 30 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 39 2d 32 31 54 31 34 3a 35 34 3a 33 Data Ascii: ards\Welcome\CHOSEN\Crops\MS-Welcome_GettyImages-481216092_1080x1920.psd saved&#xA;2017-09-21T14:54:28-07:00&#x9;File C:\Users\lv-lizagh\MS\Windows10\MSrewards\Welcome\CHOSEN\Crops\MS-Welcome_GettyImages-481216092_1080x1920.psd saved&#xA;2017-09-21T14:54:3
2022-04-08 08:02:42 UTC	997	IN	Data Raw: 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 37 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 4d 49 54 2d 53 6f 63 63 65 72 5f 41 6c 61 6d 79 2d 47 39 44 48 52 33 5f 31 30 38 30 78 31 39 32 30 35 39 38 31 39 30 46 33 43 43 46 32 36 37 43 34 30 38 45 38 31 31 30 36 46 33 43 41 45 38 35 37 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 31 30 2d 31 33 54 31 38 3a 31 34 3a 30 38 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 31 30 2d 31 37 54 31 3 0 3a 33 31 3a 34 36 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 Data Ascii: Photoshop CC 2017\AutoRecover_MIT-Soccer_Alamy-G9DHR3_1080x1920598190F3CCF267C408E81106F3CAE857.psb saved&#xA;2017-10-13T18:14:08-07:00&#x9;File C:\Users\lv-lizagh\MS\Windows10\Lockscreen_1080x1920_Portrait.psd saved&#xA;2017-10-17T10:31:46-07:00&#x9;File
2022-04-08 08:02:42 UTC	1077	IN	Data Raw: 30 39 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 6f 70 65 6e 65 64 26 23 78 41 3b 32 30 31 37 2d 31 31 2d 32 30 54 31 37 3a 34 35 3a 33 38 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 53 72 65 77 61 72 64 73 5c 41 75 73 74 72 61 6c 69 61 5c 43 68 6f 73 65 6e 5c 31 31 30 39 31 37 5c 43 72 6f 70 73 5c 4d 53 2d 52 65 77 61 72 64 73 2d 41 55 5f 47 65 74 74 79 49 6d 61 67 65 7 3 2d 38 33 36 36 34 32 39 38 36 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 31 31 2d 32 30 54 31 37 3a 35 31 3a 33 37 2d 30 38 3a 30 30 26 Data Ascii: 09-08:00&#x9;File Lockscreen_1080x1920_Portrait.psd opened&#xA;2017-11-20T17:45:38-08:00&#x9;File C:\Users\lv-lizagh\MS\Windows10\MSrewards\Australia\Chosen\110917\Crops\MS-Rewards-AU_GettyImages-836642986_1080x1920.jpg saved&#xA;2017-11-20T17:51:37-08:00&
2022-04-08 08:02:42 UTC	1124	IN	Data Raw: 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 69 63 72 6f 73 6f 66 74 5c 41 6e 64 72 6f 69 64 4c 61 75 6e 63 68 65 72 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4d 53 2d 41 6e 64 72 6f 69 64 4c 61 75 6e 63 68 65 72 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 38 32 36 36 36 38 39 38 30 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 31 32 2d 31 34 54 31 36 3a 33 33 3a 35 38 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 69 63 72 6f 73 6f 66 74 5c 41 6e 64 72 6f 69 64 4c 61 75 6e 63 68 65 72 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4d 53 2d 41 6e 64 72 6f Data Ascii: 9;File C:\Users\lv-lizagh\MS\Windows10\Microsoft\Android\Launcher\CHOSEN\Crops\MS-Android\Launcher_GettyImages-826668980_1080x1920.jpg saved&#xA;2017-12-14T16:33:58-08:00&#x9;File C:\Users\lv-lizagh\MS\Windows10\Microsoft\Android\Launcher\CHOSEN\Crops\MS-Andro
2022-04-08 08:02:42 UTC	1180	IN	Data Raw: 49 54 2d 4e 42 41 2d 49 6e 74 6c 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 34 37 32 37 31 30 37 32 5f 31 30 38 30 78 31 39 32 30 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 31 2d 30 39 54 30 38 3a 32 37 3a 30 37 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 49 54 2d 49 6e 74 65 72 6e 61 74 69 6f 6e 61 6c 5c 4e 42 41 5c 43 68 6f 73 65 6e 5c 43 72 6f 70 73 5c 4d 49 54 2d 4e 42 41 2d 49 6e 74 6c 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 34 37 32 37 31 30 37 32 5 f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 31 2d 30 39 54 30 38 3a 32 38 3a 34 34 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a Data Ascii: IT-NBA-Intl_GettyImages-147271072_1080x1920.psd saved&#xA;2018-01-09T08:27:07-08:00&#x9;File C:\Users\lv-lizagh\MS\Windows10\MIT-International\NBA\Chosen\Crops\MIT-NBA-Intl_GettyImages-147271072_1080x1920.jpg saved&#xA;2018-01-09T08:28:44-08:00&#x9;File C:
2022-04-08 08:02:42 UTC	1235	IN	Data Raw: 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 6f 70 65 6e 65 64 26 23 78 41 3b 32 30 31 38 2d 30 31 2d 32 35 54 31 32 3a 33 37 3a 30 32 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 49 54 2d 49 6e 74 65 72 6e 61 74 69 6f 6e 61 6c 5c 4e 41 5c 43 68 6f 73 65 6e 5c 41 55 54 72 61 76 65 6c 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4d 49 54 2d 41 55 2d 72 61 76 65 6c 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 38 35 34 32 30 39 30 32 5f 31 30 38 30 78 31 39 32 30 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 31 2d 32 35 54 31 32 3a 33 37 3a 33 31 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e Data Ascii: 1920_Portrait.psd opened&#xA;2018-01-25T12:37:02-08:00&#x9;File C:\Users\lv-lizagh\MS\Windows10\MIT-International\AU-Travel\CHOSEN\Crops\MIT-AU-Travel_GettyImages-185420902_1080x1920.psd saved&#xA;2018-01-25T12:37:31-08:00&#x9;File C:\Users\lv-lizagh\MS\Win
2022-04-08 08:02:42 UTC	1267	IN	Data Raw: 35 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 57 69 6e 64 6f 77 73 5c 4d 69 78 65 64 52 65 61 6c 69 74 79 5c 46 59 31 38 43 61 6d 70 61 69 67 6e 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 57 4d 52 2d 48 4d 44 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 39 31 37 38 32 31 33 33 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 32 2d 32 38 54 31 30 3a 32 33 3a 35 30 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 41 64 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 37 5c 41 75 74 6f 52 65 63 Data Ascii: 5-08:00&#x9;File C:\Users\lv-lizagh\MS\Windows10\Windows\MixedReality\FY18Campaign\CHOSEN\Crops\WMR-HMD_GettyImages-591782133_1080x1920.jpg saved&#xA;2018-02-28T10:23:50-08:00&#x9;File C:\Users\lv-lizagh\AppData\Roaming\Adobe\Adobe Photoshop CC 2017\AutoRec
2022-04-08 08:02:42 UTC	1331	IN	Data Raw: 74 61 5c 52 6f 61 6d 69 6e 67 5c 41 64 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 37 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 45 43 39 39 33 34 30 42 35 30 46 37 44 35 37 32 30 43 39 36 39 44 34 32 34 33 31 34 39 36 36 37 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 33 2d 32 36 54 31 35 3a 35 36 3a 31 38 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2d 52 65 63 6f 76 65 72 65 64 2e 70 73 64 20 6f 70 65 6e 65 64 26 23 78 41 3b 32 30 31 38 2d 30 33 2d 32 36 54 31 37 3a 32 39 3a 32 32 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 Data Ascii: tal\Roaming\Adobe\Adobe Photoshop CC 2017\AutoRecover_Lockscreen_1080x1920_PortraitEC99340B50F7D5720C969D4243149667.psb saved&#xA;2018-03-26T15:56:18-07:00&#x9;File Lockscreen_1080x1920_Po rtrait-Recovered.psd opened&#xA;2018-03-26T17:29:22-07:00&#x9;File

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	1402	IN	Data Raw: 30 44 37 45 46 36 37 34 30 38 43 44 34 35 38 42 41 46 30 30 31 34 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 35 37 46 46 39 35 45 42 39 32 41 44 44 42 45 31 37 35 30 32 41 31 33 41 46 34 39 44 39 34 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 35 38 35 36 34 41 43 42 32 36 34 31 45 42 38 36 42 39 33 35 38 37 34 33 43 44 32 45 45 37 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 35 39 32 44 37 44 39 42 35 37 37 4 4 36 30 36 32 39 38 45 44 34 34 44 38 44 42 42 42 44 44 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 35 41 36 30 42 38 36 31 43 33 30 31 32 30 31 37 33 35 44 45 43 30 34 31 39 46 32 38 39 42 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 35 42 39 41 37 45 34 31 45 36 31 34 46 Data Ascii: 0D7EF67408CD458BAF00149</rdf:li> <rdf:li>057FF95EB92ADDBE17502A13AF49D944</rdf:li> <rdf:li>058564ACB2641EB86B9358743CD2EE7F</rdf:li> <rdf:li>0592D7D9B577D606298ED44D8DBBDDF</rdf:li> <rdf:li>05A60B861C301201735DEC0419F289BC</rdf:li> <rdf:li>05B9A7E41E614F
2022-04-08 08:02:42 UTC	1739	IN	Data Raw: 72 64 66 3a 6c 69 3e 31 32 39 34 33 32 37 41 45 37 36 32 45 38 32 46 46 41 38 43 38 38 35 30 36 45 44 46 34 32 31 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 32 42 43 39 31 39 42 43 46 46 34 31 30 39 38 34 34 45 31 36 38 33 32 38 30 45 42 34 44 43 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 32 42 45 41 39 3 5 45 41 46 45 31 31 46 41 36 33 43 44 45 34 31 42 33 45 41 43 32 35 31 36 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 32 43 35 39 32 37 41 30 44 35 45 46 34 33 37 45 42 44 43 32 46 39 39 30 30 42 34 37 39 46 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 32 44 30 39 30 42 39 45 45 38 45 42 33 31 38 37 35 39 41 44 41 36 42 45 43 39 44 37 41 35 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c Data Ascii: rdf:li>1294327AE762E82FFA8C88506EDF421B</rdf:li> <rdf:li>12BC919BCFF4109844E1683280EB4DC 7</rdf:li> <rdf:li>12BEA95EAFE11FA63CDE41B3EAC2516F</rdf:li> <rdf:li>12C5927A0D5EF437EBDC2F9900B479F 6</rdf:li> <rdf:li>12D090B9DE8EB318759ADA6BEC9D7A56</rdf:li> <rdf:li>
2022-04-08 08:02:42 UTC	1755	IN	Data Raw: 45 32 43 30 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 30 43 41 38 36 34 31 31 36 36 32 38 34 43 41 42 46 31 35 44 43 39 43 45 37 38 46 45 44 33 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 30 44 32 36 39 38 37 31 39 35 42 37 31 45 34 30 41 32 35 39 38 45 43 45 36 35 36 38 32 43 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 30 44 37 33 41 46 35 32 45 41 35 44 32 38 35 30 38 35 31 38 38 44 41 46 31 33 36 46 44 36 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 30 44 43 32 33 40 41 31 43 37 33 40 41 46 36 37 45 35 32 31 34 34 43 33 39 44 32 46 38 43 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 30 45 32 44 36 46 43 42 39 39 46 39 39 34 33 32 46 41 42 32 44 36 32 42 34 36 39 42 42 46 30 Data Ascii: E2C01</rdf:li> <rdf:li>20CA8641166284CABF15DC9CE78FED38</rdf:li> <rdf:li>20D26987195B71E 40A2598ECE65682C4</rdf:li> <rdf:li>20D73AF52EA5D285085188DAF136FD6E</rdf:li> <rdf:li>20DC230A1C730AF 67E52144C39D2F8CA</rdf:li> <rdf:li>20E2D6FCB99F99432FAB2D62B469BBF0
2022-04-08 08:02:42 UTC	1762	IN	Data Raw: 32 31 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 37 31 31 34 41 34 32 32 32 41 31 37 32 34 37 32 34 33 46 31 38 31 35 46 38 42 31 44 33 35 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 37 31 36 32 45 33 46 34 36 36 46 32 37 30 36 37 31 34 45 44 37 45 38 37 44 44 36 38 35 44 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 37 31 42 46 36 31 39 46 33 45 36 38 45 37 38 30 39 46 35 34 32 38 46 45 34 41 44 42 46 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 37 32 43 41 31 34 39 41 33 32 31 36 42 43 42 33 38 39 39 31 41 42 37 42 34 34 35 35 42 33 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 37 35 44 37 44 45 45 38 31 42 42 35 30 34 31 35 34 46 30 38 44 36 30 31 34 35 46 42 36 35 43 43 42 3c Data Ascii: 211</rdf:li> <rdf:li>27114A4222A17247243F1815F8B1D351</rdf:li> <rdf:li>27162E3F466F27067 14ED7E87DDF85D0</rdf:li> <rdf:li>271BF619F3E68E7809F545B8FE4ADBFC</rdf:li> <rdf:li>272CA149A3216BCB3 8991AB7B4455B39</rdf:li> <rdf:li>275D7DEE81BB504154F08D60145FB65C</
2022-04-08 08:02:42 UTC	1778	IN	Data Raw: 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 33 32 42 45 46 33 38 32 33 45 45 31 32 35 36 31 43 31 39 42 44 35 42 35 38 33 32 35 33 31 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 33 32 43 44 46 45 32 37 38 38 30 42 35 45 34 31 31 37 37 45 36 31 35 32 45 44 39 31 39 45 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 33 32 44 32 42 30 30 43 36 37 33 45 33 42 42 35 45 30 32 44 43 44 30 37 33 41 31 33 34 35 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 33 36 38 46 32 42 44 34 35 36 38 36 38 43 33 37 36 32 36 35 39 38 46 37 38 30 39 43 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 33 33 45 43 31 45 38 44 42 39 30 45 46 42 42 36 37 38 33 36 36 41 32 44 32 35 33 36 42 41 41 3c 2f 72 64 66 3a 6c Data Ascii: rdf:li> <rdf:li>332BEF3823EE12561C19BD5B58325314</rdf:li> <rdf:li>332CDFE27880B5E41177E6 152ED919ED</rdf:li> <rdf:li>332D2B00C673E3BB5E02DCD073A13459</rdf:li> <rdf:li>33368F2BBD456868C37626 598F7809C9</rdf:li> <rdf:li>333EC1E8DB90EFBB678366A2D2536BAA</rdf:li>
2022-04-08 08:02:42 UTC	1794	IN	Data Raw: 33 34 42 37 32 43 33 32 37 45 44 35 33 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 30 39 31 38 33 34 38 30 44 39 41 30 45 35 36 38 35 37 37 32 42 38 44 46 45 38 35 42 36 37 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 30 39 32 39 38 43 38 31 43 45 31 30 39 35 46 42 34 34 35 37 36 34 36 34 45 37 42 44 35 45 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 30 39 45 43 42 31 35 41 35 36 37 45 44 34 45 35 39 45 39 35 4 5 36 31 46 39 45 32 43 37 37 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 30 41 31 36 34 43 36 34 31 36 36 44 33 36 42 39 43 41 45 36 42 37 36 30 30 37 36 41 39 35 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 30 42 32 45 44 44 34 36 37 30 41 41 32 32 31 46 34 42 44 46 36 44 Data Ascii: 34B72C327ED53D</rdf:li> <rdf:li>409183480D9A0E5685772B8DFE85B67D</rdf:li> <rdf:li>409298 C81CE1095FB44576464E7BD5EF</rdf:li> <rdf:li>409ECB15A567ED4E59E95E61F9E2C775</rdf:li> <rdf:li>40A164 C64166D36B9CAE6B760076A959</rdf:li> <rdf:li>40B2EDD4670AA221F4BDF6D
2022-04-08 08:02:42 UTC	1802	IN	Data Raw: 43 42 35 39 32 30 46 31 41 42 30 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 37 30 41 41 38 45 39 45 44 31 31 30 30 36 37 32 36 38 34 36 33 33 44 30 36 41 43 43 38 30 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 37 31 38 45 35 44 35 36 36 30 35 31 43 46 43 33 39 38 31 30 44 35 42 36 37 41 42 46 44 31 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 37 32 33 45 35 41 39 32 36 44 41 37 33 45 37 39 37 45 36 42 32 30 45 37 44 36 34 38 38 34 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 37 32 42 46 45 41 46 30 31 38 32 41 38 38 46 45 43 42 44 36 44 35 36 41 39 30 32 41 37 42 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 37 33 31 41 38 33 37 43 44 45 33 41 30 44 43 45 38 31 37 46 31 36 43 31 Data Ascii: CB5920F1AB07</rdf:li> <rdf:li>470AA8E9ED1100672684633D06ACC808</rdf:li> <rdf:li>4718E5D5 66051CFC39810D5B67ABFD14</rdf:li> <rdf:li>4723E5A926DA73E797E6B20E7D648844</rdf:li> <rdf:li>472BFEAF 0182A88FECBD6D56A902A7B3</rdf:li> <rdf:li>4731A837CDE3A0DCE817F16C1
2022-04-08 08:02:42 UTC	1810	IN	Data Raw: 46 45 36 38 37 46 36 44 43 30 45 34 45 43 44 33 35 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 44 41 36 35 45 38 34 42 45 45 37 36 43 46 35 31 44 37 46 37 38 41 36 39 36 37 31 43 31 39 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 44 42 34 31 44 31 37 38 45 44 32 37 36 31 43 32 36 45 34 36 33 34 34 44 39 45 41 46 42 44 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 44 42 37 44 39 38 37 30 34 44 37 30 43 34 30 4 6 32 42 41 32 36 31 39 46 39 37 35 35 42 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 44 42 45 35 39 31 33 34 33 46 36 31 36 44 36 33 38 38 45 31 35 37 46 31 42 44 43 33 39 32 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 44 43 37 38 43 31 31 35 39 41 38 31 43 42 37 Data Ascii: FE687F6DC0E4ECD357</rdf:li> <rdf:li>4DA65E84BEE76CF51D7F78469671C19A</rdf:li> <rdf:li>4D B41D178ED2761C26E46344D9EAFB4B</rdf:li> <rdf:li>4DB7D989704D70C40F2BA2619F9755B0</rdf:li> <rdf:li>4D BE591343F616D6388E157F1BDC3921</rdf:li> <rdf:li>4DC0D378C1159A81CB7

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	2446	IN	Data Raw: 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 31 66 35 32 34 63 32 63 2d 64 39 36 38 2d 31 31 65 34 2d 61 33 38 31 2d 65 61 36 61 34 65 65 61 35 36 62 61 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 31 66 39 37 64 34 35 33 2d 33 66 35 62 2d 31 31 64 61 2d 62 36 64 31 2d 64 66 66 65 39 65 36 32 34 34 63 31 3c 2f 72 64 66 6a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 31 66 64 65 62 34 37 62 2d 64 64 33 61 2d 31 31 37 38 2d 61 32 30 64 2d 61 66 32 65 66 39 63 31 39 37 64 66 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6 f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 32 30 Data Ascii: li>adobe:docid:photoshop:1f524c2c-d968-11e4-a381-ea6a4eea56ba</rdf:li> <rdf:li>adobe:docid:photosh op:1f97d453-3f5b-11da-b6d1-dffe9e6244c1</rdf:li> <rdf:li>adobe:docid:photoshop:1fdeb47b-dd3a-1178-a20d-af2ef9c 197df</rdf:li> <rdf:li>adobe:docid:photoshop:20
2022-04-08 08:02:42 UTC	2478	IN	Data Raw: 39 35 33 36 2d 63 65 65 36 38 66 31 63 65 36 32 62 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 34 63 33 65 64 66 37 31 2d 64 36 34 31 2d 31 31 64 62 2d 62 62 38 31 2d 66 65 39 31 66 32 33 32 30 36 31 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 34 63 34 61 37 33 63 39 2d 33 31 61 61 2d 31 31 64 61 2d 38 37 34 64 2d 61 62 31 66 63 30 32 66 39 33 63 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 34 63 39 32 39 30 62 61 2d 34 34 38 36 2d 33 39 34 64 2d 39 61 30 38 2d 32 39 35 65 32 30 34 63 36 36 37 35 3c 2f 72 64 66 3a 6c 69 3e 20 Data Ascii: 9536-cee68f1ce62b</rdf:li> <rdf:li>adobe:docid:photoshop:4c3edf71-d641-11db-bb81-fe91f2320614</rdf:li> <rdf:li>adobe:docid:photoshop:4c4a73c9-31aa-11da-874d-ab1fc02f93c4</rdf:li> <rdf:li>adobe:docid:photoshop:4c9290ba-4486-394d-9a08-295e204c6675</rdf:li>
2022-04-08 08:02:42 UTC	2486	IN	Data Raw: 68 6f 74 6f 73 68 6f 70 3a 36 34 38 36 66 64 33 31 2d 39 62 38 35 2d 31 31 65 36 2d 61 39 66 66 2d 38 64 36 36 35 36 65 64 37 65 61 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 36 34 63 35 61 37 31 36 2d 66 63 37 37 2d 64 39 34 65 2d 62 35 35 61 2d 64 61 37 61 31 39 39 35 65 36 34 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 36 35 36 66 35 34 30 32 2d 64 63 36 38 2d 31 66 34 39 2d 35 36 35 2d 35 36 37 35 39 31 30 32 62 65 66 62 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 36 35 38 62 33 32 35 63 2d 31 62 33 39 2d 31 31 65 38 Data Ascii: hotoshop:6486fd31-9b85-11e6-a9ff-8d6656ed7ea9</rdf:li> <rdf:li>adobe:docid:photoshop:64c5a716-fc77-d94e-b55a-da7a1995e645</rdf:li> <rdf:li>adobe:docid:photoshop:656f5402-dc68-1f49-8555-56759102befb</rdf:li> <rdf:li>adobe:docid:photoshop:658b325c-1b39-11e8
2022-04-08 08:02:42 UTC	2502	IN	Data Raw: 39 66 32 30 32 2d 62 35 30 39 2d 31 31 64 64 2d 38 32 32 36 2d 64 61 39 34 39 34 38 37 36 37 33 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 37 39 38 64 63 65 33 33 2d 66 63 34 35 2d 31 31 65 36 2d 62 66 62 30 2d 38 64 61 32 39 32 34 62 66 33 62 62 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 37 39 38 64 63 65 33 33 2d 66 63 34 35 2d 31 31 65 36 2d 62 66 62 30 2d 38 64 61 32 39 32 34 62 66 33 62 62 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 37 39 64 30 61 66 34 32 2 d 61 65 39 35 2d 31 31 64 61 2d 62 61 62 63 2d 39 63 30 64 65 64 Data Ascii: 9f202-b509-11dd-8226-da9498476732</rdf:li> <rdf:li>adobe:docid:photoshop:798dce33-fc45-11e6-bfb0-8 da2924bf3bb</rdf:li> <rdf:li>adobe:docid:photoshop:79cb2007-a70a-d640-bb8c-0454cb ee7cf9</rdf:li> <rdf:li>adobe :docid:photoshop:79d0af42-ae95-11da-babc-9c0ded
2022-04-08 08:02:42 UTC	2530	IN	Data Raw: 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 61 62 64 31 32 37 63 39 2d 38 34 31 33 2d 31 31 37 62 2d 62 37 36 66 2d 62 63 35 62 38 63 31 34 62 66 39 62 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 61 63 33 36 32 61 62 32 2d 30 33 63 64 2d 31 31 65 36 2d 61 34 32 62 2d 38 39 39 65 63 30 31 30 38 66 36 65 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 61 63 37 30 30 33 37 34 2d 38 65 31 62 2d 31 31 37 37 2d 61 38 33 63 2d 63 31 62 62 63 63 30 63 30 36 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f Data Ascii: rdf:li>adobe:docid:photoshop:abd127c9-8413-117b-b76f-bc5b8c14bf9b</rdf:li> <rdf:li>adobe:docid:pho toshop:ac362ab2-03cd-11e6-a42b-899ec0108f6e</rdf:li> <rdf:li>adobe:docid:photoshop:ac700374-8e1b-1177-a83c-c1b bcc0c0065</rdf:li> <rdf:li>adobe:docid:photosho
2022-04-08 08:02:42 UTC	2546	IN	Data Raw: 38 2d 31 31 64 63 2d 61 35 32 37 2d 63 36 64 63 32 30 32 31 34 61 65 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 65 31 38 63 30 66 35 61 2d 39 36 37 38 2d 31 31 37 61 2d 62 62 61 33 2d 65 37 61 64 63 38 61 63 35 63 61 66 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 65 31 63 35 32 38 37 30 2d 34 61 39 65 2d 31 31 37 38 2d 61 32 34 63 2d 66 31 30 32 63 35 38 30 64 64 32 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 65 32 33 31 31 65 31 32 2d 38 65 64 30 2d 32 30 34 38 2d 62 39 35 62 2d 38 33 39 66 63 33 64 30 36 65 30 30 3c 2f 72 Data Ascii: 8-11dc-a527-c6dc20214ae7</rdf:li> <rdf:li>adobe:docid:photoshop:e18c0f5a-9678-117a-bba3-e7adc8ac5c af</rdf:li> <rdf:li>adobe:docid:photoshop:e1c52870-4a9e-1178-a24c-f102c580dd27</rdf:li> <rdf:li>adobe:docid:ph otoshop:e2311e12-8ed0-2048-b95b-839fc3d06e00</r
2022-04-08 08:02:42 UTC	2569	IN	Data Raw: 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 66 37 61 36 34 39 33 61 2d 31 61 64 32 2d 31 31 65 35 2d 62 32 33 66 2d 61 66 34 32 32 34 65 36 32 64 31 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 66 37 64 39 33 30 64 64 2d 34 35 62 63 2d 31 31 65 36 2d 62 65 62 35 2d 64 65 39 61 62 62 62 65 32 64 38 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 66 37 66 65 33 31 33 63 2d 63 64 66 64 2d 31 31 65 35 2d 38 33 34 34 2d 65 38 64 39 33 37 30 32 37 37 66 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 66 38 30 34 37 37 37 32 2d 39 65 Data Ascii: docid:photoshop:f7a6493a-1ad2-11e5-b23f-af4224e62d18</rdf:li> <rdf:li>adobe:docid:photoshop:f7d930dd-45bc-11e6-beb5-de9abbbe2d87</rdf:li> <rdf:li>adobe:docid:photoshop:f7fe313c-c4fd-11e5-8344-e8d9370277f7</rdf:li> <rdf:li>adobe:docid:photoshop:f8047772-9e
2022-04-08 08:02:42 UTC	2585	IN	Data Raw: 69 3e 75 75 69 64 3a 32 44 34 30 37 31 34 30 42 42 36 30 44 45 31 31 42 32 30 31 43 34 30 33 34 34 39 33 32 37 39 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 32 44 36 39 32 36 43 45 46 44 43 30 31 31 44 43 41 34 41 39 43 43 34 41 45 34 46 30 30 41 36 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 7 5 69 64 3a 32 44 36 45 37 41 32 37 35 41 38 37 44 46 31 31 42 31 35 45 39 44 43 45 41 31 43 45 41 30 41 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 32 45 30 38 37 41 34 33 34 45 37 46 44 44 31 31 42 45 33 38 46 42 38 44 36 45 37 36 38 34 35 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 32 45 30 44 43 43 32 43 46 35 41 33 44 45 31 31 38 31 44 44 46 45 46 30 44 36 30 39 Data Ascii: i>uuid:2D407140BB60DE11B201C40344932790</rdf:li> <rdf:li>uuid:2D6926CEFD0C11DCA4A9CC4AE4 F00A67</rdf:li> <rdf:li>uuid:2D6E7A275A87DF11B15E9DCEA1CEA0A9</rdf:li> <rdf:li>uuid:2E087A434E7FDD11 BE38FB8D6E76845C</rdf:li> <rdf:li>uuid:2E0DCC2CF5A3DE1181DDFEF0D609

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:43 UTC	3705	IN	Data Raw: 36 66 2d 34 31 34 34 2d 38 36 38 31 2d 63 32 32 66 64 35 63 62 35 36 38 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 32 62 65 33 36 32 37 2d 37 64 30 31 2d 34 64 33 32 2d 38 37 61 36 2d 32 39 30 39 39 32 64 62 61 32 63 65 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 32 63 64 31 34 38 63 2d 37 36 35 61 2d 34 64 39 65 2d 61 63 34 35 2d 61 35 38 34 39 63 62 31 63 37 61 65 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 33 31 39 35 30 66 34 3d 65 62 31 35 2d 64 37 34 66 2d 38 38 64 39 2d 38 38 61 61 65 66 37 32 61 32 63 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 33 32 62 34 39 36 39 2d 38 38 39 35 2d 31 39 34 64 Data Ascii: 6f-4144-8681-c22fd5cb5683</rdf:li> <rdf:li>xmp.did:12be3627-7d01-4d32-87a6-290992dba2ce</rdf:li> <rdf:li>xmp.did:12cd148c-765a-4d9e-ac45-a5849cb1c7ae</rdf:li> <rdf:li>xmp.did:131950f4-eb15-d74f-88d9-88aaef72a2c0</rdf:li> <rdf:li>xmp.did:132b4969-8895-194d
2022-04-08 08:02:43 UTC	3721	IN	Data Raw: 30 37 36 33 34 2d 30 66 64 37 2d 66 32 34 64 2d 61 31 63 61 2d 31 65 63 34 38 61 65 31 33 39 33 62 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 33 35 33 38 63 65 62 2d 61 35 37 64 2d 34 33 35 38 2d 39 62 64 33 2d 33 34 32 63 31 38 63 37 35 63 39 64 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 33 35 64 37 31 34 34 2d 32 65 38 63 2d 34 36 66 62 2d 38 38 61 39 2d 33 62 38 31 64 32 33 61 62 63 64 66 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 33 36 38 42 39 34 31 42 35 32 35 36 38 31 31 38 32 32 41 46 44 38 45 36 43 42 44 39 38 43 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 33 37 41 36 36 38 39 34 41 32 30 36 38 Data Ascii: 07634-0fd7-f24d-a1ca-1ec48ae1393b</rdf:li> <rdf:li>xmp.did:23538ceb-a57d-4358-9bd3-342c18c75c9d</rdf:li> <rdf:li>xmp.did:235d7144-2e8c-46fb-88a9-3b81d23abdcf</rdf:li> <rdf:li>xmp.did:2368B941B5256811822AFD8E6CBD98C8</rdf:li> <rdf:li>xmp.did:237A66894A2068
2022-04-08 08:02:43 UTC	3737	IN	Data Raw: 65 34 2d 36 39 64 36 32 31 38 35 63 64 36 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 32 32 38 42 46 38 33 32 43 32 30 36 38 31 31 38 30 38 33 38 31 45 35 37 38 38 43 33 35 33 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 32 33 33 30 36 38 43 39 38 32 30 36 38 31 31 38 30 38 33 41 32 42 36 43 32 38 33 31 33 43 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 32 34 38 37 36 45 42 46 31 36 42 45 30 31 31 39 45 36 39 45 38 35 34 32 42 41 31 46 35 31 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 32 36 44 44 31 30 37 30 42 32 30 36 38 31 31 42 34 42 43 43 32 41 38 45 42 43 37 38 31 33 35 3c 2f 72 64 66 3a 6c 69 Data Ascii: e4-69d62185cd61</rdf:li> <rdf:li>xmp.did:3228BF832C206811808381E5788C353D</rdf:li> <rdf:li>xmp.did:3233068C982068118083A2B6C28313CA</rdf:li> <rdf:li>xmp.did:324876EBF16BE0119E69E854BBA1F514</rdf:li> <rdf:li>xmp.did:326DD1070B206811B4BCC2A8EBC78135</rdf:li>
2022-04-08 08:02:43 UTC	3744	IN	Data Raw: 3e 78 6d 70 2e 64 69 64 3a 33 38 41 32 42 38 32 44 35 39 32 31 36 38 31 31 38 44 42 42 42 41 35 30 33 32 37 39 38 31 34 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 38 41 36 38 39 39 31 41 44 44 39 45 33 31 31 39 41 43 30 46 38 31 45 34 43 41 34 43 41 41 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 38 41 37 42 38 39 33 46 41 32 34 36 38 31 31 42 37 35 42 41 39 35 30 34 31 39 32 39 38 42 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 38 43 31 39 38 33 45 43 45 32 31 36 38 31 31 39 35 46 45 44 33 33 42 46 43 34 32 30 43 42 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 38 45 34 45 31 32 31 32 30 33 34 31 31 Data Ascii: >xmp.did:38A2B82D592168118DBBBA5032798148</rdf:li> <rdf:li>xmp.did:38A68991ADD9E3119AC0F81E4CA4CAAE</rdf:li> <rdf:li>xmp.did:38A7B893FA246811B75BA950419298B8</rdf:li> <rdf:li>xmp.did:38C1983ECE21681195FED33BFC420CB1</rdf:li> <rdf:li>xmp.did:38E4E121203411
2022-04-08 08:02:43 UTC	3760	IN	Data Raw: 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 37 36 43 32 45 35 41 39 45 39 45 44 46 31 31 42 37 35 38 45 30 39 35 32 32 44 30 44 30 33 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 37 38 35 31 31 44 33 30 43 32 30 36 38 31 31 41 46 46 44 41 45 46 42 31 32 31 46 45 33 39 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 37 38 35 39 34 41 36 30 42 32 30 36 38 31 31 38 30 38 33 45 32 34 31 32 30 39 39 43 45 44 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 37 42 31 46 44 34 30 41 32 32 31 36 38 31 31 39 37 34 45 46 31 32 34 46 34 45 38 34 32 37 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 37 42 35 39 31 36 41 35 42 32 Data Ascii: :li>xmp.did:476C2E5A9E9EDF11B758E09522D0D034</rdf:li> <rdf:li>xmp.did:478511D30C206811AFFDAEFB121FE394</rdf:li> <rdf:li>xmp.did:478594A60B2068118083E2412099CEDA</rdf:li> <rdf:li>xmp.did:47B1FD40A2216811974EF124F4E8427B</rdf:li> <rdf:li>xmp.did:47B5916A5B2
2022-04-08 08:02:43 UTC	3776	IN	Data Raw: 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 36 34 30 45 36 43 43 34 35 32 30 36 38 31 31 38 46 36 32 41 45 43 44 39 35 33 31 39 32 30 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 36 35 36 46 44 42 38 32 34 39 32 45 32 31 31 42 33 45 45 44 42 30 43 42 38 36 38 44 44 39 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 36 36 45 46 46 46 36 34 32 32 30 36 38 31 31 42 36 39 39 45 38 38 35 33 45 42 42 42 43 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 36 37 42 46 31 32 38 30 44 32 30 36 38 31 31 38 41 36 44 43 36 33 38 46 39 46 43 39 35 45 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 36 38 30 31 39 34 39 30 39 32 Data Ascii: :li>xmp.did:5640E6CC452068118F62AEC95319209</rdf:li> <rdf:li>xmp.did:5656FDB82492E211B3EEDB0CB8688D94</rdf:li> <rdf:li>xmp.did:566EFFF642206811B699E88853EBBBC7</rdf:li> <rdf:li>xmp.did:567BF1280D2068118A6DC638F9FC95EE</rdf:li> <rdf:li>xmp.did:56801949092
2022-04-08 08:02:43 UTC	3784	IN	Data Raw: 32 2d 39 30 34 37 2d 38 34 63 31 2d 37 39 34 30 37 64 32 37 63 39 32 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 63 63 37 31 37 63 36 2d 30 64 31 66 2d 34 66 30 31 2d 62 35 62 65 2d 66 30 34 31 66 30 64 64 65 38 62 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 63 63 65 36 32 38 35 2d 66 38 63 64 2d 63 32 34 66 2d 38 30 61 39 2d 62 36 65 38 31 62 61 38 62 63 32 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 63 64 66 38 38 30 34 2d 66 63 64 63 2d 34 66 34 36 2d 38 38 65 32 2d 38 62 32 34 31 36 63 62 39 62 38 65 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 63 65 36 62 37 32 66 2d 37 37 63 63 2d 35 62 34 39 2d Data Ascii: 2-9047-84c1-79407d27c922</rdf:li> <rdf:li>xmp.did:5cc717c6-0d1f-4f01-b5be-f041f0dde8b0</rdf:li> <rdf:li>xmp.did:5cce6285-f8cd-c24f-80a9-b6e81ba8bc25</rdf:li> <rdf:li>xmp.did:5cdf8804-fc4c-4f46-88e2-8b2416cb9b8e</rdf:li> <rdf:li>xmp.did:5ce6b72f-77cc-5b49-
2022-04-08 08:02:43 UTC	3792	IN	Data Raw: 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 36 31 44 42 34 37 36 39 34 32 35 36 38 31 31 38 43 31 34 41 43 31 44 45 42 38 46 45 32 42 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 36 32 43 38 33 35 45 45 37 32 31 36 38 31 31 38 43 31 34 41 33 36 45 35 36 36 45 31 32 44 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 36 45 46 46 34 36 34 63 36 33 32 33 2d 61 64 36 36 2d 34 36 37 30 2d 61 39 34 39 2d 65 61 33 31 31 34 32 35 32 63 35 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 36 35 38 45 33 43 41 32 35 32 30 36 38 31 31 39 32 42 30 42 37 38 35 43 34 31 34 44 38 36 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 Data Ascii: > <rdf:li>xmp.did:661DB476942568118C14AC1DEB8FE2BE</rdf:li> <rdf:li>xmp.did:662C835EE72168118C14A36E566E12DA</rdf:li> <rdf:li>xmp.did:664c6323-ad66-4670-a949-ea3114252c52</rdf:li> <rdf:li>xmp.did:6658E3CA2520681192B0B785C414D861</rdf:li> <rdf:li>xmp.did:6

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:43 UTC	3808	IN	Data Raw: 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 34 43 39 46 38 36 33 35 38 37 39 45 34 31 31 42 41 37 42 46 44 34 37 36 35 30 35 38 34 38 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 34 43 41 37 36 33 34 31 45 30 43 45 34 31 31 39 37 46 32 38 33 44 45 41 39 46 42 44 39 44 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 34 46 31 35 36 45 41 31 42 32 33 36 38 31 31 41 35 35 46 43 37 34 43 33 35 43 39 37 31 43 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 34 61 31 34 66 33 37 2d 33 65 62 36 2d 34 39 37 61 2d 38 61 34 32 2d 37 37 33 32 64 35 39 36 61 64 63 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 34 61 Data Ascii: <rdf:li>xmp.did:74C9F8635879E411BA7BFD476505848B</rdf:li> <rdf:li>xmp.did:74CA76341E0CE41197F283DEA9FBD9D1</rdf:li> <rdf:li>xmp.did:74F156EA1B236811A55FC74C35C971C2</rdf:li> <rdf:li>xmp.di d:74a14f37-3eb6-497a-8a42-7732d596adc3</rdf:li> <rdf:li>xmp.did:74a
2022-04-08 08:02:43 UTC	3824	IN	Data Raw: 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 34 62 32 65 33 66 39 2d 32 65 65 31 2d 34 34 34 2d 62 62 64 66 2d 34 37 30 32 36 36 66 39 31 66 31 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 34 66 35 38 35 62 32 2d 64 66 32 35 2d 63 38 34 30 2d 62 61 31 66 2d 61 66 38 35 65 35 32 35 30 66 33 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 34 66 63 61 65 39 35 2d 37 36 30 35 2d 61 61 34 63 2d 61 65 35 63 2d 65 61 65 39 62 66 66 30 63 33 39 64 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 35 30 32 35 30 30 38 2d 37 39 30 37 2d 34 35 66 38 2d 39 32 63 38 2d 35 65 36 38 37 36 38 31 36 37 30 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c Data Ascii: <rdf:li>xmp.did:84b2e3f9-2ee1-4444-bbdf-470266f91f16</rdf:li> <rdf:li>xmp.did:84f585b2-df25-c840-ba1f-af85e5250f31</rdf:li> <rdf:li>xmp.did:84fcae95-7605-aa4c-ae5c-eae9bff0c39d</rdf:li> <rdf:li>xmp.did:85025008-7907-4 5f8-92c8-5e6876816709</rdf:li> <rdf:li>
2022-04-08 08:02:43 UTC	3832	IN	Data Raw: 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 43 30 46 34 45 45 36 32 31 43 43 31 31 36 38 38 35 35 38 43 30 46 34 45 45 37 32 31 43 43 31 31 36 38 38 35 35 38 43 30 36 37 34 34 30 32 30 37 35 3c 2f 72 64 66 3a 6c 69 3 e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 43 31 33 31 42 43 44 32 30 33 33 31 31 45 35 39 39 46 44 38 33 30 32 39 33 42 38 46 45 41 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 43 31 39 35 37 32 36 37 42 32 32 36 38 31 31 39 31 30 39 44 35 42 34 41 30 43 34 39 35 45 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 43 32 44 34 46 37 31 Data Ascii: rdf:li>xmp.did:8C0F4EE621CC116888558C0674402075</rdf:li> <rdf:li>xmp.did:8C0F4EE721CC116 888558C0674402075</rdf:li> <rdf:li>xmp.did:8C131BCD203311E599FD830293B8FEAF</rdf:li> <rdf:li>xmp.did :8C1957267B2268119109D5B4A0C495E5</rdf:li> <rdf:li>xmp.did:8C2D4F71
2022-04-08 08:02:43 UTC	3848	IN	Data Raw: 37 46 44 38 34 45 33 43 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 39 39 34 35 35 41 38 37 31 34 32 30 36 38 31 31 39 37 41 35 38 34 46 38 33 39 32 37 42 33 38 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 39 39 35 61 66 63 66 62 2d 64 36 63 33 2d 33 33 34 31 2d 62 66 32 34 2d 37 61 64 30 35 62 35 37 30 61 63 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 4 3a 39 39 37 33 31 34 45 30 35 44 36 31 45 35 31 31 38 37 45 36 42 37 32 31 43 44 33 35 32 43 37 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 39 39 37 33 35 43 32 33 38 38 32 46 45 34 31 31 38 37 44 41 46 38 37 30 45 39 30 42 45 46 44 32 3c 2f 72 64 66 3a 6c 69 3e 20 Data Ascii: 7FD84E3C6</rdf:li> <rdf:li>xmp.did:99455A871420681197A584F83927B384</rdf:li> <rdf:li>xmp.did:995afcfb-d6c3-3341-bf24-7ad05b5790ac</rdf:li> <rdf:li>xmp.did:997314E05D61E51187E6B721CD352C7A</rdf:li> <rdf:li>xmp .did:99735C23882FE41187DAF870E90BEFD2</rdf:li>
2022-04-08 08:02:43 UTC	3864	IN	Data Raw: 43 39 41 46 45 45 32 39 44 30 42 45 33 31 31 38 41 33 32 46 45 41 44 35 37 32 32 39 46 36 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 41 38 32 46 31 35 43 31 34 32 30 36 38 31 31 41 36 31 33 44 42 32 36 39 46 45 46 35 32 34 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 41 43 42 33 38 30 30 32 41 34 35 44 45 33 31 31 38 31 45 36 45 42 46 38 33 38 32 41 38 41 46 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 41 43 42 36 39 31 36 36 33 45 32 30 36 38 31 31 42 41 41 43 39 46 38 38 39 42 35 38 43 44 33 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 41 44 30 34 46 37 45 34 43 32 31 36 38 31 31 38 32 32 41 46 41 39 46 Data Ascii: C9AFEE29D0BE3118A32FEAD57229F64</rdf:li> <rdf:li>xmp.did:ACAEEB8BA2206811A613DB269FEF524 D</rdf:li> <rdf:li>xmp.did:ACB38002A45DE31181E6EBF8382A8AFE</rdf:li> <rdf:li>xmp.did:ACB691663E20681 1BAAC9F889B58CD3E</rdf:li> <rdf:li>xmp.did:AD04F7E4CC216811822AFA9F
2022-04-08 08:02:43 UTC	3872	IN	Data Raw: 37 30 38 32 30 36 38 31 31 38 30 38 33 39 43 37 45 38 39 37 37 35 41 45 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 41 38 32 46 31 35 43 31 34 32 30 36 38 31 31 38 44 42 42 42 38 38 39 35 37 39 31 35 34 30 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 41 38 38 38 39 30 41 41 42 38 45 45 30 31 31 41 44 33 46 46 37 36 44 30 42 41 43 39 44 43 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 6 4 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 41 38 39 43 41 42 43 32 44 32 30 36 38 31 31 39 39 34 43 45 38 33 42 42 42 43 38 36 44 37 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 41 42 39 42 41 44 45 30 45 32 33 36 38 31 31 42 44 33 35 39 32 31 36 34 43 37 30 37 30 Data Ascii: 70820681180839CE89775AE4</rdf:li> <rdf:li>xmp.did:BA82F15C142068118DBBB8895791540D</rdf:li> <rdf:li>xmp.did:BA88890AAB8EE011AD3FF76D0BAC9DC8</rdf:li> <rdf:li>xmp.did:BA89CABC2D206811994CE 83BBBC86D74</rdf:li> <rdf:li>xmp.did:BAB9BADE0E236811BD3592164C7070
2022-04-08 08:02:43 UTC	3888	IN	Data Raw: 31 31 41 36 31 33 46 42 31 30 30 36 38 45 39 38 44 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 30 46 46 30 33 34 42 30 45 32 30 36 38 31 31 39 32 42 30 32 46 41 38 42 37 43 44 46 37 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 31 31 36 41 32 38 30 39 38 32 30 36 38 31 31 38 30 38 33 41 32 42 36 43 32 38 33 31 33 43 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6 d 70 2e 64 69 64 3a 44 31 33 41 41 45 35 46 43 46 37 30 45 37 31 31 42 36 35 31 45 35 46 46 36 34 45 45 33 32 38 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 31 35 34 33 34 31 30 30 39 32 30 36 38 31 31 38 30 38 33 38 43 33 30 35 44 43 41 39 45 38 39 3c 2f 72 64 66 Data Ascii: 11A613FB10068E98D9</rdf:li> <rdf:li>xmp.did:D0FF034B0E20681192B0B2FA8B7CDF71</rdf:li> <rdf:li>xmp. did:D116A280982068118083A2B6C28313CA</rdf:li> <rdf:li>xmp.did:D13AAE5FCF70E711B651E5FF64EE3282</rdf:li> <rdf:li>xmp.did:D15434A00920681180838C305DCA9E89</rdf
2022-04-08 08:02:43 UTC	3904	IN	Data Raw: 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 45 36 33 31 42 33 34 37 30 41 32 30 36 38 31 31 39 35 42 42 38 45 32 44 39 39 41 36 37 36 44 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 45 36 34 36 30 32 33 37 46 46 45 34 45 30 31 31 42 37 34 33 39 42 36 38 41 30 31 31 33 38 45 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 45 36 34 41 43 38 44 37 30 44 45 31 44 45 31 31 39 33 43 37 38 41 33 37 37 46 33 30 38 31 33 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 45 36 35 44 32 42 41 46 39 37 32 30 36 38 31 31 38 46 36 32 38 34 35 32 38 35 44 33 33 43 35 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 45 36 36 36 46 39 46 Data Ascii: <rdf:li>xmp.did:E631B3470A20681195BB8E2D99A676D6</rdf:li> <rdf:li>xmp.did:E6460237FFE4E0 11B7439B68A01138EA</rdf:li> <rdf:li>xmp.did:E64AC8D70DE1DE1193C78A377F30813B</rdf:li> <rdf:li>xmp.di d:E65D2BAF972068118F62845285D33C56</rdf:li> <rdf:li>xmp.did:E666F9F

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:43 UTC	3911	IN	Data Raw: 69 3e 78 6d 70 2e 64 69 64 3a 46 33 33 45 39 30 34 34 44 39 42 39 44 46 31 31 41 35 44 41 45 33 34 33 31 44 35 42 35 43 31 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 33 34 36 46 39 37 43 31 34 32 30 36 38 31 31 39 31 30 39 42 36 44 42 34 38 45 39 31 38 30 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 33 35 37 34 43 34 38 46 42 34 30 45 30 31 31 42 44 43 44 41 36 44 37 45 33 44 44 46 42 39 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 33 36 34 46 42 43 44 38 32 34 36 38 31 31 39 35 46 45 46 31 37 37 45 35 34 44 38 38 39 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 33 38 33 38 31 39 35 33 44 32 30 45 Data Ascii: i>xmp.did:F33E9044D9B9DF11A5DAE3431D5B5C13</rdf:li> <rdf:li>xmp.did:F346F97C142068119109B6DB48E91803</rdf:li> <rdf:li>xmp.did:F3574C48FB40E011BDCDA6D7E3DDFB97</rdf:li> <rdf:li>xmp.did:F3652FBCD824681195FEF177E54D889B</rdf:li> <rdf:li>xmp.did:F38381953D20E
2022-04-08 08:02:43 UTC	3919	IN	Data Raw: 31 31 41 37 42 41 41 30 33 36 33 36 38 41 45 43 30 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 37 37 46 31 31 37 34 30 37 32 30 36 38 31 31 41 37 42 41 44 32 31 44 44 42 41 37 33 37 38 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 37 46 31 31 37 34 30 37 32 30 36 38 31 31 41 39 33 41 45 45 33 45 32 32 39 46 43 38 46 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 37 37 46 31 31 37 34 30 37 32 30 36 38 31 31 41 39 36 31 43 30 43 34 33 33 35 44 34 37 45 42 3c 2f 72 64 66 Data Ascii: 11A7BAA036368AEC0C</rdf:li> <rdf:li>xmp.did:F77F117407206811A7BAD21DDBA7378B</rdf:li> <rdf:li>xmp.did:F77F117407206811A86AE54FB880DE8</rdf:li> <rdf:li>xmp.did:F77F117407206811A93AEE3E229FC8F5</rdf:li> <rdf:li>xmp.did:F77F117407206811A961C0C4335D47EB</rdf
2022-04-08 08:02:43 UTC	3935	IN	Data Raw: 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 46 37 46 31 31 37 34 30 37 32 30 36 38 31 31 42 43 43 32 39 42 46 33 44 44 36 35 33 34 45 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 46 38 35 31 39 36 45 32 41 32 30 36 38 31 31 38 41 43 34 39 41 39 45 34 43 44 35 45 39 43 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 46 39 39 33 31 32 41 43 30 32 30 36 38 31 31 39 39 34 43 45 38 33 42 42 42 43 38 36 44 37 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 46 38 46 39 37 30 41 32 30 36 38 31 31 38 30 38 33 43 44 46 44 46 39 42 33 35 31 30 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 46 37 37 33 44 Data Ascii: <rdf:li>xmp.did:FF7F117407206811BCC29BF3DD6534EB</rdf:li> <rdf:li>xmp.did:FF85196E2A2068118AC49AE4CD5E9C2</rdf:li> <rdf:li>xmp.did:FF99312AC0206811994CE83BBBC86D74</rdf:li> <rdf:li>xmp.did:FFCF8F970A2068118083CDFDF9B3510D</rdf:li> <rdf:li>xmp.did:FFF573D
2022-04-08 08:02:43 UTC	3951	IN	Data Raw: 64 61 39 30 38 2d 36 63 34 31 2d 34 36 32 39 2d 39 38 38 39 2d 32 65 35 30 36 62 30 61 32 34 32 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 64 30 63 36 38 38 65 33 2d 62 30 66 63 2d 65 30 34 64 2d 62 38 35 34 2d 33 30 66 31 66 35 38 30 34 37 61 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 64 30 64 61 33 33 64 38 2d 36 37 32 36 2d 62 34 32 2d 39 37 39 34 2d 35 37 63 66 34 64 3e 2d 33 31 65 62 64 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 64 30 66 66 66 33 66 63 2d 62 61 61 36 2d 31 33 34 31 2d 62 39 35 66 2d 62 61 66 34 61 32 34 30 31 34 36 63 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 64 31 35 34 30 35 37 63 2d 33 Data Ascii: da908-6c41-4629-9889-2e506b0a2427</rdf:li> <rdf:li>xmp.did:d0c688e3-b0fc-e04d-b854-30f1f58047a5</rdf:li> <rdf:li>xmp.did:d0da33d8-6726-b542-9794-57e6f4b31ebd</rdf:li> <rdf:li>xmp.did:d0fff3fc-baa6-1341-b95f-baf4a240104f</rdf:li> <rdf:li>xmp.did:d154057c-3
2022-04-08 08:02:43 UTC	3959	IN	Data Raw: 61 37 61 64 2d 38 36 36 37 39 62 36 37 37 64 62 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 65 38 61 33 36 65 31 63 2d 64 66 32 32 2d 34 62 39 66 2d 62 63 66 35 2d 64 37 31 37 62 38 62 35 39 63 64 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 65 38 62 36 32 65 64 37 2d 65 38 66 65 2d 30 38 34 63 2d 62 36 65 33 2d 66 62 36 37 63 36 33 31 62 37 34 65 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 65 38 64 30 61 37 64 37 2d 31 37 38 65 2d 34 30 61 39 2d 61 38 63 35 2d 36 34 30 66 31 39 66 35 30 36 65 64 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 65 39 31 62 35 64 33 30 2d 39 36 37 37 2d 34 65 34 62 2d 39 37 38 66 2d 39 62 Data Ascii: a7ad-86679b6777db</rdf:li> <rdf:li>xmp.did:e8a36e1c-df22-4b9f-bcf5-d717b8b59cd7</rdf:li> <rdf:li>xmp.did:e8b62ed7-e8fe-084c-b6e3-fb67c631b74e</rdf:li> <rdf:li>xmp.did:e8d0a7d7-178e-40a9-a8c5-640f19f506ed</rdf:li> <rdf:li>xmp.did:e91b5d30-9677-4e4b-978f-9b
2022-04-08 08:02:43 UTC	3975	IN	Data Raw: af 5c ae 72 a1 b2 53 8b 2d 26 19 27 2b 56 66 4a 90 7d c7 d9 1f d9 9a ec 99 49 08 b4 6d dd 88 d4 3d 62 80 f1 b5 51 c9 8e d5 66 fd 93 5f da cc 31 96 90 9a 36 85 63 a4 92 c5 58 b8 00 ee 01 15 03 e2 e3 94 9c 92 99 a6 4c 7a f6 56 79 8c f1 82 80 d4 aa 8f e3 ef 9b 0c 70 ef 40 09 64 1a a4 b0 48 15 87 c2 09 aa d3 c7 ed 6f 99 47 18 21 35 68 8b dd 46 5b b2 f1 46 b5 8d d4 28 a9 a5 29 91 84 38 54 04 15 b5 8b 7d 8d 83 e6 54 a4 95 79 b4 96 51 40 f5 71 d0 76 c0 26 a8 17 0b 09 2b 4f 8b a1 a7 be 5a a8 b8 65 8b d2 fb 20 52 b4 07 c7 2b a5 50 bb b9 37 00 48 8b 42 3f 8f 86 4c 05 43 c3 20 46 02 b4 23 c7 2c 4a 62 f2 73 01 01 04 56 a7 6d fe fc 0a 86 22 af c8 ee d5 fb 86 15 57 b8 89 99 36 20 53 76 f1 c8 da a9 d9 d9 b9 e5 2f 44 50 3e 2f 1c 8c a4 94 4c ce 19 81 5f b0 07 7e ff 00 2c Data Ascii: lrS-&+VfJ]lm=bQf_16cXLzVyp@dHoG!5hF[F{0T}TyQ@qv&+OZe R+P7H8?LC F#,JbsVm"W6 Sv/DP>/L_-,
2022-04-08 08:02:43 UTC	3991	IN	Data Raw: 8b 08 64 84 6b 13 ea 04 9c 90 2b b8 02 a7 db 0a 50 4e 7d 37 24 2d 56 b4 df 12 84 44 36 ce 50 4b 18 ea 7a 78 e4 54 a7 36 08 63 8e 42 d5 0c cb 4a 1c 0c 50 d1 ea 31 98 3e ad 3c 60 f8 10 37 af cf c3 0b 25 d6 57 e2 d0 73 54 56 60 41 50 d5 a0 f1 6c 0c 69 05 73 3c b7 b2 2a c8 fd 5a 80 92 7b 9f f8 88 c9 25 af a9 7d 5e f4 da 02 25 72 68 ac 82 a1 ab 84 31 2a 50 19 20 bb 53 08 65 92 36 ea 46 e0 83 e1 8b 20 c8 ed a2 9a 47 fa b5 c7 a9 34 93 af 23 1b 83 c0 93 d0 fc 3e f8 a7 92 ad a7 97 da 17 f4 ae 9d db d4 60 02 16 a1 1c 77 6e 54 aa b7 f9 3f b5 8b 12 51 9a a6 97 77 01 17 d0 c6 97 10 44 dc 98 81 5f b5 b6 eb fb 5c 46 04 25 17 fa 9f d6 5d e2 bc 24 44 e1 a4 8c a8 00 17 fd 8e 9f b3 c7 f6 70 a8 46 47 63 6f a9 d9 47 15 ab 33 5d 80 4b bb b5 15 a9 fe eb 45 6f e4 19 16 76 84 d5 Data Ascii: dk+PNj}7\$-VD6PKzxT6cBJP1><?%WsTV`APlis<*Z{%)^%rh1*P Se6F G4#>^wnT?QwD_]%j}\$DPf GcoG3jKEov
2022-04-08 08:02:43 UTC	3999	IN	Data Raw: 03 9a d3 c7 fe 1b 2c e1 5b 64 77 7a e5 ae af c1 ee cb 2c eb c5 09 23 e0 50 bd 0d 3d f3 13 c2 e1 e4 8e 24 16 b9 03 ca 07 d5 9d 4c 51 b1 0a cb b1 60 4e 5f 8c 53 12 10 b6 c0 20 e0 b6 e2 49 01 24 96 dc fb 9c b1 20 27 1e 5a bb 89 6e 7d 4b b4 12 2d 09 5a d3 66 fd 9d bf c9 ca b2 02 46 cc b6 08 ce 77 13 74 f2 58 db c6 b1 13 cf ed 00 4d 3f 97 91 a1 2d fc ab 94 c4 14 25 37 1a 62 19 bd 4b 95 a3 c9 bf 03 bf 13 ff 00 1a e5 97 41 21 11 af 49 10 0b 05 92 7a 50 80 48 1f cf b5 2b fe cb 25 12 b2 62 5a b8 11 71 81 01 55 1b 90 7c 4e 66 e3 2d 45 2d 32 33 b5 6b 4a 78 0c bc 35 af 93 88 62 24 fb 54 df 0d a1 64 91 85 a0 51 f0 81 5c 59 bb d5 42 a0 0d cf be 04 39 48 61 51 f7 62 c5 54 48 d1 c7 bf c2 49 c5 69 46 77 e0 c5 5b 7a 0e d9 30 19 52 bc 51 f3 e3 52 77 07 01 0a a7 24 df 08 5a Data Ascii: ,[dwz,#P=\$LQ`N_S IS`Zn]<Z-fFwzXM?-%7bKA!zPH+%bZuqj]Nf-E-23kJx5b\$TdQYb9HaQbThIIFw[z0RQRw\$Z

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:43 UTC	4015	IN	Data Raw: 9a 38 50 e3 89 1d e9 90 a6 40 a3 6c 3e ab 77 38 b0 55 5b 78 dc f2 e2 6a d4 0a 3a 0f 8c c9 84 06 41 01 66 f2 c7 33 9b 70 79 2d 45 50 12 68 76 e9 92 a5 0a 3f ae 65 88 70 8c 86 88 50 71 71 51 f2 df 07 0b 26 ed f5 89 e0 6f ac 08 d0 28 6a d4 2f 43 fc b8 0c 6c 22 e9 15 a8 6b 13 5e 0e 37 3b d4 96 51 e1 5c ae 30 01 4c ad 2b 47 2a 68 3b ee 72 da 61 4a 69 17 36 23 b7 8e 49 28 bb 61 22 10 4f 1f 87 7d c5 6a 30 25 af 54 7a ac cb b8 6f 0d 80 c0 55 39 86 ea 48 a1 4e 14 52 76 04 6d 51 fe 56 61 48 6e ca 94 af 67 79 22 63 1b 1a 25 39 82 7b 1c 21 31 09 86 94 62 57 87 00 bc 55 40 ae e3 c7 28 99 31 6c 08 95 f2 ad bb b4 a6 e2 74 89 63 5e 45 94 7d a2 07 d8 4e 5d 7f ca 6c 90 cb 69 d9 8c 5a 19 2d 5e 43 12 87 8 c 6e cc 7d f3 2c 6e d6 54 55 e4 d4 14 47 12 80 2a 7e 2f eb 93 1b Data Ascii: 8P@!>w8U[x,j:Af3py-EPhv?epPqqQ&o(j/Cl" k^7;Q)0L+G+h;raJi6#(a"O)j0%TzoUH9NrmQVaHngy"c%9{!1bWU@(!1tc^E)NjIIZ-^Cn),nTUG*~/
2022-04-08 08:02:43 UTC	4031	IN	Data Raw: 63 2c 80 6c dd 9b a1 24 aa f2 3b bd 18 bd 40 fd db 53 a5 6b b7 1c b7 70 d7 b1 51 d6 a6 b7 93 d6 95 d3 ab 06 57 5e b4 1f ee af 0e 07 2f 89 2c 4a 45 69 76 23 b9 f5 ed 22 dd 9e a8 8c 6a bb 8f b3 96 dd 35 73 45 df e8 b2 d8 1f 88 a5 c3 3b 56 8a 7e 15 27 e2 f8 5b c7 1e 20 59 70 d2 95 c6 91 71 2b b4 f7 7c 61 76 01 50 13 b3 7c ff 00 97 07 18 5e 1b 54 b1 d0 2f e0 e5 fb e8 e3 d8 86 ab 6d ff 00 37 e5 67 28 0d 83 15 ab 5b 58 37 29 22 9e 1e 57 08 15 e3 70 b4 4e a3 96 eb 90 9c fa b3 10 4c 2f 34 e6 8c 7a b1 a0 95 97 fb c0 bb 54 1f f7 df 2c aa 39 37 6c 38 90 b7 57 51 44 de 93 7d 8e 42 88 07 12 3d f9 7f 36 5e 0d b4 d5 2a c4 b7 30 38 31 d0 8e 5b ab 1a d3 e5 bf 0f 6c 81 a4 d2 8c ba dc 16 c5 a3 1f 6d 87 16 00 0f a7 7c 02 04 a4 c8 31 a9 2e ae 2f dd 6d ed d8 9a 93 c5 46 66 08 Data Ascii: c,lA\$:@SkpQW^,JEiv#"\$jsE;V-~[Ypq+ avP ^T/m7g([X7)"WpNL/4zT,97l8WQD)B=6*"081 lm 1./mFf
2022-04-08 08:02:43 UTC	4039	IN	Data Raw: 77 03 a5 72 99 04 d3 77 37 f6 d1 aa c2 09 32 f5 2a bd f0 43 1d b1 4b e4 bc ba 9c 7a 88 78 00 45 07 86 65 47 18 8a 78 51 f6 8e 5a e1 59 df 9f 70 b4 fe 38 98 b2 01 3a b1 bc 58 19 86 c0 11 43 51 df 22 03 70 28 39 ae 60 3c a6 a8 34 0d 4f 9e 42 90 64 d5 95 c3 18 c9 e4 37 04 b1 3d bd b1 50 55 34 9b 79 27 47 91 b8 d2 b4 dc 6e 4f 6c 31 0c c0 7f ff d6 89 20 60 78 91 4a e6 21 0c 90 66 d5 a1 42 16 a5 d0 f5 ad 41 c5 0a f0 c0 24 35 5d 8f 7c 81 34 82 51 96 e0 05 ab 0a b0 db 7c ae ed 5b e1 c1 4b 1a 82 7b e3 6a ef aa c6 07 c4 b5 27 a9 f6 c6 d5 11 c2 24 5f 03 91 25 56 a0 0a 4b 03 5a e4 55 a0 60 74 21 eb f4 53 12 ab 65 7a 7c 24 d4 6f 4a 0c 56 da 85 58 bd 3f 6b b6 04 85 b7 2d 24 67 8b d6 a3 ae 1a 67 4a 6b 2a bd 36 a9 27 be 10 a8 ae 09 cc 96 3b 2f 45 1b e1 a4 80 8b 96 85 8b Data Ascii: wrw72*CKzxEEgXQZYp8:XCQ"p(9'<4OBd7=PU4y'GnOI1`xJIfBa\$5]j4Q K[fj`_ %VKZU`tlSez \$oJvX?k-\$ggJk*6';/E
2022-04-08 08:02:43 UTC	4047	IN	Data Raw: 14 0a 0f 6c 8a 40 4d ad ec 4c 96 ab 04 9f 0d 07 36 a0 f8 77 ec 32 be 26 7c 29 3e a1 a0 bc 4c 82 12 aa 6a 69 cb 61 4c 02 41 c6 9c 29 48 db 5c c6 df 19 5a 05 e4 69 e1 90 94 da e9 ff d2 8f 35 c5 d3 99 2d e4 8c c5 e9 b1 42 a7 35 65 69 7d 8c dc 54 21 3f 12 f5 07 ae 55 34 4b 64 53 1a cb 1b 45 c1 91 98 be fb 80 40 fb 05 b2 96 b6 f5 0d 2c c8 8e 1d 82 c9 18 0d ce bf 08 07 f6 7e 59 64 36 2c 84 a9 22 50 47 c0 5f e0 22 9b 78 e6 5b 37 08 e3 6a a0 24 80 3a 1d f2 56 ab 24 b6 5a 0e 3f 68 6e 06 22 54 91 ba 06 fa cd da 92 2d 59 c1 a9 03 b0 19 64 67 6a 50 8f 1b ba a8 61 53 d6 87 2d b6 2b ec d4 2a b1 55 e4 7a 1c 04 a2 95 3e a8 14 d0 91 f1 6e 30 5a b4 c8 50 32 d2 b4 f6 db 21 68 45 da b0 58 55 23 72 c1 77 3b 74 f6 c1 48 25 0f 79 6f ce 45 20 71 e7 b5 17 73 f3 38 da 82 e9 ac 56 Data Ascii: l@ML6w2& >LjiaLA)HvZI5-B5eiT!T?U4KdSE@,~Yd6,"PG_ "x[7]\$:V\$Z?hn" T-YdggPaS,+*Uz~n0ZP2hEXU#rw;th%yoE qs8V
2022-04-08 08:02:43 UTC	4063	IN	Data Raw: 0e 58 23 7b e4 d6 93 0b 5a 2e ed cb e5 d2 b9 14 d3 5c 6e 1d f9 01 b8 e9 e1 b6 04 aa a2 bc 4c b2 f1 1c d8 9e bd bd f0 85 a4 22 ce 64 70 66 50 a8 58 fc 43 b9 fe 6c 4a a6 8f 71 23 46 52 31 d3 60 4f 7d ff 00 a6 41 92 c8 6d 9c c2 2e 88 2e 4b 14 a0 ff 00 27 20 c6 95 04 51 0b c0 63 20 d7 ed 1f 7f 6c ae 5b 31 29 97 d5 d1 bd 47 63 c5 98 50 02 29 ca 9d ff 00 c9 cc 53 24 95 88 d1 5d 32 a1 56 52 6a 14 a9 e8 69 4f 8b 23 c6 c1 2c b9 b1 77 4e 22 b5 02 80 77 27 c1 7d b3 2e 12 b6 25 7d be 8d 04 51 86 bb 63 ea a9 0c 8a 37 a7 fa f9 72 40 55 85 62 54 2c aa 5b 8d 58 31 14 56 c1 20 9e 49 ed b6 a4 1c 45 73 2a 8e 6c 00 3c 7a 7c be 8c a0 b6 89 29 dc dc b4 4d c8 af 27 52 68 3e 7d b2 2a 4a 57 ab 33 3b 87 97 63 5a 91 e 1 ed 8b 54 8a 50 ce 6e 2e d0 32 92 ad 99 63 58 dd 9a c5 6f 1d cb Data Ascii: X#[Z.\nL"dpfPXClJq#FR1`O)Am..K' Qc l[1]GcP)S\$]2VRjiO#,wn" w').%)Qc7r@UbT,[X1V IE\$!<z J)M'Rh>)*JW3;cZTPn.2cXo
2022-04-08 08:02:43 UTC	4079	IN	Data Raw: bd c4 b3 b3 94 45 92 6a 50 92 76 15 ff 00 2b f9 b2 40 2d ad b7 d3 2f a1 57 65 e1 12 53 7a b0 eb 82 46 d6 d5 ed e3 9a ca 2f ac 45 23 48 cd 42 11 41 2b 41 fe 57 b9 cc 79 c0 4b 9b 21 35 15 f3 0d d0 7f ac 44 81 25 35 15 eb 4f 96 08 e3 08 24 94 b2 f5 ee 2f 0f 62 14 d4 9e f9 7c 45 31 43 b4 7e b8 51 d5 05 fe 2a 40 f6 c9 da 22 d3 36 42 0a ba 90 dd 4d 0e 57 6d 8a 53 47 25 a8 1c 40 02 5a 6e 0d 76 3b e1 64 b1 a3 9e 1a 4e 05 05 7b 8f c7 0a d2 2a d9 a5 bc 56 5b a6 e9 b2 b6 db 7b 53 23 c2 96 92 dd 9e 53 e8 82 ce a2 9b 0c 95 31 a4 1d c9 95 c5 4e cc 1e 80 53 7c 69 8a 31 c3 db 85 8e 7e bb 51 69 b9 ae 34 85 97 28 66 04 11 46 fc 3e 8c 69 98 50 fa ac 89 13 42 2a ca ef d7 65 ae 14 b5 63 7c 60 8e 50 b2 d5 80 1f 0d 2a 08 c9 18 ad a9 ad f2 b3 04 90 52 a3 c3 6c 2c 3a a3 a7 9b Data Ascii: EjPv+@-/WeSzF/E#HBA+AWyK!5D%5O\$b E1C~Q.@Qb*6BMWmSG%@Znv;dN["v{[#\$S1nSj1~Q14(fF>iPB*ec 'P*RI,;
2022-04-08 08:02:43 UTC	4086	IN	Data Raw: ae 14 d6 20 48 09 51 fc ea dd 72 52 04 b3 89 01 33 f3 0f 9a a1 9a cf 8f a5 14 73 03 42 c1 14 a5 7f d8 ee 30 e2 c2 41 e6 99 e4 04 72 61 82 e4 dc d4 d0 0e 3b d6 9b 66 ce a9 c5 b4 1d c4 3f 58 1c a9 46 a7 8d 3a 77 c9 04 da 9a 83 1c 60 95 2d 43 4d fc 70 14 21 61 be 92 de 45 9d 48 e6 bd 08 3b d7 b6 4b 84 10 85 79 75 59 af 90 47 31 3c 4d 49 f0 af f3 53 04 31 08 a6 d4 6d 20 9a 39 04 61 f8 ac 86 9c 8f 4a 65 84 aa fe 11 3c 86 13 f1 52 a2 a4 7e 38 7a 21 b9 e2 8e 29 91 21 20 82 28 47 b6 3c d1 68 ab 59 60 59 fd 38 4a 83 d8 9e 80 8f da c1 48 b4 1e ab 64 d1 c9 48 a4 12 46 45 6a 95 00 7f 37 5c 21 89 6a 0b 81 1f 32 37 f8 68 3e fc 8a 14 61 bc e2 42 83 40 77 6c 95 2a 22 cf 54 55 b9 f8 d8 8a 8d 88 f6 cb 06 ce 82 65 79 64 97 85 ae 2c b7 76 1f 1a d3 73 4f da 18 48 b6 54 91 ca Data Ascii: HQR3sB0Ara;f?XF:w'-CMP!aEH;KyuYG1<MIS1m 9aJecR~8z)! (G<h^Y8JHdHFE7lJ!27h>aB@wl""TUEyd,vsOHT
2022-04-08 08:02:43 UTC	4102	IN	Data Raw: af 45 1d 8e 53 30 a1 15 a9 5e c2 66 48 a5 06 57 43 b3 36 ca 2b fe ae ed 94 53 30 a8 97 d1 da 71 1e 89 0d 23 71 04 f4 35 3b be 54 59 d3 b5 dd 52 09 6a b6 71 88 63 26 85 80 dd 87 72 72 71 8b 24 3d a5 ac e8 86 62 01 8d 45 23 27 bd 7b f0 f6 c9 96 4a f2 da dc 5a 70 ba b8 05 39 6d b9 00 d6 9b 1e 1d 70 55 ae 95 a1 d7 9e e7 f7 51 1e 2d 5f 89 8e c7 8f fa df e5 64 7c 36 48 6b 9b e8 fd 65 92 e1 0c d0 a0 e8 86 87 fc 9a e5 a0 26 d7 5f 6a 92 5d fe f2 34 58 c0 d8 54 56 bb 7e d3 64 b9 20 ca d4 2c e0 b8 99 0a ab 28 62 e1 6a 7b 96 fe 55 c5 81 2b a4 b2 7b 49 a3 8e 56 0d 11 fb 6c bd 48 1d 97 27 74 d6 52 2b cb 29 21 97 97 13 c1 89 e3 b7 6a e4 78 99 86 4f a4 83 04 6a e4 aa 9e 24 7a 8a 0f 24 af ed 78 65 32 36 b6 ac d6 f0 c9 2f 18 a5 a5 b2 8a f3 94 ee e7 fe 6a 38 8d 99 da 13 9c Data Ascii: ES0*fHWC6+S0q#q5;TYRjqc&rrq\$=bE#[JZp9mpUQ-_dl6Hke&_j]4XTV~d ,(bj[U+{IVIh'tR+}j)xOj\$z\$xe26/j8
2022-04-08 08:02:43 UTC	4118	IN	Data Raw: ca a3 f7 4d 1f c3 f0 91 fb 47 f9 b8 e2 c9 4d 6e ae 1c d2 3d 95 c8 0c 2b b1 2b 2d ab 80 a2 d6 eb 4a d2 51 1a 94 1b 82 3f a6 4a 28 92 46 a8 a0 fa 6e 69 be dd f2 e2 58 52 71 65 78 f1 f1 36 ea 0b 0a 86 62 b5 14 ca 0a ab c9 ea 48 c6 44 05 9a 43 d1 45 01 ed 4a 60 b6 25 21 bd f8 67 75 51 4d f7 07 2f 0a af a7 30 69 18 c9 f0 85 5d be 9c 07 64 83 48 fb 59 16 16 28 a0 ec 6b 43 e3 95 5b 3e 68 da b5 c4 6e 1b fb ce 2a 57 c3 63 88 45 25 57 76 a0 1e 48 7b 50 9c 28 47 06 48 ed 44 0e 09 35 e4 a7 b9 c8 1d d4 9a 4a a6 06 e9 9a 49 07 f7 62 a4 64 80 63 6a d2 43 f5 86 12 42 38 ec 28 4f 4c 5b 01 4e 6f d6 2b 60 8d 14 fe a1 5e bb 53 b7 41 95 12 92 16 40 80 f2 76 52 1d b6 24 6f 41 91 2d 68 38 4a 81 65 50 cb ea 35 40 5a 6d d0 ee 29 8a 84 f7 50 bc 8e 5b af 5a da 34 85 d5 69 4e 23 8a Data Ascii: MGMn=++JQ?J(FniXRqex6bHDCEJ`%!guQM/0]dHY(kC[>hn"WcE%WvVH{P(GHD5JlbdcjCB8(OL[No+^SA@vR\$oS-a-h8eP5@Zm)P[Z4iN#

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:43 UTC	4126	IN	Data Raw: b5 3d 79 91 f2 c3 e1 79 af 13 52 73 8f 65 76 1e e7 23 2b 8e c0 c9 23 75 a1 ca a9 f8 c9 6a 77 15 c0 24 40 e6 a4 28 b1 99 85 39 82 0f 6d 86 54 4c ea ad 98 ae e4 38 0d 52 06 63 8b 66 ae 90 b2 8e bd 73 26 30 21 ac 95 c5 76 f8 be fa e4 c8 42 de 24 74 3d 7e 9c 03 6e 45 92 5f a9 5b 09 90 86 e8 7a e5 53 67 12 c2 fc cb a5 c9 21 8a ea dd 69 3d ba 7a 5f 06 c1 90 6e 3e 15 fd bf e6 6c be 19 25 40 1f e1 1d 3f 1f 57 f3 93 c2 99 68 92 35 dd af aa 7a 30 00 7f c6 d9 64 4d 8b 62 54 20 76 9d 99 4d 47 54 af f9 fb 64 a3 bb 19 6c a5 76 88 c0 40 08 e2 bb fc c0 cb a3 1a d9 81 4b 2e 9f 88 2e 95 64 6f 88 92 77 db f6 7e 59 6f 26 0c 53 5e b9 f5 d5 1c 82 65 6e 80 57 e8 c8 49 a2 65 5b cb 91 7d 56 27 33 7f 7c 4f 71 db 35 3a 99 f1 6d fc d4 0d d7 4d 74 80 3b 9d a4 34 e1 5c ab 17 72 94 66 Data Ascii: =yyRsev#+=ujw\$@(9mTL8Rcf&0lvB\$t=-nE_[zSgli=z_n>l%?@?Wh5z0dMbT vMGTDlv@K..dow-Y o&S^enWle]jV3jOq5:mMt;4lrf
2022-04-08 08:02:43 UTC	4142	IN	Data Raw: a0 ae c2 81 46 6d 31 50 0d 52 4d 7c 91 76 6c af d6 43 f1 33 6c 6a 3a 0e e5 72 7c 5c 2c 44 a9 9e 6b 5a e5 a8 62 62 08 c3 e4 3f 5e 5b 11 7b b6 19 bc f3 53 bc e3 f1 cf 4e 4c 6a 01 3b 7b 53 19 07 1e 46 d2 74 b9 35 7b 96 3b 30 a0 15 c8 c8 53 5a a2 4c 24 8d e6 00 84 63 40 3b d3 2b 25 28 cb 2b 06 7f b2 59 51 a8 6a 7a 0a 0c ac 96 40 20 e4 77 7b 92 ce 79 2d 78 a0 03 60 2b f6 b2 d8 8e a8 4d fd 06 5b a6 9b 95 11 54 10 01 ea 7b be df 67 2b 94 ac b2 01 37 d2 f5 6e 72 8b 82 c0 46 c7 80 1d f7 1f 6b 31 cc 80 66 0b 2c b3 be 58 2d 1e 17 e3 0a 6e 56 a2 a4 83 fb 61 7d f1 33 b1 bb 68 28 47 f2 85 e5 fd b8 ba b7 88 95 75 04 30 22 84 7b 64 63 80 91 6c 65 15 bf 97 7a f4 36 1a da 58 ce 1d 26 9e b1 53 dc 7c 54 e3 97 e0 85 1f f7 4d 04 90 f7 4e 14 4d c9 1f 8e 67 ca 3b 73 a6 60 af 1c Data Ascii: Fm1PRM v C3lj:r \\,DkZbb?^{{SNLj;{SFT5{;0SZL\$c@;+%(+YQjz@ wr{y-x'+M[T{g+7nrFk1f,X-nVa}3h(Gu0" {dclez6X&SjTMNMg;s`
2022-04-08 08:02:43 UTC	4158	IN	Data Raw: 71 be 59 09 70 a0 8b 4a 6e ec d5 89 24 66 cf 16 66 83 16 1b ae 17 d1 a4 33 c3 dc 1e db 0a f6 cd a6 3c 9c 41 a4 84 85 3c f5 14 c8 54 23 09 01 0a bb 54 56 bb f1 fe 5c b8 e2 a6 22 4c df 84 93 5a 7a d1 91 c4 9a 53 c7 e5 98 92 6e 1b a2 96 24 9e d8 bb 80 22 42 76 ef b6 c0 e4 0e e1 3d 52 2b ad 32 79 64 f4 e5 6f f4 35 40 42 81 bb 1f e5 ae 42 20 de e9 21 01 a8 ea d2 bd 4c 96 e1 2a 58 f0 01 7a 8c b2 da e9 05 ab eb cf 0c 46 34 fd 0e 89 a8 c3 9a 92 7f 9b 11 2f f6 2d 52 29 70 9d c4 2e a5 79 19 17 99 ff 00 27 32 62 5a 9f ff d5 e6 8b c4 72 11 20 2c 7f 9c f4 ff 00 62 33 5e 1b 14 ed e0 7e 40 12 16 9b 50 6c 77 cb 18 d2 94 52 24 53 18 b9 00 47 46 f7 c3 cd 42 b5 b9 91 48 63 47 00 d4 fb e4 5b 02 76 c9 38 b7 e6 59 52 35 e8 aa 28 5a bf e5 76 ca c1 64 92 de aa b3 a1 07 a0 f1 a9 Data Ascii: qYpJn\$ff3<A<T*TV\\LZzSn\$Bv=R+2ydo5@BB iL*xzF4;/r).p.y2bZr ,b3~@~Plwr\$SGFBHcg[v8YR5(Zvd
2022-04-08 08:02:43 UTC	4166	IN	Data Raw: 5c 6d fb 23 db 25 e2 23 8d 03 1e 85 c2 73 c4 19 14 03 f1 30 be b6 4f 89 3c 4b e1 b0 8c 3b 00 87 89 ea 7e 59 6c 0d 96 40 a1 a7 48 65 21 a3 20 d2 87 e4 3f 97 7e b9 97 16 d4 56 95 64 93 4c ce e0 fa 3b 31 15 ae 51 9a 74 11 22 8a bd d7 e3 8c b4 51 a8 10 a7 8e ec df d3 31 23 1b e6 d6 02 85 bc cd ab 27 33 27 06 db 7e d4 f6 c9 98 39 00 29 44 20 b2 f8 9e 45 9c 46 4d 38 8d ea 7b b6 48 27 85 5f cb db d6 d7 1a 92 49 24 71 2d 43 ec 78 ef 4e fc 9b 32 a0 5a 08 b4 b2 7b 6b 74 99 c5 c0 e5 37 2a 8a 6c 29 fe ae 64 04 11 48 99 d4 dc b4 71 d2 94 35 2c 0d 28 b9 61 0a 13 9d 36 18 e1 03 f6 4f d9 2d e0 0f b6 03 b3 6a 84 7e 5f 22 e5 6d 29 50 ea 5d a4 27 a8 af 86 47 8e 98 98 da 15 7c bc da 5c bf 5e ff 00 76 2b d6 3e 42 a0 d3 a6 c3 f9 b2 32 c9 6c 78 15 66 d3 2e 1a e8 5d 5c 90 b3 9d d9 Data Ascii: lm##s#s0<K;~Yl@He! ?~VdL;1Qr"Q1#*3~-9)D EFM8{[H- i_\$qC-XnZ2[kt7*)dHq5,(a60-j-_"m)P]Gj/v+>B2lxf.\\
2022-04-08 08:02:43 UTC	4174	IN	Data Raw: 58 f6 26 9d f9 7f 36 63 d2 af 93 cd 33 4c c3 ea 4c 2d a2 57 50 b1 38 2d fe cd 76 cb a3 b2 40 4c 2e 2d a5 d6 f9 24 f3 90 c2 4f 85 94 d4 35 47 c2 24 41 f6 57 2d e2 67 4c 71 22 bc 8e ea 41 c8 5b 4b 08 23 91 6e 94 3f b3 ed 84 c9 98 44 47 23 c9 1b 2d d3 19 15 41 61 43 d4 f8 a6 52 52 8f 81 92 6d 30 5c da 10 85 5b d3 2a c6 ac d5 f0 5f f2 7f 6b 02 0a 5f 3d 93 5d 20 95 25 56 65 0d 55 4a f3 c9 03 48 09 33 da 4b 13 70 93 90 90 10 7d c8 3d f2 f6 61 33 4f 7c 1b 9d 5c d0 85 53 bf df 90 6c 0a 90 c8 11 9f d4 8c 12 e0 9a b1 e8 06 2a 97 99 bd 60 68 38 b0 dd 80 f7 38 29 21 5e 47 46 45 da a8 7c 7b 7d 39 1a 66 ad 2d b5 c5 b8 53 e9 f3 84 d3 e2 1d ab 80 96 54 ba 4d 3d 38 9e 01 ab 4a 9e e3 00 28 21 04 a7 90 6f 50 51 69 f2 ad 3d b2 4c 13 5b 28 26 44 86 e2 ca 53 1c d2 29 02 84 Data Ascii: X&6c3LL-WP8-v@L-.\$O5G\$AW-gLq"A[K#n?DG#-AaCRRm0[* _k_=%VeUJH3Kp)=a3L\\\$I*^h88)!^GFE {}9f-STM=8J(l0PQI=L[(&DS)
2022-04-08 08:02:43 UTC	4190	IN	Data Raw: ab cc 38 4a 4b d0 3f 27 bc c7 6b 6f 04 9a 75 d4 9c 6e 0b d5 79 1f 84 83 f6 63 8f f9 73 33 41 a9 8c 47 0c bd 32 fe 1e 27 1a 51 7a a2 90 36 39 bd 0c 4a 9b 50 9a 01 4c ae ac b2 52 94 91 ba 9a 8f 02 32 b9 93 d3 fd 90 65 10 87 79 01 52 ae 06 dd 40 cc 63 30 41 06 9b 00 ad d0 33 db 7a 82 9e 9a 53 c4 9f f3 df 30 a7 8b 8b f8 63 c3 fc eb fc 7a 9b 84 ab aa 5f 3d a8 06 83 8a f8 0a 77 f7 cc 09 e3 00 ed c3 1f c7 f1 37 46 49 75 c4 01 41 32 37 c5 5e 94 e9 98 72 8d 73 3e af e6 b6 82 c7 bc c9 a9 5a 59 59 ce 97 27 93 34 4d f0 2d 79 1a ed db 2c d3 8b 2c de 53 26 a1 7b 24 09 73 56 86 68 a3 58 a3 75 dd 82 d3 97 0e 5d 9c 8c df 63 81 1b 16 a2 58 85 d5 c0 46 f5 05 7f 7a 6a 41 15 dc 7e d7 cf 33 e1 17 16 49 d5 9d e4 0b 35 8c 91 bb 3c 6a 5c b0 6f d8 ae 57 28 ee a9 ba 58 cd e6 11 3d Data Ascii: 8JK?kounycs3AG2'Qz69JPLR2eyR@c0A3zS0zc_=w7FluA27'rs>ZYY*4M-y.,S&{\$sVhXujcXfZA-3l5<j)0W (X=
2022-04-08 08:02:43 UTC	4206	IN	Data Raw: ee 70 53 68 47 3c b0 b1 a3 28 54 71 b9 f7 c8 25 2d 3c f8 3c 69 5e 2a 6a a4 e4 f9 b5 1d 96 43 7e d0 44 ec bc 1c 91 b1 3d b2 5c 36 8e 2a 45 8b e8 ef a3 8d a2 f8 64 2a 40 3e e3 db 22 76 53 2b 76 9f ae c9 6e ed 7b 72 82 e2 5a d5 62 a5 01 3d 9d bf c9 18 0c ba 35 57 54 be f5 27 b9 60 d7 04 87 3d 8f 4d 04 87 3d 89 0d 45 0e a5 02 be c0 d4 0c 85 98 2c 7d 3c 30 ab 4f 6e a0 fb f4 c5 2a 49 55 2b 41 85 57 a3 fa 6a 58 80 0d 7a e3 4a bc b3 4a 56 30 c1 81 35 35 d8 62 a8 db e7 8c d4 22 88 9c d3 e1 5f b2 07 6d fc 70 28 75 80 13 b2 99 cf a8 a0 1a ef 4e 9f e5 64 56 d5 ae ac 91 0f 28 8b 28 20 57 97 89 fe 5f f2 46 14 da 81 89 9d 96 3d c8 f7 e9 92 50 50 ed 1d 59 b9 b0 0a bf 7e 2c 90 b3 35 05 0d 40 c0 b6 a9 6c b2 5d 3a c6 bc 43 1e 84 e2 52 17 94 65 20 48 a4 54 9a 9c Data Ascii: pShG<(Tq%-<<i^*jC-D=\\6*Ed*@@>^vS+vn{rZb=5WT'^=O-EM,}<0On*IU+AWjXzJjV055b*_mp(unNdV((W_F=P PY~,5@l]:CRe HT
2022-04-08 08:02:43 UTC	4214	IN	Data Raw: 1a 35 ec 9a 60 76 7a 51 df a8 15 76 f9 7f 93 95 e3 b0 cc 15 fa cd da c0 b1 31 46 06 45 ad 00 d8 13 d3 7c ab 38 a6 56 81 4b 79 8f 19 a2 70 94 3c 91 8b 74 61 fc 46 60 f8 64 f5 5b a7 bd f9 03 cc a3 5e d3 12 46 24 dc c2 04 73 57 af 20 3e d7 fb 3f b5 9d 56 8b 37 89 0d fe b8 7a 65 f8 fe 93 8b 92 34 59 2d 73 39 ad aa 60 21 5d 4c 69 5a c0 96 f0 a1 a3 80 94 ad 91 03 8a 1c 89 16 90 69 8e eb 3a 58 e3 ca 8c dc 7a 75 3b 9c d1 eb 34 e2 af d4 78 5c ec 59 18 e5 d5 9b 85 a8 04 af 73 4d ab e1 9a 5c 98 88 16 2f e4 e6 02 93 5f 58 89 3a 8d f0 63 c8 62 b2 16 c7 35 2d 30 47 56 0b b1 ad 57 b1 f0 cd be 1c f6 e3 98 b0 e6 fa dd 82 fa 2b 24 6c a1 b9 49 ca bb 83 fb 19 99 4c 80 b4 1e bb 03 6a 30 17 81 16 38 6a 02 f1 14 0c 4f b6 4c 06 61 5f 46 bd b7 08 b6 e2 8d 70 ae 36 a8 15 23 b9 ff Data Ascii: 5'vzQv1FEj8VKyp-taF`d[^F\$Sw >?V7ze4Y-s9`]LiZi:Xzu;4xYsMV_X:cb5-0GVW+\$iIlj08jOLA_Fp6#
2022-04-08 08:02:43 UTC	4230	IN	Data Raw: b2 05 2d 68 1c a6 ba 0a 54 2c 20 fc 6c 7a 50 6e 07 fc 16 41 43 26 b7 b9 79 a4 71 28 e0 b5 24 15 ee 06 01 cd b6 d0 d6 d1 d2 57 81 10 0e 4d cc 9c b8 2d a0 7c c7 78 63 e5 20 51 56 14 e4 3c 3d b2 c0 2c b1 29 66 90 91 a1 57 8e 3e 09 5a 16 ae ec 7c 38 e4 c9 40 46 5d da c6 d2 15 8c 55 96 9c 94 f5 a6 04 d2 5b 24 92 47 ce 68 7e 11 f6 47 6d b2 24 35 94 65 be a2 07 0b 68 d6 8f c7 93 37 cf f6 70 f3 65 68 59 a4 05 99 28 be a3 ee 29 d8 0e b8 d2 82 9a 68 53 c9 c9 63 89 96 30 8e 40 42 7a 8c ac 84 02 cd ad b5 0b 77 b7 7f 59 93 d5 63 c5 0a 8a ee 0d 0f 15 3e 19 8d 28 f3 6c 05 8f ea ba 64 96 8d ce bc cb 52 ae 46 d5 3d 80 cd 4e 78 70 b6 04 fb c8 3e 73 b8 d0 2e 63 81 e5 06 cd dc 09 14 f4 15 fd a1 fc b4 c1 a6 d4 cb 04 f6 3e 8b f5 c7 f8 5a e4 2f 9b e8 0b 6b a8 ee 90 4b 03 07 46 Data Ascii: -hT, lZpNAC&yq{ \$WM-jxc QV<=,}fW>Zj8@FjUj\$Gh-Gm\$5eh7pehYj)hSc0@BzwYc>{ldRF=Nxp>s.c>Z/KKF

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:43 UTC	4246	IN	Data Raw: 15 11 9d c2 ff 00 ad fe 56 6e 71 61 ef 6b 94 9e b5 1c 09 18 0a 8a 14 2e c2 83 33 00 03 93 55 af a0 c2 84 15 f6 8d 6b 7c 29 3c 60 9f 1e 87 ef ca 32 60 84 f9 86 42 44 3c 47 f3 91 e3 f2 e4 b6 da 71 89 5e 0b b6 69 8c 81 68 c3 85 14 43 ea 7f 2b 72 e4 cb 9a 6c ba 61 88 f4 e1 9f fa 7f f4 ff 00 cd 76 38 a7 c4 18 64 37 d2 de 81 34 bd c5 68 36 0a 07 6c 0d 85 0d 72 95 41 24 5b 71 24 fd fd b2 a2 36 42 69 67 60 b3 5b 2c 47 ec 1a 54 9d b6 fe ad 98 a6 16 82 99 79 7b 5b 58 ef 9b 4e 2c b1 5b 13 56 6a 6e 48 fb 28 a3 04 d4 1a e5 16 be 68 df 37 e9 96 b1 31 60 15 10 9a a2 93 f1 5f 6a 60 cd 00 39 24 31 27 65 e3 e9 91 bf b1 cc 22 69 6e 9f 45 79 42 ea 3b cd 32 de 78 c1 e0 50 0f 88 ef b6 db e7 55 a6 90 9c 04 83 46 4e 69 a3 50 0a 8c b0 ed c9 01 a0 37 c8 25 ba 8a 81 92 b5 43 dc 05 Data Ascii: Vnqak.3Uk <'2 BD<Gq^ihC+rIav8d74h6lrA\$[q\$6Big'[,GTy{[XN,VjnH(Mh71`W'9\$1`e"ieYb;2xPUFNiP7%C
2022-04-08 08:02:43 UTC	4253	IN	Data Raw: 41 a4 e7 21 0c cf 4a 0a 7c 4a 3e 9c c6 cb 8c 63 a0 3a b7 63 95 dd bc bb 4f d7 16 f2 49 63 e1 c0 2b 6c 48 00 04 ff 00 24 7f 36 58 03 3e 24 d3 40 be b6 b5 bd 93 58 95 4c 96 f0 86 40 de 2d 4a 51 3e 59 5c 83 24 c2 c0 4b ae b4 77 e4 70 5e 47 d3 1f b5 c4 ff 00 c6 d9 89 28 af 34 75 f5 95 b5 ac 35 8d 78 a2 d0 b2 9f 89 8b d7 a5 73 4f a8 20 36 8d 96 5c 5c 5b dd a0 59 5b d2 90 b2 93 c7 63 cb b5 4e 63 cb 24 65 cf ea 54 9f 51 d3 e5 76 e0 ea 1a 95 d8 9a 82 3a 80 d8 20 48 34 18 d2 19 b4 db 83 74 25 99 bf 7a b4 00 0e 8a a3 c7 fe 23 99 11 9e e8 e1 4a 64 68 f8 ca c6 41 54 91 a8 a3 a8 ae 6e a0 76 6a 2a 6b 6a 49 a1 0b c2 95 53 5e a7 21 29 f4 61 6e d6 b5 f9 6f 0a 9b 86 32 85 5e 2b f1 54 d7 31 e3 0d ed 8c e5 6b b4 8d 61 ad 85 4d 14 1d ca 78 1c bb 87 66 21 ab 7d 42 09 2e 49 f8 Data Ascii: A J J>c:OIc+IH\$6X>\$@XL@-JQ>Y!\$Kwp^G(4u5xsO 6\ Y[cNc\$eTQv: H4t%z#JdhAtnvj^kjlS^!)ano2^++T1kaMxf)B.I
2022-04-08 08:02:43 UTC	4269	IN	Data Raw: 5d 5d cd 79 34 82 d8 06 28 b5 15 e8 09 c9 85 57 8e d6 38 ed e8 f2 15 95 93 61 d7 8f cf dd 5f 8b 08 60 87 b8 f3 55 e6 85 14 29 6f 27 fa 44 cd 56 2e 4b 6d fb 4d c4 fc 35 c0 43 22 54 c5 8d f6 be 1a fe 49 96 59 55 41 04 51 48 19 89 93 01 99 b4 71 25 57 90 dd 69 b2 24 57 4f b3 2d 40 04 1a 0f f2 a9 df 35 b9 b1 11 b1 67 19 32 8f 2a 79 c5 34 89 89 7a bc 4d b7 06 ad 6b fe 46 63 62 9c b1 1b 03 8b c9 b8 91 2d 9e bf 61 ab 5b 5e 0f dc 1e 41 81 a5 0e 6f 71 e6 8c f9 6e d3 28 90 e6 1c 48 63 d1 7b 65 12 14 6d 9a 98 28 e6 80 53 7a ef 95 58 25 97 25 78 e9 18 a2 d4 5a 7c f2 e8 0e 1e 4c 48 b5 55 a8 6d c6 fd 4e 5b c8 b0 42 cb 10 35 61 f0 93 b1 f9 f8 e6 2c a3 6d 80 a8 f0 29 50 0d 47 cf 2b 02 bc d3 6b 5d d1 85 58 0e 64 fd 9c 91 c8 08 df ea fe 6a d5 14 2e a1 60 c0 16 34 a0 fd Data Ascii: Jjy4(W8a_`U)o'DV.KmM5C"TIYUAQHq%Wi\$WO~@5g2*y4zKfCb-a[^Aoqn(Hc{em(SzX%%xZLHUm N[B5a,m)PG+k Xdj.`4
2022-04-08 08:02:43 UTC	4285	IN	Data Raw: 6f aa 41 24 22 e2 e3 e0 50 dc 40 ec 7b 64 59 2a c3 c0 96 7a 80 87 65 23 c0 63 69 53 5b 88 6d 9e 2b 50 4f a9 3d 43 7f aa 30 2a 9d da 20 91 e5 44 0c 29 40 7b d0 64 82 69 8e 5e c5 f5 b7 48 63 52 25 ec 3e 5f b4 46 02 d1 2d d1 77 97 61 4c 71 ae db 00 cd 4f 6c 89 2a 54 61 af ab f1 12 57 ed 6c 69 d3 b6 46 98 b2 4d 29 22 bd f5 2f 64 90 46 c7 75 52 7a d3 db b8 c8 c2 09 8e 99 aa 3a 34 a9 01 22 e0 37 36 7a 6e 77 fd 9a 7c cf f2 e6 2d df 26 c0 59 3d a7 98 04 d7 0c ec 86 65 42 15 55 56 bd 47 c5 23 7b 60 19 2c b6 02 98 69 7a 8c d0 b8 b9 81 84 91 c7 c9 68 e2 82 a3 f6 5b e5 fc d8 41 ad f9 f0 b3 e6 29 97 f9 6b cc 76 fa 82 01 25 12 e8 ad 4c 75 dc 03 97 61 c9 1b a3 fd e3 19 c4 f4 64 91 29 27 61 41 4a 54 e6 c2 20 ff 00 55 c7 25 55 49 a6 f9 60 62 55 42 fd d9 6d 31 b5 39 20 Data Ascii: oA\$*P@{dY*ze#ciS[m+PO=C0* D)@{di^HcR%>_F-waLqOI^TaWiIFM)}'dFuRz2:4"76znmw~-&Y=eYBUVG#{"iz h[A)kv%Luad)'aAJT U%UI'bUBm19
2022-04-08 08:02:43 UTC	4293	IN	Data Raw: 5c 49 26 95 fb 86 4f 8a f9 21 57 42 11 c4 ee c8 79 24 6d c9 49 1d 47 cb 21 94 b3 82 3a f2 ef 94 81 98 8e 0f b1 fa 73 1c 06 e2 be 28 7d 14 a3 90 08 04 ad 76 db c3 24 0b 59 08 50 bf 59 2f 35 1a a4 6d dc 0a 65 8c 29 d0 1b 48 3c b2 21 e2 48 a0 20 ed 81 21 11 12 ab aa 97 a0 75 53 4a 6d 51 80 a5 46 66 32 48 a0 90 a8 36 af be 00 12 8d 83 d1 48 cf 06 de bb d3 b6 54 59 04 4c be 8b c4 90 7a 8e 5d 8e e3 b0 07 f9 46 42 92 77 42 41 6e 53 94 44 7c 68 78 ab 53 a8 f7 c9 10 d6 ff 00 ff d1 87 e9 fa d5 e5 a3 7d 68 00 02 b5 55 4f d9 61 fe 57 8d 33 5f 4e 75 a3 35 5f 31 49 74 ca 66 22 38 a5 fb 40 74 df f9 47 6c 02 2b 6d c1 70 7f 60 8e 09 d1 b0 33 40 8b 23 70 c0 13 cb 9b f2 f8 b6 e9 e1 91 25 40 66 3a 32 44 50 17 15 63 b5 3b 01 5c 6e 22 db 08 4d 22 b5 fa ef c4 aa 19 12 a1 54 1a Data Ascii: \lO\WBBy\$mIG!:s(!v\$YPY/5me)!H !uSJmQFf2H6HTYLz FBWBANSD hxS}hUoAw3_Nu5_1ltf'8@tGl+mp'3@#p%@f:2DPC;\'M"\"T
2022-04-08 08:02:43 UTC	4301	IN	Data Raw: 59 59 6a 3a 79 65 88 84 5e c4 3f fc 11 5a 66 b3 36 8a cb 6c 72 90 19 56 89 f9 91 ae 69 30 a4 37 10 fd 62 31 52 64 63 be e7 e0 e5 fe 4e 64 63 cd 93 0c 78 47 d3 f5 7a bd 5f ec 90 44 65 cf 9b 24 b2 fc e9 d3 d6 01 fa 51 5a 29 4b f1 f8 7e 35 a7 8f c3 db 36 10 d7 90 2a 63 d5 fd 1f a1 af c2 04 d8 2c 8a 2f 36 e9 17 ae b0 04 d3 70 8e ce 01 03 c4 1f 7c 99 d5 e2 91 11 bf b3 fd f2 04 08 5d 2d 8a 32 93 0d 0e d4 5f f6 f2 bf 0c 1f a7 bb d2 9b 29 5d cd 82 c2 02 90 68 d5 24 11 b8 db 31 e5 8c 47 bf 74 89 5a 0b f4 4b c8 3d 48 94 b2 8f 1d ab 95 1c 27 98 67 c4 a7 2e 8e c4 16 84 06 1b 7c c7 cf 1f 08 91 b2 44 d0 d3 59 b4 4d c6 9b 1e 84 f7 f1 c8 18 d3 2e 24 39 b7 20 d3 60 72 14 92 5a 16 ac f5 60 36 1e d9 30 0b 12 56 7d 4d 88 00 0d ce fe d9 3e 12 8b 53 36 46 94 2a 7b e4 41 2a 83 92 Data Ascii: YYj:ye^?Zf6lrVl07b1RdcNdcxGz_De\$QZ)K~56*c,/6Cp]-2_)h\$1GtZK=H'g ,DYM.\$9`rZ'60V M>S6F*{A*
2022-04-08 08:02:43 UTC	4317	IN	Data Raw: c8 97 7a f4 1e 1e d8 aa 14 43 eb 44 fb 70 2d f0 93 dc 50 61 52 af f5 36 6e 31 09 39 34 74 14 1b 57 25 68 45 11 15 6a bf 69 3e 13 4f 7c 0c 79 25 3a a5 cc 4b 1c b6 68 c1 40 50 5d 80 e8 4f 4c 90 63 23 b2 41 ad 73 8b d2 9a 26 e4 95 54 03 dc 0f e3 96 92 d0 76 52 2f 6e ab 24 12 6f 71 4e 60 0e c0 f6 ae 45 53 3f 2a 35 c5 b8 e1 52 18 92 c0 1e d4 5c af 85 20 b2 fd 2b cc 13 24 f0 c2 1c 50 96 e2 2b f6 a8 3e 21 4e b9 1e 45 b8 10 9a ea 29 fa 46 d0 4f fb a8 bd 4a 9e 3c 2a 49 07 f9 ff 00 99 b2 bc b8 f8 87 4f 92 41 a2 c6 62 d1 f5 8d 2c 8b cb 54 62 c2 b4 00 6e 3e 79 a5 96 9c c4 f2 2e 40 93 24 b5 fc d2 b9 8a 38 e0 bf 82 93 56 8e dd a9 e3 93 fc dc c0 af a9 af 6b dd 9d 1b 88 66 09 28 20 87 5e 60 8c cd 9c a2 48 3f e7 32 00 8e 48 4b a9 8b 29 f4 c7 81 e2 73 0b 2c f6 35 fe c9 b2 Data Ascii: zCDp-PaR6n194tW%hEji>O y%:Kh@P JOLc#As&TvR/n\$oqN'ES?*5R!+\$P>+INE)FOJ<^IOAb,Tbn>y.@\$BvKf(^H?2HK)s.5
2022-04-08 08:02:43 UTC	4333	IN	Data Raw: 29 b0 90 0f 87 e4 e9 fc b8 08 6c 84 d1 67 58 5b 59 8d b0 fe f5 d7 72 07 63 e1 81 ca 13 49 b5 69 83 ca a9 6e 7d 59 7a 31 27 6a 78 65 f0 53 25 b6 11 30 8d 8b 40 1e 24 72 a4 50 d3 7f f2 b1 93 0b 57 d3 b5 28 62 4e 48 92 30 aa eb b7 35 a9 1e ca 4e 0a 4d af d1 35 2b 68 22 92 39 60 22 5d e8 c4 7d d8 78 52 24 84 6b 47 09 26 a1 2a 3b 26 ca 58 f4 f6 a7 b6 1a bd 9c 69 20 6e ef 52 59 7d 58 36 e6 07 20 36 02 9b 76 cb 62 18 09 b7 14 6a a0 b3 7e df 6a e4 8b 30 56 ad 89 9a 42 d1 bf 0e 1d 41 ee 31 55 9a b6 8e 42 7d 65 0d 01 23 6e ff 00 3c 31 92 54 e2 d5 0d b4 0a 5d 16 62 64 20 06 1e 03 ed 6 2 63 c6 84 a9 76 b3 14 46 38 ae 63 2e 85 c0 2c b5 db 7f e5 c9 43 9d 35 cc 24 67 d4 95 b9 8a 27 cb be 5d c9 a0 a7 36 1a 52 5d 46 5e 49 52 29 00 1b b9 da a3 2b 94 a9 31 8d a3 6c 74 b6 b1 Data Ascii:)lgX[Yrclin)Yz1'jxeS%0@\$rPW(bH05NM5+h"9")xR\$K&*&X;i nRY)X6 6vb j-j0VBA1UB)e#n<1T bd bc lvF8c.,C5\$g 6R F^iR)+1lt
2022-04-08 08:02:43 UTC	4341	IN	Data Raw: 38 73 65 c1 f4 9b 87 f3 32 7f c5 35 c8 47 27 d4 37 fe 7c 1e 97 a6 fe 70 e8 d7 16 cb 3d db 9b 77 6a d5 08 26 99 b3 c7 da 91 23 d5 19 c6 5f d0 1e 27 e3 89 a6 5a 33 7e 93 13 f1 e1 64 7a 47 9b 34 dd 5a 77 b4 b3 99 5e 78 80 2e 9d c5 73 61 8b 55 1c 86 87 d5 fd 2f 4b 8f 3c 12 80 b3 c9 37 ae 65 38 ee 3b e2 95 19 ad 96 51 46 01 87 b8 ae 53 3c 62 42 8b 21 2a 49 6f bc ba a2 33 e9 02 4d 3e ca 50 66 a3 36 83 d3 e9 ff 00 4b 0e 18 b9 10 cc 41 dd 84 cd 17 07 31 90 01 53 4a 75 39 c6 4b 29 8c b8 76 89 1f 8f e1 76 a0 5e e8 29 6c 95 ab 99 10 9f 7b 12 10 52 c0 4f 9d 3b 9c cd 8e 4b 6a 31 42 cb e5 0d 10 76 cc 8e 26 ba 41 4f a7 06 14 23 2d 86 42 18 98 a4 7a bf 95 e1 ba 42 84 75 df ad 0e 66 43 53 4c 38 18 e6 a3 e5 a9 61 00 db ad 05 29 b7 5d b3 32 19 44 97 92 55 f5 49 60 91 64 90 Data Ascii: 8se25G'7 p=wj&#_Z3-dzG4Zw^x.saU/K<7e8;QFS<bB!*Io3M>Pf6KA1SJuKj)vv^){RB;Kj1Bv&AO#-BzBuf CSL8a))2DUI'd

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:43 UTC	4357	IN	Data Raw: 46 5b 18 99 9a fe 1f 7f 08 a4 17 d7 f5 22 15 10 50 f1 05 ca 8a 9f bf bd 2d f0 a1 cd 90 34 85 d4 85 f5 95 b8 7d 38 55 8b 7a 93 28 6f 88 8e b9 7e 21 19 ca a7 dd e8 40 34 94 df 79 a2 5b 98 0f d6 58 86 8e 36 1c 7a 83 5f e6 cc dc 5a 7a 96 dd 7a b2 26 d8 a4 82 1b 96 0d 10 08 1b 72 07 41 b7 41 9d 24 62 40 dd 90 0a fa 14 4b 05 f2 2b ee 55 c1 af cf 24 79 33 8f 35 0d 43 49 45 b8 95 99 89 0a cc 29 df ae 4e 32 64 46 e9 2c 31 b2 b1 7a 0f 87 2e 2c 11 96 d7 6c 6a ab c7 89 dc a9 db 20 43 25 78 ca b4 ca d2 b3 50 76 5c 8a b5 fb 99 19 a6 49 82 b1 db 83 0d f0 2a 3a 26 d0 18 54 19 0a f0 a8 10 7a e3 4c d0 76 76 46 49 6b 1b 0e 4b fa b0 93 4b 49 aa da 38 97 d4 66 20 7f 2f f1 c8 5b 30 81 bb bc 2e 84 11 c8 73 a0 1e f9 30 18 92 83 9e d0 72 f4 a4 23 a7 22 7e 79 34 52 95 ab 24 6e Data Ascii: F["P-4]8Uz(o-!@4y[X6z_Zzz&rAA\$b@K+U\$y35CIE)N2dF,1z.,lj C%xpVl*:&T;ZLvFikKKI8f /{0.s0r#"~y4R\$n
2022-04-08 08:02:43 UTC	4373	IN	Data Raw: a9 07 b7 33 5f da 6c c2 cd 80 72 0b 18 52 0f 52 bb 92 2d 2d 9e 19 3d 05 66 11 b1 06 84 d7 7e 2b f4 7d ac b3 0e 3b 95 d7 12 77 0a 6a 2c b5 96 8c df ab dd 24 4b c6 36 2e 41 27 e6 7f dd 63 f9 72 44 cb 15 f0 ff 00 12 c8 71 f3 4c a1 bc d3 cd af d6 23 8e 22 63 2c a1 5a 81 99 bf 95 57 fe 36 cc 68 e2 9f 15 12 5a e4 18 66 a1 34 92 85 96 78 44 72 25 79 91 d4 ef 5d c7 b6 6d 61 11 1f 48 28 08 9d 67 cc c9 ad cb 6b 6b 37 2f aa 5b a2 ac 68 00 1b f5 73 f0 f5 e5 93 86 29 63 8d b7 df 11 a6 4f 0e b8 d6 ba a0 b8 53 e8 da 9f dd 8a f4 50 47 da e3 e2 33 4d 93 4e 25 0a e7 2f aa 95 51 b5 2d a9 95 51 b5 2d 57 53 b3 8d 1a 3b 49 5e 47 35 3f bc ec bd db 6f f8 5c 71 62 91 36 47 0c 7f a2 c4 86 33 69 ab 7a 6c 68 4a a4 87 ec f7 a7 f3 66 ce 58 d8 d2 ae 89 ae cc 2e 1d 02 02 0b 6d e2 b8 72 69 c1 03 bd 97 Data Ascii: 3_lrRR--f-+;wj,\$K6.A'crDqL#"c,ZW6hZf4xDr%y)maH(gkk7/[hs)cOSPG3MN%/Q-WS;l"G5?o!qb6G3izl hJfX.mri
2022-04-08 08:02:43 UTC	4381	IN	Data Raw: 24 37 ef 2a b0 94 33 89 09 ec 6a 37 19 b0 86 3b 8a 29 bd 4b 5a fa dc ab 33 28 09 c6 81 46 f4 f9 e2 21 41 40 a4 ef 4a d4 5c 43 e8 4a 83 d1 02 a7 fc a3 fe 51 cd 6e 58 8b 64 0a d3 6f 75 04 5c 62 60 11 c9 7e 27 a8 1f cb cb 24 08 2a 0a 43 34 72 ac 8d 50 40 6f 88 03 d3 36 98 c8 23 67 20 15 b7 5a 9c ab 10 83 91 0a 07 c2 05 32 c8 e3 de d2 83 b4 46 9a 44 1b b1 eb bf 86 5e 52 e9 9f 93 16 35 a5 7f 0c 21 4a 83 a5 47 c2 76 3d f2 4c 51 36 73 7d 5c b4 95 f8 d2 84 7d f9 09 0b 48 44 6a f7 29 70 ef 3a 0e a4 10 0f b8 c8 44 33 50 b6 bb 91 19 65 5a 72 42 2b 84 85 4e 6d 8a 5f c3 2c 51 d3 9e c4 07 e8 2b fd 32 b3 b3 2e 69 35 ee 98 63 4f 53 90 52 bb 32 d7 7a e5 f1 9d b5 f0 d2 95 bc 6d 3a fa 44 6f d5 49 fd 59 32 ad c5 a7 cb 3b 05 45 27 e8 c8 d8 55 69 ed 4c 47 94 9b 53 7d fc 3f 97 Data Ascii: \$7*3j7;)KZ3(FIA@JlCJQnXdoulb'~\$*C4rP@o6#g Z2FD^R5IJGv=LQ6s)}HdJ)p:D3PeZrB+Nm_,Q+2.i5cO SR2zm:DoLY2;E'UiLGSJ)?
2022-04-08 08:02:43 UTC	4397	IN	Data Raw: 40 ce b4 0a 77 07 df d2 8c b7 6e 05 ff d7 95 bc 34 04 0f bf 38 80 5d b2 c3 1d 05 06 e4 ef 86 d5 69 4a f6 af b6 36 85 16 84 7d 9d b6 e9 92 12 a4 52 9c b6 a4 fc 43 a7 86 4c 48 94 52 12 4b 05 91 78 b0 a0 f6 eb 96 c7 21 08 22 d2 7b ef 2c c5 37 4f 84 ef bf 4c cd 8e a6 9a b8 52 77 f2 d3 c4 c1 d9 b9 d2 a2 87 2d 8e 71 24 f2 4a ef ed 66 8e 70 78 9e 03 2d 04 24 2f b3 bd 26 51 14 ec 52 26 ea d4 ad 00 c8 ca 2c c1 4d b4 d4 fa f2 19 79 d1 cd 68 b4 ec 3e cf d3 95 53 30 99 5b 99 ad 17 d4 8c 96 2b f0 90 77 eb 92 8c 54 af be d4 c4 a6 34 08 89 c9 03 48 ca 3a 9a f4 f9 63 20 c4 36 52 19 e3 11 d4 03 52 08 ef 91 a4 a0 f5 ad 32 19 a1 53 15 56 45 db 90 dc fc b2 24 2d 28 40 5a 25 10 c6 d5 14 35 04 56 bf ec b1 4d 2f f4 64 22 bc 4c 84 8a 0e 27 ec 78 b3 0f b5 b6 4e 98 94 2d e6 ac ca Data Ascii: @w-n48jJ6)RCLHRRx!["f,7OLRw-q\$Jfpx-\$/&QR&,Myh>S0[+wT4H:c 6RR2SVE\$-(@Z%5VM/d"LxN-
2022-04-08 08:02:43 UTC	4413	IN	Data Raw: 5d 2e a3 24 4a 5d 18 a8 5e 81 46 df 45 32 54 a8 3f ac 4f 2b fa 85 99 d9 f6 df c3 20 52 98 5d 5d b4 30 34 2b 50 64 23 6e d4 f7 ca c8 64 0a f1 37 d5 20 49 6d d8 86 52 00 f9 e5 26 16 cc 14 6d 9c f1 4e 7d 4b a9 8a cc 49 a5 3a 6f fe 98 e5 52 14 cb 9a b2 d8 b7 a0 13 ec aa b7 d2 df 4f 86 55 c4 9a 5b 7f 66 92 5b a8 7e 28 c4 9a 61 05 48 b4 45 9d bc 11 21 49 18 82 12 84 d7 62 47 ec e5 f1 28 a4 3e a3 cf ea 1e 94 a0 05 eb 1f d9 f0 9a ef cb 2d 07 66 05 2b d3 04 e2 50 15 c8 e2 2a 49 e8 14 7d ac 21 08 f5 d6 22 92 d0 3f 10 e9 cc c7 24 6d fc a7 74 20 64 ad 5d 65 e5 d8 9c 96 b7 1e ac 24 16 a9 34 e0 3b ab 7f 36 46 5e 48 5c 25 8a 08 4f e8 22 20 2e a4 3c ef bc a6 9f 69 61 1f ee b4 3f 67 fc ac a8 4f 75 0e ee 63 aa 1e 18 89 6d cb d6 a7 fa e5 8a 13 8f 33 22 c8 6c 54 90 a8 f6 b1 Data Ascii:].\$J]^FE2T?O+ R]]04+Pd#nd7 lmr&mN)Kl:oROU[[~(aHEllBg(>-f+P!)"?&mt dje\$4;6F^H%O" .<ia? gOucm3"IT
2022-04-08 08:02:43 UTC	4420	IN	Data Raw: d5 23 78 d0 cd 2a 4a 9e a5 22 27 92 8e b4 eb ff 00 01 cb 31 e0 14 a4 d6 fc 65 b4 6b 9b 95 31 da 46 db bf 76 23 f6 23 fe 62 d9 97 8f 11 bb 62 91 6b 5a d9 bf 9c 4c d5 fb 34 45 1b 04 03 ec d0 7f c4 b3 69 10 84 b6 f5 3e d0 8c 7c 5b 10 4f 7a e5 b1 63 49 d7 94 75 f6 8a 6f aa 4c df 1f 63 d8 9f e5 c9 11 d5 83 7e 69 b6 58 48 36 c4 c6 67 3f 18 e9 bf cf c3 2c 01 41 62 a0 a7 a8 b1 86 e8 78 d7 09 0a 13 67 93 82 2c 6c 68 ea d5 1f d7 28 21 9d a7 2c f6 d7 d6 87 58 9c 11 34 6c 62 23 f6 5d a9 f6 ab fe 4f ed 64 69 16 92 5c 6a 33 ce 56 53 41 d0 20 1b 0f 0a d3 25 4c 6d a9 6e 9a d2 f8 04 62 ce 54 2a d3 72 0b 0f 8b 0d 6c ca d3 a9 e0 4d 1a d4 7d 70 73 b9 61 b2 06 e8 4f 4f 53 fe 25 95 18 d9 4f 12 4d 75 e6 1b fb a7 0a f2 fa 71 c6 36 e0 28 36 f9 65 c2 0c 49 6c 6b b7 f2 2d 2e 1b d7 Data Ascii: #x*J""1ek1Fv##bbkZL4Ei>[OzcluLc~iXH6g?,Abxg,lh(!,X4lb#)Odij3VSA %LmnbT'rIm)psaOOS%OMu q6(6ellk~.
2022-04-08 08:02:43 UTC	4428	IN	Data Raw: 69 59 19 79 25 3e d0 cd 1a f7 c1 6a 97 13 c2 46 54 f7 1b e5 81 0b 91 38 b7 05 ef e3 8d a5 5a 38 84 52 2a 1e e4 64 4a 4b 7a 95 1e 52 01 f9 63 14 29 b4 a1 4d 1b b0 eb de b8 55 50 4d e9 c2 ca ee b2 6d 5f 96 34 8b 50 96 4e 4c 85 45 0d 77 f9 e4 80 41 28 fb 18 d4 16 e4 4f 21 43 5e d9 5c 94 14 2e a7 23 5c 38 63 ca 68 b4 8c 82 b1 6c a1 07 83 92 ac 4f 5c 49 64 22 a9 a8 69 12 d9 a2 b9 a3 20 fd a1 d2 b8 23 90 1d 93 28 d2 0e de c8 cc fc 01 15 63 4a 9e 99 6b 5a ad e1 10 31 b6 e5 cb 8e c4 8c 88 43 a6 98 a0 48 9a 84 0e fe 35 c6 95 ab a9 3d 5e 2a a2 81 46 2b 6b e3 56 58 8b 11 b7 6f 9e 25 8a 8a 58 cd 70 6b 15 18 f8 54 0f d7 85 55 63 96 58 d1 d2 45 dc 0e f8 52 ff 00 ff d5 e4 d6 f6 33 59 84 11 d5 19 88 a6 e6 b9 a3 94 ef 9b 99 1b 0c 9e e6 de 1d 5e d9 22 bc 09 06 a7 06 ea Data Ascii: iYy%>jFT8Z8R*dJKzRc)MUPMm_4PNLEwA(OlC^\.#8clO!ld"i #cJkZ1CH5=^*F+kVXo%XpkTucXER3Y^"
2022-04-08 08:02:43 UTC	4444	IN	Data Raw: cc 8a 8a 01 80 a5 b9 a3 48 ea 62 26 9d f0 02 94 48 96 39 6c e3 8d f6 08 cc 6a 3b ea 43 a4 a5 a1 94 6e 09 cb 98 af 31 bb 2a d3 a1 38 aa 3b 4c 65 42 d6 b3 b5 22 94 10 7d 8f 66 ca c8 64 10 52 c2 60 91 a0 9b 62 a6 99 20 c4 ac 08 54 d3 b9 e9 85 5b 9c 99 37 2b bf 7c 52 54 08 2a 6a 31 50 ab c8 ad 1d 5a 87 bd 31 a4 5a 35 35 43 31 55 9c 06 00 d7 61 42 7e 79 03 16 60 a2 d0 46 92 99 cd 1e dc 9a 15 1f 69 6b d3 6c 83 35 93 e9 e6 61 c8 29 e5 4a a9 f1 51 84 49 d9 16 82 8b fd 15 d6 53 b8 e5 51 92 3b a0 35 7f 2f ef 5c 91 d7 a7 cb 27 15 28 6a 02 2a 32 6c 17 a5 c3 29 1d c0 39 1a 55 7b a8 04 f1 9b 88 8e d5 f8 97 c3 df 22 d0 32 43 a2 54 aa 8d ab 85 57 48 38 fc 0f b3 03 f4 61 55 17 42 56 a7 b6 2c 6d 74 23 8b 0f a3 14 aa 86 2b 2f 31 b9 3e 39 12 90 8f 72 56 20 e7 ed 48 6a 7e 8c Data Ascii: Hb&H9l];:n1*8;LeB")fdR' b T[7+!RT*j1PZ1Z55C1UaB~y' Fikl5a)JQISQ;5/\(j!t2)9U["2CTWH8aUBV,mt#/+1>9rV Hj~
2022-04-08 08:02:43 UTC	4460	IN	Data Raw: cf 25 4c 0a c9 dc b0 0d 4a 56 bf 4e f9 20 c0 b4 f7 2c f4 a9 a1 51 4c 69 16 b4 a3 cc e1 4e 4c 9c 3c 92 af e9 bc 2e 62 a1 0e 3a fb 60 29 58 39 8f 8b bd 69 8b 17 7d 5c 85 24 90 38 ee 47 7c 55 62 d7 a8 1f 0a 9a e2 86 4d ab 0f ad d8 1b a9 a9 19 75 e4 8a bd 3e 1a 57 31 e2 6a 4e 41 1b 31 35 76 e8 3e ce 65 b8 ca fa f3 1e e3 15 54 86 d9 9c 85 5d c9 f0 c8 b2 57 fa 8f a7 46 63 c5 87 4a 62 95 f1 35 5c 24 c0 9e df 7e 56 5b 41 74 b6 e8 a7 8a b0 6d f7 ef 81 90 56 b6 bd 8e c6 42 61 a4 91 b0 a3 21 e9 82 93 74 a7 34 75 84 18 b6 35 24 83 d4 7f 66 48 31 28 49 59 88 af 61 b6 4d 83 8c a2 30 d4 a1 3d 71 55 3f 59 8f 4d 81 c5 16 dc 07 e2 2d d2 98 0a 42 aa 32 a3 9e 04 d4 8c 89 67 6d c9 3b 03 c3 a8 18 29 16 d1 7e 6d 49 07 6d bd b0 a9 58 50 d2 ab f6 87 5c 28 08 c5 9f d3 21 36 35 f1 Data Ascii: %LJVN_QLin<.b:')X9i)\$8GjUbMu>W1jNA15v>eTjWfCJb5\$~V[AtmVBal4u5\$fh1(IYaM0=QU?YM-B2gm;) ~mlmXP(!65

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:43 UTC	4468	IN	Data Raw: 29 b6 42 99 5a 37 4e b9 06 91 10 09 62 01 f6 c8 10 c8 29 6a d0 f0 24 7e da 9c 30 44 90 d1 51 c1 92 6a 90 3f 1c 91 62 9d 68 57 3f bd 61 12 d1 58 6f f2 ca e4 1b 22 a5 ac 42 6e d5 e7 8c d7 81 1b 7f c6 d9 18 6c 99 25 b6 17 de 9f c0 db ad 6b f4 e4 e7 16 31 29 c8 b7 12 32 f1 23 a5 72 86 d0 9b 59 48 45 ab f3 db e2 00 fc 86 50 46 ed 81 2d 98 21 af 23 ef 96 02 b4 ba ca ef 8c 81 49 a2 80 7f db c3 cd 09 34 3a 9a 76 03 73 c8 8f ed cb 0b 02 9e 5d 5b 47 50 ef bd 40 a5 3d b2 b4 a1 a3 a3 bb 31 d9 68 46 10 a5 2e b8 8c 28 a8 df 2d 8b 10 a3 1a b4 3f bd a0 a7 20 69 f2 c2 77 54 de ea e1 35 48 8b cb 18 59 86 c2 9d 3e 8c a6 23 84 a4 d1 41 45 6d f5 65 f4 c7 da ad 4e 4c 9b 63 4b 27 91 62 4e 4a 3e 26 ea b8 a5 e8 3a a5 d4 7f 55 85 58 33 7c 08 0a 13 ed b6 00 92 18 b6 aa 91 81 e9 c6 Data Ascii:)BZ7Nb)j\$-0DQj?bhW?aXo"Bnl%k1)2#rYHEPF-!#l44vs][GP@=1hF.(-? iwT5HY>#AEmeNLcK'bNJ>&:UX3]

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49993	23.10.249.43	443	C:\Users\user\Desktop\l.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	82	OUT	GET /cms/api/am/imageFileData/RWP0UC?ver=2f44 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate, br User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134 Host: img-prod-cms-rt-microsoft-com.akamaized.net Connection: Keep-Alive
2022-04-08 08:02:42 UTC	1426	IN	HTTP/1.1 200 OK Content-Type: image/jpeg Content-Location: https://image.prod.cms.rt.microsoft.com/cms/api/am/imageFileData/RWP0UC?ver=2f44 Last-Modified: Thu, 07 Apr 2022 10:42:26 GMT Access-Control-Allow-Origin: * X-Source-Length: 1654488 X-Datcenter: northeu X-ActivityId: abdce6fd-750b-4250-8d13-1c71db5b1df8 Timing-Allow-Origin: * X-Frame-Options: deny X-ResizerVersion: 1.0 Content-Length: 1654488 Cache-Control: public, max-age=355227 Expires: Tue, 12 Apr 2022 10:43:09 GMT Date: Fri, 08 Apr 2022 08:02:42 GMT Connection: close
2022-04-08 08:02:42 UTC	1427	IN	Data Raw: ff d8 ff e1 14 ed 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 07 01 12 00 03 00 00 00 01 00 01 00 00 01 1a 00 05 00 00 00 01 00 00 00 62 01 1b 00 05 00 00 00 01 00 00 00 6a 01 28 00 03 00 00 00 01 00 02 00 00 01 31 00 02 00 00 00 1f 00 00 00 72 01 32 00 02 00 00 14 00 00 00 91 87 69 00 04 00 00 00 01 00 00 00 a8 00 00 00 d4 00 0e a6 00 00 00 27 10 00 0e a6 00 00 00 27 10 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 32 31 2e 31 20 28 57 69 6e 64 6f 77 73 29 00 32 30 32 31 3a 31 31 3a 31 31 20 30 36 3a 35 35 3a 33 38 00 00 00 00 00 03 a0 01 00 03 00 00 00 01 ff ff 00 00 a0 02 00 04 00 00 00 01 00 00 04 38 a0 03 00 04 00 00 00 01 00 00 07 80 00 00 00 00 00 00 00 06 01 03 00 03 00 00 00 01 00 06 00 00 01 1a 00 05 00 00 00 01 00 00 01 22 01 1b 00 05 00 Data Ascii: ExifMM*bj(1r2i"Adobe Photoshop 21.1 (Windows)2021:11:11 06:55:388"
2022-04-08 08:02:42 UTC	1442	IN	Data Raw: 44 6f 63 75 6d 65 6e 74 49 44 3d 22 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 66 31 31 36 35 37 37 66 2d 35 37 35 64 2d 38 33 34 37 2d 39 38 64 36 2d 38 39 30 65 32 65 30 33 31 30 32 32 22 20 78 6d 70 4d 4d 3a 4f 72 69 67 69 6e 61 6c 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 61 38 35 33 32 65 62 65 2d 62 34 31 32 2d 34 37 34 36 2d 39 35 30 62 2d 32 65 31 31 64 66 33 66 66 34 37 31 22 20 78 6d 70 4e 6f 74 65 3a 48 61 73 45 78 74 65 6e 64 65 64 58 4d 50 3d 22 44 30 41 33 39 39 46 34 41 45 41 43 31 44 35 32 33 36 45 36 43 31 37 41 31 39 33 42 34 41 33 44 22 3e 20 3c 70 68 6f 74 6f 73 68 6f 70 3a 54 65 78 74 4c 61 79 65 72 73 3e 20 3c 72 64 66 3a 42 61 67 3e 20 3c 72 64 66 3a 6c 69 20 70 68 6f 74 6f 73 68 6f 70 3a 4c Data Ascii: DocumentID="adobe:docid:photoshop:f116577f-575d-8347-98d6-890e2e031022" xmpMM:OriginalDocumentID="xmp.did:a8532ebe-b412-4746-950b-2e11df3ff471" xmpNote:HasExtendedXMP="D0A399F4AEAC1D5236E6C17A193B4A3D"> <photoshop:TextLayers> <rdf:Bag> <rdf:li photoshop:L
2022-04-08 08:02:42 UTC	1458	IN	Data Raw: 67 65 5c 5f 43 72 6f 70 73 5c 45 64 67 65 2d 4c 69 66 65 73 74 79 6c 65 5f 73 68 75 74 74 65 72 73 6f 63 6b 5f 33 35 33 34 31 36 30 30 37 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 37 2d 32 36 54 31 31 3a 30 33 3a 33 30 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 45 64 67 65 5c 5f 43 72 6f 70 73 5c 45 64 67 65 2d 4c 69 66 65 73 74 79 6c 65 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 38 37 33 34 31 30 36 31 5f 31 30 38 30 78 31 39 3 2 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 37 2d 32 36 54 31 31 3a 30 34 3a 33 36 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 Data Ascii: ge_Crops\Edge-Lifestyle_shutterstock_353416007_1080x1920.jpg saved
2016-07-26T11:03:30-07:00	File C:\Users\lv-lizagh\MS\Windows10\Edge_Crops\Edge-Lifestyle_GettyImages-87341061_1080x1920.jpg saved
2016-07-26T11:04:36-07:00	File C:\Users\lv
2022-04-08 08:02:42 UTC	1460	IN	Data Raw: 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 37 2d 32 36 54 31 38 3a 31 37 3a 33 39 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 37 2d 32 36 54 31 38 3a 32 33 3a 32 39 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 37 2d 32 36 54 31 38 3a 32 34 3a 33 31 2d 30 37 3a 30 30 26 23 Data Ascii: ved
2016-07-26T18:17:39-07:00	File C:\Users\lv-lizagh\MS\Windows10\Lockscreen_1080x1920_Por trait.psd saved
2016-07-26T18:23:29-07:00	File C:\Users\lv-lizagh\MS\Windows10\Lockscreen_1080x1920_Por trait.psd saved
2016-07-26T18:24:31-07:00&#

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	1476	IN	Data Raw: 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 38 2d 33 31 54 31 33 3a 34 32 3a 33 39 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 39 2d 31 32 54 31 30 3a 32 36 3a 30 38 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 6f 70 65 6e 65 64 26 23 78 41 3b 32 30 31 36 2d 30 39 2d 31 32 54 31 30 3a 32 38 3a 35 30 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a Data Ascii: 0.jpg saved
2016-08-31T13:42:39-07:00	File C:\Users\lv-lizagh\MS\Windows10\Lockscreen_1080x1920_Portrait.psd saved
2016-09-12T10:26:08-07:00	File Lockscreen_1080x1920_Portrait.psd opened
2016-09-12T10:28:50-07:00	File C:\Users\lv-liz
2022-04-08 08:02:42 UTC	1492	IN	Data Raw: 69 74 79 5c 45 64 67 65 53 75 72 67 65 2d 52 65 61 64 69 6e 67 56 69 65 77 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 39 35 36 39 35 32 39 31 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 31 30 2d 31 37 54 31 38 3a 33 34 3a 35 33 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 45 64 67 65 5c 53 75 72 67 65 5c 52 65 61 64 69 6e 67 56 69 65 77 5f 4e 6f 64 69 73 74 72 61 63 74 69 6f 6e 73 2d 43 6f 6e 63 65 6e 74 72 61 74 69 6e 67 2d 46 6f 63 75 73 2d 53 69 6d 70 6c 69 63 69 74 79 5c 45 64 67 65 53 75 72 67 65 2d 52 65 61 64 69 6e 67 56 69 65 77 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 36 35 3a 35 38 37 35 5f 31 30 38 30 78 3 Data Ascii: ity\EdgeSurge-ReadingView_GettyImages-95695291_1080x1920.jpg saved
2016-10-17T18:34:53-07:00	File C:\Users\lv-lizagh\MS\Windows10\Edge\Surge\ReadingView_Nodistractions-Concentrating-Focus-Simplicity\EdgeSurge-ReadingView_GettyImages-578195377_1080x
2022-04-08 08:02:42 UTC	1723	IN	Data Raw: 73 31 30 5c 43 6f 72 74 61 6e 61 5c 43 6f 72 74 61 6e 61 2d 52 65 6d 69 6e 64 65 72 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 36 32 30 39 32 38 32 33 39 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 31 31 2d 31 34 54 31 35 3a 35 35 3a 33 37 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 43 6f 72 74 61 6e 61 5c 43 6f 72 74 61 6e 61 2d 52 65 6d 69 6e 64 65 72 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 36 35 3a 35 38 37 35 5f 31 30 38 30 78 3 Data Ascii: s10\Cortana\Cortana-Reminder_GettyImages-620928239_1080x1920.jpg saved
2016-11-14T15:55:37-08:00	File C:\Users\lv-lizagh\MS\Windows10\Cortana\Cortana-Reminder_GettyImages-665495875_1080x1920.jpg saved
2016-11-14T15:55:45-08:00	File C:\Users
2022-04-08 08:02:42 UTC	2462	IN	Data Raw: 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 41 64 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 2e 35 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 4d 49 54 2d 57 69 6e 74 65 72 45 6e 74 65 72 74 61 69 6e 6d 65 6e 74 2d 4f 73 63 61 72 73 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 35 30 38 30 78 31 39 32 30 45 36 44 39 31 43 44 33 36 38 33 31 39 46 44 30 32 34 37 46 39 43 34 36 31 44 39 41 46 30 30 37 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 31 2d 32 30 54 31 31 3a 31 38 3a 35 39 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 6f 6d 65 6e 74 73 49 6e 54 69 Data Ascii: -lizagh\AppData\Roaming\Adobe\Adobe Photoshop CC 2015.5\AutoRecover__MIT-WinterEntertainment-Oscar_s_GettyImages-150892480_1080x1920E6D91CD368319FD0247F9C461D9AF007.psb saved
2017-01-20T11:18:59-08:00	File C:\Users\lv-lizagh\MS\Windows10\Moments\InTi
2022-04-08 08:02:42 UTC	2494	IN	Data Raw: 41 45 45 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 34 37 34 37 36 33 39 35 32 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 32 2d 32 33 54 30 39 3a 34 35 3a 30 33 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 45 64 67 65 5c 4e 41 41 45 45 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 45 64 67 65 2d 4e 41 41 45 45 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 34 38 34 30 30 36 30 35 34 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 32 2d 32 33 54 30 39 3a 34 36 3a 34 39 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 Data Ascii: AEE_GettyImages-474763952_1080x1920.jpg saved
2017-02-23T09:45:03-08:00	File C:\Users\lv-lizagh\MS\Windows10\Edge\NAAEE\CHOSEN\Crops\Edge-NAAEE_GettyImages-484006054_1080x1920.jpg saved
2017-02-23T09:46:49-08:00	File C:\Users\lv-lizagh\MSWi
2022-04-08 08:02:42 UTC	2518	IN	Data Raw: 74 2d 41 70 72 69 6c 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 31 37 31 38 38 36 38 38 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 33 2d 31 34 54 31 32 3a 31 31 3a 30 33 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 33 2d 31 35 54 31 35 3a 31 36 3a 33 30 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 6f 70 65 6e 65 64 26 23 78 41 3b 32 30 31 37 2d 30 33 2d 31 35 54 Data Ascii: t-April_GettyImages-517188688_1080x1920.jpg saved
2017-03-14T12:11:03-07:00	File C:\Users\lv-lizagh\MS\Windows10\Lockscreen_1080x1920_Portrait.psd saved
2017-03-15T15:16:30-07:00	File Lockscreen_1080x1920_Portrait.psd opened
2017-03-15T
2022-04-08 08:02:42 UTC	2553	IN	Data Raw: 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 34 2d 31 32 54 31 31 3a 34 30 3a 32 37 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 41 64 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 2e 35 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 42 69 6e 67 41 74 57 6f 72 6b 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 33 37 31 34 34 32 39 33 5f 31 30 38 30 78 31 39 32 30 30 39 39 45 36 30 37 34 41 43 31 42 42 33 35 41 31 34 38 39 37 31 46 39 34 30 45 42 30 41 30 44 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 34 2d 31 32 54 31 31 3a 34 30 3a 35 36 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c Data Ascii: jpg saved
2017-04-12T11:40:27-07:00	File C:\Users\lv-lizagh\AppData\Roaming\Adobe\Adobe Photoshop CC 2015.5\AutoRecover__BingAtWork_GettyImages-137144293_1080x1920099E6074AC1BB35A148971F940EB0A0D.psb saved
2017-04-12T11:40:56-07:00	File C:\
2022-04-08 08:02:42 UTC	2609	IN	Data Raw: 65 64 26 23 78 41 3b 32 30 31 37 2d 30 35 2d 31 31 54 31 35 3a 31 39 3a 34 32 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 6f 6d 65 6e 74 73 49 6e 54 69 6d 65 5c 4e 42 41 5c 4d 61 79 5c 43 68 6f 73 65 6e 5c 43 72 6f 70 73 5c 4d 49 54 2d 4e 42 41 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 36 35 39 31 35 38 37 30 30 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 35 2d 31 31 54 31 35 3a 32 30 3a 31 36 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 Data Ascii: ed
2017-05-11T15:19:42-07:00	File C:\Users\lv-lizagh\MS\Windows10\Moments\InTime\NBA\May\Chosen\Crops\MIT-NBA_GettyImages-659158700_1080x1920.jpg saved
2017-05-11T15:20:16-07:00	File C:\Users\lv-lizagh\MS\Windows10\Lockscreen_1080x1920_Portra

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	2625	IN	Data Raw: 32 5c 5f 43 48 4f 53 45 4e 2d 4f 33 36 35 52 65 6e 65 77 61 6c 5c 4f 66 66 69 63 65 2d 42 32 5f 35 30 30 70 78 2d 31 35 32 32 38 37 36 32 31 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 36 2d 31 31 54 31 39 3a 34 36 3a 32 34 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4f 66 66 69 63 65 5c 4f 66 66 69 63 65 2d 42 61 74 63 68 32 5c 5f 43 48 4f 53 45 4e 2d 4f 33 36 35 52 65 6e 65 77 61 6c 5c 4f 66 66 69 63 65 2d 42 32 5f 35 30 30 70 78 2d 31 35 34 31 33 30 33 31 35 5f 31 30 38 30 78 31 39 32 30 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 36 2d 31 31 54 31 39 3a 34 36 3a 33 34 2d 30 37 3a 30 30 26 Data Ascii: 2_CHOSEN-O365Renewal\Office-B2_500px-152287621_1080x1920.jpg saved&#xA;2017-06-11T19:46:24-07:00&#x9;File C:\Users\lv-lizagh\MSI\Windows10\Office\Office-Batch2_CHOSEN-O365Renewal\Office-B2_500px-154130315_1080x1920.psd saved&#xA;2017-06-11T19:46:34-07:00&
2022-04-08 08:02:42 UTC	2633	IN	Data Raw: 26 23 78 41 3b 32 30 31 37 2d 30 37 2d 30 39 54 31 36 3a 31 34 3a 34 39 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 2e 70 73 64 20 6f 70 65 6e 65 64 26 23 78 41 3b 32 30 31 37 2d 30 37 2d 30 39 54 31 36 3a 31 34 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 41 64 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 37 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 30 38 30 78 31 39 32 30 5f 50 6f 72 74 72 61 69 74 46 30 31 39 34 34 45 44 31 42 37 43 33 38 42 38 44 46 35 33 38 45 43 44 33 39 43 34 43 Data Ascii: &#xA;2017-07-09T16:14:49-07:00&#x9;File Lockscreen_1080x1920_Portrait.psd opened&#xA;2017-07-09T16:24:26-07:00&#x9;File C:\Users\lv-lizagh\AppData\Roaming\Adobe\Adobe Photoshop CC 2017\AutoRecover_Lockscreen_1080x1920_Portrait\F01944ED1B7C38B8DF538ECD39C4C
2022-04-08 08:02:42 UTC	3031	IN	Data Raw: 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 37 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 42 69 6e 67 53 70 6f 74 6c 69 67 68 74 51 75 69 7a 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 30 34 35 30 38 32 33 30 5f 31 30 38 30 78 31 39 32 30 41 37 30 32 45 36 46 36 44 37 38 38 31 31 33 46 46 35 44 39 31 30 39 45 38 38 30 37 31 32 39 46 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 37 2d 32 33 31 54 31 34 3a 35 35 3a 35 32 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 42 69 6e 67 5c 53 70 6f 74 6c 69 67 68 74 51 75 69 7a 5c 5f 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 42 69 6e 67 53 70 6f 74 6c 69 67 68 74 51 75 69 7a 5f 73 68 Data Ascii: be\Adobe Photoshop CC 2017\AutoRecover_BingSpotlightQuiz_GettyImages-504508230_1080x1920A702E6F6D788113FF5D9109E8807129F.psb saved&#xA;2017-07-31T14:55:52-07:00&#x9;File C:\Users\lv-lizagh\MSI\Windows10\Bing\SpotlightQuiz_CHOSEN\Crops\BingSpotlightQuiz_sh
2022-04-08 08:02:42 UTC	3047	IN	Data Raw: 32 33 3a 32 37 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 41 64 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 37 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 57 69 6e 64 6f 77 73 4d 4d 58 2d 52 64 32 5f 35 30 30 70 78 2d 31 38 32 32 36 35 37 33 5f 31 30 38 30 78 31 39 32 30 30 42 45 35 43 34 30 42 45 35 43 34 38 42 38 45 31 43 46 46 38 33 33 38 37 45 34 46 34 31 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 39 2d 32 35 54 31 36 3a 31 34 3a 32 35 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 6f 6d 65 6e Data Ascii: 23:27-07:00&#x9;File C:\Users\lv-lizagh\AppData\Roaming\Adobe\Adobe Photoshop CC 2017\AutoRecover_WindowsMMX-Rd2_500px-18226573_1080x19200BE5C9CDD93C48B8E1CFF83387E4F41.psb saved&#xA;2017-09-25T16:14:25-07:00&#x9;File C:\Users\lv-lizagh\MSI\Windows10\Momen
2022-04-08 08:02:42 UTC	3054	IN	Data Raw: 74 6f 72 73 55 70 64 61 74 65 5c 46 61 6c 6c 43 72 65 61 74 6f 72 73 55 70 64 61 74 65 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 36 38 35 31 30 37 35 38 5f 31 30 38 30 78 31 39 32 30 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 31 30 2d 31 38 54 31 35 3a 34 36 3a 31 38 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 46 61 6c 6c 43 72 65 61 74 6f 72 73 55 70 64 61 74 65 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 3 6 38 35 31 30 37 35 38 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 31 30 2d 31 38 54 31 35 3a 34 37 3a 35 35 2d 30 37 3a 30 30 26 23 78 39 Data Ascii: torsUpdate\FallCreatorsUpdate_GettyImages-168510758_1080x1920.psd saved&#xA;2017-10-18T15:46:18-07:00&#x9;File C:\Users\lv-lizagh\MSI\Windows10\FallCreatorsUpdate\FallCreatorsUpdate_GettyImages-168510758_1080x1920.jpg saved&#xA;2017-10-18T15:47:55-07:00&#x9
2022-04-08 08:02:42 UTC	3070	IN	Data Raw: 70 70 69 6e 67 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4d 49 54 2d 42 6c 61 63 6b 46 72 69 64 61 79 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 33 36 32 30 31 33 33 39 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 31 31 2d 32 32 54 31 30 3a 34 34 3a 30 35 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 6f 6d 65 6e 74 73 49 6e 54 69 6d 65 5c 42 6c 61 63 6b 46 72 69 64 61 79 43 68 72 69 73 74 6d 61 73 53 68 6f 70 70 69 6e 67 5c 43 48 4f 5 3 45 4e 5c 43 72 6f 70 73 5c 4d 49 54 2d 42 6c 61 63 6b 46 72 69 64 61 79 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 30 36 38 34 32 33 38 33 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 Data Ascii: pping\CHOSEN\Crops\MIT-BlackFriday_GettyImages-136201339_1080x1920.jpg saved&#xA;2017-11-22T10:44:05-08:00&#x9;File C:\Users\lv-lizagh\MSI\Windows10\MomentsInTime\BlackFridayChristmasShopping\CHOSEN\Crops\MIT-BlackFriday_GettyImages-506842383_1080x1920.jpg
2022-04-08 08:02:42 UTC	3086	IN	Data Raw: 65 73 2d 31 37 37 34 32 37 39 31 37 5f 31 30 38 30 78 31 39 32 30 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 31 32 2d 32 30 54 32 30 3a 35 31 3a 34 32 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 49 54 2d 49 6e 74 65 72 6e 6 1 74 69 6f 6e 61 6c 5c 43 72 69 63 6b 65 74 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4d 49 54 2d 41 73 68 65 73 43 72 69 63 6b 65 74 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 37 37 34 32 37 39 31 37 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 31 32 2d 32 30 34 32 30 3a 35 34 3a 32 36 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 Data Ascii: es-177427917_1080x1920.psd saved&#xA;2017-12-20T20:51:42-08:00&#x9;File C:\Users\lv-lizagh\MSI\Windows10\MIT-International\Cricket\CHOSEN\Crops\MIT-AshesCricket_GettyImages-177427917_1080x1920.jpg saved&#xA;2017-12-20T20:54:26-08:00&#x9;File C:\Users\lv-liza
2022-04-08 08:02:42 UTC	3094	IN	Data Raw: 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4d 49 54 2d 47 72 61 6d 6d 79 73 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 37 38 30 37 32 34 33 30 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 31 2d 31 37 54 31 34 3a 33 31 3a 32 33 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 6f 6d 65 6e 74 73 49 6e 54 69 6d 65 5c 47 52 41 4d 4d 59 53 5c 32 30 31 37 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4d 49 54 2d 47 72 61 6d 6d 79 73 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 38 30 37 34 39 32 34 31 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 31 2d 31 37 54 31 34 3a 33 33 3a 35 31 Data Ascii: \CHOSEN\Crops\MIT-Grammys_GettyImages-578072430_1080x1920.jpg saved&#xA;2018-01-17T14:31:23-08:00&#x9;File C:\Users\lv-lizagh\MSI\Windows10\MomentsInTime\GRAMMYS\2017\CHOSEN\Crops\MIT-Grammys_GettyImages-580749241_1080x1920.jpg saved&#xA;2018-01-17T14:33:51

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	3102	IN	Data Raw: 54 31 33 3a 35 37 3a 30 39 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 53 72 65 77 61 72 64 73 5c 41 75 73 74 72 61 6c 69 61 2d 55 4b 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4d 53 72 65 77 61 72 64 73 2d 41 55 2d 55 4b 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 36 31 31 39 36 31 35 38 36 5f 31 30 38 30 78 31 39 32 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 31 2d 32 39 54 31 33 3a 35 39 3a 32 35 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 53 72 65 77 61 72 64 73 5c 41 75 73 74 72 61 6c 69 61 2d 55 4b 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 Data Ascii: T13:57:09-08:00&#x9;File C:\Users\lv-lizagh\MSI\Windows10\MSrewards\Australia-UK\CHOSEN\Crops\ops\MSrewards-AU-UK_GettyImages-611961586_1080x1920.jpg saved&#xA;2018-01-29T13:59:25-08:00&#x9;File C:\Users\lv-lizagh\MSI\Windows10\MSrewards\Australia-UK\CHOSEN\Crops
2022-04-08 08:02:42 UTC	3118	IN	Data Raw: 26 23 78 41 3b 32 30 31 38 2d 30 33 2d 30 31 54 31 31 3a 34 31 3a 33 38 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 49 54 2d 49 6e 74 65 72 6e 61 74 69 6f 6e 61 6c 5c 54 72 61 76 65 6c 2d 53 41 2d 45 75 72 6f 70 65 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 33 2d 30 31 54 31 31 3a 34 31 3a 35 39 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 49 54 2d 49 6e 74 65 72 6e 61 74 69 6f 6e 61 6c 5c 54 72 61 76 65 6c 2d 53 41 2d 45 75 72 6f 70 65 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4d 49 54 2d 54 72 61 76 Data Ascii: &#xA;2018-03-01T11:41:38-08:00&#x9;File C:\Users\lv-lizagh\MSI\Windows10\MIT-International\Travel-SA-Europe\CHOSEN\Crops.jpg saved&#xA;2018-03-01T11:41:59-08:00&#x9;File C:\Users\lv-lizagh\MSI\Windows10\MIT-International\Travel-SA-Europe\CHOSEN\Crops\MIT-Trav
2022-04-08 08:02:42 UTC	3134	IN	Data Raw: 3a 6c 69 3e 30 31 33 41 34 38 31 44 37 30 39 45 44 33 43 46 31 45 37 41 36 43 34 36 35 46 35 43 38 30 43 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 31 34 33 37 39 43 33 43 39 31 44 45 32 38 33 46 46 46 43 32 42 45 34 44 37 38 45 39 34 46 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 31 34 33 37 45 34 39 33 3 0 30 44 38 42 31 43 32 36 36 34 37 32 46 32 36 35 45 36 35 43 38 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 31 35 32 45 44 44 46 43 37 44 38 33 32 34 46 45 32 43 32 31 39 37 41 45 42 39 36 46 43 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 31 35 39 44 31 43 31 39 43 35 32 44 31 46 32 45 30 34 37 42 43 31 34 35 41 43 44 38 35 43 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 Data Ascii: .li>013A481D709ED3CF1E7A6C465F5C80C8</rdf:li> <rdf:li>014379C3C91DE283FFFC2BE4D78E94F2</rdf:li> <rdf:li>01437E49300D8B1C266472F265E65C8A</rdf:li> <rdf:li>0152EDDFC7D8324FE2C2197AEB96FFC3</rdf:li> <rdf:li>0159D1C19C52D1F2E047BC145ACD85CB</rdf:li> <rdf:li>0
2022-04-08 08:02:42 UTC	3142	IN	Data Raw: 69 3e 30 37 35 42 30 34 38 37 43 38 41 38 33 37 36 31 46 43 39 38 44 35 31 46 42 36 44 41 36 38 46 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 37 37 39 31 31 36 37 45 30 31 42 35 41 34 37 33 34 43 32 46 34 35 33 45 42 42 44 41 38 42 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 37 38 32 38 36 44 36 39 43 38 34 41 43 41 36 34 43 45 42 39 45 44 44 33 39 37 41 39 39 41 42 3c 2f 72 64 66 3a 6c 69 3e 30 3c 72 64 66 3a 6c 69 3e 30 3 7 38 33 44 42 45 35 33 41 32 37 31 45 43 46 39 35 39 44 39 37 45 46 42 44 46 41 33 36 33 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 37 38 39 36 31 34 43 39 33 43 36 37 41 43 38 35 35 38 33 42 33 38 45 30 46 31 32 39 39 43 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 37 39 Data Ascii: i>075B0487C8A83761FC98D51FB6DA68FC</rdf:li> <rdf:li>07791167E01B5A4734C2F453EBBDA8B4</rdf:li> <rdf:li>078286D69C84ACA64CEB9EDD397A99AB</rdf:li> <rdf:li>0783DBE53A271ECF959D97EFBDF3A3638</rdf:li> <rdf:li>0789614C93C67AC85583B38E0F1299C3</rdf:li> <rdf:li>079
2022-04-08 08:02:42 UTC	3158	IN	Data Raw: 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 34 36 44 42 31 41 36 36 42 46 46 30 46 43 39 42 30 35 43 32 37 33 43 39 46 33 38 35 39 31 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 34 37 32 31 41 42 35 37 39 36 39 32 32 38 31 43 44 36 33 31 44 33 43 33 42 46 37 32 43 30 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 34 37 45 30 36 45 31 44 45 46 33 35 33 31 45 30 45 36 33 43 39 30 39 46 36 32 35 37 33 46 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 34 38 34 38 30 42 44 38 33 35 38 32 38 44 31 30 33 45 35 36 37 39 41 33 32 34 45 46 39 45 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 34 39 32 34 36 42 37 36 46 41 45 43 44 41 38 37 31 37 43 32 33 32 42 41 39 44 33 30 35 35 30 3c 2f 72 64 66 Data Ascii: </rdf:li> <rdf:li>146DB1A66BFF0FC9B05C273C9F385917</rdf:li> <rdf:li>14721AB579692281CD631D3C3BF72C08</rdf:li> <rdf:li>147E06E1DEF3531E0E63C909F62573F5</rdf:li> <rdf:li>148480BD835828D103E5679A324EF9E5</rdf:li> <rdf:li>149246B76FAECD8A717C232BA9D30550</rdf
2022-04-08 08:02:42 UTC	3174	IN	Data Raw: 31 31 36 31 43 44 35 34 31 38 37 44 34 44 44 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 32 37 39 32 30 45 34 42 41 35 30 34 32 36 33 32 33 42 39 37 33 45 35 42 34 39 44 34 43 31 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 32 37 46 32 31 43 35 44 33 33 35 35 37 31 39 39 34 36 35 31 37 45 37 32 31 31 30 30 31 38 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 32 39 33 38 31 44 41 30 36 36 31 34 38 30 41 38 31 43 3 8 32 37 36 35 30 36 42 36 31 39 42 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 32 39 35 38 39 35 46 38 43 30 35 34 32 37 37 44 37 42 46 45 33 30 43 43 35 32 36 37 42 41 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 32 41 42 46 32 42 46 45 31 42 33 35 37 44 39 38 45 44 46 33 Data Ascii: 1161CD54187D4DD1</rdf:li> <rdf:li>227920E4BA50426323B973E5B49D4C17</rdf:li> <rdf:li>227F21C5D3355719946517E721100188</rdf:li> <rdf:li>229381DA0661480A81C8276506B619B5</rdf:li> <rdf:li>2295895F8C054277D7BFE30CC5267BA7</rdf:li> <rdf:li>22ABF2BFE1B357D98EDF3
2022-04-08 08:02:42 UTC	3182	IN	Data Raw: 45 38 41 45 44 42 34 31 42 36 35 34 36 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 38 41 32 39 31 31 33 45 44 44 38 43 45 33 43 39 44 32 31 45 44 45 33 32 32 43 37 31 33 36 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 38 41 44 43 37 37 33 30 30 41 38 38 31 33 34 36 42 42 38 36 39 30 30 34 31 39 31 34 37 43 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 38 42 37 32 38 36 30 44 33 35 33 36 30 36 45 35 39 43 43 45 3 9 43 36 46 31 33 36 44 35 31 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 38 42 45 46 30 39 32 46 35 36 30 33 45 36 35 32 30 37 34 35 33 45 45 34 30 35 35 33 33 39 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 38 43 30 37 46 46 41 41 41 37 46 38 34 45 41 42 31 38 37 45 32 38 Data Ascii: E8AEDB41B65468</rdf:li> <rdf:li>28A29113EDD8CE3C9D21EDE322C71368</rdf:li> <rdf:li>28ADC77300A881346BB86900419147CF</rdf:li> <rdf:li>28B72860D353606E59CCE96F136D513</rdf:li> <rdf:li>28BEF092F5603E65207453EE40553398</rdf:li> <rdf:li>28C07FFAAAF784EAB187E28
2022-04-08 08:02:42 UTC	3198	IN	Data Raw: 35 36 38 37 36 30 36 46 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 34 42 44 44 35 38 43 34 30 41 39 32 45 30 35 39 37 34 41 32 38 45 31 45 41 37 46 33 31 46 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 34 44 33 33 31 44 41 46 30 39 31 45 36 38 35 36 30 44 39 38 32 44 42 42 30 36 42 32 33 32 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 34 44 43 46 30 37 37 45 38 31 46 43 38 45 45 36 38 43 39 44 37 32 35 46 43 35 33 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 34 44 44 34 41 32 33 42 41 37 38 45 46 38 37 45 38 36 36 31 30 35 39 38 42 30 44 46 36 32 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 34 45 36 30 33 35 35 45 33 33 41 34 35 34 34 39 31 32 33 35 45 32 37 35 30 34 37 Data Ascii: 5687606F1</rdf:li> <rdf:li>34BD58C40A92E05974A28E1EA7F31F9</rdf:li> <rdf:li>34D331DAF091E68560D982DBB06B2324</rdf:li> <rdf:li>34DCF077EC8A81FC8EE68C9D725FC533</rdf:li> <rdf:li>34DD4A23BA78EF87E86610598B0DF627</rdf:li> <rdf:li>34E60355E33A454491235E275047

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	3214	IN	Data Raw: 33 39 36 38 44 37 43 33 32 33 35 43 30 41 42 44 39 44 36 44 33 41 41 35 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 32 35 36 42 43 37 43 43 30 42 30 33 44 35 38 41 41 37 35 45 33 33 43 34 32 32 33 42 43 35 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 32 36 34 46 35 35 42 39 36 31 44 39 43 35 42 42 43 44 45 37 38 34 41 42 44 33 39 34 41 31 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 32 37 44 45 45 36 45 45 38 3 1 37 36 41 31 44 41 42 30 36 37 45 46 37 31 39 35 46 38 33 34 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 32 38 37 36 36 46 41 35 42 36 30 43 38 36 45 36 30 37 41 37 39 46 31 35 31 32 33 42 46 46 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 32 38 41 34 33 45 36 46 45 45 35 Data Ascii: 3968D7C3235C0ABD9D6D3AA54</rdf:li> <rdf:li>4256BC7CC0B03D58AA75E33C4223BC5F</rdf:li> <rdf:li>4264F55B961D9C5BBBCDE784ABD394A13</rdf:li> <rdf:li>427DEE6EE8176A1DAB067EF7195F8340</rdf:li> <rdf:li>428766FA5B60C86E607A79F15123BFFF</rdf:li> <rdf:li>428A43E6FEE5
2022-04-08 08:02:42 UTC	3221	IN	Data Raw: 43 39 37 30 33 43 46 33 44 46 33 46 46 38 37 45 44 35 32 30 39 46 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 38 37 42 41 37 43 30 44 31 35 46 44 46 36 32 34 44 41 36 35 34 46 42 34 45 41 45 32 31 39 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 38 38 35 31 38 33 35 31 38 35 30 44 41 32 39 46 32 45 45 41 32 36 43 36 41 37 34 43 41 42 37 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 38 39 30 30 32 39 35 37 30 34 35 3 1 35 41 45 32 46 30 31 31 31 33 31 43 38 37 39 41 32 38 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 38 41 31 39 37 33 30 31 42 34 37 39 37 32 37 32 33 39 42 31 34 37 45 34 31 42 33 33 41 36 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 38 41 35 44 43 43 33 44 45 42 45 38 39 Data Ascii: C9703CF3DF3FF87ED5209F0</rdf:li> <rdf:li>487BA7C0D15FDF624DA654FB4EAE219B</rdf:li> <rdf:li>4885183A850DA29F2EEA26C6A74CAB7E</rdf:li> <rdf:li>48900295704515AE2F011131C879A287</rdf:li> <rdf:li>48A197301B479727239B147E41B33A65</rdf:li> <rdf:li>48A5DCC3DEBE89
2022-04-08 08:02:42 UTC	3229	IN	Data Raw: 32 35 30 31 32 34 31 36 37 45 37 32 45 33 41 33 33 35 38 42 35 44 45 38 44 37 45 38 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 45 45 36 34 32 38 38 39 38 32 32 44 33 32 32 35 43 35 31 34 41 36 42 38 35 32 35 34 32 34 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 45 45 36 35 34 44 41 44 44 42 41 33 34 33 43 42 36 46 37 33 34 39 33 46 35 30 43 33 37 31 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 45 45 42 30 33 3 4 41 35 42 43 46 41 43 39 37 38 38 37 31 33 41 33 34 43 45 36 35 43 38 41 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 46 30 38 33 42 34 39 34 37 45 35 38 36 35 34 38 41 44 45 38 31 34 31 37 38 35 32 45 44 43 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 46 31 31 42 31 32 30 Data Ascii: 250124167E72E3A3358B5DE8D7E83</rdf:li> <rdf:li>4EE642889822D3225C514A6B85254241</rdf:li> <rdf:li>4EE654DADDBA343CB6F73493F50C371B</rdf:li> <rdf:li>4EEB034A5BCFAC9788713A34CE65C8A2</rdf:li> <rdf:li>4F083B4947E586548ADE81417852EDC4</rdf:li> <rdf:li>4F11B120
2022-04-08 08:02:42 UTC	3245	IN	Data Raw: 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 43 45 34 46 42 41 43 46 35 32 38 46 30 35 30 32 36 42 36 38 36 37 31 39 34 32 34 30 37 46 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 43 46 31 36 33 41 44 43 45 30 46 44 46 33 44 31 35 30 36 46 36 34 39 31 33 31 30 37 31 30 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 3 5 44 31 41 33 33 42 39 43 34 37 43 34 34 39 43 38 45 36 42 44 33 42 43 36 43 39 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 44 32 31 32 30 41 33 44 46 31 32 42 43 31 34 36 37 38 44 43 41 39 34 41 33 33 37 30 34 43 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 44 32 36 39 33 38 38 42 32 32 42 33 30 36 38 36 35 45 36 32 45 36 30 36 39 38 30 41 41 33 36 3c 2f 72 64 66 3a 6c 69 3e 20 Data Ascii: :li> <rdf:li>5CE4FBACF528F05026B68671942407F2</rdf:li> <rdf:li>5CF163ADCE0FDF3D1506F6491 310710F</rdf:li> <rdf:li>5D1A33B9C47C449C8E6BD3BE7F390309</rdf:li> <rdf:li>5D2120A3DF12BC14678DCA94A 33704CE</rdf:li> <rdf:li>5D269388B22B306865E62E606980AA36</rdf:li>
2022-04-08 08:02:42 UTC	3261	IN	Data Raw: 3c 72 64 66 3a 6c 69 3e 36 42 31 46 37 39 44 31 31 34 30 45 43 39 30 38 37 39 46 37 32 43 46 30 42 35 31 37 46 35 35 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 42 32 34 41 37 41 44 43 36 43 44 39 46 39 32 30 36 41 32 32 41 31 41 35 32 43 37 42 44 33 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 42 34 32 31 3 5 31 37 38 33 37 41 36 44 41 35 31 42 34 38 34 31 34 33 39 43 35 39 31 30 34 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 42 34 36 33 33 34 36 31 33 43 39 46 34 33 44 31 30 41 39 30 33 42 32 37 32 34 42 43 34 30 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 42 35 41 34 32 34 39 45 38 40 45 36 44 37 45 39 45 30 35 35 42 43 44 32 41 39 32 38 33 36 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a Data Ascii: <rdf:li>6B1F79D1140EC90879F72CF0B517F55E</rdf:li> <rdf:li>6B24A7ADC6CD9F9206A22A1A52C7BD 3E</rdf:li> <rdf:li>6B421517837A6DA51B4841439C59104A</rdf:li> <rdf:li>6B46334613C9F43D10A903B2724BC4 05</rdf:li> <rdf:li>6B5A4249E80E6D7E9E055BCD2A92836B</rdf:li> <rdf:li>
2022-04-08 08:02:42 UTC	3269	IN	Data Raw: 64 66 3a 6c 69 3e 37 32 44 32 33 43 44 43 46 31 44 41 30 33 43 46 41 44 41 39 31 31 34 38 33 30 30 32 32 36 42 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 32 44 33 37 42 31 32 32 36 41 44 43 37 39 31 41 32 30 45 45 38 41 30 34 30 38 42 33 33 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 32 44 36 34 39 32 3 7 34 37 42 39 30 30 41 36 33 44 32 33 44 37 39 33 33 36 44 39 30 45 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 32 45 44 32 41 43 34 32 46 33 44 33 34 38 39 39 43 39 35 33 30 44 33 33 42 30 36 30 42 33 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 32 46 46 35 30 33 43 34 32 33 43 41 46 43 38 35 31 43 38 35 39 30 39 38 41 45 46 44 31 46 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 Data Ascii: df:li>72D23CDCF1DA03CFADA91148300226BD</rdf:li> <rdf:li>72D377B1226ADC791A20EE8A0408B333 </rdf:li> <rdf:li>72D6492747B9000A63D3CD79336D90EB</rdf:li> <rdf:li>72ED2AC42F3D34899C9530D33B060B38 </rdf:li> <rdf:li>72FF503C423CAFC851C859098AEFD1F5</rdf:li> <rdf:li>
2022-04-08 08:02:42 UTC	3285	IN	Data Raw: 31 35 39 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 30 43 34 32 46 38 43 38 31 32 36 37 36 31 41 39 34 39 31 45 30 46 43 30 41 30 39 34 33 36 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 30 43 37 39 33 30 43 32 42 33 42 35 35 41 44 34 33 35 44 43 41 39 37 30 46 34 46 31 46 31 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 30 44 30 46 46 43 38 46 45 33 45 45 44 39 33 31 38 44 41 36 39 37 37 42 39 38 39 46 34 33 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 30 44 31 45 44 35 38 36 35 34 37 37 34 45 36 45 44 34 41 35 38 46 38 35 43 33 39 36 36 42 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 30 44 43 34 36 41 35 45 33 42 37 31 39 38 37 33 38 31 39 37 30 45 46 41 39 38 41 44 46 46 33 3c Data Ascii: 159F</rdf:li> <rdf:li>80C42F8C8126761A9491E0FC0A094365</rdf:li> <rdf:li>80C7930C2B3B55AD 435DCA970F4F1F13</rdf:li> <rdf:li>80DOFFC8FE3EED9318DA6977B989F43B</rdf:li> <rdf:li>80D1ED58654774E6 ED4A58F85C3966B2</rdf:li> <rdf:li>80DC46A5E3B71987381970EFA98ADFF3<
2022-04-08 08:02:42 UTC	3301	IN	Data Raw: 32 32 37 31 46 44 46 44 46 35 43 35 34 36 45 44 36 33 37 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 43 39 41 34 34 42 45 31 46 32 42 36 45 35 33 45 32 41 35 38 36 44 44 43 34 30 32 30 33 32 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 43 41 36 33 31 31 44 31 41 45 35 46 38 45 36 38 42 31 36 44 32 43 34 36 39 35 31 30 30 44 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 43 42 31 45 45 38 45 30 34 32 30 38 34 37 4 6 39 34 30 35 45 42 31 37 36 37 43 30 44 43 44 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 43 44 41 46 38 35 42 42 33 31 45 34 31 43 34 30 41 36 34 31 41 41 41 42 45 31 45 38 39 33 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 43 44 41 46 64 66 3a 6c 69 3e 38 43 44 43 38 39 45 43 31 31 39 32 34 35 34 30 39 Data Ascii: 2271FDFDF5C546ED6373</rdf:li> <rdf:li>8C9A44BE1F2B6E53E2A586DDC4020320</rdf:li> <rdf:li>8CA6311D1AE5F8E68B16D2C4695100D0</rdf:li> <rdf:li>8CB1EE8E0420847F9405EB1767C0DCD0</rdf:li> <rdf:li>8CDAF85BB31E41C40A641AAABE1E8939</rdf:li> <rdf:li>8CDC89EC119245409

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	3309	IN	Data Raw: 39 41 41 32 33 41 43 39 44 44 42 30 39 43 43 37 42 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 34 39 41 41 32 42 33 36 43 31 32 38 41 39 32 31 36 38 35 37 44 41 35 31 39 42 34 37 37 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 34 39 41 37 32 43 46 41 37 33 37 36 37 30 43 45 41 36 30 32 31 30 41 38 32 32 46 34 32 39 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 34 41 35 41 42 32 43 42 38 34 38 31 46 37 41 37 3 5 37 38 36 43 44 35 41 42 39 32 42 46 31 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 34 41 41 31 35 46 34 39 32 44 34 33 32 33 34 46 44 35 31 31 43 42 35 44 31 33 37 33 43 33 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 34 42 36 44 46 41 43 38 33 42 42 30 34 31 41 43 41 42 Data Ascii: 9AA23AC9DDB09CC7BD</rdf:li> <rdf:li>9494AA2B36C128A9216857DA519B477F</rdf:li> <rdf:li>94 9A72CFA737670CEA60210A822F429B</rdf:li> <rdf:li>94A5AB2CB8481F7A75786CD5AB92BF13</rdf:li> <rdf:li>94 AA15F492D43234FD511CB5D1373C3A</rdf:li> <rdf:li>94B6DFAC83BB041ACAB
2022-04-08 08:02:42 UTC	3325	IN	Data Raw: 38 46 33 45 44 43 32 34 32 33 30 33 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 32 31 31 35 34 46 32 34 32 42 41 38 31 43 44 31 37 36 34 38 35 31 33 39 44 39 39 36 34 41 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 32 31 35 32 34 44 35 36 43 33 41 36 36 45 33 30 46 39 37 41 41 30 31 36 39 32 31 37 43 30 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 32 32 34 30 44 33 31 42 42 33 38 43 38 32 41 42 38 46 37 44 33 35 33 36 45 33 45 35 42 43 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 32 33 42 42 32 41 35 44 36 45 45 38 44 44 32 33 37 38 32 31 32 43 35 41 31 33 36 35 35 46 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 32 33 43 45 43 46 30 44 33 37 42 38 31 33 38 36 30 46 38 46 37 38 42 Data Ascii: 8F3EDC2423037</rdf:li> <rdf:li>A21154F242BA81CD176485139D9964AF</rdf:li> <rdf:li>A21524D 56C3A66E30F97AA0169B17C0D</rdf:li> <rdf:li>A2240D31BB38C82AB8F7D3536E3E5BC0</rdf:li> <rdf:li>A23BB2A 5D6EE8DD2378212C5A13655FE</rdf:li> <rdf:li>A23CECF0D37B813860F8F78B
2022-04-08 08:02:42 UTC	3341	IN	Data Raw: 43 42 38 44 38 44 42 43 34 32 35 42 44 43 37 31 36 36 37 37 41 39 42 32 31 34 38 30 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 46 39 34 38 33 42 31 31 37 41 35 38 43 34 31 35 45 32 34 30 36 38 43 34 36 32 45 30 32 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 46 39 45 32 32 45 42 34 34 43 34 44 43 45 32 39 33 42 32 31 38 33 41 32 37 36 33 43 43 30 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 46 43 46 34 41 4 4 39 44 39 39 43 41 31 34 39 44 37 32 36 41 31 37 34 34 35 33 42 37 45 38 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 46 44 31 36 39 42 30 41 37 38 38 42 45 44 33 35 45 46 37 46 31 41 38 42 30 41 34 44 36 36 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 46 44 32 39 32 31 36 Data Ascii: CB8D8DBC425BDC716677A9B21480F</rdf:li> <rdf:li>AF9483B117A584C415E24068C462E023</rdf:li> <rdf:li>AF9E22EB44C4DCE293B2183A2763CC0F</rdf:li> <rdf:li>AFCF4AD9D99CA149D726A174453B7E8D</rdf:li> <rdf:li>AFD169B0A788BED35EF7F1A8B0A4D66E</rdf:li> <rdf:li>AFD29216
2022-04-08 08:02:42 UTC	3349	IN	Data Raw: 35 43 45 43 41 41 44 38 44 33 43 41 43 41 38 32 33 46 36 35 46 33 42 37 39 34 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 35 42 35 30 32 43 33 31 31 41 33 30 46 35 37 39 41 41 37 39 46 43 45 31 38 46 32 42 37 42 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 35 42 38 37 33 39 44 44 44 38 45 41 39 43 35 37 35 37 38 45 37 32 42 43 44 32 43 35 36 37 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 35 43 49 43 30 42 46 3 1 46 45 41 31 41 36 45 46 30 33 41 41 45 45 45 33 42 42 32 45 33 35 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 35 42 43 32 34 44 42 32 37 45 30 31 33 42 46 35 33 31 46 31 37 43 35 38 38 45 42 45 37 43 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 35 43 33 43 45 44 38 34 38 Data Ascii: 5CECAAD8D3CACA823F65F3B794D</rdf:li> <rdf:li>B5B502C311A30F579AA79FCE18F2B7B7</rdf:li> <rdf:li>B5B8739DD8EA9C57578E72BCD2C5675</rdf:li> <rdf:li>B5B9D0BF1FEA1A6EF03AAEEE3BB2E35F</rdf:li> <rdf:li>B5BC24DB27E013BF531F17C588EBE7C1</rdf:li> <rdf:li>B5C3CED848
2022-04-08 08:02:42 UTC	3357	IN	Data Raw: 3e 42 43 39 43 32 31 33 45 42 33 31 31 37 36 36 31 42 44 38 36 31 43 31 31 36 42 36 46 45 37 41 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 43 42 30 37 45 31 30 43 38 45 39 35 41 46 31 30 43 36 43 32 39 44 43 34 38 45 35 45 39 33 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 43 42 31 37 36 32 31 34 38 44 33 3 2 38 37 35 30 43 30 31 43 32 33 33 30 34 36 34 41 33 34 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 43 42 33 32 34 35 44 35 38 44 32 36 39 31 39 35 35 31 37 35 44 39 41 35 46 43 45 33 32 44 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 43 45 32 45 36 43 43 33 37 30 35 30 46 46 30 44 36 41 35 38 35 32 42 46 39 33 38 46 36 37 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 43 46 42 Data Ascii: >BC9C213EB3117661BD861C116B6FE7AB</rdf:li> <rdf:li>BCB07E10A8E95AF10C6C29DC48E5E931</rdf:li> <rdf:li>BCB1762148D328750C01C2330464A348</rdf:li> <rdf:li>BCB3245D58D2691955175D9A5FCE32DA</rdf:li> <rdf:li>BCE2E6CC37050FF0D6A5852BF938F67D</rdf:li> <rdf:li>BCFB
2022-04-08 08:02:42 UTC	3373	IN	Data Raw: 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 41 31 45 37 42 38 41 32 44 32 37 39 35 30 35 44 34 36 46 39 43 35 35 42 42 30 41 36 44 36 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 41 33 30 46 39 43 35 46 32 36 41 46 34 42 35 35 46 37 37 32 44 42 41 43 41 43 31 42 32 38 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 41 33 35 42 41 42 31 32 38 38 34 38 36 37 44 35 34 34 36 46 41 32 44 34 30 31 34 36 31 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 41 34 33 35 41 44 39 30 30 35 44 39 31 45 38 34 39 39 45 42 30 42 43 33 36 41 39 34 43 42 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 41 34 41 38 30 32 42 36 32 37 43 44 41 45 32 33 31 45 41 46 39 34 32 30 43 35 38 43 37 33 30 3c 2f 72 64 66 3a Data Ascii: /rdf:li> <rdf:li>CA1E7B8A2D279505D46F9C55BB0A6D6F</rdf:li> <rdf:li>CA30F9C5F26AF4B55F772 DBACAC1B287</rdf:li> <rdf:li>CA35BAB12884867D5446FA2D40144618</rdf:li> <rdf:li>CA435AD9005D91E8499EB 0BC36A94CB7</rdf:li> <rdf:li>CA4A802B627CDAE231EAF9420C58C730</rdf:li>
2022-04-08 08:02:42 UTC	3389	IN	Data Raw: 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 37 38 33 37 46 37 39 33 43 67 31 44 32 30 37 33 34 42 44 39 39 42 41 43 45 37 31 36 45 34 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 37 38 38 46 41 35 41 39 43 41 43 42 33 38 30 45 43 35 39 34 43 31 39 41 43 36 38 41 30 44 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 3 7 38 39 43 31 30 41 41 33 36 46 44 38 37 32 33 36 46 32 46 35 34 41 35 35 44 30 41 33 32 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 37 39 37 42 46 42 32 43 30 36 35 30 37 41 36 38 46 30 43 38 30 33 35 34 33 45 30 42 41 42 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 37 39 41 31 36 34 36 43 43 37 35 32 38 43 33 39 31 32 32 43 31 35 30 42 36 46 30 36 37 32 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c Data Ascii: li> <rdf:li>D7837F793C71D20734BD99BACE716E49</rdf:li> <rdf:li>D788FA5A9CACB380EC594C19AC 68A0D7</rdf:li> <rdf:li>D789C10AA36FD87236F2F54A55D0A322</rdf:li> <rdf:li>D797BFB2C06507A68F0C803543 E0BAB3</rdf:li> <rdf:li>D79D1646CC7528C39122C150B6F06720</rdf:li> <
2022-04-08 08:02:42 UTC	3396	IN	Data Raw: 3e 20 3c 72 64 66 3a 6c 69 3e 44 45 32 37 45 36 46 46 43 43 30 44 33 31 34 31 37 38 33 43 32 34 36 32 34 39 42 45 34 30 43 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 45 34 35 34 35 39 34 41 30 37 44 42 45 45 34 32 39 43 46 46 34 36 30 38 44 46 33 34 43 44 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 45 34 3 5 44 43 38 35 32 43 31 38 36 39 45 35 31 38 36 31 43 31 35 43 44 44 46 44 42 45 45 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 45 35 39 44 31 31 37 42 32 35 34 45 33 43 46 34 41 43 41 34 34 36 38 33 42 44 36 30 37 42 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 45 36 31 45 31 39 30 41 42 37 39 39 33 41 43 45 45 41 33 46 39 41 33 32 36 38 39 46 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 Data Ascii: > <rdf:li>DE27E6FFCC0D3141783C246249BE40CF</rdf:li> <rdf:li>DE454594A07DBEE429CFF4608DF3 4CDC</rdf:li> <rdf:li>DE45DC852C1869E51861C15CDDFDBEED</rdf:li> <rdf:li>DE59D117B254E3CF4ACA44683BD6 07BD</rdf:li> <rdf:li>DE61E190AB7993ACEEA3F9A326898FC6</rdf:li> <rdf:li> <

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	3412	IN	Data Raw: 42 44 33 45 44 43 39 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 41 45 31 42 45 37 42 39 35 38 31 35 43 42 36 35 42 39 35 44 45 35 41 39 35 31 38 41 33 30 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 41 45 41 31 43 30 31 31 46 42 45 34 31 43 34 33 36 46 39 39 35 43 42 34 42 44 33 39 32 35 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 42 30 30 38 31 44 41 33 32 46 32 46 42 46 31 42 31 32 37 43 37 37 37 32 39 38 38 46 32 33 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 42 30 36 45 42 30 36 45 37 37 31 34 36 36 34 37 46 44 33 42 32 32 30 35 45 34 45 31 38 43 46 46 33 32 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 42 30 42 30 37 44 46 30 41 45 31 33 44 46 44 46 46 34 36 37 35 38 45 46 45 37 39 46 Data Ascii: BD3EDC9E</rdf:li> <rdf:li>EAE1BE7B95815CB65B95DE5A9518A300</rdf:li> <rdf:li>EAEAC011FBE41C436F995CB4BD3925A</rdf:li> <rdf:li>EB0081DA32F2FBF1B127C7772988F239</rdf:li> <rdf:li>EB06E07146647FD3B2205E4E18CFF328</rdf:li> <rdf:li>EB0B07DFOAE13DFDFF46758EFE79F
2022-04-08 08:02:42 UTC	3428	IN	Data Raw: 46 31 30 41 42 33 41 36 45 31 37 43 30 31 37 42 35 30 34 39 31 33 34 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 37 34 42 39 39 31 32 43 45 41 31 31 45 30 44 30 33 39 39 46 38 39 34 44 36 46 38 45 38 41 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 37 35 35 45 46 42 39 45 45 36 37 37 35 43 44 36 41 39 41 37 44 46 38 45 39 36 33 35 31 34 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 37 36 34 44 35 46 36 44 43 32 4 5 30 32 42 43 33 45 45 42 43 46 41 34 45 42 36 30 36 43 36 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 37 37 35 43 36 46 42 33 46 45 33 39 31 46 37 35 45 36 37 30 31 45 44 44 37 42 33 46 37 32 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 37 38 39 32 33 37 45 37 41 43 43 45 Data Ascii: F10AB3A6E17C017B5049134D</rdf:li> <rdf:li>F74B9912CEA11E0D0399F894D6F8E8A3</rdf:li> <rdf:li>F755EFB9EE6775CD6A9A7DF8E9635143</rdf:li> <rdf:li>F764D5F6DC2E02BC3EEBCFA4EB606C67</rdf:li> <rdf:li>F775C6B3FE391F75E6701EDD7B3F729</rdf:li> <rdf:li>F789237E7ACCE
2022-04-08 08:02:42 UTC	3436	IN	Data Raw: 32 41 45 42 33 43 42 32 34 34 31 39 35 35 45 43 41 31 34 36 44 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 44 44 37 44 35 37 38 31 36 43 46 39 46 31 44 35 41 39 33 45 39 45 36 45 35 46 43 41 45 31 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 44 44 44 41 32 46 33 32 34 45 41 36 42 38 36 45 37 31 36 32 30 31 41 44 32 41 45 34 33 35 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 44 44 45 36 37 41 37 42 44 36 39 38 3 4 31 33 35 37 35 33 42 35 45 46 43 32 30 36 38 31 41 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 44 45 32 37 35 35 43 34 42 31 34 38 33 36 39 44 44 41 43 32 35 44 44 39 46 30 41 38 35 35 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 44 45 32 39 41 32 35 36 33 31 46 32 42 30 Data Ascii: 2AEB3CB2441955ECA146D2</rdf:li> <rdf:li>FDD7D57816CF9F1D5A93E9E6E5FCAE15</rdf:li> <rdf:li>FDDDDA2F324EA6B86E716201AD2AE4351</rdf:li> <rdf:li>FDDE67A7BD698413575B5EFC20681A8</rdf:li> <rdf:li>FDE2755C4B148369DDAC25DD9F0A855C</rdf:li> <rdf:li>FDE29A25631F2B0
2022-04-08 08:02:42 UTC	3452	IN	Data Raw: 31 31 64 61 2d 62 30 62 34 2d 38 34 66 38 31 62 33 62 39 32 61 61 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 32 61 64 63 65 34 65 62 2d 34 31 31 64 2d 31 31 64 38 2d 38 30 34 32 2d 62 30 32 63 37 33 64 35 30 39 36 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 32 61 66 33 30 33 62 31 2d 39 63 37 63 2d 31 31 37 38 2d 62 37 62 37 2d 62 30 34 62 61 38 36 63 62 66 66 66 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 32 62 30 38 66 64 37 37 2d 61 31 63 66 2d 31 31 37 37 2d 61 32 39 30 2d 38 37 66 33 66 35 30 61 33 32 66 63 3c 2f 72 64 66 Data Ascii: 11da-b0b4-84f81b3b92aa</rdf:li> <rdf:li>adobe:docid:photoshop:2adce4eb-411d-11d8-8042-b02c73d50967</rdf:li> <rdf:li>adobe:docid:photoshop:2af303b1-9c7c-1178-b7b7-b04ba86cbfff</rdf:li> <rdf:li>adobe:docid:photoshop:2b08fd77-a1cf-1177-a290-87f3f50a32fc</rdf
2022-04-08 08:02:42 UTC	3468	IN	Data Raw: 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 35 62 65 34 37 63 63 32 2d 35 39 61 36 2d 31 31 37 38 2d 62 39 37 35 2d 39 33 62 63 69 33 37 36 62 32 38 63 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 35 62 66 30 38 36 65 36 2d 64 32 39 39 2d 31 31 37 38 2d 61 32 30 64 2d 61 66 32 65 66 39 63 31 39 37 64 66 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 35 62 66 34 61 62 62 30 2d 38 33 30 36 2d 31 31 65 37 2d 62 62 32 62 30 2d 62 34 33 31 31 62 65 38 32 30 35 65 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 35 63 34 66 32 62 32 36 2d Data Ascii: e:docid:photoshop:5be47cc2-59a6-1178-b975-93bc9376b28c</rdf:li> <rdf:li>adobe:docid:photoshop:5bf086e6-d299-1178-a20d-af2ef9c197df</rdf:li> <rdf:li>adobe:docid:photoshop:5bf4abb0-8306-11e7-bb20-b4311be8205e</rdf:li> <rdf:li>adobe:docid:photoshop:5c4f2b26-
2022-04-08 08:02:42 UTC	3476	IN	Data Raw: 38 61 34 34 36 64 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 37 32 65 31 37 32 31 64 2d 64 32 39 39 2d 31 31 37 38 2d 61 32 30 64 2d 61 66 32 65 66 39 63 31 39 37 64 66 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 37 33 31 31 34 37 37 34 2d 32 65 34 65 2d 31 31 64 38 2d 38 62 30 36 2d 64 33 63 33 63 65 61 39 32 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 37 33 31 65 64 39 38 30 2d 34 30 35 30 2d 31 31 37 38 2d 61 34 37 33 2d 39 37 30 30 35 65 39 33 37 63 31 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f Data Ascii: 8a446d</rdf:li> <rdf:li>adobe:docid:photoshop:72e1721d-d299-1178-a20d-af2ef9c197df</rdf:li> <rdf:li>adobe:docid:photoshop:73114774-2e4e-11d8-8b06-f435c3cea923</rdf:li> <rdf:li>adobe:docid:photoshop:731ed980-4050-1178-a473-97005e937c10</rdf:li> <rdf:li>ado
2022-04-08 08:02:42 UTC	3484	IN	Data Raw: 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 38 37 30 62 39 65 32 64 2d 63 34 65 36 2d 31 31 37 39 2d 39 39 65 66 2d 62 31 62 33 30 30 35 61 34 38 36 65 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 38 37 31 66 64 39 36 35 2d 35 39 32 64 2d 31 31 65 36 2d 39 36 31 38 2d 65 30 32 63 61 38 64 32 32 61 38 64 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 38 37 37 30 62 63 36 30 2d 37 61 63 61 2d 31 31 64 36 2d 39 62 31 35 2d 38 65 31 64 31 61 37 32 33 31 32 63 3c 2f 72 64 66 3a 6c 69 3e 20 3c 7 2 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f Data Ascii: li> <rdf:li>adobe:docid:photoshop:870b9e2d-c4e6-1179-99ef-b1b3005a486e</rdf:li> <rdf:li>adobe:docid:photoshop:871fd965-592d-11e6-9618-e02ca8d22a8d</rdf:li> <rdf:li>adobe:docid:photoshop:8770bc60-7aca-11d6-9b15-8e1d1a72312c</rdf:li> <rdf:li>adobe:docid:pho
2022-04-08 08:02:42 UTC	3500	IN	Data Raw: 36 61 66 2d 31 31 65 31 2d 62 36 61 36 2d 64 32 65 36 37 34 30 63 33 37 61 66 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 62 63 35 61 61 39 34 39 2d 62 36 61 65 2d 31 31 65 31 2d 62 36 61 36 2d 64 32 65 36 37 34 30 63 33 37 61 66 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 62 63 37 32 37 62 32 38 2d 36 38 65 62 2d 31 31 65 37 2d 39 30 37 37 2d 66 34 34 62 62 38 66 62 63 64 63 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 62 63 61 33 35 66 62 61 2d 61 31 32 65 2d 31 31 37 37 2d 61 32 39 30 2d 38 37 66 33 66 35 30 61 33 32 66 63 3c Data Ascii: 6af-11e1-b6a6-d2e6740c37af</rdf:li> <rdf:li>adobe:docid:photoshop:bc5aa949-b6ae-11e1-b6a6-d2e6740c37af</rdf:li> <rdf:li>adobe:docid:photoshop:bc727b28-68eb-11e7-9077-f44bb8fbcdcl</rdf:li> <rdf:li>adobe:docid:photoshop:bca35fba-a12e-1177-a290-87f3f50a32fc<

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	3516	IN	Data Raw: 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 65 65 63 38 61 30 66 62 2d 62 32 31 39 2d 31 31 64 37 2d 62 31 31 36 2d 61 34 32 31 39 34 66 61 62 66 64 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 65 65 63 38 61 30 66 64 2d 62 32 31 39 2d 31 31 64 37 2d 62 31 31 36 2d 61 34 32 31 39 34 66 61 62 66 64 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 65 66 31 61 62 65 30 34 2d 35 65 63 38 2d 62 34 34 30 2d 38 31 36 38 2d 65 64 32 65 66 61 39 32 63 63 38 62 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 65 66 Data Ascii: li>adobe:docid:photoshop:eec8a0fb-b219-11d7-b116-a42194fabfd8</rdf:li> <rdf:li>adobe:docid:photoshop:eec8a0fd-b219-11d7-b116-a42194fabfd8</rdf:li> <rdf:li>adobe:docid:photoshop:ef1abe04-5ec8-b440-8168-ed2efa92cc8b</rdf:li> <rdf:li>adobe:docid:photoshop:ef
2022-04-08 08:02:42 UTC	3524	IN	Data Raw: 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 30 38 44 37 42 34 45 45 34 46 36 37 44 45 31 31 42 45 39 36 39 30 45 43 30 32 38 31 35 39 41 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 30 39 31 36 46 38 37 31 30 42 38 39 44 45 31 31 42 33 31 44 41 41 43 31 46 31 44 39 33 33 2d 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 30 39 32 38 33 41 33 33 43 36 46 34 31 31 44 41 42 37 44 42 41 46 45 43 45 30 46 38 42 33 41 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 30 39 41 30 35 34 33 31 38 42 45 38 44 43 31 31 41 38 45 30 45 31 42 34 39 36 45 33 39 39 34 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 30 39 41 38 41 37 37 30 43 46 35 30 44 45 31 31 Data Ascii: f:li> <rdf:li>uuid:08D7B4EE4F67DE11BE9690EC028159A9</rdf:li> <rdf:li>uuid:0916F8710B89DE11B31DAAC1F1D93333</rdf:li> <rdf:li>uuid:09283A33C6F411DAB7DBAFEC0F8B3A0</rdf:li> <rdf:li>uuid:09A054318BE8DC11A8E0E1B496E39948</rdf:li> <rdf:li>uuid:09A8A770CF50DE11
2022-04-08 08:02:42 UTC	3540	IN	Data Raw: 30 39 43 39 36 44 33 34 37 36 42 35 43 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 34 31 36 41 43 36 43 45 37 46 41 34 31 31 44 41 41 45 42 37 42 30 31 36 32 36 36 31 41 36 31 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 34 31 39 36 31 35 45 38 46 39 43 42 44 41 31 31 38 36 38 38 42 44 39 31 37 34 41 44 32 45 46 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 34 31 43 45 31 44 4 2 34 43 35 46 41 44 42 31 31 41 44 33 45 44 36 35 31 36 33 39 39 46 33 31 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 34 31 45 36 46 31 34 31 32 33 43 43 45 30 31 31 42 33 46 45 44 32 34 38 33 31 38 34 38 46 35 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 Data Ascii: 09C96D3476B5CF</rdf:li> <rdf:li>uuid:416AC6CE7FA411DAAEB7B0162661A619</rdf:li> <rdf:li>uuid:419615E8F9CDBA11868BD9174AD2EFE</rdf:li> <rdf:li>uuid:41CE1DB4C5FADB11AD3ED6516399F31D</rdf:li> <rdf:li>u uid:41E6F14123CCE011B3FED24831848F59</rdf:li> <rdf:li>uui
2022-04-08 08:02:42 UTC	3556	IN	Data Raw: 75 75 69 64 3a 37 33 32 34 32 63 30 65 2d 31 63 32 36 2d 34 38 33 61 2d 62 33 66 34 2d 39 38 36 63 30 30 37 31 32 66 66 64 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 37 33 45 41 45 36 34 46 45 33 44 35 44 44 31 31 38 44 45 30 42 32 37 33 31 39 30 37 45 35 42 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 37 33 45 43 38 46 46 30 46 44 34 45 44 45 31 31 39 38 46 36 39 46 34 39 39 43 42 41 45 46 31 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 37 33 46 30 43 36 38 36 30 44 38 46 44 45 31 31 41 31 41 34 32 44 34 38 43 36 42 39 32 45 32 38 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 37 33 46 37 37 32 39 32 36 36 45 31 31 44 42 38 31 35 45 45 36 33 36 39 46 Data Ascii: uuid:73242c0e-1c26-483a-b3f4-986c00712ffd</rdf:li> <rdf:li>uuid:73EAE64FE3D5DD118DE0B2731907E5B8</rdf:li> <rdf:li>uuid:73EC8FF0FD4EDE1198F69F499C7AEF19</rdf:li> <rdf:li>uuid:73F0C6860D8FDE11A3A4B48C6B9E2E8F</rdf:li> <rdf:li>uuid:73F77292666E11DB815EE6369F
2022-04-08 08:02:44 UTC	6490	IN	Data Raw: 31 41 37 36 42 39 32 34 33 36 42 33 42 44 39 42 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 38 42 37 33 42 44 34 45 42 31 34 35 44 46 31 31 42 35 34 43 41 38 45 43 43 31 31 38 31 33 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 38 42 39 37 42 44 35 32 35 35 43 36 44 45 31 31 39 45 45 42 41 36 45 45 44 30 43 32 32 37 37 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 38 42 41 3 1 41 42 44 30 33 34 43 43 45 30 31 31 42 33 46 45 44 32 34 38 33 31 38 34 38 46 35 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 38 42 42 44 34 34 32 34 39 38 45 32 45 30 31 31 39 31 33 33 43 30 35 35 38 33 34 34 37 44 34 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e Data Ascii: 1A76B92436B3BD9BD</rdf:li> <rdf:li>uuid:8B73BD4EB145DF11B544CA8ECC118138</rdf:li> <rdf:li>i>uuid:8B97BD5255C6DE119EEBA6EED0C2277C</rdf:li> <rdf:li>uuid:8BA1ABD034CCE011B3FED24831848F59</rdf:li> <rdf:li>uuid:8BBD442498E2E0119133C05583447D48</rdf:li> <rdf:li>
2022-04-08 08:02:44 UTC	6506	IN	Data Raw: 31 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 43 30 30 32 44 34 35 31 46 44 43 42 45 30 31 31 42 33 46 45 44 32 34 38 33 31 38 34 38 46 35 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 43 30 31 38 30 44 45 31 30 43 38 44 44 46 31 31 39 46 31 44 43 37 37 37 39 30 44 41 42 39 42 32 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 43 30 42 38 41 35 33 35 44 43 35 42 44 46 31 31 41 32 33 39 42 44 37 33 31 39 32 43 45 41 43 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 43 30 46 31 41 37 44 46 30 45 44 41 44 43 31 31 41 30 35 30 46 46 45 41 36 32 44 37 39 31 45 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 43 31 31 32 38 43 41 46 37 42 Data Ascii: 19</rdf:li> <rdf:li>uuid:C002D451FDCBE011B3FED24831848F59</rdf:li> <rdf:li>uuid:C0180DE10C8DDF119F1DC7790DAB9B2C</rdf:li> <rdf:li>uuid:C0B8A535DC5BDF11A239BD73192CEAC0</rdf:li> <rdf:li>uuid:C0F1A7DF0EDADC11A050FFEA62D791E9</rdf:li> <rdf:li>uuid:C1128CA7B7
2022-04-08 08:02:44 UTC	6522	IN	Data Raw: 33 39 33 32 32 33 46 41 33 46 31 39 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 46 46 41 37 39 43 46 39 31 31 46 41 44 45 31 31 38 46 44 43 39 37 46 31 36 44 34 38 46 35 44 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 61 36 39 66 64 38 65 32 2d 34 65 66 39 2d 34 31 65 37 2d 62 31 65 33 2d 37 66 63 38 37 66 61 37 32 37 63 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 63 64 37 3 5 34 65 30 34 2d 33 62 31 63 2d 34 37 66 63 2d 39 64 65 66 2d 37 32 34 33 63 64 63 36 33 30 62 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 64 33 38 63 64 66 63 62 2d 34 32 62 65 2d 34 37 63 33 2d 62 30 34 61 2d 63 31 66 66 36 34 66 62 34 32 38 63 3c 2f 72 64 66 3a 6c 69 3e 20 Data Ascii: 393223FA3F19B</rdf:li> <rdf:li>uuid:FFA79CF911FADE118FDC97F16D48F5D7</rdf:li> <rdf:li>uuid:a69fd8e2-4ef9-41e7-b1e3-7fc87fa727c1</rdf:li> <rdf:li>uuid:cd754e04-3b1c-47fc-9def-7243cdc630b2</rdf:li> <rdf:li>uuid :d38cdfcb-42be-47c3-b04a-c1ff64fb428c</rdf:li>
2022-04-08 08:02:44 UTC	6530	IN	Data Raw: 70 2e 64 69 64 3a 30 31 38 30 31 31 37 34 30 37 32 30 36 38 31 31 39 32 42 30 41 44 41 36 45 44 46 43 35 41 45 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 31 38 30 31 31 37 34 30 37 32 30 36 38 31 31 39 32 42 30 42 41 41 39 30 34 44 45 30 46 38 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 31 38 30 31 31 37 34 30 37 32 30 36 38 31 31 39 32 42 30 43 35 44 45 41 45 30 32 30 31 35 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 31 38 30 31 31 37 34 30 37 32 30 36 38 31 31 39 32 42 30 43 35 44 45 41 45 30 32 30 31 35 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 31 38 30 31 31 37 34 30 37 32 30 36 38 31 31 39 Data Ascii: p.did:018011740720681192B0ADA6EDFC5AED</rdf:li> <rdf:li>xmp.did:018011740720681192B0BAA904DE0F8D</rdf:li> <rdf:li>xmp.did:018011740720681192B0C4C39BD4227F</rdf:li> <rdf:li>xmp.did:018011740720681192B0C5DEAE020159</rdf:li> <rdf:li>xmp.did:01801174072068119

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:44 UTC	6538	IN	Data Raw: 38 30 31 31 37 34 30 37 32 30 36 38 31 31 39 31 30 39 45 36 44 38 45 34 31 32 32 31 37 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 32 38 30 31 31 37 34 30 37 32 30 36 38 31 31 39 31 30 39 46 35 44 43 32 32 39 39 35 37 38 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 32 38 30 31 31 37 34 30 37 32 30 36 38 31 31 39 31 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 32 38 30 31 31 37 34 30 37 32 30 36 38 31 31 39 32 42 30 39 46 35 39 41 34 45 46 36 45 32 46 3c 2f 72 64 66 3a 6c 42 33 32 39 33 44 33 37 39 43 45 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 32 38 30 31 31 37 34 30 37 32 30 36 38 31 31 39 32 42 30 43 39 33 33 42 Data Ascii: 801174072068119109E6D8E4122179</rdf:li> <rdf:li>xmp.did:02801174072068119109F5DC2299578C</rdf:li> <rdf:li>xmp.did:028011740720681192B09F59A4EF6E2F</rdf:li> <rdf:li>xmp.did:028011740720681192B0B3293D379CEF</rdf:li> <rdf:li>xmp.did:028011740720681192B0C933B
2022-04-08 08:02:44 UTC	6554	IN	Data Raw: 38 43 31 34 45 43 36 39 39 31 34 43 38 35 36 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 36 43 32 30 31 43 31 31 33 32 30 36 38 31 31 38 32 32 41 41 34 30 36 36 39 31 45 44 37 33 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 36 44 1 39 43 30 36 39 32 37 32 30 36 38 31 31 38 46 38 35 41 33 34 45 37 43 32 41 35 30 35 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 36 46 46 41 30 32 41 41 33 34 36 45 35 31 31 39 32 39 33 45 30 30 36 41 43 33 32 37 37 32 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 36 66 37 39 32 62 36 2d 36 36 30 39 2d 34 66 61 30 2d 62 31 62 39 2d 61 61 61 39 30 66 33 61 38 33 38 62 3c 2f 72 Data Ascii: 8C14EC69914C8563</rdf:li> <rdf:li>xmp.did:06C201C113206811822AA406691ED732</rdf:li> <rdf:li>xmp.did:06DA9C59272068118F85A34E7C2A5058</rdf:li> <rdf:li>xmp.did:06FFA02AA346E5119293E006AC32772F</rdf:li> <rdf:li>xmp.did:06f792b6-6609-4fa0-b1b9-aaa90f3a838b</rdf:li>
2022-04-08 08:02:44 UTC	6570	IN	Data Raw: 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 30 33 33 32 64 62 65 2d 33 33 32 37 2d 34 64 65 37 2d 62 36 64 61 2d 35 61 37 32 61 34 32 36 35 31 38 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 30 34 42 35 46 46 44 36 44 33 36 45 30 31 31 39 30 44 41 41 45 31 34 30 37 32 37 32 35 30 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 30 37 63 31 64 33 34 2d 32 31 66 35 2d 65 61 34 35 2d 39 39 61 61 2d 35 64 39 63 64 30 63 36 38 31 66 63 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 30 42 38 42 31 35 45 31 41 32 30 36 38 31 31 39 37 33 34 45 30 36 31 44 44 33 31 41 30 35 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a Data Ascii: rdf:li>xmp.did:10332dbe-3327-4de7-b6da-5a72a4265188</rdf:li> <rdf:li>xmp.did:104B5FFD6D36E01190DAAE1407272500</rdf:li> <rdf:li>xmp.did:107cd3d4-21f5-ea45-99aa-5d9cd0c681fc</rdf:li> <rdf:li>xmp.did:10B8B15E1A2068119734E061DD31A05F</rdf:li> <rdf:li>xmp.did:
2022-04-08 08:02:44 UTC	6577	IN	Data Raw: 43 46 38 39 43 41 44 37 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 38 38 42 38 37 45 45 30 46 32 30 36 38 31 31 39 31 30 39 46 44 37 35 31 43 36 42 30 33 43 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 38 39 37 65 35 65 34 2d 39 30 33 62 2d 34 61 62 35 2d 39 33 65 33 2d 36 31 66 66 32 36 64 31 66 31 36 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 38 39 65 32 31 33 32 2d 33 39 34 38 2d 36 35 34 62 2d 38 61 66 32 2d 39 31 63 32 62 62 62 33 35 37 61 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 38 39 65 62 62 33 63 2d 61 34 30 38 2d 37 36 34 32 2d 38 63 62 34 2d 37 34 37 63 64 64 30 38 66 32 64 33 3c 2f Data Ascii: CF89CAD76</rdf:li> <rdf:li>xmp.did:188B87EE0F2068119109FD751C6B03C1</rdf:li> <rdf:li>xmp.did:1897e5e4-903b-4ab5-93e3-61f726d1f167</rdf:li> <rdf:li>xmp.did:189e2132-3948-654b-8af2-91c2bbb357a1</rdf:li> <rdf:li>xmp.did:189ebb3c-a408-7642-8cb4-747cdd08f2d3</rdf:li>
2022-04-08 08:02:44 UTC	6593	IN	Data Raw: 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 38 33 37 31 43 45 35 41 36 32 32 36 38 31 31 38 32 32 41 39 45 34 31 38 46 34 35 35 43 35 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 38 33 46 33 43 44 46 41 45 32 31 36 38 31 31 39 31 30 39 43 39 45 30 32 35 43 34 42 42 38 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 38 34 30 31 42 32 31 37 44 32 38 36 38 31 31 38 43 31 34 41 46 39 44 32 37 33 35 41 34 38 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 38 34 44 35 41 35 42 30 38 32 30 36 38 31 31 42 45 39 43 38 38 46 42 34 46 36 44 39 32 35 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 38 35 62 30 64 39 63 2d 61 61 36 Data Ascii: li>xmp.did:28371CE5A6226811822A9E418F455C5D</rdf:li> <rdf:li>xmp.did:283F3CDAE2168119109C9E025C4BB86</rdf:li> <rdf:li>xmp.did:28401B217D2B68118C14AF9D2735A483</rdf:li> <rdf:li>xmp.did:284D5A5B08206811BE9C88FB4F6D925B</rdf:li> <rdf:li>xmp.did:285b0d9c-aa6
2022-04-08 08:02:44 UTC	6609	IN	Data Raw: 39 2d 61 39 37 39 2d 39 64 34 34 2d 61 63 61 66 2d 36 64 38 39 37 31 39 30 34 65 63 66 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 36 39 33 65 31 30 32 2d 38 37 32 33 2d 34 39 37 34 2d 62 35 66 64 2d 38 66 32 66 63 39 36 66 39 31 63 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 36 39 36 35 35 31 34 31 32 32 30 36 38 31 31 42 34 42 43 43 31 41 38 45 42 43 37 38 31 33 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 36 42 45 32 34 43 44 33 46 32 30 36 38 31 31 41 39 42 35 39 38 36 35 46 39 46 31 35 36 32 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 36 44 31 34 31 36 45 31 44 32 30 36 38 31 31 38 38 43 36 43 46 Data Ascii: 9-a979-9d44-acaf-6d8971904ecf</rdf:li> <rdf:li>xmp.did:3693e102-8723-4974-b5fd-8f2cf96f91c6</rdf:li> <rdf:li>xmp.did:3696551412206811B4BCC2A8EBC78135</rdf:li> <rdf:li>xmp.did:36BE24CD3F206811A9B59865F9F1562B</rdf:li> <rdf:li>xmp.did:36D1416E1D20681188C6CF
2022-04-08 08:02:44 UTC	6617	IN	Data Raw: 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 45 46 35 31 46 35 30 30 41 32 30 36 38 31 31 38 46 36 32 46 36 45 44 33 34 45 44 44 44 37 43 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 45 46 43 36 36 36 46 30 43 32 30 36 38 31 31 38 38 43 36 43 31 33 33 34 42 42 42 35 37 34 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 45 46 43 46 30 37 46 31 46 32 30 36 38 31 31 38 37 31 46 39 39 30 42 39 43 44 30 43 38 44 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 46 30 32 42 42 44 31 35 31 32 30 36 38 31 31 38 41 36 44 42 34 34 42 46 46 36 41 41 30 43 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 46 31 32 32 38 44 45 30 37 Data Ascii: f:li>xmp.did:3EF51F500A2068118F62F6ED34EDD7C7</rdf:li> <rdf:li>xmp.did:3EFC666F0C20681188C6C1334BBB574E</rdf:li> <rdf:li>xmp.did:3EFCF07F1F206811871F990B9CD0C8DF</rdf:li> <rdf:li>xmp.did:3F02BBD1512068118A6DB44BFF61A0C6</rdf:li> <rdf:li>xmp.did:3F1228DE07
2022-04-08 08:02:44 UTC	6633	IN	Data Raw: 45 33 33 38 31 32 30 46 32 30 36 38 31 31 41 42 36 31 39 39 36 44 35 46 36 41 41 33 32 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 45 32 43 30 45 31 38 35 45 43 44 45 30 31 31 38 43 41 36 46 30 33 42 39 39 35 44 33 43 43 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 45 35 39 45 41 32 37 31 43 32 30 36 38 31 31 38 44 42 42 46 45 34 41 37 36 37 46 34 38 46 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 45 36 35 37 30 46 33 33 39 32 30 36 38 31 31 39 31 30 39 38 32 36 31 33 44 30 44 38 34 33 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 45 38 33 41 38 33 41 32 42 32 30 36 38 31 31 41 42 30 38 42 46 42 43 36 Data Ascii: E338120F206811AB61996D5F6AA328</rdf:li> <rdf:li>xmp.did:4E2C0E185ECDE0118CA6F03B995D3CCCE</rdf:li> <rdf:li>xmp.did:4E59EA271C2068118DBBFE4A767F48FE</rdf:li> <rdf:li>xmp.did:4E6570F339206811910982613D0D8437</rdf:li> <rdf:li>xmp.did:4E83A83A2B206811AB08BFBFC6

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:44 UTC	6745	IN	Data Raw: 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 43 31 34 38 43 37 39 42 36 32 44 42 44 46 31 31 39 41 36 35 39 46 33 45 33 44 35 39 46 30 31 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 43 31 36 34 44 46 44 38 34 36 32 32 36 38 31 31 39 37 41 35 46 35 36 32 31 32 39 45 41 38 31 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 43 31 37 32 30 44 36 37 43 36 38 30 45 30 31 31 42 36 44 46 38 35 44 41 46 34 31 43 44 39 30 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 43 31 44 37 41 32 38 42 30 37 32 30 36 38 31 31 39 35 46 45 38 41 37 43 39 38 43 31 33 38 32 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 43 31 46 34 Data Ascii: i> <rdf:li>xmp.did:C148C79B62BDBF119A659F3E3D59F01C</rdf:li> <rdf:li>xmp.did:C164DFD84622681197A5F562129EA81F</rdf:li> <rdf:li>xmp.did:C1720D67C680E011B6DF85DAF41CD900</rdf:li> <rdf:li>xmp.did:C1D7A28B0720681195FE8A7C98C1382D</rdf:li> <rdf:li>xmp.did:C1F4
2022-04-08 08:02:44 UTC	6761	IN	Data Raw: 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 36 44 39 43 37 35 39 35 41 32 30 36 38 31 31 39 32 42 30 42 46 30 39 37 46 37 43 35 37 38 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 36 46 45 45 34 41 39 45 35 31 33 45 34 31 31 38 30 45 37 43 37 41 34 35 41 43 38 34 46 37 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 37 30 41 32 43 31 35 31 33 33 39 45 30 31 31 39 31 32 33 42 44 32 33 32 32 30 46 30 45 41 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 37 30 43 38 31 39 37 32 43 32 30 36 38 31 31 39 31 30 39 38 30 35 41 34 35 37 46 42 44 35 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 37 32 38 31 42 35 35 43 33 32 Data Ascii: :li>xmp.did:D6D9C7595A20681192B0BF097F7C5780</rdf:li> <rdf:li>xmp.did:D6FEE4A9E513E41180E7C7A45AC84F73</rdf:li> <rdf:li>xmp.did:D70A2C151339E0119123BD23220F0EAC</rdf:li> <rdf:li>xmp.did:D70C81972C2068119109805A457FBD57</rdf:li> <rdf:li>xmp.did:D7281B55C32
2022-04-08 08:02:44 UTC	6777	IN	Data Raw: 42 32 36 46 41 32 32 30 35 42 44 32 33 46 32 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 45 45 38 39 30 34 39 43 30 41 32 30 36 38 31 31 41 39 36 34 46 36 37 32 31 34 37 33 31 41 46 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 45 45 39 37 34 41 39 33 35 34 32 33 36 38 31 31 41 44 33 39 42 31 41 36 39 43 31 32 37 46 36 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 45 45 42 42 38 30 33 42 30 38 39 36 45 30 31 31 41 38 34 39 36 39 33 39 44 31 39 36 42 33 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 45 45 42 46 36 38 44 32 39 43 32 33 36 38 31 31 41 36 44 44 42 30 39 35 42 30 31 45 30 42 33 39 3c 2f 72 64 66 3a 6c Data Ascii: B26FA2205BD23F27</rdf:li> <rdf:li>xmp.did:EE89049C0A206811A964F67214731AFC</rdf:li> <rdf:li>xmp.did:EE974A9354236811AD39B1A69C127F67</rdf:li> <rdf:li>xmp.did:EEBB803B0896E011A89D96939D196B3F</rdf:li> <rdf:li>xmp.did:EEBF68D29C236811A6DDB095B01E0B39</rdf:li>
2022-04-08 08:02:44 UTC	6784	IN	Data Raw: 46 41 42 36 37 42 45 39 39 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 37 37 46 31 31 37 34 30 37 32 30 36 38 31 31 38 46 36 32 44 37 36 41 34 42 33 43 35 36 35 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 37 37 46 31 37 34 30 37 32 30 36 38 31 31 38 46 36 32 46 41 37 41 43 33 32 44 36 36 30 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 37 37 46 31 31 37 34 30 37 32 30 36 38 31 31 38 46 36 32 46 43 42 46 32 46 44 33 33 39 33 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 37 37 46 31 31 37 34 30 37 32 30 36 38 31 31 39 30 32 37 38 39 41 46 39 46 42 37 36 31 36 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 Data Ascii: FAB67BE993</rdf:li> <rdf:li>xmp.did:F77F1174072068118F62D76A4B3C5656</rdf:li> <rdf:li>xmp.did:F77F1174072068118F62FA7AC32D660A</rdf:li> <rdf:li>xmp.did:F77F1174072068118F62FCBF2FD33937</rdf:li> <rdf:li>xmp.did:F77F117407206811902789AF9FB7616E</rdf:li> <rdf:li>
2022-04-08 08:02:44 UTC	6792	IN	Data Raw: 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 39 37 46 31 31 37 34 30 37 32 30 36 38 31 31 39 37 41 35 44 43 38 31 43 33 31 38 45 33 46 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 39 37 46 31 31 37 34 30 37 32 30 36 38 31 31 39 41 38 32 46 45 32 41 43 42 43 35 37 34 33 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 39 37 46 31 31 37 34 30 37 32 30 36 38 31 31 39 41 38 32 46 45 32 41 43 42 43 35 37 34 33 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 39 37 46 31 31 37 34 30 37 32 30 36 38 31 31 41 37 42 41 45 39 33 30 45 31 44 46 42 36 32 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 46 39 37 46 31 31 37 34 30 37 32 Data Ascii: :li>xmp.did:F97F11740720681197A5DC81C318E3FF</rdf:li> <rdf:li>xmp.did:F97F1174072068119A82FE2ACBC547436</rdf:li> <rdf:li>xmp.did:F97F1174072068119F73E07BD102BE60</rdf:li> <rdf:li>xmp.did:F97F117407206811A7BAE930E1DFB621</rdf:li> <rdf:li>xmp.did:F97F1174072
2022-04-08 08:02:44 UTC	6808	IN	Data Raw: 65 64 65 65 31 36 30 61 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 61 66 30 62 38 34 62 38 2d 34 36 64 63 2d 34 65 39 62 2d 62 38 66 65 2d 61 66 37 32 35 34 62 35 62 34 34 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 61 66 35 35 65 30 62 37 2d 36 34 63 33 2d 36 35 34 61 2d 39 33 65 38 2d 66 65 61 33 37 33 38 32 35 36 33 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 61 66 35 39 61 37 33 30 2d 36 61 33 32 2d 65 65 34 32 2d 61 63 39 65 2d 32 64 32 38 33 32 31 37 35 66 64 61 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 61 66 35 64 36 33 30 31 2d 62 62 66 64 2d 31 33 34 39 2d 62 31 31 66 2d 33 63 64 62 37 62 38 33 64 33 62 Data Ascii: edee160a</rdf:li> <rdf:li>xmp.did:af0b84b8-46dc-4e9b-b8fe-af7254b5b443</rdf:li> <rdf:li>xmp.did:af55e0b7-64c3-654a-93e8-fea373825632</rdf:li> <rdf:li>xmp.did:af59a730-6a32-ee42-ac9e-2d2832175fda</rdf:li> <rdf:li>xmp.did:af5d6301-bbfd-1349-b11f-3cdb7b83d3b
2022-04-08 08:02:44 UTC	6824	IN	Data Raw: 30 35 38 34 63 31 31 33 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 65 30 62 33 39 65 63 63 2d 35 63 38 33 2d 35 39 34 66 2d 61 33 63 34 2d 62 65 33 66 31 34 32 30 37 34 61 66 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 65 30 62 64 36 64 36 38 2d 66 62 37 62 2d 34 64 32 34 2d 61 36 30 32 2d 39 32 30 36 33 65 39 61 30 63 34 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 65 30 65 36 30 31 63 39 2d 32 35 30 61 2d 61 36 34 36 2d 38 63 30 61 2d 32 31 61 64 30 63 61 34 39 36 38 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 65 31 32 37 66 37 36 33 2d 32 35 36 38 2d 34 37 35 36 2d 38 62 35 65 2d 31 39 37 63 32 33 34 65 33 39 Data Ascii: 0584c1135</rdf:li> <rdf:li>xmp.did:e0b39ecc-5c83-594f-a3c4-be3f142074af</rdf:li> <rdf:li>xmp.did:e0bd6d68-fb7b-4d2a-a602-92063e9a0c40</rdf:li> <rdf:li>xmp.did:e0e601c9-250a-a646-8c0a-21ad0ca49689</rdf:li> <rdf:li>xmp.did:e127f763-2568-4756-8b5e-197c234e39
2022-04-08 08:02:44 UTC	6832	IN	Data Raw: 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 66 39 66 34 33 33 37 31 2d 38 34 39 65 2d 34 66 30 30 2d 61 61 39 2d 35 31 66 64 61 35 32 39 61 30 38 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 66 61 31 35 66 62 66 31 2d 62 30 38 36 2d 34 37 66 33 2d 61 38 63 37 2d 31 63 63 62 64 36 62 37 30 37 39 63 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 66 61 35 31 62 39 61 30 2d 30 65 37 61 2d 34 31 32 62 2d 39 63 62 37 2d 34 31 34 33 33 33 38 39 62 64 61 65 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 66 61 35 34 35 62 61 61 2d 61 65 37 35 2d 34 62 63 39 2d 61 66 38 63 2d 36 34 32 38 65 63 61 65 31 34 37 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 Data Ascii: i> <rdf:li>xmp.did:f9f43371-849e-4f00-aaa9-51fda529a083</rdf:li> <rdf:li>xmp.did:fa15fbf1-b086-47f3-a8c7-1ccb6b7079c</rdf:li> <rdf:li>xmp.did:fa51b9a0-0e7a-412b-9cb7-41433389bdae</rdf:li> <rdf:li>xmp.did:fa545baa-ae75-4bc9-af8c-6428ecae1478</rdf:li> <rdf:li>

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:44 UTC	6959	IN	Data Raw: 62 c7 78 00 0c 41 03 d8 3f 0d 72 d6 67 51 99 18 98 f9 f1 42 c9 99 22 3a ea 4b 29 b1 b5 be 0a eb bd a8 dc d5 34 0e 0a e3 f4 f7 9c 7e a7 1a 56 88 31 b6 ba dc 0f f3 d5 3f 53 1c b6 5b 84 8d fc 29 41 80 5f 94 91 c2 b8 2e b5 2e 41 a6 c7 70 59 95 82 b6 84 93 ad af 5a 2b 21 30 0c 3e 8f 26 42 94 79 fc d0 fb 99 ae 38 8f b7 e5 ae 8b e6 55 e0 b6 82 72 3e 6f 4b c2 45 f3 9e 56 36 b2 1b 1b 8f b8 05 2a 65 bb d2 3e d1 b6 13 06 1c 0b 17 93 13 ef 8a c6 e2 fa db fc 35 9d ae db 96 b5 1a 2d 9b 18 e3 c4 17 10 aa 11 a8 66 b9 d0 54 2b 6e 7c c2 60 4b d3 3a 9a 4f 2a 9a 60 92 0f de f6 ad 64 db 1b 8b 69 ae d3 e1 ad de 5c 6e a9 44 5a a0 4e 4c 91 16 57 d3 47 ce de 58 22 e7 b4 fc 43 ec a9 55 9a ee 7e f2 42 e3 4c 82 02 4b 62 dd 96 16 d2 f5 93 75 ec 18 e2 63 b4 b5 94 2a dc 16 26 d6 b1 b5 1b 75 1c Data Ascii: bxA?rgQB"K)4~V1?S]A...ApYZ+!0>&By8Ur>oKEV6*e>5-ft+ñ\K:O\$ph\$!nDZNLWGX"CU~BLKbuc*&u
2022-04-08 08:02:44 UTC	6975	IN	Data Raw: c5 d1 20 9e 58 a5 cf 91 4e 4a dc ab 27 29 70 0f c2 d5 c8 f3 da a9 aa 2e 4f 8b ba 23 47 17 1f ce 55 c8 46 dd 19 5d 49 6b 91 f6 13 bb 75 73 de db 74 7c 4b 46 f2 4e 31 b1 3c 98 46 e2 e6 fc 78 db bb a9 ec a8 77 e5 8f 17 51 d3 ba 14 1c c7 4b 87 ab 7d 64 92 ca a1 61 b9 b5 99 77 13 6e c5 e6 ad f2 db 16 d4 97 57 f3 da 73 e8 6a 64 45 0e 4c 8a 25 8d 4c b6 b8 04 6b 71 af 67 f8 6b 96 ad d5 68 f9 4c c1 24 0a 19 da 62 25 6d fc d6 d0 ae 97 54 1f 2d 6c b8 28 e5 d3 ef 0c b0 c1 8e 19 65 3b 1d 8d 82 dc 5e d6 f6 13 ec a9 dd 6e 1a 8e 02 d2 18 c7 98 57 93 6e 9a 68 0f de f6 ad 64 db d0 10 28 fc 9c b2 c8 db 81 03 7a a8 e3 6e eb a1 f0 ec f8 7c 5f 0d 6b d5 5f ca 29 2b c3 ea 18 9d 40 ee 98 23 3c 72 35 99 88 d0 a9 b5 d3 fc d4 ef 8e d8 f8 4f 32 5f 88 a9 02 83 ad 83 9f 2c 73 dc ac ad Data Ascii: XNJ}p.O#GUF]lkustjKFN1<FwxQK}dawnWsjdEL%Lkqgkhl\$b%mt-l(-e;^nWnhd(zn_l_)+@<#r5O2_s
2022-04-08 08:02:44 UTC	6991	IN	Data Raw: b3 e5 05 13 48 4a c4 d1 b1 5b 0b 73 2b f1 e5 ae 99 4b 4a f4 d7 af 71 52 8f ff d2 e0 65 f4 d7 56 62 af e6 2b 20 3d 95 ae 6f fb 1e fa f8 b5 ea 71 70 83 cf 84 69 c5 0e 7c 00 6f 91 05 96 0d fd b5 ca ed 4b 70 c4 d9 11 cc 5e a5 3a f3 ba 5a f7 00 02 2f 6e 1f aa aa 9e 5d 78 26 54 05 4d 3b e4 aa c5 99 ba 42 c0 0b 46 2c b7 f9 bb 6b 2a d5 57 5a f2 fc dd 41 0c bd 3a 06 22 8f 39 e2 bb 8d 4d c9 3d ba 36 da cd fa 8b 70 4c 52 5a 53 0a 76 11 b7 23 a6 80 5f 40 0f ee d4 cd ea a4 44 32 3a 66 36 64 7f 42 cb f9 36 0c 75 ed 3e fa 75 cb 6a 3d dd e2 93 80 1c 7c 1e 99 d3 41 50 ed 33 37 2e d2 74 1f 65 6f 6c 99 32 7c 25 49 a1 1f 4d c4 d6 79 51 12 e2 e4 71 01 45 60 f2 db 82 92 24 6f 2a 1c 74 df 8b 1a ef 94 68 0e a5 80 a2 5d 9c 59 f4 88 b1 31 83 8f cc 8c 58 db 94 f6 54 bb 47 06 5a Data Ascii: HJ[s+kJqKreVb+ ;oqpi]onKpLi^:Z/n]x&TM;BF,k*WZA:"9M=6pLRZsv#_-@D2:f6dB6u=uj= AP37.teol2 9!m yQqE`\$o*thjY1XTGZ
2022-04-08 08:02:44 UTC	6999	IN	Data Raw: 07 85 9a dd ef f3 54 aa bb 38 48 52 0e 9e a1 82 42 62 89 4c 8d 6d 02 dc 93 71 a6 83 b7 75 68 fd 3d 96 af 94 12 1f a2 48 bd 47 13 6d f4 ee b5 ce b7 e2 d7 61 dd a5 9d 79 76 1b d0 9f 4c 7c 6d 9e 4c 2c c0 46 6d 66 24 fb f4 f6 d2 ca ad 32 fb c1 25 4f d4 0b cc 32 21 61 e4 06 d8 41 b8 0d d8 9b 1b e6 6e f5 52 c7 0a 1f 57 50 07 bc 8c 48 89 18 6e 65 de 56 da 5b ef 1a c1 57 b4 7c 4c cc 9e 93 8f 24 2f f4 71 af 9a 6e 41 23 94 30 ed 7b f2 d7 4d 72 d9 35 b9 f2 fe 2f a4 19 8d d2 7a 0f 54 e9 b3 3e 5b 4a b3 63 0b 9b 45 ab 12 de 1b 37 76 bb 32 fa 8c 79 16 d8 db 7f 8f a4 90 ae 9f d6 8f 9e 7a 6e 5a 36 3b 4c 58 dc e8 48 f6 a6 ea cf 26 1d 37 d5 ef d9 05 d4 e8 c4 40 46 11 50 3a 58 2d 98 df 41 ed dd de 6a f3 67 5e 21 60 7c 8e a7 12 93 8f 23 22 b1 52 e4 36 84 02 6c 3e ea 6d ee d6 Data Ascii: T8HRBbLmquh=HGmayvLjml,Fmf\$2%O2!aAnRWPHeV[W]L\$/qnA#0[Mr5/zT>JcE7v2yznZ6;LXH&7@FP:X-Ajg^! "#R6l>m
2022-04-08 08:02:44 UTC	7015	IN	Data Raw: d2 1b 83 c6 46 f6 31 08 9e 2d a7 46 24 11 6f 7d af 58 6d 8d 65 58 bd c4 95 15 54 16 90 94 3d ac 46 bf f4 d2 99 ec 29 58 99 05 6c ab db ec a9 0b 39 29 8e 33 29 3b e3 1b 90 d8 6a 1a df ab bb 56 dc 76 90 40 f4 f8 84 c7 20 44 82 73 c5 ed 66 3f 6b 55 79 8e 22 5e df 08 16 34 0f aa 91 1e de 06 c7 fc b6 a9 56 5f 10 99 99 9b d1 d3 31 82 c8 ac 18 02 2e b6 e0 7e fe ed 7e 6e f5 74 d3 33 a7 02 50 56 36 27 d3 28 89 0b 32 8e 01 bb 3f 4d af 59 5a fb 9c b2 cb af da e0 92 3b 01 d2 f5 1f c0 06 19 0a aa 40 0f 61 a9 d2 ff 00 ab b6 8d bf c0 64 e4 3e 50 f3 2c 40 b8 07 68 d7 fd 96 92 d7 40 2b 58 d6 4b 3a ee 61 6e de 3a ff 00 6d 53 6d 08 9c 98 25 c5 bc c6 00 f6 1b 58 54 ab c7 60 30 47 e9 d8 52 39 0f 1a c8 e4 73 10 b7 e1 f1 11 5b 2c 97 4b 8c 08 1b aa 74 dc 25 c7 f2 dd cc 31 27 30 Data Ascii: F1-F\$o}XmeXT=F)Xl9)3;)jVv@ Dsf?kUy^^4V_1,~~nt3PV6'(2?MYZ;@ad>P,@h@+XK:an:mSm%XT"0GR9s[K t%1'0
2022-04-08 08:02:44 UTC	7031	IN	Data Raw: 28 d4 10 39 45 bf b0 55 79 96 b7 8a c0 5c aa b7 f2 58 a9 24 77 49 bd c7 d9 51 f6 8b 43 34 e3 e1 42 4e 34 31 c4 92 31 ee 80 3b 35 6b fd b5 d3 ba ef 99 bb 10 d9 7e 36 36 24 2a 62 48 e3 54 b5 f6 5e fa 7b 92 b3 b5 ac f5 6d ff 00 10 92 d4 87 1a 31 74 55 0b 7e 28 bf ef da 2a 5d ac f8 fe 21 40 23 f4 fe 9f 30 67 5c 71 21 d7 77 29 1f 6d f8 6e ad 56 4b d7 49 8f e6 29 05 e9 9d 0b a5 2c 82 6c 6c 5f 29 f5 37 6b 82 bf f2 ad 72 e7 c9 11 6b 6e 1a 72 5f 2f a7 71 5f 20 64 c6 cc b2 86 24 15 ec 1d ab 7e da 85 ea 6c ab b5 f4 80 40 e8 aa 5c ba b3 ab 5e fa 37 13 f6 30 6d bf 86 b3 f3 f4 8f fd 01 22 cc 8c 41 20 2b b3 7b 1f 8d 89 17 1f ef a9 ad e3 b6 3e 54 10 d0 36 1a 3e cf ab 62 8b 7d a4 23 10 ba 8b 9d ab f3 56 95 bb 53 b7 5f 98 50 5d 83 2c 58 e8 b2 46 ce 50 90 2c d6 b8 24 fe 8e Data Ascii: (9EUy\X\$wIQC4BN411;5k~66\$*bHT^m1tU~(*)!@#0glq!w)mnnVKl),ll_7krknr_/q_ d\$~!@^70m"A +>T 6>b}#VS_P],XFP,\$
2022-04-08 08:02:44 UTC	7039	IN	Data Raw: 63 b8 dd e6 5e e7 5e cb 0e 15 0f 15 56 ad f3 2e e9 ad 57 68 7a e3 06 4b 39 60 58 85 da 0d ad db c4 78 ab 9d db 5d 05 7b fb 8c ce a7 d1 61 cd 0e ab 2b c3 2d f9 9c 6a 4d c7 0b b7 60 f9 2b a7 16 77 48 d1 5a be 13 9c c8 e8 be 83 38 7b 96 5c 82 f1 31 b8 1a 82 a7 e2 bf c5 5d 79 fd 7e 0b 98 5b a0 d1 9f d3 18 6d 0a e2 6e 2c 57 c4 d4 bf bb 5c f5 57 4f 71 4a de f0 16 f4 76 24 6e d2 66 48 44 40 81 b4 1b ed 03 82 ad fd a7 bd b2 b7 ff 00 32 cd 45 57 31 72 bb 0d 7c 7c 9c 78 f2 47 4e 8d 19 08 42 41 b0 02 c4 f1 3f 37 de ae 4b 56 ce bb db 90 de 4a 78 a1 9f 24 e2 99 18 4a ea 1a d7 d3 f5 52 ab 75 ae e8 e5 44 4e a5 a8 cd 88 b8 1b ce a8 9c 14 91 db f7 9a a1 ad ee 62 46 cb 4c 17 8e f2 15 2a 7b 5b ed ff 00 8d 4e ed 74 11 5c 98 51 c4 5d 62 01 46 9b ac 09 24 f1 50 3e 2a a5 Data Ascii: c^^V.WhzK9`Xxj}[a+-jm`+wHZ8{1jy-[mn,WMWOqJv\$nfHD@2EW1rj]xGNBA?7KJVJ\$JRuDnBFL^!{[nQ]bF\$ P>*
2022-04-08 08:02:44 UTC	7047	IN	Data Raw: d3 06 fe 64 f0 84 1a f2 dc 7e 8f c3 5a 34 97 46 e2 22 09 e3 fd 24 c4 98 00 90 2e 8c 34 16 f6 36 be 16 a5 6d cb 8e 81 56 10 ea 87 43 12 ed 07 5d 6e 45 66 9b f7 8c b5 1e 25 e5 1a 1c ba 6b 50 d3 25 91 49 e1 7e e1 5d e3 56 4b 83 6f bd 6a a7 56 b8 fd e1 26 01 9d d6 57 0e 45 8c 91 7d 2e b7 00 58 fb 3e ed 6f 4c 3b d4 91 6b c1 07 ea d0 34 e3 14 b9 59 5a c4 12 46 b7 34 d6 17 1b a3 94 cd 97 36 46 5e f2 b8 f2 24 9a db 6a ea 46 bd bb bd f5 0a b5 8d 56 d0 4c 2e 25 94 31 13 b6 c6 3a 6b 6b fe af 0d 64 da 8d 0e 94 d4 13 67 55 52 c8 c7 ef 58 f6 71 b5 4a 53 c4 c5 d8 91 c5 6d c3 c9 2a 91 83 73 71 c6 f9 69 6e f7 8d 64 1b c8 97 42 a0 58 9d 6e dc 3f 47 8b ee d3 dc 8a de 8a c9 8a 39 8c 3b ef 36 d0 da 8d 35 b8 b0 17 aa d5 a9 8e 52 93 92 99 16 2e 04 12 c7 4e 54 05 78 f8 aa d3 7e Data Ascii: d~Z4F"\$.46mVC]nEf%kP%l~]VKojV&WE;.X>oL;k4YZF46F*\$jFVL.%1:kkdgURXqJSm*squindBXn?G9;65R.NTx ~
2022-04-08 08:02:44 UTC	7063	IN	Data Raw: ab c7 8e b6 7a bf fa 19 ed 2c e4 ea 39 39 21 f7 37 e6 06 37 4d b6 0b fa ea 6f 8e b5 8f 77 88 a5 54 15 26 34 b9 0b b2 7b ed e2 4d 87 ea bf c3 59 2b 2a ea 81 a4 01 89 d3 f0 60 95 d6 22 09 dd ab 04 f6 7d 9d d1 5b df 25 ec 94 81 a6 3a 7c 12 ad 96 e0 7f 6f e9 ae 6f 31 a2 8a 8e 04 70 ed 31 c6 ec a0 f0 1c 3f 16 b5 5e 63 7c 5a 14 97 43 93 91 66 60 04 ab 7b 00 40 4b 7d ad c6 a1 d6 bf 2f e3 05 50 06 e9 18 d2 39 96 78 84 4f c7 62 bd c9 f6 5f c5 6a e8 f3 ac 94 27 bb e2 82 a0 c8 eb f0 3f 48 85 a4 c3 c5 68 f6 90 41 b6 a6 ff 00 f0 ae bf 4f 65 99 c5 ad 26 6d 49 e7 91 e7 e4 cf 0b 2d 9c 99 64 1b ec ba 5b b3 5f 8a f5 f4 0f 1d 6a fb 39 6b ca 56 c3 d1 3d 31 9c 45 e2 9d 5f cb 5e 64 2f fa cf b5 6b fd f7 55 3b 54 49 75 46 c6 06 14 b1 39 9b 12 49 59 1a ec cb 28 04 30 1c 76 ee Data Ascii: z,99!77MowT&4{MY+*"}[%: oo1p1?^c ZCF{ @Kj/P9xOb_j"?HhAOe&ml-df_j9kV=1E_^d/kU;TiuF9lY(0v

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:44 UTC	7206	IN	Data Raw: 9e 04 9f 1a 7d 95 d5 95 4d 14 17 06 fe 36 2c f8 f3 3f 92 fb c9 bb 28 20 dc 10 4e ad f2 fc b5 83 aa b7 14 49 ac 52 1c 5c 68 a3 70 4a 4c fe 6e 4b 05 65 d5 9c df 9b 95 bb b5 9b dd 31 a6 c5 f8 8c 9a 28 cd c0 18 70 ef 4d 86 c3 73 ed 6d a6 c0 df 9a 4e f7 e8 a8 ad 1b 7a 33 3e 00 98 21 32 ca c9 d3 18 6d d0 ed ec 07 c5 cd f7 bb bf 1d 2b 51 ce d6 3e 06 b6 6c e7 0b 6c 08 ed 24 ef c7 55 2a 4f b0 f8 77 37 ed ed a7 0a 9c 09 e2 60 f4 ff 00 50 26 76 53 63 21 0b 3a 6f 50 41 22 35 24 73 38 dd ca a7 e6 ad 9e 2b 25 3d db 12 3e 2a 4b 90 15 fc e1 1b a3 ac 6d bb b3 00 d5 1f de ac 32 35 5e 2b 77 84 4d 03 e7 cb 95 83 2b c9 18 12 42 ea 14 34 7b 5f 98 5c 59 3e 6a aa 56 b6 50 f4 b2 f1 72 fd e0 2e cd eb 79 33 62 e3 b3 45 1a 20 4e 66 1a 06 37 1b 77 8f 0b a6 df da ad ad b6 dc Data Ascii: }M6,?(NIR\hpJLnKe1(pMsmNz3>!2m+Q> \$U*Ow7`P&vScI:oPA"5\$5s+%=>*Km25^+wM+B4[_\Y> VPr.y3bE Nf7w
2022-04-08 08:02:44 UTC	7214	IN	Data Raw: e5 44 93 f7 d9 40 2a a1 7b 9a af 36 ef ef 52 b3 dd c0 4d c9 57 50 59 32 22 7c 91 19 7c 86 fe 25 8d f4 43 f9 7c 80 72 c9 b7 bd bb 92 9d 1d 53 4a 62 bd df ab a8 5a 20 ac 4f 32 25 f2 50 49 22 ca b6 db 21 0d 71 6d c0 47 bb ba cb 52 dc fb be 91 a2 ac 5c 84 ea 19 48 a4 12 63 70 0c 8c 7c 03 6e e6 dc bd df 15 69 5c 70 a3 de 26 8d 4c e3 8f 06 4c 99 f1 22 64 4a 59 96 36 53 7d b6 ed d8 ba 8f 87 9e a6 f2 9e d9 5b 09 44 7a 3c 19 12 99 b2 42 6c 4b b3 6e 60 0d 47 88 e6 f7 ee e5 4a c3 35 77 15 77 2c 94 19 90 e5 64 63 8c 82 d0 22 15 56 b1 b2 b2 f8 99 7c bf 87 e0 f1 51 8f 1d 6b c7 59 7f 74 c9 98 f8 fd 2f f9 57 54 9b 27 16 12 d8 6e c4 44 18 5d 95 87 74 3b b7 71 bc 7f e5 ae dc d9 55 eb a3 88 fc a6 89 e8 1f d1 f0 f0 f2 b3 a5 79 04 9f 50 b2 6d 11 a3 5c ca 74 f8 f7 30 2f f1 77 Data Ascii: D@*{6RMWPY2"} %C[rSJbZ O2%PI"lqmGR\Hcp n!p&LL"dJY6S)[Dz<B!Kn`J5ww,dc"V QkYt\WTnD]t;qUy Pm!t0/w
2022-04-08 08:02:44 UTC	7230	IN	Data Raw: 6d 6d d2 20 1c ec 97 ee 72 d7 4e 3a 43 95 d7 f6 8a 0e ae 47 8d d0 ae 19 12 2a 91 e6 2c c0 12 49 ef 16 e1 e2 ee a2 d7 22 51 79 68 a3 23 ae 60 8c 18 2d 23 03 8c a4 15 29 7b 06 3c 17 6b 73 33 29 ef 77 ab 75 5e 6e 5e 6d c4 59 82 43 8c ea 22 8d ca c6 c8 d7 04 82 6f af 10 bf dd f8 a9 2b 29 6c db 1e 88 d2 86 4c cc 50 d3 1d d2 46 77 15 62 db 4e bd d6 61 ed ac ed 74 f4 9d a3 6c cd 79 e4 cb 46 9a 32 ea de 51 0b 23 31 24 b5 fb 80 5b e2 ee b5 6e a5 3f e7 cd f2 9e ae a6 96 36 1c 88 40 ea 5b 25 9c 11 20 08 2f b5 ad b4 05 73 dd b7 8b e2 a8 cb 9d fe 2e 4f b4 a9 35 64 e8 d0 75 08 f7 64 b0 56 7d 42 c4 d6 bd 9b 72 a4 d2 f1 9b c2 bd da df 14 35 3e f2 60 c8 cc 8f ce cf 78 b2 e3 31 c2 79 ca 30 ba dd 47 96 ee d6 d9 b5 2d c9 f1 b5 45 da 9d 1f 36 ed 82 80 07 e9 98 58 c2 6c ec 79 24 Data Ascii: mm rN:CG*,!~Qyh#`-#{<ks3)wu^n^mYc"o+)ILPFwbNatlyF2Q#1\$[n?6@[/% ./s.O5dudV]Br5>~x1y0G-E6Xly\$
2022-04-08 08:02:44 UTC	7246	IN	Data Raw: 27 10 60 c3 14 d2 bb 16 97 76 e0 a9 1d fb 13 c4 13 77 c4 d5 74 ca ad ab 5f 27 7b 98 aa a0 2e a7 95 30 ea 41 33 ef 8e 5b f8 6a b2 0b 8d a7 46 d9 fc 24 49 3c 3b fe 1d b4 28 86 ea a7 c5 cb 9f 7b dc a5 34 6a 2c d3 62 c8 89 90 26 94 ca e0 24 8c 8a 4a b7 b7 f2 46 ca e7 cc d6 59 b2 ec fa 77 57 ea 12 40 dd 5f 0d 11 55 72 02 31 7b f9 60 9d 3b 77 ef f8 94 72 fe 2a 8c 57 6f 84 fc 5f d2 6b c4 d3 87 3b 1e 16 55 44 54 8e 08 c8 02 f7 bb db 94 58 ee 7e 70 bb b6 a7 35 6b b1 64 45 aa e9 a1 9d d0 fa a7 51 81 bc e9 a1 59 e7 04 84 2d ca c0 11 bb f2 d1 fb dc dc ab fb 55 6d d3 15 a6 af 6f e2 a8 ec d5 74 0e 7f 52 47 2e d1 d4 22 7c 8b b5 a5 f2 fe 90 8f c0 23 af 68 5f 13 ee ae aa dd 37 2f fb 8a 94 80 a1 c6 68 72 04 84 5e 15 24 01 7e 23 41 e6 72 be 6e ed 3c 2b 89 58 fe d3 77 a3 64 Data Ascii: `vwt_'.0A3jF\$!<:{4j,b&\$JFYwW@_Ur1';wr*Wo_k;UDTX~p5kdEQY-UmotRG."#h_7/hr%^~#Arn<+Xwd
2022-04-08 08:02:44 UTC	7254	IN	Data Raw: 47 b4 0b a3 f5 bc 33 d5 95 5e 15 92 44 04 24 92 48 7b c3 5b c6 bf 1b 7c ed 5b e6 c1 6f 2b 8e d9 ea ad 6b dd f8 85 10 6b 75 29 33 5d 64 92 49 a4 86 24 22 44 0c 03 02 46 bb 6c de 1f 7d 73 63 75 4d 42 56 b7 49 52 98 34 31 e0 f5 18 c7 57 cc 91 b1 67 da 49 8b 60 da db 47 2b 69 f1 fe d3 57 4e 5b d9 3d aa 2f a8 9f d8 0b 8e d2 4c d0 e4 4b 33 63 c8 cd 75 12 21 0a c9 71 7d b6 e5 4f 87 99 3f 15 4d 92 49 a4 b7 fc af 9b 78 f6 87 f5 c2 32 e2 77 8f 77 d6 85 31 ee 5b 59 96 fc aa aa da ed b7 35 63 e9 f9 1e bf f8 fa 82 0d 6e 8e 23 86 33 87 8f 28 c8 ca 24 ac 8d 36 d6 70 77 6d 8e c5 95 76 af c3 51 e6 5f c2 ab 57 d1 b4 ab 3d 0a d7 15 a3 78 af 72 5b 9b 78 7b 96 6e 0a 9e 5f 87 77 2d 15 ba b7 f1 21 06 e4 cb 1c c8 93 c2 ca 43 b3 29 36 b6 d6 5f f4 d5 78 0f 86 8f 2d a5 b9 fd d3 Data Ascii: G3^D\$H[[[[[o+kku)]3]d!\$DF]}scuMBVIR41Wgl`G+iWN[=LK3cu!q]O?Mlx2ww1[Y5cn#3(\$6pwmvQ_W=xr!x[n_w-!C)6_x-
2022-04-08 08:02:44 UTC	7270	IN	Data Raw: 7c 35 12 28 c7 e8 b8 78 b8 a5 7a 9c ed e7 4b 73 12 be dd ab ee 1e 56 ee ff 00 c5 5d 4b 2e f9 da a3 6f 86 79 be 6d c3 82 d2 57 3e 44 38 f1 ac 4d 3c 62 26 20 14 5b 2f 37 e3 3d bd da e5 4d e3 4d 37 bb 6b dd e2 b0 ad 2c d1 e8 ed 6c 99 b0 e3 c4 3f 51 18 58 c9 57 04 6d b7 7d 7c c3 e2 ef 69 5b c7 07 e2 91 41 5f 51 c2 76 9f cb 12 98 dd 06 d7 0a 45 9f e1 df bb bf b7 bb cb 5c b4 c9 0b 86 ef 70 93 ec 2c c0 cb c9 c1 2d 83 8c 56 4c ee 5b 28 b1 65 b9 1f c3 51 c7 93 fc d5 a5 53 dd b9 27 5e e9 aa 5d 86 44 de ae cd f4 df 58 85 0b ee 33 bd a5 8c af 25 ef 68 f7 3e 8d 27 7b f3 36 d7 7f a7 c6 9a 77 5d 58 fd af ca 0d c1 d0 b7 5c ea 00 94 2c c0 a4 a4 b5 d8 ca 1a e0 b7 99 0c 7c e1 39 77 2a 57 03 ca ef c5 bb 56 dc db 7a 36 fc e4 4c 99 bd 53 d6 f1 cc 1f a5 f4 ec 70 13 20 b3 36 c9 Data Ascii: [5(xzKsV]K.oymW>D8M<b& [/7=MM7k,l?QXWm)]i[A_QvE!p,-VL{[eQS^]DX3%h>{6w}Xl,j9w*WVz6LSp 6
2022-04-08 08:02:44 UTC	7286	IN	Data Raw: e6 4d ad 23 74 fe 8b 83 93 2a 49 33 79 7e 52 08 d6 34 51 b7 e2 e7 24 6e 76 f8 5d bb d5 96 5c f6 55 85 af e6 23 49 3f ff d7 cd e9 b1 e2 f4 6c 89 a0 87 0d 0c c0 f3 b6 d2 c1 89 f8 07 dd ef 6d af 8b ae 65 7a ae f9 b4 38 a4 0b a6 c2 f9 59 8f 8e c8 62 81 c3 2b 49 60 00 24 f0 56 3a 05 55 ae 7b 57 74 34 d6 e9 33 7a b1 fd 3c 25 20 e3 62 46 52 1c 69 48 95 ef 6b 81 cd d8 cd fb ff 00 15 65 ea b6 ad 6c e6 f7 5c a5 b7 a7 da 68 4d 21 5b a9 64 34 b0 03 ca 79 75 2f f8 8d 67 82 62 17 bb ee 10 b5 d4 d5 ea 78 fd 33 1b 02 18 64 58 d6 4d cc 36 aa f3 58 71 95 91 7b db aa ec 95 aa af 47 37 e9 b1 73 06 1b c7 8c b8 f1 ae 3e d5 9e 42 c0 aa 83 b8 af 1f d9 16 e5 ac d2 b3 72 fa 49 69 b2 30 ba c9 9e 91 4c d2 42 e5 83 21 2b 6d 96 ef 58 0f f5 1b e2 ad b1 a7 5e 11 f1 1b 4e 90 Data Ascii: M#*!3y~R4Q\$Nv]U#?lmez8Yb+!`\$V:U[Wt43z<% bFRiHkelhM[d4m0yu/gbx3dXM6Xq[G7s>Brl0LB!+mX^N
2022-04-08 08:02:44 UTC	7293	IN	Data Raw: 66 5c ac be ab 24 71 92 04 6a 0a 39 d0 0b eb b5 fe 24 f9 ab 4a aa d7 1a 9e f7 51 9a 96 c3 3a 66 16 34 6d 93 9f d6 a6 f2 a2 66 b1 8c b7 29 20 58 6d 1d e7 d3 b8 ab 58 e5 bd 9e da 62 5b ad e2 f6 e9 36 af da 03 97 14 72 ff 00 fa 37 99 f4 4c 11 cb 21 09 ce 4f e5 eb f2 a7 7d ab ae 8d d7 47 d7 e1 1b 90 7e 9d 16 43 6f 8b 26 65 3a 92 82 40 77 39 51 e1 ec 8d 7e f5 5d f6 ae 0b 6f f0 05 a0 4c 9d 37 1d 59 64 ca bc 8e a0 9d a0 1b 10 35 11 b9 26 fa a5 ee f2 54 d3 22 8d 34 1c 85 60 e0 c7 34 21 d1 44 06 68 ec f1 be a0 ee 04 05 67 ef 72 37 36 cf 86 b9 af 91 d5 f8 b5 ea af b7 78 73 08 a3 eb 61 c7 48 94 43 1b c2 ec 55 de 21 76 54 ee ad 9b b3 77 77 98 f8 aa b6 3b 37 ad b7 2e 9d fd 36 b8 27 ef 0a 22 58 f2 20 41 18 c7 8f 16 30 61 dd ac c6 3d 6e b6 b7 ef af de ad f2 59 5a a9 39 Data Ascii: fl\$qj9JQ:f4mf) XmXb[6rL!O]G~Co&e:@w9Q~JoL7Yd5T^4!Dhgr76xaHCU!vTww;7.6""X A0a=nYZ9
2022-04-08 08:02:44 UTC	7301	IN	Data Raw: 3b 32 63 15 1b b9 7c cb 3d ae b2 3a ae df 30 ff 00 b6 da d9 3a 25 af 2b fe 3d d2 62 4c 6c e9 72 73 d5 ba 7a 29 77 45 0a 48 0c 86 6b 1e 49 19 0f 73 68 ef 1b 6e ad 26 b4 e6 e1 5f cb fb 88 bc b3 ab e9 be 99 9d 20 51 94 e0 e2 f9 61 d9 64 3a 0f fe 11 72 59 ff 00 15 79 f7 97 36 4b 6b f1 78 fe 32 a0 1f 11 e4 c6 2d 8b 12 3c 28 ee 59 1a 22 02 9b fb 81 e6 e7 ff 00 65 a8 97 68 69 ee 7e 1b 10 9f 61 08 73 9a 59 65 59 1a 56 11 90 84 3c 85 d4 5c 8f cc 95 75 5f d9 ee d5 5a ad c4 c7 37 d9 f8 6a 6a 8b f3 67 38 7d 4d 31 f2 76 ae a4 67 6f 6e de 08 e8 cd 7a 7d 4d 55 ff 00 22 1b 01 e9 3d 33 19 13 21 b1 d8 a0 60 23 92 63 ab 9b f3 3a a2 9d 0c 8f b9 39 bf 62 ba 55 9d a3 7c 47 57 ca 64 91 25 e9 38 bd 3e 38 4a 44 66 11 3d ca 39 3a ee ef 7f 0b f8 ae 9d ee 6e 4a 8f 3d 5a Data Ascii: ;2c =:0:%+=bLlrsz)wEHklshn&_ Qad:ryY6Kkx2-<(Y"ehi~asYeYV<lu_Z7jjg8)M1vgon~MyMU'=3!`#c:9b UjGWD%8>8JDF=9.nJ=Z

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:44 UTC	7317	IN	Data Raw: e5 ae 65 9b e8 9f 95 51 98 a8 00 06 b8 f2 f8 6f 93 e3 ff 00 b7 5e 75 b1 d5 57 6f fe e5 7d ba be 1f cc 68 b5 46 9f 4c f4 aa f5 78 27 97 3b 39 71 36 80 e1 36 96 ed e1 29 ff 00 0a 57 a1 e9 31 52 fa cf 48 eb 5d 35 33 fa cc fd 46 09 d9 71 c3 65 19 11 49 2f b9 2f 6f 1b b6 ed df 9b e1 e6 5a e6 d9 44 f9 fb af ef 7f 69 29 ea 1f 00 cd 30 49 89 04 89 24 e9 18 2e c5 89 44 53 df dd fd c4 ff 00 b9 58 e3 c5 b9 f9 89 6d a5 77 7c c3 99 32 fa e6 3f 55 c6 95 33 3a 50 46 8d 57 70 42 6c 1c f8 f7 20 ef 7c ab 4f 05 f1 db 4c 9c 67 ee 98 d9 99 9d 33 0d b2 a0 9f 23 a9 a4 91 99 24 2e 47 6a b7 b5 7c 4a ab f0 d7 46 6b ed b2 54 db ca bf 09 3d a0 d9 b9 59 5d 47 a4 98 b2 e4 69 42 c8 4c 71 de ec 7c 2a ac 57 bc ad c7 6f 2d 69 4a 57 1e 59 aa db cb cd 6e e9 4e c6 27 59 9a 44 c0 4e 9d 02 aa Data Ascii: eQno^uWo)hFLx';9q66)W1RH)53Fqel//oZDi)0l\$.DSXmwj[2?U3:PFWpBl OLg3#\$.Gj JfKt=Y GiBLq *Wo-iJWYnN'YDN
2022-04-08 08:02:44 UTC	7333	IN	Data Raw: 54 9a 4d d3 fa 9e 36 2c f9 b9 3b 1e 3c dc 75 d5 0d c0 11 92 cd 6f 2b 70 54 dc cc 8b 5d 4f 16 d4 a3 a6 59 d9 06 77 a6 72 b1 32 9d 89 94 99 7c 6b 7b e9 dd d6 da 5f 68 fb b5 c7 ea 69 6a ae 1c bd d2 2c 5b 9f 9d 26 1e 33 c5 d2 d9 63 8c ca cb 2e 81 98 69 e6 6d f3 5b b7 e2 a8 c7 45 7b 4e 4e 67 b7 93 bb f0 f4 0a c8 e7 3a 77 4a 6f 54 23 e4 ca ea 91 e3 0d a6 dc 4b 12 59 4b 26 9b b9 2b d2 c9 93 fc 6d 12 9d e6 6a 91 c0 dc 98 ac 3d 25 14 37 d4 02 f6 47 75 da 76 6a 0d c7 ef 2e ee e7 2d 72 2d 72 be e9 33 a9 e7 7d 47 ab ae 3c e3 18 b9 48 c1 dd bc 2d db 70 1f 0d fe 2a f7 b1 e1 dc b7 47 d3 3d d2 9a 3a 2e 91 d4 71 27 e9 90 e5 bb 04 9f 1d 64 69 40 3b 77 0b ec f2 f6 f8 9a 6d c9 fb d5 e7 e5 c7 7a e4 75 5d 37 db b7 f7 7d 00 b4 3b 7e 92 8e e9 0b 4f 1a 4b 1b 21 91 54 39 da 1c 77 Data Ascii: TM6;<uo+pT OYwr2[k_hij,[&3c.im[E{NNg:wJoT#KYK&+mj=%7Guvj.-r3}G<H-p'G=:.q'di@:wmzu]7};~OK!T9w
2022-04-08 08:02:44 UTC	7341	IN	Data Raw: 7a 3f 13 a4 af d6 64 5d b2 05 da 49 5d 8d f5 d5 bd ca b5 e6 64 f5 96 cb ca ba 3b b4 26 cd c1 8c 7a d4 11 cb 17 5e cb 1b a3 8e 65 f2 d3 60 e6 00 f3 59 4f 29 8f 67 2f 37 8f 9a bd 1c 34 74 b6 c5 f3 5f db c4 5d 56 a7 51 d5 27 69 d8 e7 62 ec 18 aa 59 d7 50 c1 3c 57 60 fc 87 75 fc 35 cb 9a d5 b5 b4 ef 77 3b c5 59 43 02 e9 fd 5b 37 e5 52 c3 d8 a2 81 48 6f 36 38 c2 ee b7 7b 6d f9 5b 69 a9 58 6b 46 9f 36 ef 8a dd 03 ae ac 59 5e 9a 83 33 2c 75 79 7c c0 77 a7 96 8a 00 5b 28 da a4 69 dd b7 ed 54 bf 58 d2 74 5b 7b 77 09 30 21 d0 e4 39 93 99 09 87 11 98 32 45 b8 16 37 e0 24 f8 77 1d b6 f9 6b 5b e7 ac 2d bd 5e 2f 0f cb e2 35 75 93 47 a5 85 00 8c c8 d2 e1 8b 3b 8f 68 16 58 d1 bf 76 b9 ed 12 a1 bd be 1f 84 cd 68 55 90 8b d5 11 3e a1 7c 88 a2 90 79 11 89 2e 2f 6d 1e 63 c3 Data Ascii: z?d]j]d;&z^e`YO)g/74t_VQ'ibYP<W`u5w;YC[7>R<Ho68[m IXkF6Y^3,uy w (ITXt[{w0!92E7\$wk[-^/5uG;hXvhU> y./mc
2022-04-08 08:02:44 UTC	7357	IN	Data Raw: c9 99 db 43 3f 39 d7 a2 99 1d e3 12 79 df c3 51 c3 ee d6 d8 d7 9d 10 e3 6f 51 9d 6d 2e 4c 9e 9b 99 9c 8f e7 63 7e 5c b0 30 60 38 82 3f ed bf dd ae bc 94 a3 51 6e 6a df db 70 3c 9b 5f cc 74 9d 4d 46 79 59 f2 d9 f0 b0 ca ed 89 a1 1f ea 90 1d 94 ee e6 6f c3 5c d5 b3 4b 95 79 96 f8 bc 15 3b 15 93 39 1c 0e 93 17 4c 7f 3b 69 c8 cd 42 ac 46 eb 2d d8 f8 b6 ee dc 47 8b bb b6 bb af 95 e5 51 d1 8f 5f 9b 94 6e a2 cd c1 7c 1e ba 1a 37 49 cb 46 59 5a 35 e5 2c 79 76 22 fd fe 5a 75 b2 be 28 e9 e6 24 d9 f4 87 5d 9b c8 7e 98 ea 77 43 23 17 ba f7 10 82 8c ac fe 11 cc dd ce 76 ae 7f 53 85 27 bd 77 91 4b 40 de 8d 04 cd 3a 60 f4 d8 63 76 43 b7 6e c0 02 5b 9f cc 79 1f 76 e5 b7 3e b5 85 96 ed 6c df 37 db d5 f4 99 2b 36 c0 ba 8f 45 ce f5 07 fe 24 4f e6 b4 25 9d e5 1e c0 6e 6d f1 Data Ascii: C?9yQoQm.Lc~l0'8?Qnjp<_tMFyYoKy;9L;iBF-GQ_n]7IFYZ5,yv"Zu({~wC#s\$wK@:'`cvCn yv>I7+6E\$O%nm
2022-04-08 08:02:44 UTC	7373	IN	Data Raw: 94 2c 52 65 44 bb 71 a1 65 01 99 86 a4 fc 0b df da bf 17 76 9a c3 66 a4 bd bd a6 57 5c 18 59 51 41 d4 32 95 12 5c 05 da 06 e0 18 ee 6d cb 20 4f 13 fc 6d f3 d7 a7 5c ce d4 58 eb fd c1 75 2b 40 0c 8c 3c de ac f1 64 cc fb 71 5d 4e d0 8e 09 17 1f 07 1e 6f 15 61 5b d3 12 75 5d 7f c3 f5 1c d0 e7 53 71 b0 d3 19 1a 1c 78 ca 41 60 be 74 b6 6e 23 99 97 b0 7d d5 db cd 59 dd ce a6 ea 2a 05 06 7a e1 60 c5 1b 46 8e ac e3 62 a2 05 bd 1d f9 da 49 7b c7 7d 6b bd da d1 e1 ea dd d5 7b f8 45 be 4c ef 45 16 cc ca 96 48 81 5c 65 25 51 5f ba c0 9f ef 2d 6b ea da a2 8e f4 1a 55 1b 5e a7 10 62 60 19 67 26 19 a0 3b 63 8e 30 4f 39 21 f6 96 f9 bc 55 e7 fa 5b 5a f7 85 cd 5b 6b 5b 6b c3 e2 1c 41 b7 d2 f1 ba 6f a8 30 86 4b bf 3b c6 a1 c0 16 2c 46 a4 6e fe fb eb b2 f9 9d 16 d8 e7 a9 70 Data Ascii: ,ReDqevfMYQA2lM Om\Xu+@<dq Noa[u]SqxA`tn#}Y*z'Fbl{k{ELEHle%Q_-kU^b`g&;c0O9!U Z[kk[AoOK,;Fnp
2022-04-08 08:02:44 UTC	7381	IN	Data Raw: c4 da fb 97 ee f8 be 5a db ce 8e 2b 62 f8 bb e6 d8 9a ab 3b 68 3a f6 3c 33 49 1f 51 44 c8 45 c7 0b 11 95 6f a2 9b 71 1f 17 c3 55 4c d1 ac 4f 65 4a 76 d4 e7 ff 00 ab fe a8 4e bb 86 62 c3 41 1a c0 ca b3 72 d8 28 db c8 91 fd ea eb c3 9b 7d d3 7e ee 43 3c b9 37 00 7f 4e 3d 3b d7 3a ca 45 91 81 0e d8 42 bc 23 21 db 6a 29 3a 33 27 fd de 53 e1 56 d9 5d b5 a3 dc c1 55 b2 df 56 ff 00 4b 32 3d 2c f1 f5 1c b7 53 8f 1a ed 93 68 62 a7 71 e5 44 df e2 ef 33 2a d1 9e 8d 56 11 9d ea d2 83 2f a7 f5 ec ac 68 1f 23 a7 ed 5e 9e 96 60 93 b8 2c 45 f9 b6 25 ee ab f0 d7 8d 93 d3 d6 ce 2f ff 00 95 f6 e3 5f 98 c9 1d 46 0f aa e5 e9 31 c9 d4 15 bc d8 27 62 f1 90 b7 06 fa 38 da de 14 ae 3a 62 7b d2 5c b9 31 f2 db 77 b7 78 e8 a3 83 53 a3 47 1e 6e 3f 99 03 46 b8 8e cd 29 3b 36 0b 9e 21 Data Ascii: Z+b;h:<3lQDEoqULoeJvNbAr()~C<7N=;;EB#l}):3'SV]UVK2=,ShbqD3^V/h#^',E%/_F1'b8:b{1wxSGn?F);6!

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49995	23.10.249.43	443	C:\Users\user\l\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	82	OUT	GET /cms/api/am/imageFileData/RWP8kk?ver=8c62 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate, br User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134 Host: img-prod-cms-rt-microsoft-com.akamaized.net Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	231	IN	HTTP/1.1 200 OK Content-Type: image/jpeg Content-Location: https://image.prod.cms.rt.microsoft.com/cms/api/am/imageFileData/RWP8kk?ver=8c62 Last-Modified: Sun, 03 Apr 2022 23:44:39 GMT Access-Control-Allow-Origin: * X-Source-Length: 1829994 X-Datacenter: northeu X-ActivityId: b692f3e9-5950-4927-a446-404fc0aad364 Timing-Allow-Origin: * X-Frame-Options: deny X-ResizerVersion: 1.0 Content-Length: 1829994 Cache-Control: public, max-age=56590 Expires: Fri, 08 Apr 2022 23:45:52 GMT Date: Fri, 08 Apr 2022 08:02:42 GMT Connection: close
2022-04-08 08:02:42 UTC	232	IN	Data Raw: ff d8 ff e1 13 12 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 07 01 12 00 03 00 00 00 01 00 01 00 00 01 1a 00 05 00 00 00 01 00 00 00 62 01 1b 00 05 00 00 00 01 00 00 00 6a 01 28 00 03 00 00 00 01 00 02 00 00 01 31 00 02 00 00 00 1f 00 00 00 72 01 32 00 02 00 00 00 14 00 00 00 91 87 69 00 04 00 00 00 01 00 00 00 a8 00 00 00 d4 00 0e a6 00 00 00 27 10 00 0e a6 00 00 00 27 10 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 32 1e 31 20 28 57 69 6e 64 6f 77 73 29 00 32 30 32 31 3a 31 31 3a 31 31 20 30 36 3a 35 34 3a 33 34 00 00 00 00 00 00 03 a0 01 00 03 00 00 00 01 ff ff 00 00 a0 02 00 04 00 00 00 01 00 00 07 80 a0 03 00 04 00 00 00 01 00 00 04 38 00 00 00 00 00 00 00 06 01 03 00 03 00 00 00 01 00 06 00 00 01 1a 00 05 00 00 00 01 00 00 01 22 01 1b 00 05 00 Data Ascii: ExifMM*bj(1r2i"Adobe Photoshop 21.1 (Windows)2021:11:11 06:54:348"
2022-04-08 08:02:42 UTC	263	IN	Data Raw: 61 35 39 62 32 66 34 38 2d 39 63 62 38 2d 66 31 34 66 2d 39 61 36 37 2d 66 37 36 31 32 64 31 61 64 61 62 32 22 20 73 74 45 76 74 3a 77 68 65 6e 3d 22 32 30 31 35 2d 30 34 2d 32 39 54 31 32 3a 31 38 3a 33 35 2d 30 37 3a 30 30 22 20 73 74 45 76 74 3a 73 6f 66 74 77 61 72 65 41 67 65 6e 74 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 34 20 28 57 69 6e 64 6f 77 73 29 22 20 73 74 45 76 74 3a 63 68 61 6e 67 65 64 3d 22 2f 22 2f 3e 20 3 c 72 64 66 3a 6c 69 20 73 74 45 76 74 3a 61 63 74 69 6f 6e 3d 22 73 61 76 65 64 22 20 73 74 45 76 74 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 64 64 38 33 61 66 34 35 2d 39 66 63 39 2d 64 66 34 66 2d 39 64 64 65 2d 62 61 66 39 30 32 38 32 62 32 31 65 22 20 73 74 45 76 74 3a 77 68 65 Data Ascii: a59b2f48-9cb8-f14f-9a67-f7612d1adab2" stEvt:when="2015-04-29T12:18:35-07:00" stEvt:softwareAgent="Adobe Photoshop CC 2014 (Windows)" stEvt:changed="/"/> <rdf:li stEvt:action="saved" stEvt:instanceID="xmp.iid:dd83af45-9fc9-df4f-9dde-baf90282b21e" stEvt:wh
2022-04-08 08:02:42 UTC	279	IN	Data Raw: 30 30 26 23 78 39 3b 46 69 6c 65 20 44 3a 5c 57 6f 72 6b 5c 57 69 6e 31 30 2d 4c 6f 63 6b 73 63 72 65 65 6e 73 5c 5f 4c 41 54 45 53 54 74 72 61 6e 73 66 65 72 2d 4e 65 77 43 6f 6d 70 75 74 65 72 5c 54 65 6d 70 6c 61 74 65 73 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 31 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 37 2d 32 36 54 31 38 3a 32 33 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 3 6 2d 30 37 2d 32 37 54 31 32 3a 30 32 3a 32 33 2d 30 37 3a 30 30 Data Ascii: 00	File D:\Work\Win10-Lockscreens_LATESTransfer-NewComputer\Templates\Lockscreen_1920x1080_Landscape1.psd saved
2016-07-26T18:23-07:00	File C:\Users\lv-lizagh\MS\Windows10\Lockscreen_1920x1080_Landscape.psd saved
2016-07-27T12:02:23-07:00
2022-04-08 08:02:42 UTC	281	IN	Data Raw: 6e 64 6f 77 73 50 72 6f 5f 47 65 74 79 49 6d 61 67 65 73 2d 36 34 31 30 32 37 32 35 37 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 38 2d 30 34 54 31 37 3a 32 35 3a 32 38 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 41 64 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 2e 35 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 57 69 6e 64 6f 77 73 50 72 6f 5f 47 65 74 79 49 6d 61 67 65 73 2d 36 34 31 30 32 37 32 35 37 5f 31 39 32 30 78 31 30 38 30 46 39 31 42 31 36 31 39 42 41 33 46 39 44 43 37 45 32 32 46 45 38 37 35 31 32 32 39 36 34 36 30 2e 70 73 62 20 73 61 76 65 64 26 23 Data Ascii: ndowsPro_GettyImages-641027257_1920x1080.jpg saved
2016-08-04T17:25:28-07:00	File C:\Users\lv-lizagh\AppData\Roaming\Adobe\Adobe Photoshop CC 2015.5\AutoRecover_WindowsPro_GettyImages-641027257_1920x1080F91B1619BA3F9DC7E22FE87512296460.psb saved&#
2022-04-08 08:02:42 UTC	452	IN	Data Raw: 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 2e 35 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 46 61 6c 6c 45 6e 74 65 72 74 61 69 6e 6d 65 6e 74 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 34 37 38 38 36 33 30 32 31 5f 31 39 32 30 78 31 30 38 30 31 39 38 36 36 37 31 38 41 31 33 33 41 37 43 36 32 33 37 33 39 35 38 31 45 42 31 33 39 30 42 39 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 39 2d 32 36 54 31 30 3a 31 33 3a 35 39 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 7 3 31 30 5c 46 61 6c 6c 45 6e 74 65 72 74 61 69 6e 6d 65 6e 74 5c 46 61 6c 6c 45 6e 74 65 72 74 61 69 6e 6d 65 6e 74 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 34 30 37 31 37 36 31 30 5f Data Ascii: e Photoshop CC 2015.5\AutoRecover_FallEntertainment_GettyImages-478863021_1920x108019866718A133A7C623739581EB1390B9.psb saved
2016-09-26T10:13:59-07:00	File C:\Users\lv-lizagh\MS\Windows10\FallEntertainment\FallEntertainment_GettyImages-540717610_
2022-04-08 08:02:42 UTC	468	IN	Data Raw: 34 37 39 32 30 44 35 46 34 31 44 38 35 43 33 30 44 45 36 34 33 44 46 35 42 35 37 39 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 31 31 2d 31 36 54 31 33 3a 35 32 3a 31 31 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 41 6 4 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 2e 35 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 30 30 31 46 34 37 39 32 30 44 35 46 34 31 44 38 35 43 33 30 44 45 36 34 33 44 46 35 42 35 37 39 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 31 31 2d 31 36 54 31 33 3a 35 34 2d 30 38 3a 30 Data Ascii: 47920D5F41D85C30DE643DF5B579.psb saved
2016-11-16T13:52:11-08:00	File C:\Users\lv-lizagh\AppData\Roaming\Adobe\Adobe Photoshop CC 2015.5\AutoRecover_Lockscreen_1920x1080_Landscape01F47920D5F41D85C30DE643DF5B579.psb saved
2016-11-16T13:54-08:0
2022-04-08 08:02:42 UTC	508	IN	Data Raw: 32 38 30 36 44 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 31 31 2d 32 33 54 31 35 3a 35 34 3a 31 35 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4f 66 66 69 63 65 5c 4f 66 66 69 63 65 2d 42 61 74 63 68 32 5c 5f 43 48 4f 53 45 4e 2d 53 77 61 79 5c 43 72 6f 70 73 5c 4f 66 66 69 63 65 5f 53 77 61 79 2d 55 73 65 72 73 5f 70 31 30 32 33 6d 38 33 37 31 34 39 66 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 31 31 2d 32 33 54 31 35 3a 35 36 3a 30 38 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4f 66 66 69 63 65 5c Data Ascii: 2806D.psb saved
2016-11-23T15:54:15-08:00	File C:\Users\lv-lizagh\MS\Windows10\Office\Office-Batch2_CHOSEN-Sway\Crops\Office_Sway-Users_p1023m837149f_1920x1080.jpg saved
2016-11-23T15:56:08-08:00	File C:\Users\lv-lizagh\MS\Windows10\Office\

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	524	IN	Data Raw: 35 2e 35 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 30 30 31 46 34 37 39 32 30 44 35 46 34 31 44 38 35 43 33 30 44 45 36 34 33 44 46 35 42 35 37 39 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 31 2d 33 31 54 30 39 3a 34 36 3a 31 30 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 38 33 5c 43 48 4f 53 45 4e 5c 4d 38 33 5f 47 65 73 74 79 49 6d 61 67 65 73 2d 35 31 36 31 31 34 36 37 35 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 31 2d 33 31 54 30 39 3a 34 37 3a 30 38 2d 30 38 3a 30 26 23 78 39 3b 46 69 6c 65 Data Ascii: 5.5\AutoRecover_Lockscreen_1920x1080_Landscape001F47920D5F41D85C30DE643DF5B579.psb save d&#xA;2017-01-31T09:46:10-08:00&#x9;File C:\Users\lv-lizagh\MSI\Windows10\M83\CHOSEN\M83_GettyImages-516114675_1920x1080.jpg saved&#xA;2017-01-31T09:47:08-08:00&#x9;File
2022-04-08 08:02:42 UTC	540	IN	Data Raw: 30 37 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 43 6f 72 74 61 6e 61 5c 53 70 6f 74 6c 69 67 68 74 5c 43 48 4f 53 45 4e 5c 43 6f 72 74 61 6e 61 2d 53 70 6f 74 6c 69 67 68 74 5f 73 68 75 74 74 65 72 73 74 6f 63 6b 5f 39 31 39 38 30 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 33 2d 30 36 54 31 33 3a 33 39 3a 35 37 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 Data Ascii: 07-08:00&#x9;File C:\Users\lv-lizagh\MSI\Windows10\Cortana\Spotlight\CHOSEN\Cortana-Spotlight_shutte rstock_91911980_1920x1080.jpg saved&#xA;2017-03-06T13:39:57-08:00&#x9;File C:\Users\lv-lizagh\MSI\Wind ows10\Lockscreen_1920x1080_Landscape.psd saved&#xA;2017-0
2022-04-08 08:02:42 UTC	818	IN	Data Raw: 32 30 36 32 35 35 35 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 33 2d 32 37 54 31 32 3a 30 37 3a 30 37 2d 30 37 3a 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 57 69 6e 64 6f 77 73 5c 53 65 72 76 69 63 69 6e 67 5c 43 48 4f 53 45 4e 5c 52 6f 75 6e 64 31 5c 57 69 6e 64 6f 77 73 53 65 72 76 69 63 69 6e 67 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 30 38 33 34 32 36 33 34 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 Data Ascii: 2062555_1920x1080.jpg saved&#xA;2017-03-27T12:07:07-07:00&#x9;File C:\Users\lv-lizagh\MSI\Windows10\ Windows\Servicing\CHOSEN\Round1\Windows\Servicing_GettyImages-508342634_1920x1080.jpg saved&#xA;2017-03- 27T12:08:28-07:00&#x9;File C:\Users\lv-lizagh\MSI\Window
2022-04-08 08:02:42 UTC	862	IN	Data Raw: 69 63 72 6f 73 6f 66 74 5c 45 6d 70 6f 77 65 72 69 6e 67 43 6c 61 73 73 72 6f 6f 6d 54 6f 6f 6c 73 5c 43 48 4f 53 45 4e 5c 45 6d 70 6f 77 65 72 69 6e 67 54 6f 6f 6c 73 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 34 38 36 37 37 36 36 37 36 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 34 2d 31 38 54 31 30 3a 35 38 3a 35 34 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 69 63 72 6f 73 6f 66 74 5c 45 6d 70 6f 77 65 72 69 6e 67 43 6c 61 73 73 72 6f 6f 6d 54 6f 6f 6c 73 5c 43 48 4f 53 45 4e 5c 45 6d 70 6f 77 65 72 69 6e 67 54 6f 6f 6c 73 5f 47 65 74 74 79 49 6d 61 67 Data Ascii: icrosoft\EmpoweringClassroomTools\CHOSEN\EmpoweringTools_GettyImages-486776676_1920x1080.jpg saved&#xA;2017-04-18T10:58:54-07:00&#x9;File C:\Users\lv-lizagh\MSI\Windows10\Microsoft\EmpoweringClassroom Tools\CHOSEN\EmpoweringTools_GettyImages-512526623_1920x1
2022-04-08 08:02:42 UTC	949	IN	Data Raw: 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 30 30 31 46 34 37 39 32 30 44 35 46 34 31 44 38 35 43 33 30 44 45 36 34 33 44 46 35 42 35 37 39 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 35 2d 31 31 54 31 35 3a 30 30 3a 34 38 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 6f 6d 65 6e 74 73 49 6e 54 69 6d 65 5c 4e 42 41 5c 4d 61 79 5c 43 68 6f 73 65 6e 5c 43 72 6f 70 73 5c 4d 49 54 2d 4e 42 41 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 32 30 34 37 31 33 32 32 5f 31 39 32 30 78 31 30 38 30 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 35 2d 31 31 54 31 35 3a 30 34 3a 31 31 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 Data Ascii: 1920x1080_Landscape001F47920D5F41D85C30DE643DF5B579.psb saved&#xA;2017-05-11T15:00:48-07 :00&#x9;File C:\Users\lv-lizagh\MSI\Windows10\MomentsInTime\NBA\May\Chosen\Crops\MIT_NBA_GettyImages-1 20471322_1920x1080.psd saved&#xA;2017-05-11T15:04:11-07:00&#x9;File
2022-04-08 08:02:42 UTC	965	IN	Data Raw: 42 42 35 37 35 32 36 38 36 38 38 35 31 44 32 37 31 43 42 31 43 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 36 2d 31 31 54 32 30 3a 32 34 3a 31 36 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4f 66 66 69 63 65 5c 4f 66 66 69 63 65 2d 42 61 74 63 68 32 5c 5f 43 48 4f 53 45 4e 2d 4f 33 36 35 52 65 6e 5f 77 61 6c 5c 4f 66 66 69 63 65 2d 42 32 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 36 37 34 34 37 39 38 34 31 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 36 2d 31 31 54 32 30 3a 32 35 3a 33 33 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c Data Ascii: BB57526868851D271CB1C.psb saved&#xA;2017-06-11T20:24:16-07:00&#x9;File C:\Users\lv-lizagh \MSI\Windows10\Office\Office-Batch2_CHOSEN-O365Renewal\Office-B2_GettyImages-674479841_1920x1080.jpg saved&#xA;2017-06-11T20:25:33-07:00&#x9;File C:\Users\lv-lizagh\MSI\
2022-04-08 08:02:42 UTC	1061	IN	Data Raw: 52 65 63 6f 76 65 72 5c 5f 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 30 30 31 46 34 37 39 32 30 44 35 46 34 31 44 38 35 43 33 30 44 45 36 34 33 44 46 35 42 35 37 39 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 37 2d 30 39 54 31 39 3a 34 34 3a 33 33 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 2e 70 73 64 20 73 61 76 65 64 26 2 3 78 41 3b 32 30 31 37 2d 30 37 2d 31 31 54 31 32 3a 35 37 3a 33 34 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 Data Ascii: Recover_Lockscreen_1920x1080_Landscape001F47920D5F41D85C30DE643DF5B579.psb saved&#xA;20 17-07-09T19:44:33-07:00&#x9;File C:\Users\lv-lizagh\MSI\Windows10\Lockscreen_1920x1080_Landscape.psd s aved&#xA;2017-07-11T12:57:34-07:00&#x9;File Lockscreen_1920x1080_La
2022-04-08 08:02:42 UTC	1132	IN	Data Raw: 51 75 69 7a 5c 5f 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 42 69 6e 67 53 70 6f 74 6c 69 67 68 74 51 75 69 7a 5f 73 68 75 74 74 65 72 73 74 6f 63 6b 5f 31 39 34 31 38 35 39 39 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 37 2d 33 31 54 31 34 3a 35 36 3a 33 35 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3 b 32 30 31 37 2d 30 37 2d 33 31 54 31 35 3a 33 33 3a 34 34 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c Data Ascii: Quiz_CHOSEN\Crops\BingSpotlightQuiz_shutterstock_19418599_1920x1080.jpg saved&#xA;2017-07- 31T14:56:35-07:00&#x9;File C:\Users\lv-lizagh\MSI\Windows10\Lockscreen_1920x1080_Landscape.psd saved&#xA;2017 -07-31T15:33:44-07:00&#x9;File C:\Users\lv-lizagh\AppData\

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	1188	IN	Data Raw: 2d 34 35 32 31 36 32 38 39 35 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 39 2d 31 35 54 31 33 3a 35 30 3a 35 31 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 43 6f 72 74 61 6e 61 5c 41 63 71 75 6 9 73 69 74 69 6f 6e 73 52 65 6d 69 6e 64 65 72 73 5c 43 68 6f 73 65 6e 5c 43 72 6f 70 73 5c 41 63 71 52 65 6d 69 6e 64 65 72 73 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 31 31 30 35 38 30 34 33 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 39 2d 31 35 54 31 33 3a 35 31 3a 30 33 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 Data Ascii: -452162895_1920x1080.jpg saved&#xA;2017-09-15T13:50:51-07:00&#x9;File C:\Users\lv-lizagh\MSI\Windows 10\Cortana\AcquisitionsReminders\Chosen\Crops\AcqReminders_GettyImages-111058043_1920x1080.jpg saved &#xA;2017-09-15T13:51:03-07:00&#x9;File C:\Users\lv-lizagh
2022-04-08 08:02:42 UTC	1299	IN	Data Raw: 53 2d 52 65 77 61 72 64 73 2d 57 65 6c 63 6f 6d 65 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 34 36 37 31 37 39 32 33 39 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 39 2d 32 38 54 31 31 3a 33 31 3a 32 37 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 41 64 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 37 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 30 30 31 46 34 37 39 32 30 44 35 46 34 31 44 38 35 43 33 30 44 45 36 34 33 44 46 35 42 35 37 39 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 Data Ascii: S-Rewards-Welcome_GettyImages-467179239_1920x1080.jpg saved&#xA;2017-09-28T11:31:27-07:0 0&#x9;File C:\Users\lv-lizagh\AppData\Roaming\Adobe\Adobe Photoshop CC 2017\AutoRecover\Lockscreen_1 920x1080_Landscape001F47920D5F41D85C30DE643DF5B579.psb saved&#xA;20
2022-04-08 08:02:42 UTC	1386	IN	Data Raw: 20 6f 70 65 6e 65 64 26 23 78 41 3b 32 30 31 37 2d 31 31 2d 31 35 54 31 36 3a 30 35 3a 33 32 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4f 66 66 69 63 65 5c 53 70 6f 74 6c 69 67 68 74 5f 46 59 31 37 5c 5f 43 48 4f 53 45 4e 5c 52 65 61 63 71 75 69 73 69 74 69 6f 6e 5c 43 72 6f 70 73 5c 4f 66 66 69 63 65 2d 52 65 61 63 71 75 69 73 69 74 69 6f 6e 5f 73 68 75 74 74 65 72 73 74 6f 63 6b 5f 33 36 30 37 38 36 37 32 35 5f 31 39 32 30 78 31 30 38 30 2e 70 73 64 20 73 61 76 65 64 26 23 7 8 41 3b 32 30 31 37 2d 31 31 2d 31 35 54 31 36 3a 30 37 3a 31 31 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e Data Ascii: opened&#xA;2017-11-15T16:05:32-08:00&#x9;File C:\Users\lv-lizagh\MSI\Windows10\Office\Spotlight_FY1 7\CHOSEN\Reacquisition\Crops\Office-Reacquisition_shutterstock_360786725_1920x1080.psd saved&#xA;2017-11-15T16:07:11-08:00&#x9;File C:\Users\lv-lizagh\MSI\Win
2022-04-08 08:02:42 UTC	2088	IN	Data Raw: 65 6e 74 73 49 6e 54 69 6d 65 5c 43 6f 6c 6c 65 67 65 46 6f 6f 74 62 61 6c 6c 42 6f 77 6c 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4d 49 54 2d 43 6f 6c 6c 65 67 65 46 6f 6f 74 62 61 6c 6c 42 6f 77 6c 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 38 32 36 32 31 30 38 38 36 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 31 32 2d 31 34 54 31 32 3a 33 36 3a 33 30 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 31 32 2d 31 34 54 31 34 3a 31 34 3a 30 34 2d 30 38 3a 30 30 26 23 78 39 3b Data Ascii: entsInTime\CollegeFootballBow\CHOSEN\Crops\MIT-CollegeFootballBowl_GettyImages-82621088 6_1920x1080.jpg saved&#xA;2017-12-14T12:36:30-08:00&#x9;File C:\Users\lv-lizagh\MSI\Windows10\Lockscre en_1920x1080_Landscape.psd saved&#xA;2017-12-14T14:14:04-08:00&#x9;
2022-04-08 08:02:42 UTC	2096	IN	Data Raw: 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 31 32 2d 32 30 54 32 33 3a 33 32 3a 34 35 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 6f 6d 65 6e 74 73 49 6e 54 69 6d 65 5c 4e 46 4c 5c 44 65 63 32 30 31 37 2d 50 6f 73 74 53 65 61 73 6f 6e 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4d 49 54 2d 4e 46 4c 2d 50 6f 73 74 53 65 61 73 6f 6e 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 34 37 34 30 35 34 36 38 5f 31 39 32 30 78 31 30 38 30 2e 7 0 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 31 32 2d Data Ascii: -lizagh\MSI\Windows10\Lockscreen_1920x1080_Landscape.psd saved&#xA;2017-12-20T23:32:45-08 :00&#x9;File C:\Users\lv-lizagh\MSI\Windows10\MomentsInTime\NFL\Dec2017-PostSeason\CHOSEN\Crops\MIT-NFL- PostSeason_GettyImages-547405468_1920x1080.psd saved&#xA;2017-12-
2022-04-08 08:02:42 UTC	2104	IN	Data Raw: 23 78 41 3b 32 30 31 38 2d 30 31 2d 32 34 54 31 35 3a 30 30 3a 33 39 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 53 72 65 77 61 72 64 73 5c 41 55 2d 58 62 6f 78 47 61 6d 69 6e 67 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4d 53 52 65 77 61 72 64 73 58 62 6f 78 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 36 30 30 31 34 35 35 38 38 5f 31 39 32 30 78 31 30 38 30 2e 6 a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 31 2d 32 34 54 31 35 3a 30 33 3a 34 35 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 5f 5f 54 65 6d 70 6c 61 74 65 73 5c 4c 6f 63 6b 73 63 72 65 65 6e Data Ascii: #xA;2018-01-24T15:00:39-08:00&#x9;File C:\Users\lv-lizagh\MSI\Windows10\MSrewards\AU-XboxG aming\CHOSEN\Crops\MSRewardsXbox_GettyImages-600145588_1920x1080.jpg saved&#xA;2018-01-24T15:03:45-0 8:00&#x9;File C:\Users\lv-lizagh\MSI\Windows10_Templates\Lockscreen
2022-04-08 08:02:42 UTC	2120	IN	Data Raw: 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 49 54 2d 49 6e 74 65 72 6e 61 74 69 6f 6e 61 6c 5c 48 6f 6d 65 77 6f 72 6b 41 69 64 5f 73 68 75 74 74 65 72 73 74 6f 63 6b 5f 35 33 36 34 30 32 35 34 35 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 32 2d 31 35 54 31 35 3a 31 38 3a 30 34 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 49 54 2d 49 6e 74 65 72 6e 61 74 69 6f 6e 61 6 c 5c 48 6f 6d 65 77 6f 72 6b 41 69 64 5c 43 48 4f 53 45 4e 5c 43 Data Ascii: #x9;File C:\Users\lv-lizagh\MSI\Windows10\MIT-International\HomeworkAid\CHOSEN\Crops\MIT-Intl_Homewo rkAid_shutterstock_536402545_1920x1080.jpg saved&#xA;2018-02-15T15:18:04-08:00&#x9;File C:\Users\lv-lizagh\MSIW indows10\MIT-International\HomeworkAid\CHOSEN\C
2022-04-08 08:02:42 UTC	2136	IN	Data Raw: 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 69 63 72 6f 73 6f 66 74 5c 4d 69 78 65 72 45 6e 67 61 67 65 6d 65 6e 74 2d 46 59 31 38 5c 52 6f 75 6e 64 32 5c 5f 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4d 69 78 65 72 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 30 33 37 30 30 38 32 38 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 33 2d 32 31 54 31 35 3a 34 37 3a 34 35 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 5f 5f 54 65 6d 70 6c 61 74 65 73 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 33 2d 32 31 54 31 36 3a 34 Data Ascii: MSI\Windows10\Microsoft\MixerEngagement-FY18\Round2\CHOSEN\Crops\Mixer_GettyImages-50370 0828_1920x1080.jpg saved&#xA;2018-03-21T15:47:45-07:00&#x9;File C:\Users\lv-lizagh\MSI\Windows10_Tem plates\Lockscreen_1920x1080_Landscape.psd saved&#xA;2018-03-21T16:4

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	2144	IN	Data Raw: 6c 69 3e 30 33 33 41 43 36 41 32 36 44 38 36 35 46 43 46 41 35 30 38 32 31 30 35 37 42 37 43 32 32 32 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 33 33 41 45 34 34 43 43 44 37 45 36 39 30 45 35 45 35 46 38 32 35 45 31 37 44 32 46 44 32 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 33 34 46 43 35 44 39 38 32 3 5 46 42 36 32 33 39 33 39 41 31 34 46 33 32 39 31 42 33 35 44 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 33 35 35 30 43 42 35 30 33 36 37 34 45 46 46 32 39 37 36 43 30 45 39 34 33 37 43 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 33 35 35 33 39 45 36 34 30 38 42 43 37 46 33 45 45 45 34 42 30 44 33 45 32 42 37 31 41 35 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 30 33 Data Ascii: li>033AC6A26D865FCFA50821057B7C222F</rdf:li> <rdf:li>033AE44CCD7E690E5E5F825E17D2FD2B</rdf:li> <rdf:li>034FC5D9825FB623939A14F3291B35D0</rdf:li> <rdf:li>03550CB503674EFF2976C0E9F38A37CD</rdf:li> <rdf:li>035539E6408BC7F3EEE4B0D3E2B71A54</rdf:li> <rdf:li>03
2022-04-08 08:02:42 UTC	2160	IN	Data Raw: 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 30 37 32 43 35 43 37 39 39 44 30 33 41 41 39 46 31 45 38 34 31 41 34 42 43 46 44 31 38 39 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 30 37 38 39 36 34 44 39 30 33 36 30 44 36 34 38 44 46 34 44 44 30 36 34 37 36 39 43 31 37 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 30 39 31 37 46 38 33 46 45 33 36 39 31 30 45 34 33 31 32 44 30 43 39 37 34 37 30 34 44 44 39 3c 2f 7 2 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 30 39 33 42 46 38 46 41 37 45 39 35 38 37 34 36 38 46 36 36 38 46 44 44 31 37 43 46 37 42 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 30 39 38 36 34 42 42 43 46 45 39 46 38 45 37 41 44 37 44 30 32 43 44 31 37 32 33 44 39 33 42 3c 2f 72 64 Data Ascii: C</rdf:li> <rdf:li>1072C5C799D03AA9F1E841A4BCFD1894</rdf:li> <rdf:li>1078964D90360D648DF4DD064769C17F</rdf:li> <rdf:li>10917F83FE36910E4312D0C974704DD9</rdf:li> <rdf:li>1093BF8FA7E9587468F668FDD17CF7B2</rdf:li> <rdf:li>109864BBCFE9F8E7AD7D02CD1723D93B</rd
2022-04-08 08:02:42 UTC	2176	IN	Data Raw: 30 31 38 45 34 38 37 42 36 37 41 42 43 41 36 46 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 45 33 30 37 42 46 46 30 37 33 43 34 44 41 41 37 31 37 34 36 46 33 38 39 31 36 34 35 38 32 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 45 36 32 39 37 39 38 44 38 36 38 42 44 41 43 45 39 45 36 43 31 36 39 34 36 31 46 31 33 32 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 45 36 35 46 35 32 35 32 42 46 44 41 31 33 37 35 35 3 4 34 38 45 45 39 34 37 34 44 45 34 33 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 45 36 38 43 31 45 36 38 43 41 38 41 46 41 36 31 43 35 32 33 42 46 32 43 36 34 43 39 32 38 35 37 32 37 46 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 31 45 36 44 31 31 35 32 31 38 46 32 41 36 37 44 35 33 32 36 Data Ascii: 018E487B67ABCA6F0</rdf:li> <rdf:li>1E307BFF073C4DAA71746F389164582B</rdf:li> <rdf:li>1E629798D868BDACE9E6C169461F132A</rdf:li> <rdf:li>1E65F5252BFDA13755448EE9474DE43A</rdf:li> <rdf:li>1E68CA8AFA61C5232F2C64C9285727F8</rdf:li> <rdf:li>1E6D115218F2A67D5326
2022-04-08 08:02:42 UTC	2184	IN	Data Raw: 42 39 43 32 42 39 36 45 43 36 42 38 37 38 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 34 44 31 34 44 45 46 46 33 38 38 42 41 32 32 38 45 44 31 36 41 36 35 37 30 32 31 36 43 30 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 34 44 32 38 42 46 43 42 36 43 39 32 35 42 36 33 32 43 42 44 38 33 36 37 37 35 36 36 34 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 34 44 45 37 44 32 37 41 37 34 43 37 41 43 30 45 30 33 6 38 45 44 37 36 32 30 46 33 45 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 34 45 33 43 45 41 38 39 45 31 36 32 41 43 33 44 42 30 41 34 34 42 33 41 46 32 45 45 36 30 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 32 34 46 36 39 30 39 38 32 42 41 42 41 31 36 41 31 32 44 38 36 46 Data Ascii: B9C2B96EC6B8786</rdf:li> <rdf:li>24D14DEFF388BA228ED16A6570216C0E</rdf:li> <rdf:li>24D28BFCB6C925B6322CBD836775664A</rdf:li> <rdf:li>24DE7D27A743C47AE0E068ED7620F3E3</rdf:li> <rdf:li>24E3CEA89E162AC3DB0A44B3AF2EE60B</rdf:li> <rdf:li>24F690982BABA16A12D86F
2022-04-08 08:02:42 UTC	2200	IN	Data Raw: 46 31 45 30 41 33 34 44 30 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 30 45 34 41 46 32 35 44 32 45 38 37 35 42 45 31 37 32 35 32 45 35 45 31 38 33 45 35 43 37 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 30 46 39 32 41 46 42 46 37 46 45 35 33 39 33 39 39 38 30 44 37 32 30 36 34 34 45 38 30 45 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 31 30 31 43 44 42 30 36 43 43 36 39 34 42 32 33 31 33 38 32 33 36 45 36 35 36 43 36 33 30 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 31 31 34 41 46 39 31 44 30 33 38 38 43 44 45 30 30 41 37 32 37 34 46 39 37 35 46 36 43 35 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 31 31 39 41 39 30 36 44 35 38 46 37 33 38 35 44 38 36 36 39 45 32 32 41 36 33 Data Ascii: F1E0A34D07</rdf:li> <rdf:li>30E4AF25D2E875BE17252E5E183E57C</rdf:li> <rdf:li>30F92AFBF7FE53939980D720644E80E5</rdf:li> <rdf:li>3101CDB06CC694B23138236E656C630A</rdf:li> <rdf:li>31114AF91D0388CDE00A7274F975F6C54</rdf:li> <rdf:li>3119A906D58F7385D8669E22A63
2022-04-08 08:02:42 UTC	2216	IN	Data Raw: 34 45 32 46 33 38 46 41 39 39 32 41 34 35 45 36 34 30 38 46 44 33 38 39 37 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 45 37 36 37 37 43 34 42 34 34 43 39 33 46 38 32 43 34 33 43 39 34 30 35 38 38 39 45 43 44 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 45 38 32 37 39 35 33 37 35 33 38 37 30 31 30 36 38 36 43 39 36 44 33 33 30 42 36 36 41 42 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 45 38 39 31 44 38 32 3 8 39 30 41 37 45 41 44 46 42 39 44 38 33 30 30 44 32 37 38 36 32 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 45 38 39 33 37 42 32 39 45 31 41 43 31 43 34 30 34 45 34 38 35 41 32 33 41 45 45 45 39 41 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 33 45 38 39 35 34 36 38 31 33 35 Data Ascii: 4E2F38FA992A45E6408FD3897D</rdf:li> <rdf:li>3E7677C4B44C93F82C43C9405889ECD8</rdf:li> <rdf:li>3E82795375387010686C96D330B66AB2</rdf:li> <rdf:li>3E891D482890A7EADF89D8300D27862A</rdf:li> <rdf:li>3E8937B29E1AC1C404E485A23AEEE9AD</rdf:li> <rdf:li>3E895468135
2022-04-08 08:02:42 UTC	2223	IN	Data Raw: 35 42 39 39 41 45 35 31 31 30 31 45 43 44 39 32 36 43 41 41 44 33 42 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 34 41 36 43 43 30 32 32 43 30 32 34 45 39 33 34 33 45 30 38 30 45 32 35 38 31 39 45 33 38 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 34 43 38 35 43 34 36 46 31 32 41 38 38 45 34 43 42 43 34 39 42 41 36 37 45 43 45 38 36 38 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 34 44 32 37 44 31 39 45 39 30 3 6 35 41 35 46 35 31 38 33 38 36 30 45 34 31 36 36 34 43 42 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 44 38 43 31 31 36 36 31 32 35 44 30 45 32 38 39 46 44 33 35 30 43 41 41 43 44 35 38 41 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 34 44 45 37 44 39 42 44 34 33 36 45 Data Ascii: 5B99AE51101ECD926CAAD3B3</rdf:li> <rdf:li>44A6CC022C024E9343E080E25819E384</rdf:li> <rdf:li>44C85C46F12A88E4CBC49BA67ECE8682</rdf:li> <rdf:li>44D27D19E9065A5F5183860E41664CB5</rdf:li> <rdf:li>44D8C1166125D0E289FD350CAACD58AA</rdf:li> <rdf:li>44DE7D98BD436E
2022-04-08 08:02:42 UTC	2231	IN	Data Raw: 41 35 30 45 33 36 37 38 34 45 44 43 37 39 30 39 39 32 30 42 44 32 46 46 33 44 37 36 35 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 41 41 45 36 46 37 43 37 39 43 35 41 38 43 36 32 41 34 45 37 32 46 31 36 45 32 43 37 41 37 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 41 41 46 46 41 35 43 33 42 44 42 45 39 30 4 1 33 44 46 46 39 39 35 31 44 36 46 46 45 33 39 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 41 42 34 39 37 41 32 36 41 34 41 43 32 32 33 31 46 39 33 34 45 38 36 41 37 33 33 42 45 41 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 41 43 38 31 42 33 31 33 43 36 44 44 33 39 41 46 37 41 36 43 37 34 32 35 36 30 42 30 39 46 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 41 45 41 32 44 33 Data Ascii: A50E36784EDC7909920BD2FFD7655</rdf:li> <rdf:li>4AAE6F7C79C5A8C62A4E72F16E2C7A7C</rdf:li> <rdf:li>4AAFFA5C3BDBE90A3DFF9951D6FFE397</rdf:li> <rdf:li>4AB497A26A4AC2231F934E86A733BEAA</rdf:li> <rdf:li>4AC81B313C6DD39AF7A6C742560B09FE</rdf:li> <rdf:li>4AEA2D3

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	2247	IN	Data Raw: 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 38 37 36 34 38 30 35 41 35 45 39 34 37 38 33 46 46 30 36 45 45 42 37 35 44 43 31 42 39 34 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 38 38 36 33 37 37 35 42 46 45 44 30 34 39 36 36 44 43 32 32 39 42 41 44 33 35 39 35 39 31 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 38 39 36 41 34 37 44 32 45 31 46 43 36 33 34 32 42 39 42 37 43 43 37 37 35 41 46 39 33 46 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 38 42 44 31 45 35 39 37 44 33 44 38 41 41 30 41 43 46 39 45 37 34 46 31 43 32 42 39 31 42 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 38 43 34 41 38 42 32 42 43 37 39 36 34 42 46 44 32 46 33 32 38 31 36 44 42 37 38 36 43 33 33 3c 2f 72 64 66 3a 6c 69 3e Data Ascii: f.li> <rdf:li>58764805A5E94783FF06EEB75DC1B94A</rdf:li> <rdf:li>58863775BFED04966DC229BA D3595915</rdf:li> <rdf:li>5896A47D2E1FC6342B9B7CC775AF93F4</rdf:li> <rdf:li>58BD1E597D3D8AA0ACF9E74F 1C2B91B2</rdf:li> <rdf:li>58C4A8B2BC7964BFD2F32816DB786C33</rdf:li>
2022-04-08 08:02:42 UTC	2263	IN	Data Raw: 20 3c 72 64 66 3a 6c 69 3e 36 37 33 42 31 36 31 35 41 42 32 33 43 36 42 43 39 36 32 38 46 34 46 39 45 36 43 45 30 31 32 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 37 34 32 35 36 44 36 44 37 31 44 46 34 42 32 38 38 44 39 38 43 43 43 35 41 43 39 33 43 41 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 37 34 38 3 3 38 45 39 46 30 31 37 44 43 44 36 38 39 37 44 45 42 30 35 38 46 42 42 38 31 44 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 37 35 30 45 35 39 46 42 45 31 30 42 41 34 45 31 34 45 43 37 37 46 36 38 39 35 44 38 34 31 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 37 36 32 41 37 34 32 44 42 30 31 35 45 42 32 38 32 34 33 39 42 43 39 38 44 46 45 44 44 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 Data Ascii: <rdf:li>673B1615AB23C6BC9628F4F9E6CE012C</rdf:li> <rdf:li>674256D6D71DF4B288D98CCC5AC93 CAE</rdf:li> <rdf:li>674838E9F017DCD6897DEB058FBB81D6</rdf:li> <rdf:li>6750E59FBE10BA4E14EC77F6895D8 416</rdf:li> <rdf:li>6762A742DB015EB282439BC98DFEEDD7</rdf:li> <rdf
2022-04-08 08:02:42 UTC	2271	IN	Data Raw: 72 64 66 3a 6c 69 3e 36 44 44 44 39 45 43 45 36 34 41 43 30 34 33 44 39 35 41 43 32 38 42 38 38 35 35 41 45 42 30 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 45 30 35 34 35 39 45 44 42 37 39 37 43 41 41 41 41 38 35 38 43 30 37 35 36 34 35 38 37 41 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 45 30 38 46 41 3 4 44 32 34 35 31 33 32 44 46 32 35 33 41 39 30 32 32 33 34 43 35 46 36 32 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 45 30 41 43 45 46 36 44 35 30 42 46 41 43 41 45 35 45 41 43 43 37 31 38 32 45 31 35 39 45 42 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 45 31 30 38 43 35 38 41 41 42 39 41 45 36 45 37 34 39 38 44 41 37 42 41 33 36 35 37 43 42 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c Data Ascii: rdf:li>6DDD9ECE64AC043D95AC28B8855AEB01</rdf:li> <rdf:li>6E05459EDB797CAAAA858C07564587A 8</rdf:li> <rdf:li>6E08FA4D245132DF253A902234C5F621</rdf:li> <rdf:li>6E0ACEF6D50BFACAE5EACC712E159EB A</rdf:li> <rdf:li>6E108C58AAB9AE6E7498DA7BA3657CBF</rdf:li> <rdf:li>
2022-04-08 08:02:42 UTC	2287	IN	Data Raw: 41 31 30 33 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 43 30 37 46 43 39 37 32 36 44 43 43 38 39 31 36 32 45 46 33 37 44 35 32 35 39 41 39 31 46 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 43 30 46 43 37 38 33 38 41 30 35 44 42 41 43 41 30 44 34 33 44 39 46 37 45 44 44 33 45 42 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 43 31 31 31 31 34 32 31 38 32 39 43 33 34 30 35 39 34 46 39 34 44 31 35 47 32 34 41 39 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 43 32 31 36 44 46 32 30 33 36 46 30 30 38 38 44 37 45 31 43 43 39 46 39 34 42 44 45 36 31 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 43 32 45 44 36 31 42 44 32 35 31 41 42 36 44 32 39 36 31 36 45 43 34 34 31 43 38 39 37 33 34 Data Ascii: A103E</rdf:li> <rdf:li>7C07FC9726DCC89162EF37D5259A91FB</rdf:li> <rdf:li>7C0FC7838A05DBA CA0D43D9F7EDD3EBB</rdf:li> <rdf:li>7C111421829C340594F91D41E7B4A97</rdf:li> <rdf:li>7C216DF2036F008 8D7E1CC9F94BDE610</rdf:li> <rdf:li>7C2ED61BD251AB6D29616EC441C89734
2022-04-08 08:02:42 UTC	2303	IN	Data Raw: 34 45 32 46 45 35 38 46 35 41 37 33 43 33 46 42 38 42 44 35 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 38 44 32 35 31 35 39 42 34 46 39 39 45 44 37 36 45 35 36 42 43 31 38 31 42 30 36 33 35 44 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 38 45 39 32 46 38 37 41 37 41 30 45 46 41 33 41 36 30 34 39 44 43 44 34 43 45 42 31 39 39 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 38 46 30 32 38 41 45 30 30 43 35 41 37 3 9 44 38 32 46 31 34 42 41 37 44 33 44 44 34 32 38 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 38 46 32 31 35 36 34 45 46 38 35 37 36 34 44 38 43 32 37 32 38 41 41 30 31 41 46 30 42 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 38 46 33 39 38 43 32 41 32 39 32 39 37 42 36 Data Ascii: 4E2FE58F5A73C3FB8BD5B</rdf:li> <rdf:li>88D25159B4F99ED76E56BC181B0635DA</rdf:li> <rdf:li>88E92F87A7A0EFA3A6049DCD4CEB1992</rdf:li> <rdf:li>88F028AE00C5A79D82F14BA7D3DD4283</rdf:li> <rdf:li>88F221564EF85764D8C2728AA01AF0BC</rdf:li> <rdf:li>88F398C2A29297B6
2022-04-08 08:02:42 UTC	2311	IN	Data Raw: 41 33 37 33 45 39 38 30 46 43 35 42 31 46 41 31 36 43 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 46 39 35 42 39 43 42 33 41 30 34 31 37 34 34 41 44 38 38 39 46 33 38 41 39 39 35 43 42 34 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 46 41 32 32 32 37 34 41 35 36 36 30 39 43 33 45 35 46 32 43 38 32 42 46 32 45 43 30 39 42 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 46 41 32 42 37 38 36 35 38 37 45 38 32 31 46 30 3 8 41 30 43 38 43 42 30 36 46 44 36 34 44 39 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 46 42 43 42 44 31 39 46 43 41 34 44 33 31 37 38 37 39 32 34 44 36 45 33 43 39 35 35 38 38 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 46 44 33 38 31 35 46 42 42 33 33 45 35 45 38 44 77 Data Ascii: A373E980FC5B1FA16C4</rdf:li> <rdf:li>8F95B9CB3A04174AD889F38A995CB45</rdf:li> <rdf:li>8 FA22274A56609C3E5F2C82BF2EC09B8</rdf:li> <rdf:li>8FAB786587E821F08A0C8CB06FD64D9F</rdf:li> <rdf:li>8 FBCBD19FCA4D31787924D6E3C955886</rdf:li> <rdf:li>8FDC815FBB33E5E8D7
2022-04-08 08:02:42 UTC	2327	IN	Data Raw: 45 30 36 37 41 42 34 30 31 41 36 33 39 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 44 41 32 39 30 42 41 32 35 34 31 39 42 38 39 37 33 34 39 37 30 41 39 41 44 34 45 45 34 34 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 44 42 31 46 41 37 34 33 33 34 38 46 34 44 33 43 34 31 45 41 46 35 36 37 41 30 35 46 31 30 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 44 42 36 44 37 38 34 45 34 32 30 34 44 44 42 38 39 34 43 43 3 1 32 45 43 38 46 46 46 42 37 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 44 42 45 30 38 34 37 44 32 44 38 37 44 44 32 34 44 41 33 32 42 33 31 31 34 41 33 41 30 35 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 44 42 45 42 31 36 42 41 33 38 39 32 39 41 44 31 41 45 45 35 45 33 Data Ascii: E067AB401A639C</rdf:li> <rdf:li>9DA290BA25419B89734970A9AD4EE44D</rdf:li> <rdf:li>9DB1FA 743348F4D3C41EAF567A05F10E</rdf:li> <rdf:li>9DB6D784E4204DD8894CC12EC8FFB74</rdf:li> <rdf:li>9DBE08 47D2D87DD24DA32B3114A3A059</rdf:li> <rdf:li>9DBEB16BA38929AD1AE5E53
2022-04-08 08:02:42 UTC	2343	IN	Data Raw: 46 30 31 46 34 41 32 39 38 46 34 41 31 36 34 38 42 41 45 30 30 38 33 33 42 31 46 31 38 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 42 30 35 36 44 41 46 35 30 45 33 31 38 35 31 34 46 32 30 38 35 42 36 37 42 36 38 33 39 30 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 42 34 39 30 45 33 43 44 42 36 36 38 43 39 4 3 44 35 35 32 33 42 43 32 35 32 43 38 37 31 32 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 42 35 42 30 32 45 34 32 44 41 32 46 33 42 33 41 46 46 37 44 32 43 43 36 31 44 36 43 44 41 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 42 35 43 32 35 39 43 39 37 33 31 38 45 42 31 30 37 42 36 33 38 41 31 45 31 42 32 30 46 43 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 42 37 30 32 31 36 Data Ascii: F01FA4298F4A1648BAE0083B1F182</rdf:li> <rdf:li>AB056DAF50E318514F2085B67B683903</rdf:li> <rdf:li>AB490E3CD2668C9CD5523BC252C8712C</rdf:li> <rdf:li>AB5B0E242DA2F3B3AFF7D2CC61D6CDA4</rdf:li> <rdf:li>AB5C259C97318EB107B638A1E1B20FCE</rdf:li> <rdf:li>AB70216

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	2351	IN	Data Raw: 38 46 31 39 42 42 36 31 37 39 42 37 44 38 35 45 36 35 43 39 37 38 43 32 39 45 30 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 31 44 33 44 30 45 33 34 32 43 34 35 33 41 35 45 43 39 34 37 45 43 32 37 44 38 37 42 41 37 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 31 44 41 46 38 44 33 37 37 36 41 43 30 32 37 44 39 43 32 33 42 37 41 33 41 44 32 45 31 39 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 31 45 32 30 45 41 3 9 35 44 34 42 36 30 41 33 33 36 30 43 31 37 46 44 43 34 41 43 30 37 43 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 31 45 37 33 36 42 38 45 39 43 34 41 33 34 43 33 35 32 41 39 34 46 46 35 46 43 31 37 32 32 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 31 45 38 34 42 34 32 31 Data Ascii: 8F19B8B6179B7D85E65C978C29E09</rdf:li> <rdf:li>B1D3D0E342C453A5EC947EC27D87BA7B</rdf:li> <rdf:li>B1DAF8D3776AC027D9C23B7A3AD2E193</rdf:li> <rdf:li>B1E20EA95D4B60A3360C17FDC4AC07C1</rdf:li> <rdf:li>B1E736B8E9C4A34C352A94FF5FC17226</rdf:li> <rdf:li>B1E84B421
2022-04-08 08:02:42 UTC	2358	IN	Data Raw: 69 3e 42 38 36 42 44 45 34 37 35 35 34 36 42 31 36 34 35 41 43 37 43 45 31 36 32 39 44 36 34 35 31 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 38 37 34 31 32 42 35 37 32 38 33 43 32 32 46 43 41 44 41 32 44 36 36 46 32 43 31 42 45 38 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 38 37 33 35 37 38 34 46 33 39 31 36 33 30 31 45 42 41 30 30 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 3 8 38 32 31 45 42 35 42 35 41 30 45 38 34 44 43 38 35 33 45 42 44 33 33 35 46 39 39 44 44 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 38 38 43 30 33 33 46 38 35 36 41 34 39 45 34 30 36 32 30 37 35 42 38 30 46 41 32 37 46 44 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 38 39 Data Ascii: i>B86BDE475546B1645AC7CE1629D64516</rdf:li> <rdf:li>B87412B57283C22FCADA2D66F2C1BE82</rdf:li> <rdf:li>B87C64C1D4CC735784F3916301EBA00F</rdf:li> <rdf:li>B8821EB5B5A0E84DC853EBD335F99DD0</rdf:li> <rdf:li>B88C033F856A49E4062075B80FA27FD1</rdf:li> <rdf:li>B89
2022-04-08 08:02:42 UTC	2374	IN	Data Raw: 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 36 35 30 43 37 37 35 30 34 31 42 36 45 34 43 46 44 45 42 34 37 31 37 46 44 33 41 30 42 38 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 36 35 31 41 30 43 41 38 31 32 44 32 30 46 45 44 41 31 42 38 45 30 38 37 38 42 44 34 46 31 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 36 36 41 45 43 34 39 31 45 32 46 34 34 41 30 32 37 32 32 45 42 39 44 43 35 46 45 37 36 38 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 36 37 46 32 44 39 35 45 42 34 42 42 37 41 45 35 32 42 46 35 37 38 42 38 45 46 36 30 38 35 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 36 42 31 43 32 31 37 34 45 31 42 30 43 41 45 39 36 46 31 36 31 33 33 46 46 44 44 33 39 31 38 3c 2f 72 64 66 Data Ascii: </rdf:li> <rdf:li>C650C775041B6E4CFDEB4717FD3A0B81</rdf:li> <rdf:li>C651A0CA812D20FEDA1B8E0878BD4F11</rdf:li> <rdf:li>C66AEC491E2F44A02722EB9DC5FE7688</rdf:li> <rdf:li>C67F2D95EB4BB7AE52BF578B8EF60858</rdf:li> <rdf:li>C6B1C2174E1B0CAE96F16133FFDD3918</rdf:li>
2022-04-08 08:02:42 UTC	2649	IN	Data Raw: 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 33 37 32 45 39 34 42 32 33 30 34 33 42 42 36 37 41 37 34 38 37 42 36 38 31 34 43 46 45 34 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 33 37 36 30 35 41 41 30 33 41 34 31 39 43 31 45 46 36 33 45 44 35 32 46 43 32 37 42 45 31 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 4 4 33 37 38 39 32 37 41 37 43 43 30 33 46 38 41 32 36 31 45 35 43 31 32 31 38 30 38 31 32 32 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 33 38 35 41 31 46 36 34 44 46 32 34 43 44 37 31 37 35 31 38 46 42 32 42 38 32 39 41 43 30 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 33 41 30 43 37 41 41 34 36 32 39 36 30 30 38 35 45 36 37 33 35 42 41 34 45 45 33 30 43 35 39 3c 2f 72 64 66 3a 6c 69 3e 20 Data Ascii: :li> <rdf:li>D372E94B23043BB67A7487B6814CFE4C</rdf:li> <rdf:li>D37605AA03A419C1EF63ED52FC27BE15</rdf:li> <rdf:li>D378927A7CC03F8A261E5C121808122A</rdf:li> <rdf:li>D385A1F64DF24CD717518FB2B829AC00</rdf:li> <rdf:li>D3A0C7AA462960085E6735BA4EE30C59</rdf:li>
2022-04-08 08:02:42 UTC	2657	IN	Data Raw: 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 39 46 43 33 35 37 30 43 37 36 42 38 33 37 45 32 42 46 41 35 31 41 32 43 38 35 32 35 30 32 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 41 30 35 31 34 45 38 30 33 35 46 39 39 43 41 36 32 39 45 32 33 43 44 41 44 43 33 44 39 35 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 41 3 0 35 43 39 36 41 34 33 44 39 38 35 43 33 42 31 41 30 31 46 44 34 35 39 42 36 38 31 39 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 41 30 41 41 44 46 39 45 31 31 32 38 30 42 34 34 39 32 41 45 45 33 44 31 43 45 33 42 37 37 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 41 30 43 41 37 41 44 44 41 41 45 44 39 34 33 44 45 46 37 38 35 31 34 44 45 45 36 44 44 34 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 Data Ascii: i> <rdf:li>D9FC3570C76B837E2BFA51A2C8525024</rdf:li> <rdf:li>DA0514E8035F99CA629E23CDADC3D957</rdf:li> <rdf:li>DA05C96AA43D985C3B1A01FD459B68191</rdf:li> <rdf:li>DA0AADF9E11280B4492AEE3D1CE3B773</rdf:li> <rdf:li>DA0CA7ADDDAED943DEF78514DEE6DD4D</rdf:li> <r
2022-04-08 08:02:42 UTC	2673	IN	Data Raw: 31 35 36 32 35 31 39 30 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 37 38 42 33 33 35 37 42 41 34 46 43 35 43 45 38 35 38 43 35 42 45 39 34 31 38 45 31 31 42 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 37 39 31 45 32 46 39 36 37 43 35 45 41 33 39 37 33 32 39 45 43 35 46 31 44 33 44 33 43 35 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 31 38 30 44 45 31 38 30 44 45 31 38 30 44 45 46 46 35 43 31 39 30 31 45 31 35 32 44 43 35 41 44 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 37 39 35 38 45 39 36 44 33 41 41 43 32 41 34 45 44 45 30 30 32 43 37 30 38 34 30 42 33 31 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 37 41 35 33 30 36 31 38 46 35 33 46 46 39 38 45 44 33 43 32 38 41 45 31 32 31 46 Data Ascii: 15625190F</rdf:li> <rdf:li>E78B3357BA4FC5CE858C5BE9418E11B5</rdf:li> <rdf:li>E791E2F967C5EA397329EC5F1D3D3E36</rdf:li> <rdf:li>E793A4A80DE18BFF5C1901E152DC5AD7</rdf:li> <rdf:li>E7958E96D3AAC2A4EDE002C70840B316</rdf:li> <rdf:li>E7A530618F53FF98ED3C28AE121F
2022-04-08 08:02:42 UTC	2689	IN	Data Raw: 30 41 30 41 32 33 34 44 36 30 35 44 31 36 32 41 42 41 46 30 33 46 38 39 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 32 45 45 33 33 43 32 35 36 43 33 35 46 46 43 37 34 42 43 33 35 39 42 45 30 36 38 33 42 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 33 30 33 34 42 46 30 38 37 33 45 45 42 43 44 41 37 44 41 33 42 42 32 44 34 41 43 34 37 35 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 33 30 37 42 35 34 32 46 42 3 6 30 30 46 34 36 30 39 38 42 30 38 44 46 43 35 41 35 30 30 41 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 33 31 39 35 33 32 32 35 32 35 33 41 46 43 32 30 44 46 36 43 31 46 31 42 31 30 37 44 33 32 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 33 31 42 34 38 44 37 41 33 38 34 Data Ascii: 0A0A234D605D162ABAF03F89F</rdf:li> <rdf:li>F2EE333C256C35FFC74BC359BE0683B6</rdf:li> <rdf:li>F3034BF0873EEBCDA7DA3BB2D4AC4759</rdf:li> <rdf:li>F307B542FB600FA4609808DFC5A500A8</rdf:li> <rdf:li>F31953225253AFC20DF6C1F1B107D326</rdf:li> <rdf:li>F31B48D7A384
2022-04-08 08:02:42 UTC	2696	IN	Data Raw: 33 42 37 45 33 33 38 44 42 38 30 45 46 34 30 34 44 35 42 39 39 31 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 39 36 39 33 46 38 44 32 43 35 35 37 44 33 41 44 37 42 41 33 30 39 34 37 43 33 34 39 34 42 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 39 37 45 42 33 38 46 36 35 36 36 45 36 31 35 37 43 45 36 35 36 43 31 42 30 46 33 41 38 46 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 39 38 31 30 42 35 33 36 43 32 45 3 4 41 41 44 30 39 41 42 41 45 37 44 44 35 31 36 44 39 31 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 39 38 42 32 34 42 45 36 39 31 32 38 34 41 30 31 39 30 42 46 33 36 39 45 45 31 42 36 39 30 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 39 35 40 42 33 32 30 34 31 37 44 32 Data Ascii: 3B7E338DB80EF404D5B8915</rdf:li> <rdf:li>F9693F8D2C557D3AD7BA30947C3494BD</rdf:li> <rdf:li>F97EB38F6566E6157CE656C1B0F3A8F6</rdf:li> <rdf:li>F9810B536C2E4AAD09ABAE7DD516D91A</rdf:li> <rdf:li>F98B24BE691284A0190BF369EE1B690F</rdf:li> <rdf:li>F99E0B320417D2

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	2712	IN	Data Raw: 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 31 62 36 38 31 63 61 38 2d 65 66 30 37 2d 31 31 37 38 2d 39 31 37 33 2d 66 63 65 35 31 62 62 36 32 39 35 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 31 62 62 32 61 38 37 36 2d 30 64 63 30 2d 31 31 65 37 2d 61 36 65 64 2d 66 64 3a 66 37 63 37 62 35 34 35 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 31 62 65 30 37 66 65 39 2d 3a 64 66 65 2d 31 31 64 64 2d 38 61 33 63 2d 64 37 36 63 30 65 33 66 33 31 32 66 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 6 4 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 31 63 64 31 38 35 Data Ascii: dobe:docid:photoshop:1b681ca8-ef07-1178-9173-fce51bb62952</rdf:li> <rdf:li>adobe:docid:photoshop:1bb2a876-0dc0-11e7-a6ed-fd4f7c7b5452</rdf:li> <rdf:li>adobe:docid:photoshop:1be07fe9-44fe-11dd-8a3c-d76c0e3f312f</rdf:li> <rdf:li>adobe:docid:photoshop:1cd185
2022-04-08 08:02:42 UTC	2728	IN	Data Raw: 2d 39 64 34 39 30 61 61 39 34 37 66 63 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 34 62 33 65 63 67 61 37 2d 33 38 63 65 2d 31 31 65 36 2d 39 35 33 36 2d 63 65 65 36 38 66 31 63 65 36 32 62 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 34 62 39 35 38 35 64 61 2d 34 31 30 33 2d 31 31 65 37 2d 62 32 63 31 2d 61 64 36 61 35 37 66 63 38 66 30 62 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 34 62 62 63 36 2d 33 63 63 30 2d 31 31 65 36 2d 61 31 39 37 2d 63 37 34 37 65 38 65 63 63 35 66 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 Data Ascii: -9d490aa947fc</rdf:li> <rdf:li>adobe:docid:photoshop:4b3ec7a7-38ce-11e6-9536-cee68f1ce62b</rdf:li> <rdf:li>adobe:docid:photoshop:4b9585da-4103-11e7-b2c1-ad6a57fc8f0b</rdf:li> <rdf:li>adobe:docid:photoshop:4bb c62c6-3cc0-11e6-a197-c747e8ecc5f2</rdf:li> <rdf
2022-04-08 08:02:42 UTC	2736	IN	Data Raw: 73 68 6f 70 3a 36 34 34 31 64 65 35 30 2d 30 32 34 65 2d 31 31 64 39 2d 61 62 33 32 2d 66 32 33 37 30 64 31 38 35 36 63 64 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 36 34 35 30 34 39 39 36 2d 35 61 65 35 2d 31 31 64 65 2d 39 34 32 30 2d 38 62 39 39 30 38 63 35 35 65 62 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 36 34 38 36 66 64 33 31 2d 39 62 38 35 2d 31 31 65 36 2d 61 39 66 66 2d 38 64 36 36 35 65 64 37 65 61 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 3 6 34 63 35 61 37 31 36 2d 66 63 37 37 2d 64 39 34 65 2d 62 35 35 Data Ascii: shop:6441de50-024e-11d9-ab32-f2370d1856cd</rdf:li> <rdf:li>adobe:docid:photoshop:64504996-5ae5-11de-9420-8b9908c55eb1</rdf:li> <rdf:li>adobe:docid:photoshop:6486fd31-9b85-11e6-a9ff-8d6656ed7ea9</rdf:li> <rdf:li>adobe:docid:photoshop:64c5a716-fc77-d94e-b55
2022-04-08 08:02:42 UTC	2744	IN	Data Raw: 32 2d 62 35 30 39 2d 31 31 64 64 2d 38 32 32 36 2d 64 61 39 34 39 34 38 37 36 37 33 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 37 39 38 64 63 65 33 33 2d 66 63 34 35 2d 31 31 65 36 2d 62 66 62 30 2d 38 64 61 32 39 32 34 62 66 33 62 62 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 37 39 39 63 62 32 30 30 37 37 2d 61 37 30 61 2d 64 36 34 30 2d 62 62 38 63 2d 30 34 35 34 63 62 65 65 37 63 66 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 37 39 64 30 61 66 34 32 2d 61 65 39 35 2d 31 31 64 61 2d 62 61 62 63 2d 39 63 30 64 65 64 32 61 34 36 Data Ascii: 2-b509-11dd-8226-da9494876732</rdf:li> <rdf:li>adobe:docid:photoshop:798dce33-fc45-11e6-bfb0-8da29 24bf3bb</rdf:li> <rdf:li>adobe:docid:photoshop:79cb2007-a70a-d640-bb8c-0454cbee7cf9</rdf:li> <rdf:li>adobe:doc id:photoshop:79d0af42-ae95-11da-babc-9c0ded2a46
2022-04-08 08:02:42 UTC	2760	IN	Data Raw: 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 61 64 34 62 32 65 33 66 2d 39 31 31 65 2d 31 31 65 36 2d 38 63 33 62 2d 38 66 35 30 35 34 62 65 39 35 64 64 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 61 64 65 32 34 32 36 37 2d 38 35 39 64 2d 31 31 64 38 2d 62 31 38 36 2d 62 34 65 38 30 31 34 32 63 36 64 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 61 64 65 36 34 66 66 35 2d 32 61 62 33 2d 31 31 65 37 2d 62 66 34 66 2d 61 32 33 65 38 33 39 35 38 64 65 65 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 61 65 Data Ascii: li>adobe:docid:photoshop:ad4b2e3f-911e-11e6-8c3b-8f5054be95dd</rdf:li> <rdf:li>adobe:docid:photoshop:ade24267-859d-11d8-b186-b4e80142c6d8</rdf:li> <rdf:li>adobe:docid:photoshop:ade64ff5-2ab3-11e7-bf4f-a23e839 58dee</rdf:li> <rdf:li>adobe:docid:photoshop:ae
2022-04-08 08:02:42 UTC	2776	IN	Data Raw: 64 63 2d 39 32 65 64 2d 38 39 32 35 65 61 61 30 63 65 39 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 65 34 63 38 37 30 37 62 2d 62 36 30 61 2d 31 31 64 38 2d 39 63 62 38 2d 63 66 31 32 38 38 35 30 32 64 62 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 65 34 65 36 38 31 39 38 2d 31 31 65 35 2d 62 32 30 61 2d 65 33 35 31 39 34 38 65 35 66 62 62 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 65 35 30 61 39 64 62 39 2d 66 34 39 39 2d 37 32 34 37 2d 62 34 64 65 2d 32 31 32 33 37 33 30 39 39 36 31 3c 2f 72 64 66 3a 6c Data Ascii: dc-92ed-8925eaa0ce95</rdf:li> <rdf:li>adobe:docid:photoshop:e4c8707b-b60a-11d8-9cb8-cf1288502db2</rdf:li> <rdf:li>adobe:docid:photoshop:e4e68198-4e26-11e5-b20a-e351948e5fbb</rdf:li> <rdf:li>adobe:docid:photoshop:e50a9db9-f499-7247-b4de-212373078961</rdf:li>
2022-04-08 08:02:42 UTC	2784	IN	Data Raw: 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 66 63 61 39 62 65 31 63 2d 63 32 66 39 2d 31 31 65 36 2d 62 30 38 65 2d 39 63 61 38 64 30 38 30 34 61 66 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 66 64 31 33 66 34 39 33 2d 39 66 62 64 2d 31 31 64 61 2d 62 30 62 34 2d 38 34 66 38 31 62 33 62 39 32 61 61 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 66 64 37 30 31 32 34 34 2d 32 36 64 63 2d 31 31 64 39 2d 62 33 61 39 2d 64 62 32 66 38 65 38 33 35 64 37 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 66 64 37 36 30 38 33 64 2d 66 63 36 61 2d 31 Data Ascii: d:photoshop:fca9be1c-c2f9-11e6-b08e-9ca8d0804af8</rdf:li> <rdf:li>adobe:docid:photoshop:fd13f493-9fbd-11da-b0b4-84f81b3b92aa</rdf:li> <rdf:li>adobe:docid:photoshop:fd701244-26dc-11d9-b3a9-db2f8e835d77</rdf:li> <rdf:li>adobe:docid:photoshop:fd76083d-fc6a-1
2022-04-08 08:02:42 UTC	2800	IN	Data Raw: 64 3a 33 33 46 37 33 39 46 45 32 37 39 33 44 45 31 31 39 37 42 34 41 33 30 44 39 46 43 42 42 35 44 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 33 34 33 31 46 34 33 34 35 35 36 34 45 30 31 31 41 32 31 33 45 34 30 42 37 45 34 36 41 38 31 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 33 34 33 38 33 43 31 39 43 39 31 45 44 45 31 31 38 45 32 33 45 35 43 46 35 45 32 46 35 34 42 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 33 34 35 31 62 39 30 37 2d 39 30 61 63 2d 33 62 34 34 2d 62 35 66 33 2d 36 66 33 64 39 61 34 63 34 34 66 63 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 33 34 36 30 30 42 36 32 31 41 43 31 44 46 31 31 38 32 33 42 43 38 30 41 38 34 39 43 35 Data Ascii: d:33F739FE2793DE1197B4A30D9FCBB5DD</rdf:li> <rdf:li>uid:3431F4345564E011A213E40B7E46A81 7</rdf:li> <rdf:li>uid:34383C19C91EDE118E23E5CF5E2F54B5</rdf:li> <rdf:li>uid:3451b907-90ac-3b44-b5f3-6f3d9a4 c44fc</rdf:li> <rdf:li>uid:34600B621AC1DF11823BC80A849C5

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	2816	IN	Data Raw: 32 36 42 34 33 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 36 38 31 30 31 39 39 38 38 46 31 42 31 31 44 41 41 37 34 31 42 34 41 41 30 31 31 41 43 35 39 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 36 38 31 30 31 39 39 41 38 46 31 42 31 31 44 41 41 37 34 31 42 34 41 41 30 31 31 41 43 35 39 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 36 38 44 35 31 44 30 36 38 37 39 38 31 31 4 4 43 41 46 43 37 43 42 46 35 32 34 37 37 33 39 35 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 36 38 45 43 41 30 42 37 42 39 38 35 44 46 31 31 38 32 46 39 38 44 33 39 42 39 39 38 46 34 34 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 36 38 46 44 30 34 Data Ascii: 26B430</rdf:li> <rdf:li>uuid:681019988F1B11DAA741B4AA011AC59A</rdf:li> <rdf:li>uuid:6810199A8F1B11DAA741B4AA011AC59A</rdf:li> <rdf:li>uuid:68D51D06879811DCAFC7CBF524773955</rdf:li> <rdf:li>uuid:68EC A0B7B985DF1182F98D39B998F44E</rdf:li> <rdf:li>uuid:68FD04
2022-04-08 08:02:44 UTC	5416	IN	Data Raw: 75 75 69 64 3a 38 30 45 43 41 30 45 30 46 41 33 34 45 30 31 31 38 36 30 45 38 38 41 41 39 46 42 39 36 37 33 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 38 31 34 35 43 34 43 33 35 42 34 42 45 30 31 31 38 35 42 37 45 44 44 35 46 46 43 30 42 31 39 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 38 31 35 30 42 35 32 44 36 36 39 43 44 44 31 31 41 32 36 30 43 44 36 35 43 42 39 30 30 39 35 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 38 31 38 43 34 43 36 36 35 34 34 42 44 46 31 31 41 41 30 37 46 37 41 32 46 34 39 45 35 32 42 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 38 32 30 44 37 32 38 36 37 37 44 43 44 44 31 31 42 37 39 33 41 34 45 31 46 30 39 42 43 44 Data Ascii: uuid:80ECA0E0FA34E011860E88AA9FB9673B</rdf:li> <rdf:li>uuid:8145C4C35B4BE01185B7EDD5FFC0 B198</rdf:li> <rdf:li>uuid:8150B52D669CDD11A260CD65CB90095E</rdf:li> <rdf:li>uuid:818C4C66544BDF11AA 077A2F49E52BE</rdf:li> <rdf:li>uuid:820D728677DCDD11B793A4E1F09BCD
2022-04-08 08:02:44 UTC	5432	IN	Data Raw: 45 35 30 35 34 32 45 35 31 31 39 37 43 43 39 44 32 36 39 34 31 46 39 41 38 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 42 34 35 32 36 38 45 43 44 33 43 42 45 30 31 31 42 33 46 45 44 32 34 38 33 31 38 34 38 46 35 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 42 34 36 45 37 33 45 31 45 46 31 42 45 30 31 31 38 45 30 35 39 46 31 34 41 31 41 45 38 33 39 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 42 34 37 30 32 38 36 42 34 32 33 31 45 31 31 31 38 44 42 46 35 46 38 42 30 41 31 39 37 31 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 42 34 38 43 43 33 37 34 46 36 45 32 44 43 31 31 39 33 44 36 45 35 39 33 46 37 30 34 45 46 39 34 3c 2f 72 64 66 3a 6c 69 3e Data Ascii: E50542E51197CC9D26941F9A8B</rdf:li> <rdf:li>uuid:B45268ECD3CBE011B3FED24831848F59</rdf:li> <rdf:li>uuid:B46E73E1EF1BE0118E059F14A1AE839B</rdf:li> <rdf:li>uuid:B470286B4231E1118DBBF5E8B0A19 711</rdf:li> <rdf:li>uuid:B48CC374F6E2DC1193D6E593F704EF94</rdf:li>
2022-04-08 08:02:44 UTC	5448	IN	Data Raw: 75 75 69 64 3a 46 32 44 32 41 30 44 44 32 32 43 43 45 30 31 31 42 33 46 45 44 32 34 38 33 31 38 34 38 46 35 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 46 32 44 41 45 34 41 32 41 34 30 45 45 34 31 31 39 38 39 33 38 35 39 35 33 39 37 37 43 39 36 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 46 33 31 41 37 30 42 45 43 37 36 35 44 43 31 31 41 34 30 31 43 40 31 43 42 38 34 31 37 43 42 38 34 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 46 33 33 42 43 33 39 37 42 46 44 30 31 31 44 41 41 33 36 42 46 44 41 31 35 43 42 45 30 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 46 33 35 38 45 42 37 34 32 39 36 43 31 31 44 44 38 39 45 34 39 35 33 42 39 31 45 36 33 34 Data Ascii: uuid:F2D2A0DD22CCE011B3FED24831848F59</rdf:li> <rdf:li>uuid:F2DAE4A2A40EE411989385953977 C96F</rdf:li> <rdf:li>uuid:F31A70BEC765DC11A401C0AC04A7CB84</rdf:li> <rdf:li>uuid:F33BC397BFD011DAA3 6BFDAAC15CBE0D</rdf:li> <rdf:li>uuid:F358EB74296C11DD89E4953B91E634
2022-04-08 08:02:44 UTC	5456	IN	Data Raw: 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 31 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 38 43 36 42 38 33 32 38 46 36 43 30 39 31 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 31 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 38 43 36 43 36 39 36 36 46 46 44 45 32 30 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 31 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 38 43 36 44 30 45 35 45 38 39 44 41 46 46 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 Data Ascii: rdf:li> <rdf:li>xmp.did:018011740720681188C6B8328F6C0912</rdf:li> <rdf:li>xmp.did:0180117407206811 88C6C05E0AC1CB3B</rdf:li> <rdf:li>xmp.did:018011740720681188C6C966FFDE204</rdf:li> <rdf:li>xmp.did: 018011740720681188C6D0E5E89DAFF9</rdf:li> <rdf:li>xmp.did
2022-04-08 08:02:44 UTC	5464	IN	Data Raw: 64 69 64 3a 30 32 31 38 38 36 31 34 45 30 36 42 31 31 45 30 41 37 34 35 45 36 36 34 34 39 43 42 30 39 42 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 32 31 45 34 41 43 41 30 38 32 30 36 38 31 31 38 32 32 41 46 31 44 41 44 36 44 46 33 45 33 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6 d 70 2e 64 69 64 3a 30 32 31 64 33 34 62 63 2d 31 37 30 33 2d 34 31 61 33 2d 62 38 36 63 2d 39 32 64 61 35 31 32 38 36 33 62 62 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 32 35 32 65 39 63 35 2d 33 36 62 65 2d 34 36 34 36 2d 39 36 31 37 2d 63 34 35 33 30 38 64 62 64 35 39 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 32 35 33 31 37 38 36 32 44 32 Data Ascii: did:02188614E06B11E0A745E66449CB09B8</rdf:li> <rdf:li>xmp.did:021E4ACA08206811822AF1DAD6 DF3E30</rdf:li> <rdf:li>xmp.did:021d34bc-1703-44a3-b86c-92da512863bb</rdf:li> <rdf:li>xmp.did:0252e9c5-36be-4646- 9617-c45308dbd592</rdf:li> <rdf:li>xmp.did:025317862D2
2022-04-08 08:02:44 UTC	5480	IN	Data Raw: 46 35 44 35 33 37 45 31 31 31 38 30 32 43 46 33 31 38 42 36 34 39 35 39 31 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 36 36 35 34 30 65 30 2d 64 37 36 35 2d 34 31 39 62 2d 39 32 64 38 2d 37 33 63 34 39 38 61 32 36 66 38 64 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 36 36 41 42 30 37 44 30 41 32 30 36 38 31 31 39 31 30 39 43 45 37 42 34 46 41 31 41 46 31 32 3c 2f 72 64 66 3a 6c 6 9 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 36 36 41 43 45 44 35 36 45 46 39 45 31 31 41 30 43 34 42 46 45 32 30 41 37 41 33 42 36 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 36 37 41 41 41 42 39 30 34 32 33 36 38 31 31 38 32 39 31 44 31 43 45 45 Data Ascii: F5D537E111802CF318B6495919</rdf:li> <rdf:li>xmp.did:066540e0-d765-419b-92d8-73c498a26f8d</rdf:li> <rdf:li>xmp.did:066AB07D0A2068119109CE7B4FA1AF12</rdf:li> <rdf:li>xmp.did:066ACED56FE9E111A0C4BEF20A 7A3B6B</rdf:li> <rdf:li>xmp.did:067AAAB9042368118291D1CEE
2022-04-08 08:02:44 UTC	5496	IN	Data Raw: 2e 64 69 64 3a 30 45 33 43 32 36 31 39 36 30 43 37 45 31 31 31 42 36 45 43 41 36 39 30 41 41 43 37 45 45 36 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 45 37 46 36 42 44 46 35 36 37 32 45 31 31 31 38 38 44 35 44 30 44 37 46 30 34 42 32 30 36 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 7 8 6d 70 2e 64 69 64 3a 30 45 38 42 39 45 42 44 42 43 32 30 36 38 31 31 41 46 46 44 42 32 46 36 42 33 46 45 32 46 44 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 45 39 35 39 31 45 46 33 35 43 38 45 30 31 31 41 42 41 38 37 34 46 31 37 46 31 45 37 42 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 45 41 42 41 30 44 30 39 32 30 36 38 31 31 38 46 Data Ascii: .did:0E3C261960C7E111B6ECA690AAC7EE61</rdf:li> <rdf:li>xmp.did:0E7F6BDF5672E11188D5D0D7F 04B2064</rdf:li> <rdf:li>xmp.did:0E8B9EBDBC206811AFFDB2F6B3FE2FD6</rdf:li> <rdf:li>xmp.did:0E9591EF3 5C8E011AABA874F17F1E7BB</rdf:li> <rdf:li>xmp.did:0EABA00D092068118F

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:44 UTC	5504	IN	Data Raw: 35 35 41 41 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 35 34 30 46 46 43 33 37 30 35 45 31 31 45 30 38 46 30 31 44 46 42 32 30 46 35 44 37 42 46 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 35 34 43 42 38 39 45 43 30 32 30 36 38 31 31 38 38 43 36 39 36 45 44 46 38 38 43 39 45 36 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 35 35 41 36 33 3 1 39 30 41 32 30 36 38 31 31 38 46 36 32 45 31 39 30 32 36 33 31 31 35 46 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 35 35 63 64 37 38 33 2d 65 38 65 34 2d 62 63 34 64 2d 62 65 37 64 2d 38 64 38 33 61 36 33 62 35 37 63 65 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 Data Ascii: 55AA0</rdf:li> <rdf:li>xmp.did:1540FFC3705E11E08F01DFB20F5D7BF9</rdf:li> <rdf:li>xmp.did:154CB89EC020681188C696EDF88C9E6F</rdf:li> <rdf:li>xmp.did:155A63190A2068118F62E190263115F9</rdf:li> <rdf:li>xmp.did:155cd783-e8e4-bc4d-be7d-8d83a63b57ce</rdf:li> <rdf
2022-04-08 08:02:44 UTC	5520	IN	Data Raw: 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 35 32 37 39 66 37 61 2d 35 37 34 65 2d 62 35 34 33 2d 38 33 39 33 2d 30 32 66 66 64 64 36 62 35 66 37 61 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 35 33 38 36 41 38 45 34 39 32 30 36 38 31 31 39 31 30 39 42 45 32 32 31 43 34 33 46 37 33 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 35 34 34 35 44 4 3 42 39 35 45 38 44 46 31 31 42 34 30 34 43 37 30 32 44 45 32 33 42 41 37 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 35 36 37 39 30 41 33 42 36 37 44 45 33 31 31 38 34 34 32 38 33 32 45 42 37 32 38 32 46 33 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e Data Ascii: 9</rdf:li> <rdf:li>xmp.did:25279f7a-574e-b543-8393-02fdd6b5f7a</rdf:li> <rdf:li>xmp.did:25386A8E492068119109BE221C43F738</rdf:li> <rdf:li>xmp.did:25445DCB95E8DF11B404C702DE23BA7A</rdf:li> <rdf:li>xmp.did:256790A3B67DE3118442832EB7282F36</rdf:li> <rdf:li>
2022-04-08 08:02:44 UTC	5536	IN	Data Raw: 2e 64 69 64 3a 33 33 43 35 33 39 35 35 30 41 32 30 36 38 31 31 38 30 38 33 42 46 44 39 41 39 46 38 31 37 33 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 33 43 43 30 31 38 31 33 32 32 36 36 38 31 31 38 43 31 34 46 31 45 38 34 42 43 43 43 39 45 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 7 8 6d 70 2e 64 69 64 3a 33 33 44 46 36 31 46 41 44 34 32 31 36 38 31 31 42 36 43 38 39 31 43 38 45 30 42 37 37 43 39 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 33 46 34 42 36 41 34 42 36 44 38 43 45 31 31 31 39 36 42 38 43 42 34 42 46 35 30 45 31 36 43 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 33 46 39 42 38 46 35 33 37 32 36 36 38 31 31 38 32 Data Ascii: .did:33C539550A2068118083BFD9A9F81730</rdf:li> <rdf:li>xmp.did:33CC0181322668118C14F1E84BCC9EA</rdf:li> <rdf:li>xmp.did:33DF61FAD4216811B6C891C8E0B77C98</rdf:li> <rdf:li>xmp.did:33F6A4B6D84CE11196B8CB4BF50E16C8</rdf:li> <rdf:li>xmp.did:33F9B8F53726681182
2022-04-08 08:02:44 UTC	5544	IN	Data Raw: 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 41 34 33 37 43 36 45 41 43 32 30 36 38 31 31 41 42 30 38 45 36 42 36 30 42 43 41 34 45 41 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 41 35 41 37 45 38 35 39 33 39 30 31 31 45 35 39 41 44 38 44 37 45 43 38 36 38 35 33 43 30 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 41 37 33 44 43 42 37 32 46 3 2 30 36 38 31 31 38 30 38 33 42 41 42 41 42 44 32 46 37 30 38 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 41 38 30 45 30 46 45 35 42 32 30 36 38 31 31 38 37 31 46 44 32 45 37 33 30 31 43 44 33 45 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e Data Ascii: 1</rdf:li> <rdf:li>xmp.did:3A437C6EAC206811AB08E6B60BCA4EAA</rdf:li> <rdf:li>xmp.did:3A5A7E85939011E59AD8D7E786853C0B</rdf:li> <rdf:li>xmp.did:3A73DCB72F2068118083BABABD2F7089</rdf:li> <rdf:li>xmp.did:3A80E0FE5B206811871FD2E7301CD3E0</rdf:li> <rdf:li>xmp.
2022-04-08 08:02:44 UTC	5560	IN	Data Raw: 61 64 35 36 64 38 61 35 63 35 36 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 39 36 32 34 35 62 2d 64 30 66 62 2d 34 39 35 64 2d 61 30 63 30 2d 31 35 34 31 62 62 36 39 35 34 36 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 39 37 36 34 31 42 37 45 31 31 38 45 30 31 31 41 35 34 46 42 42 44 30 34 36 31 38 39 31 37 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 39 38 35 33 45 34 33 37 42 32 30 36 38 31 31 38 30 38 33 44 38 36 43 41 31 35 46 41 46 33 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 39 38 35 38 35 39 65 2d 62 64 31 61 2d 34 64 64 34 2d 61 35 66 33 2d 31 36 38 61 61 35 38 62 64 38 37 33 3c 2f 72 Data Ascii: ad56d8a5c569</rdf:li> <rdf:li>xmp.did:4966245b-d0fb-495d-a0c0-1541bb695461</rdf:li> <rdf:li>xmp.di d:497641B7E118E011A54FBB046189173</rdf:li> <rdf:li>xmp.did:49855859</rdf:li> <rdf:li>xmp.did:49855859e-bd1a-4dd4-a5f3-168aa58bd873</r
2022-04-08 08:02:44 UTC	5576	IN	Data Raw: 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 39 37 34 45 37 43 31 37 31 31 39 44 45 31 31 41 32 45 43 43 43 30 36 35 45 41 35 46 38 37 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 39 37 38 36 45 41 36 36 35 37 31 45 30 31 31 39 45 38 34 46 43 37 30 42 34 35 43 34 35 45 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 7 2 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 39 38 33 36 39 61 63 2d 35 39 35 37 2d 34 33 36 38 2d 38 38 33 41 2d 65 33 33 63 62 30 61 35 38 66 64 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 39 38 41 41 36 38 34 38 38 32 30 36 38 31 31 38 32 33 46 44 31 34 44 45 32 43 38 43 38 37 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 39 41 37 39 30 43 Data Ascii: :li>xmp.did:5974E7C17119DE11A2ECCC065EA5F877</rdf:li> <rdf:li>xmp.did:59786EA66571E0119E84FC70B45C45EF</rdf:li> <rdf:li>xmp.did:598369ac-5957-4368-8831-e33cb0a58fd5</rdf:li> <rdf:li>xmp.did:598AA68488206811823FD14DE2C8C875</rdf:li> <rdf:li>xmp.did:59A790C
2022-04-08 08:02:44 UTC	5583	IN	Data Raw: 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 30 62 62 66 32 62 65 38 2d 33 63 64 37 2d 34 35 66 33 2d 39 38 62 66 2d 66 64 39 66 63 39 63 35 64 65 33 63 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 30 64 61 38 36 65 62 2d 39 39 33 31 2d 34 33 35 33 2d 62 61 34 63 2d 31 61 31 64 35 33 63 63 32 65 31 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 31 30 30 37 39 44 38 32 39 32 30 36 38 31 31 42 31 41 34 44 35 36 36 30 30 44 39 31 39 43 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 31 30 32 64 30 65 30 2d 63 34 34 65 2d 61 61 39 65 2d 37 64 33 63 64 37 64 35 63 37 65 63 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 Data Ascii: li> <rdf:li>xmp.did:60bf2be8-3cd7-45f3-98bf-fd9fc9c5de3c</rdf:li> <rdf:li>xmp.did:60da86eb-9931-4353-ba4c-1a1d53cc2e16</rdf:li> <rdf:li>xmp.did:610079D829206811B1A4D56600D919C7</rdf:li> <rdf:li>xmp.did:6102d0e0-c44b-a44e-aa9e-7d3cd7d5c7ec</rdf:li> <rdf:li>
2022-04-08 08:02:44 UTC	5591	IN	Data Raw: 37 34 34 32 2d 38 38 37 36 2d 33 30 61 39 33 35 35 63 31 65 39 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 38 36 42 38 32 30 45 33 34 32 33 36 38 31 31 38 32 32 41 44 30 37 43 37 43 43 34 33 38 44 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 38 36 43 46 44 45 31 33 30 32 30 36 38 31 31 39 35 46 45 44 38 42 44 46 38 34 31 43 37 37 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6 c 69 3e 78 6d 70 2e 64 69 64 3a 36 38 38 31 35 34 45 36 31 36 32 30 36 38 31 31 38 30 38 33 44 38 36 43 41 31 35 46 41 46 33 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 38 38 37 43 31 42 30 44 45 32 30 36 38 31 31 39 31 30 39 46 45 39 45 38 32 38 34 31 32 35 30 3c Data Ascii: 7442-8876-30a9355c1e90</rdf:li> <rdf:li>xmp.did:686B820E34236811822AD07C7CC438D7</rdf:li> <rdf:li>xmp.did:686CFDE13020681195FED8BDF841C77D</rdf:li> <rdf:li>xmp.did:688154E6162068118083D86CA15FAF3B</rdf:li> <rdf:li>xmp.did:6887C1B0DE2068119109FE9E82841250<

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:44 UTC	5607	IN	Data Raw: 37 36 65 36 63 34 37 34 2d 32 64 62 33 2d 34 61 34 37 2d 62 35 31 66 2d 35 38 36 32 35 66 63 39 64 34 31 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 37 30 36 43 37 46 41 45 31 32 30 36 38 31 31 41 33 45 46 39 33 37 43 37 31 39 35 30 31 31 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 37 31 39 45 38 35 42 36 37 31 33 45 30 31 31 41 34 30 39 41 35 43 37 35 46 43 44 35 43 41 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 37 31 41 41 45 42 38 39 32 32 32 36 38 31 31 38 32 32 41 39 45 34 31 38 46 34 35 35 43 35 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 37 31 42 34 35 37 36 32 32 32 33 36 38 31 31 41 37 45 Data Ascii: 76e6c474-2db3-4a47-b51f-58625fc9d415</rdf:li> <rdf:li>xmp.did:7706C7FAE1206811A3EF937C719501114</rdf:li> <rdf:li>xmp.did:7719E85B6713E011A409A5C75FCD5CA4</rdf:li> <rdf:li>xmp.did:771AAEB892226811822A9E418F455C5D</rdf:li> <rdf:li>xmp.did:771B457622236811A7E
2022-04-08 08:02:44 UTC	5623	IN	Data Raw: 32 36 38 31 31 38 32 32 41 39 45 34 31 38 46 34 35 35 43 35 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 36 42 46 45 44 46 30 37 36 39 37 45 30 31 31 38 38 42 32 46 31 36 42 44 42 38 42 31 38 45 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 36 44 36 35 46 36 43 30 43 32 30 36 38 31 31 39 32 42 30 42 32 46 41 38 42 37 43 44 46 37 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 36 46 37 46 45 39 39 30 37 32 30 36 38 31 31 39 35 46 45 38 41 37 43 39 38 43 31 33 38 32 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 36 46 38 37 37 42 38 30 37 32 30 36 38 31 31 39 32 42 30 45 39 30 44 30 34 38 45 41 37 32 43 3c 2f Data Ascii: 26811822A9E418F455C5D</rdf:li> <rdf:li>xmp.did:86BFEDF07697E01188B2F16BDB8B18E6</rdf:li> <rdf:li>xmp.did:86D65F6C0C20681192B0B2FA8B7CDF71</rdf:li> <rdf:li>xmp.did:86F7FE990720681195FE8A7C98C1382D</rdf:li> <rdf:li>xmp.did:86F877B80720681192B0E90D048EA72C</
2022-04-08 08:02:44 UTC	5631	IN	Data Raw: 41 32 41 32 42 36 38 31 31 42 31 41 34 44 43 41 45 39 31 41 39 46 37 37 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 45 46 32 38 33 41 45 32 31 32 30 36 38 31 31 38 43 31 34 46 39 35 44 33 43 39 34 44 44 32 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 46 31 35 44 36 36 32 36 41 39 31 31 31 45 30 42 32 36 32 46 31 41 42 34 35 44 46 43 34 33 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 46 32 41 43 43 39 37 32 32 30 36 38 31 31 39 32 40 31 36 41 45 34 39 36 31 38 35 37 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 46 33 45 32 44 43 37 32 44 44 30 45 31 31 31 41 38 44 37 45 36 34 32 45 32 46 46 38 45 Data Ascii: A2A2B6811B1A4DCAE91A9F771</rdf:li> <rdf:li>xmp.did:8EF2831E212068118C14F95D3C94DD26</rdf:li> <rdf:li>xmp.did:8F15D6626A9111E0B262F1AB45DFC43F</rdf:li> <rdf:li>xmp.did:8F2ACC972220681192B0A6AE49618576</rdf:li> <rdf:li>xmp.did:8F3E2DC72DD0E111A8D7E642E2FF8E
2022-04-08 08:02:44 UTC	5647	IN	Data Raw: 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 39 43 34 41 38 43 35 45 43 41 37 39 45 32 31 31 38 32 38 31 46 42 33 31 38 34 32 39 30 42 42 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 39 43 35 31 43 34 39 34 42 33 34 32 45 34 31 31 41 41 41 37 39 45 30 31 32 34 46 38 45 33 30 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 39 43 36 32 32 35 35 41 46 44 37 46 45 35 31 31 39 45 45 44 46 42 32 34 43 43 45 30 37 39 39 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 39 43 37 39 38 38 41 42 33 37 32 30 36 38 31 31 38 32 32 41 45 38 31 44 43 42 38 45 43 44 39 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 39 43 Data Ascii: :li> <rdf:li>xmp.did:9C4A8C5ECA79E2118281FB3184290BB9</rdf:li> <rdf:li>xmp.did:9C51C494B342E411AAA79E0124F8E303</rdf:li> <rdf:li>xmp.did:9C62B55AFD7FE5119EEDFB24CCE0799B</rdf:li> <rdf:li>xmp.did:9C7988AB37206811822AE81DCB8ECD93</rdf:li> <rdf:li>xmp.did:9C
2022-04-08 08:02:44 UTC	5663	IN	Data Raw: 41 39 42 33 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 31 37 41 32 36 39 32 30 39 32 30 36 38 31 31 38 30 38 33 43 37 44 39 41 46 31 46 31 34 39 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 31 39 32 36 46 46 31 34 30 32 30 36 38 31 31 38 37 31 46 45 42 45 41 39 37 33 42 46 37 44 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 31 44 41 44 30 36 45 33 41 32 30 36 38 31 31 39 35 46 45 44 45 38 33 33 36 41 43 43 42 35 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 31 45 36 44 33 32 35 31 30 32 34 36 38 31 31 41 43 41 46 42 46 45 45 41 36 46 39 30 31 33 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e Data Ascii: A9B34</rdf:li> <rdf:li>xmp.did:B17A2692092068118083C7D9AF1F1492</rdf:li> <rdf:li>xmp.did:B1926FF140206811871FEBEA973BF7D7</rdf:li> <rdf:li>xmp.did:B1DAD06E3A20681195FEDE8336ACCB52</rdf:li> <rdf:li>xmp.did:B1E6D32510246811ACAFBFEEA6F90131</rdf:li> <rdf:li>
2022-04-08 08:02:44 UTC	5671	IN	Data Raw: 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 44 42 33 34 34 32 39 30 38 32 30 36 38 31 31 41 39 36 34 46 36 37 32 31 34 37 33 31 41 46 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 44 42 35 42 32 43 37 30 37 32 30 36 38 31 31 38 30 38 33 43 44 46 44 46 39 42 33 35 31 30 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 44 43 36 37 43 42 30 41 36 42 30 36 38 31 31 39 37 41 35 39 44 37 45 45 37 35 46 43 44 41 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 44 45 30 43 33 36 34 30 43 32 30 36 38 31 31 38 30 38 33 44 38 30 41 34 39 42 41 35 37 32 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 Data Ascii: /rdf:li> <rdf:li>xmp.did:BDB3442908206811A964F67214731AFC</rdf:li> <rdf:li>xmp.did:BDB5B2C7072068118083CDFDF9B3510D</rdf:li> <rdf:li>xmp.did:BDC67CB60F20681197A59D7EE75FCDA5</rdf:li> <rdf:li>xmp.did:BDE0C3640C2068118083D80A49BA572B</rdf:li> <rdf:li>xmp.di
2022-04-08 08:02:44 UTC	5687	IN	Data Raw: 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 34 35 34 33 34 41 30 30 39 32 30 36 38 31 31 38 30 38 33 43 33 30 35 44 43 41 39 45 38 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 34 35 41 35 36 41 45 30 33 36 34 45 31 31 31 41 37 38 38 46 38 36 46 36 41 38 42 39 44 44 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 34 35 44 36 30 36 31 44 43 44 36 44 46 31 31 41 46 34 46 41 37 42 43 31 37 39 38 37 39 33 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 34 36 46 33 46 38 42 32 31 32 30 36 38 31 31 39 37 41 35 42 34 37 41 37 35 34 39 35 43 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 44 34 37 34 35 Data Ascii: > <rdf:li>xmp.did:D45434A00920681180838C305DCA9E89</rdf:li> <rdf:li>xmp.did:D45A56AE0364E111A788F86F6A8B9DD</rdf:li> <rdf:li>xmp.did:D45D6061DCD6DF11AF4FA7BC17987931</rdf:li> <rdf:li>xmp.did:D46F3F8B2120681197A5B4E7A75495C2</rdf:li> <rdf:li>xmp.did:D4745
2022-04-08 08:02:44 UTC	5703	IN	Data Raw: 32 35 36 38 31 31 39 39 34 43 41 30 45 36 41 42 31 43 31 35 37 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 45 41 46 32 45 36 41 37 32 41 32 30 36 38 31 31 41 42 30 38 41 34 38 30 39 31 46 31 36 37 35 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 45 42 32 42 32 34 45 44 36 37 30 46 45 31 31 31 41 32 36 31 39 35 41 39 35 31 38 45 34 44 37 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 45 42 33 45 39 30 37 31 35 31 42 37 45 32 31 31 42 45 46 38 46 42 35 41 30 45 38 35 43 34 36 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 45 42 34 43 30 31 37 41 42 41 43 37 31 31 45 30 42 44 43 42 31 33 34 37 33 46 32 33 32 36 37 3c Data Ascii: 256811994CA0E6AB1C1578</rdf:li> <rdf:li>xmp.did:EAFA2E6A72A206811AB08A48091F1675E</rdf:li> <rdf:li>xmp.did:EB2B24ED670FE111A26195A9518E4D7C</rdf:li> <rdf:li>xmp.did:EB3E907151B7E211BEF8FB5A0E85C46F</rdf:li> <rdf:li>xmp.did:EB4C017ABAC711E0BDCB913473F23267<

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	83	OUT	GET /cms/api/am/imageFileData/RWNck1?ver=d266 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate, br User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134 Host: img-prod-cms-rt-microsoft-com.akamaized.net Connection: Keep-Alive
2022-04-08 08:02:42 UTC	115	IN	HTTP/1.1 200 OK Last-Modified: Mon, 04 Apr 2022 07:42:26 GMT Access-Control-Allow-Origin: * X-Datacenter: northeu X-ActivityId: 91a5ddd4-6211-4db6-b10c-2878ecdb9ba1 Timing-Allow-Origin: * X-Frame-Options: deny X-ResizerVersion: 1.0 Content-Type: image/jpeg Content-Location: https://image.prod.cms.rt.microsoft.com/cms/api/am/imageFileData/RWNck1?ver=d266 X-Source-Length: 1819181 Content-Length: 1819181 Cache-Control: public, max-age=85099 Expires: Sat, 09 Apr 2022 07:41:01 GMT Date: Fri, 08 Apr 2022 08:02:42 GMT Connection: close
2022-04-08 08:02:42 UTC	116	IN	Data Raw: ff d8 ff e1 17 e7 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 07 01 12 00 03 00 00 00 01 00 01 00 00 01 1a 00 05 00 00 01 00 00 00 62 01 1b 00 05 00 00 00 01 00 00 00 6a 01 28 00 03 00 00 00 01 00 02 00 00 01 31 00 02 00 00 00 1f 00 00 00 72 01 32 00 02 00 00 00 14 00 00 00 91 87 69 00 04 00 00 00 01 00 00 00 a8 00 00 00 d4 00 0e a6 00 00 00 27 10 00 0e a6 00 00 00 27 10 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 32 31 2e 31 20 28 57 69 6e 64 6f 77 73 29 00 32 30 32 31 3a 30 38 3a 30 35 20 31 33 3a 35 37 3a 33 39 00 00 00 00 00 03 a0 01 00 03 00 00 00 01 ff ff 00 00 a0 02 00 04 00 00 00 01 00 00 07 80 a0 03 00 04 00 00 00 01 00 00 04 38 00 00 00 00 00 00 00 06 01 03 00 03 0c 00 00 01 00 06 00 00 01 1a 00 05 00 00 00 01 00 00 01 22 01 1b 00 05 00 Data Ascii: ExifMM*bj(1r2i"Adobe Photoshop 21.1 (Windows)2021:08:05 13:57:398"
2022-04-08 08:02:42 UTC	149	IN	Data Raw: ee 6b 5e 7d 4a 60 82 fe ce ed df a3 ff 00 8c fe 6f fe dc 56 7e b3 7d 3f cd e4 ff 00 5b e8 b5 0f ea 9f f4 5e a7 cf f3 16 fd 2f e8 bf 45 ff 00 d3 3f d7 fd 32 92 1f 21 bf 97 fa 8a 35 62 bf 17 5a f7 74 af ad 98 95 3f 0e fa db d5 31 db ee aa c8 6b dd 03 df 55 ac ff 00 0b 56 ff 00 ec 2c 1c 5e a1 9d d3 f7 e3 ba 97 52 5c ff 00 77 4f c9 d0 7b 4e df d1 ba 3f 3d bf e8 97 25 93 fc ff 00 e6 fd 31 fc d7 3f f5 8f fd 14 bb 43 ff 00 24 37 fa 5f d0 1f f2 e7 1f f5 af fd 16 8e 5e 1f 57 15 1d b8 f8 b4 1b 7a bf f4 3f fd 88 8d de 95 b7 e8 b8 dd 4d 98 19 65 8e 3b f0 8b 09 70 a6 c0 1f 4b 4f cb 6f bf 7b ba 6b 03 f1 6c 2f 65 9f 66 b2 0e eb e8 7c 31 c2 7e 81 8f 77 e7 7d 07 28 dd fd 1a cf e7 bf f4 27 e9 7d 2e df c8 fd c5 9f d6 bf 9a 67 3c ff 00 83 fa 3c 3b fd 6d 47 1f ca 2b 8b db e9 Data Ascii: k*)J"oV-~}[*/E?2!5bZt?1kUV,^RlwO{N?=%1?C\$?_ ^Wz?Me;p;K0Oj ef 1~w (');g<;cmG+
2022-04-08 08:02:42 UTC	165	IN	Data Raw: 5c 45 64 67 65 5c 5f 43 72 6f 70 73 5c 45 64 67 65 2d 4c 69 66 65 73 74 79 6c 65 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 34 39 30 36 37 35 33 35 33 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 37 2d 32 36 54 31 30 3a 35 36 3a 35 30 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 45 64 67 65 5c 5f 43 72 6f 70 73 5c 45 64 67 65 2d 4c 69 66 65 73 74 79 6c 65 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 38 34 32 37 35 32 38 36 5f 31 39 32 30 7 8 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 37 2d 32 36 54 31 30 3a 35 38 3a 31 32 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 Data Ascii: \Edge_Crops\Edge-Lifestyle_GettyImages-490675353_1920x1080.jpg saved
2016-07-26T10:56:50-07:00
File C:\Users\lv-lizagh\MSI\Windows10\Edge_Crops\Edge-Lifestyle_GettyImages-184275286_1920x1080.jpg saved
2016-07-26T10:58:12-07:00
File C:\User
2022-04-08 08:02:42 UTC	199	IN	Data Raw: 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 45 64 67 65 5c 43 72 6f 70 73 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 37 2d 32 36 54 31 31 3a 30 36 3a 33 34 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 37 2d 32 36 54 31 34 3a 35 32 3a 34 32 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 2e 70 Data Ascii: -lizagh\MSI\Windows10\Edge\Crops\Lockscreen_1920x1080_Landscape.psd saved
2016-07-26T11:06:34-07:00
File C:\Users\lv-lizagh\MSI\Windows10\Lockscreen_1920x1080_Landscape.psd saved
2016-07-26T14:52:42-07:00
File Lockscreen_1920x1080_Landscape.p
2022-04-08 08:02:42 UTC	305	IN	Data Raw: 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 2e 70 73 64 20 6f 70 65 6e 65 64 26 23 78 41 3b 32 30 31 36 2d 30 39 2d 31 35 54 31 36 3a 31 30 3a 34 31 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4f 66 66 69 63 65 5c 45 78 74 72 61 34 30 5c 43 72 6f 70 73 5c 4f 66 66 69 63 65 34 30 5f 5f 35 30 30 70 78 2d 31 34 37 39 39 32 30 31 35 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 30 39 2d 31 35 54 31 36 3a 31 34 3a 30 32 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 61 6d 6 9 6e 67 5c 41 64 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 Data Ascii: x1080_Landscape.psd opened
2016-09-15T16:10:41-07:00
File C:\Users\lv-lizagh\MSI\Windows10\Office\Extra40\Crops\Office40__500px-147992015_1920x1080.jpg saved
2016-09-15T16:14:02-07:00
File C:\Users\lv-lizagh\AppData\Roaming\Adobe\Adobe Photos
2022-04-08 08:02:42 UTC	337	IN	Data Raw: 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 41 64 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 2e 35 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 34 39 43 45 36 31 41 33 35 44 34 38 32 35 42 30 39 39 42 36 34 30 30 33 36 44 41 38 37 32 38 38 34 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 31 31 2d 31 30 54 32 32 3a 33 32 3a 32 31 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 2e 70 73 64 20 73 Data Ascii: serslv-lizagh\AppData\Roaming\Adobe\Adobe Photoshop CC 2015.5\AutoRecover_Lockscreen_1920x1080_Landscape49CE61A35D4825B099B640036DA872884.psb saved
2016-11-10T22:32:21-08:00
File C:\Users\lv-lizagh\MSI\Windows10\Lockscreen_1920x1080_Landscape.psd s

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	385	IN	Data Raw: 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 2e 35 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 4f 66 66 69 63 65 5f 53 6b 79 70 65 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 38 36 36 37 38 39 30 31 5f 31 39 32 30 78 31 30 38 30 44 31 36 35 39 45 36 43 45 44 41 34 32 38 36 34 30 42 41 36 35 35 37 39 44 32 36 44 32 44 39 46 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 36 2d 31 31 2d 32 33 54 31 35 3a 31 32 3a 33 36 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 4f 66 66 69 63 65 5f 53 6b 79 70 65 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 38 36 36 37 38 39 30 31 5f 31 39 32 30 78 31 30 38 30 2d 52 65 63 6f 76 65 72 65 64 2e 70 73 64 20 6f 70 65 6e 65 64 2 6 23 78 41 3b 32 30 31 36 2d 31 31 2d 32 33 54 31 35 3a 31 33 3a Data Ascii: be\Adobe Photoshop CC 2015.5\AutoRecover\Office_Skype_GettyImages-186678901_1920x1080D1659E6CEDA428640BA65579D26D2D9F.psb saved
2016-11-23T15:12:36-08:00	File Office_Skype_GettyImages-186678901_1920x1080-Recovered.psd opened
2016-11-23T15:13:
2022-04-08 08:02:42 UTC	436	IN	Data Raw: 45 45 46 45 38 41 32 43 31 46 42 31 37 41 44 37 39 39 34 44 44 41 34 38 30 39 37 34 38 46 34 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 31 2d 33 30 54 31 30 3a 35 34 3a 35 34 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 6f 6d 65 6e 74 73 49 6e 54 69 6d 65 5c 4e 41 53 43 41 52 5c 46 65 62 72 75 61 72 79 5c 43 48 4f 53 45 4e 5c 4d 49 54 2d 4e 41 53 43 41 52 2d 46 65 62 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 31 33 30 32 30 34 36 39 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 31 2d 33 30 54 31 31 3a 30 30 3a 34 39 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 Data Ascii: EEFE8A2C1FB17AD7994DDA4809748F4.psb saved
2017-01-30T10:54:54-08:00	File C:\Users\l-lizagh\MS\Windows10\MomentsInTime\NASCAR\February\CHOSEN\MIT-NASCAR-Feb_GettyImages-513020469_1920x1080.jpg saved
2017-01-30T11:00:49-08:00	File C:\Users\l
2022-04-08 08:02:42 UTC	476	IN	Data Raw: 30 32 2d 32 36 54 31 33 3a 32 38 3a 35 30 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 6f 6d 65 6e 74 73 49 6e 54 69 6d 65 5c 57 6f 6d 65 6e 73 4d 6f 6e 74 68 5c 43 48 4f 53 45 4e 5c 4d 49 54 5f 57 6f 6d 65 6e 73 48 69 73 74 6f 72 79 4d 6f 6e 74 68 5f 35 30 30 70 78 2d 39 30 35 38 39 33 30 33 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 32 2d 32 36 54 31 33 3a 32 39 3a 34 32 2d 30 38 3a 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 6f 6d 65 6e 74 73 49 6e 54 69 6d 65 5c 57 6f 6d 65 6e 73 4d 6f 6e 74 68 5c 43 48 4f 53 45 4e 5c Data Ascii: 02-26T13:28:50-08:00	File C:\Users\l-lizagh\MS\Windows10\MomentsInTime\WomensMonth\CHOSEN\MIT_WomensHistoryMonth_500px-90589303_1920x1080.jpg saved
2017-02-26T13:29:42-08:00	File C:\Users\l-lizagh\MS\Windows10\MomentsInTime\WomensMonth\CHOSEN\
2022-04-08 08:02:42 UTC	547	IN	Data Raw: 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 41 64 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 2e 35 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 2f 4c 61 6e 64 73 63 61 70 65 30 30 31 46 34 37 39 32 30 44 35 46 34 31 44 38 35 43 33 30 44 45 36 34 33 44 46 35 42 35 37 39 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 33 2d 31 36 54 31 34 3a 30 32 3a 31 34 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 Data Ascii: le C:\Users\l-lizagh\AppData\Roaming\Adobe\Adobe Photoshop CC 2015.5\AutoRecover_Lockscreen_1920x1080_Landscape001F47920D5F41D85C30DE643DF5B579.psb saved
2017-03-16T14:02:14-07:00	File C:\Users\l-lizagh\MS\Windows10\Lockscreen_1920x1080_Landscape
2022-04-08 08:02:42 UTC	575	IN	Data Raw: 35 37 39 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 34 2d 31 32 54 31 35 3a 32 34 3a 32 36 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 42 69 6e 67 5c 42 69 6e 67 41 74 57 6f 72 6b 5c 43 48 4f 53 45 4e 5c 42 69 6e 67 41 74 57 6f 72 6b 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 33 37 31 34 34 32 39 33 5f 31 39 32 30 78 31 30 38 30 2e 70 73 64 2 0 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 34 2d 31 32 54 31 35 3a 33 34 3a 32 36 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 42 69 6e 67 5c 42 69 6e 67 41 74 57 6f 72 6b 5c 43 48 4f 53 45 4e 5c 42 69 Data Ascii: 579.psb saved
2017-04-12T15:24:26-07:00	File C:\Users\l-lizagh\MS\Windows10\Bing\BingAtWork\CHOSEN\BingAtWork_GettyImages-137144293_1920x1080.psd saved
2017-04-12T15:34:26-07:00	File C:\Users\l-lizagh\MS\Windows10\Bing\BingAtWork\CHOSEN\B
2022-04-08 08:02:42 UTC	627	IN	Data Raw: 76 65 72 5c 5f 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 30 30 31 46 34 37 39 32 30 44 35 46 34 31 44 38 35 43 33 30 44 45 36 34 33 44 46 35 42 35 37 39 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 35 2d 30 35 54 31 34 3a 32 33 3a 33 36 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 41 64 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 37 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 30 30 31 46 34 37 39 32 30 44 35 46 34 31 44 38 35 43 33 30 44 45 36 34 33 44 46 35 42 35 37 Data Ascii: ver_Lockscreen_1920x1080_Landscape001F47920D5F41D85C30DE643DF5B579.psb saved
2017-05-05T14:23:36-07:00	File C:\Users\l-lizagh\AppData\Roaming\Adobe\Adobe Photoshop CC 2017\AutoRecover_Lockscreen_1920x1080_Landscape001F47920D5F41D85C30DE643DF5B57
2022-04-08 08:02:42 UTC	675	IN	Data Raw: 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 57 69 6e 64 6f 77 73 49 6e 73 69 64 65 72 5c 52 53 33 2d 52 65 52 65 63 72 75 69 74 5c 43 68 6f 73 65 6e 5c 43 72 6f 70 73 5c 57 69 6e 64 6f 77 73 49 6e 73 69 64 65 72 2d 52 53 33 2d 52 65 52 65 63 72 75 69 74 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 34 39 37 36 38 39 36 37 36 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 36 2d 30 37 54 30 39 3a 32 31 3a 32 39 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 41 64 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 37 5c 41 75 74 6f 52 65 63 6f 76 65 Data Ascii: \Users\l-lizagh\MS\Windows10\WindowsInsider\RS3-ReRecruit\Chosen\Crops\WindowsInsider-RS3-ReRecruit_GettyImages-497689676_1920x1080.jpg saved
2017-06-07T09:21:29-07:00	File C:\Users\l-lizagh\AppData\Roaming\Adobe\Adobe Photoshop CC 2017\AutoRecove
2022-04-08 08:02:42 UTC	699	IN	Data Raw: 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 41 64 6f 62 65 5c 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 37 5c 41 75 74 6f 52 65 63 6f 76 65 72 5c 5f 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 30 30 31 46 34 37 39 32 30 44 35 46 34 31 44 38 35 43 33 30 44 45 36 34 33 44 46 35 42 35 37 39 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 37 2d 30 33 54 32 32 3a 35 33 3a 33 31 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f Data Ascii: 7:00	File C:\Users\l-lizagh\AppData\Roaming\Adobe\Adobe Photoshop CC 2017\AutoRecover_Lockscreen_1920x1080_Landscape001F47920D5F41D85C30DE643DF5B579.psb saved
2017-07-03T22:53:31-07:00	File C:\Users\l-lizagh\MS\Windows10\Lockscreen_1920x1080_

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	738	IN	Data Raw: 30 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 37 2d 32 36 54 31 33 3a 35 36 3a 35 35 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 57 69 6e 64 6f 77 73 5c 4d 4d 58 5c 5f 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 57 69 6e 64 6f 77 73 4d 4d 58 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 35 31 34 31 31 30 32 39 36 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 6 7 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 37 2d 32 36 54 31 33 3a 35 38 3a 30 34 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 57 69 6e 64 6f 77 73 5c 4d 4d 58 5c 5f 43 48 4f 53 45 4e 5c 43 72 6f 70 Data Ascii: 0.psb saved&#xA;2017-07-26T13:56:55-07:00&#x9;File C:\Users\lv-lizagh\MS\Windows10\Window s\MMX_CHOSEN\Crops\WindowsMMX_GettyImages-514110296_1920x1080.jpg saved&#xA;2017-07-26T13:58:04-07: 00&#x9;File C:\Users\lv-lizagh\MS\Windows10\Windows\MMX_CHOSEN\Crop
2022-04-08 08:02:42 UTC	778	IN	Data Raw: 43 30 32 34 37 32 45 33 31 45 45 31 41 46 37 41 35 30 42 46 45 43 45 43 30 34 41 32 33 37 43 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 38 2d 32 39 54 31 37 3a 32 39 3a 32 36 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 2e 70 73 64 20 73 61 76 65 64 26 2 3 78 41 3b 32 30 31 37 2d 30 38 2d 33 30 54 31 34 3a 33 34 3a 31 31 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 2e 70 73 64 20 6f 70 65 6e 65 64 26 23 78 41 3b 32 30 31 37 2d 30 38 2d 33 30 54 31 34 3a 33 35 3a Data Ascii: C02472E31EE1AF7A50BFCECEC04A237C.psb saved&#xA;2017-08-29T17:29:26-07:00&#x9;File C:\Users\lv-lizagh\MS\Windows10\Lockscreen_1920x1080_Landscape.psd saved&#xA;2017-08-30T14:34:11-07:00&#x9;File Locksc reen_1920x1080_Landscape.psd opened&#xA;2017-08-30T14:35:
2022-04-08 08:02:42 UTC	838	IN	Data Raw: 44 42 44 32 39 43 30 34 31 35 43 44 30 30 31 37 39 42 31 31 2e 70 73 62 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 39 2d 32 35 54 31 36 3a 31 39 3a 33 34 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 6f 6d 65 6e 74 73 49 6e 54 69 6d 6 5 5c 46 61 6c 6c 45 6e 74 65 72 74 61 69 6e 6d 65 6e 74 5c 4f 63 74 6f 62 65 72 5c 5f 43 68 6f 73 65 6e 5c 43 72 6f 70 73 5c 46 61 6c 6c 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 38 34 30 37 31 35 37 35 30 37 31 39 32 30 37 3a 30 30 2e 6a 7 0 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 30 39 2d 32 35 54 31 36 3a 32 35 3a 35 37 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a Data Ascii: DBD29C0415CD00179B11.psb saved&#xA;2017-09-25T16:19:34-07:00&#x9;File C:\Users\lv-lizagh\ MS\Windows10\MomentsInTime\FallEntertainment\October_Chosen\Crops\Fall_GettyImages-840715750_1920x1080.jpg saved&#xA;2017-09-25T16:25:57-07:00&#x9;File C:\Users\lv-liz
2022-04-08 08:02:42 UTC	917	IN	Data Raw: 38 3a 35 30 2d 30 37 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 42 69 6e 67 5c 54 72 61 76 65 6c 5c 5f 42 69 6e 67 48 50 2d 50 72 65 76 69 6f 75 73 5c 43 72 6f 70 73 5c 42 69 6e 67 54 72 61 76 65 6c 5f 47 65 74 79 49 6d 61 67 65 73 2d 31 32 2d 31 31 54 31 32 3a 33 33 3a 32 32 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 42 69 6e 67 5c 54 72 61 76 65 6c 5c 5f 42 69 6e 67 48 50 2d 50 72 65 76 69 6f 75 73 5c 43 72 6f 70 73 5c 42 69 6e 67 54 72 61 76 65 6c 5f Data Ascii: 8:50-07:00&#x9;File C:\Users\lv-lizagh\MS\Windows10\Bing\Travel_BingHP-Previous\Crops\BingTravel_G ettyImages-474858115_1920x1080.jpg saved&#xA;2017-11-03T12:12:17-07:00&#x9;File C:\Users\lv-lizagh\MS \Windows10\Bing\Travel_BingHP-Previous\Crops\BingTravel_
2022-04-08 08:02:42 UTC	973	IN	Data Raw: 31 2d 53 65 72 76 69 63 69 6e 67 5c 52 41 57 53 5c 43 48 4f 53 45 4e 5c 57 69 6e 64 6f 77 73 2d 52 53 31 53 65 72 76 69 63 69 6e 67 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 35 35 33 36 31 38 34 34 5f 31 39 32 30 78 31 30 38 30 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 31 31 54 31 32 3a 33 33 3a 32 32 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 52 41 57 53 5c 43 48 4f 53 45 4e 5c 57 69 6e 64 6f 77 73 2d 52 53 31 53 65 72 76 69 63 69 6e 67 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 31 35 35 33 36 31 38 34 34 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 Data Ascii: 1-Servicing\RAWS\CHOSEN\Windows-RS1\Servicing_GettyImages-155361844_1920x1080.psd saved&# xA;2017-12-11T12:33:22-08:00&#x9;File C:\Users\lv-lizagh\MS\Windows10\Windows\RS1-Servicing\RAWS\CHOS EN\Windows-RS1\Servicing_GettyImages-155361844_1920x1080.jpg saved&#
2022-04-08 08:02:42 UTC	981	IN	Data Raw: 31 37 2d 31 32 2d 32 30 54 31 32 3a 30 32 3a 33 39 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 43 6f 72 74 61 6e 61 5c 4e 65 77 59 65 61 72 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 43 6f 72 74 61 6e 61 2d 4e 65 77 59 65 61 72 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 36 30 37 34 31 30 35 35 34 5f 31 39 32 30 78 31 30 38 30 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 37 2d 31 32 2d 32 30 54 31 32 3a 30 33 3a 33 34 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 43 6f 72 74 61 6e 61 5c 4e 65 77 59 65 61 72 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 43 6f 72 74 61 Data Ascii: 17-12-20T12:02:39-08:00&#x9;File C:\Users\lv-lizagh\MS\Windows10\Cortana\NewYear\CHOSEN\Crops\Corta na-NewYear_GettyImages-607410554_1920x1080.psd saved&#xA;2017-12-20T12:03:34-08:00&#x9;File C:\Users\lv-lizagh\MS\Windows10\Cortana\NewYear\CHOSEN\Crops\Corta
2022-04-08 08:02:42 UTC	1029	IN	Data Raw: 37 31 33 39 39 35 34 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 31 2d 31 37 54 30 39 3a 32 34 3a 33 38 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 4d 49 54 2d 49 6e 74 65 72 6e 61 74 69 6f 6e 61 6c 5c 53 6b 69 69 6e 67 5c 43 48 4f 53 45 4e 5c 43 72 6f 70 73 5c 4d 49 54 2d 53 6b 69 69 6e 67 5f 47 65 74 74 79 49 6d 61 67 65 73 2d 38 32 34 33 32 37 33 37 36 5f 31 39 32 30 78 31 30 38 30 2e 6a 70 67 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 31 2d 31 37 54 30 39 3a 32 35 3a 34 31 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 Data Ascii: 7139954_1920x1080.jpg saved&#xA;2018-01-17T09:24:38-08:00&#x9;File C:\Users\lv-lizagh\MS\Windows10\ MIT-International\Skiing\CHOSEN\Crops\MIT-Skiing_GettyImages-824327376_1920x1080.jpg saved&#xA;2018-01- 17T09:25:41-08:00&#x9;File C:\Users\lv-lizagh\MS\Window
2022-04-08 08:02:42 UTC	1093	IN	Data Raw: 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 73 31 30 5c 5f 5f 54 65 6d 70 6c 61 74 65 73 5c 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 2e 70 73 64 20 73 61 76 65 64 26 23 78 41 3b 32 30 31 38 2d 30 32 2d 31 33 54 31 33 3a 32 30 3a 31 38 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 4c 6f 63 6b 73 63 72 65 65 6e 5f 31 39 32 30 78 31 30 38 30 5f 4c 61 6e 64 73 63 61 70 65 2e 70 73 64 20 6f 70 65 6e 65 64 26 23 78 41 3b 32 30 31 38 2d 30 32 2d 31 33 54 31 33 3a 32 32 3a 35 33 2d 30 38 3a 30 30 26 23 78 39 3b 46 69 6c 65 20 43 3a 5c 55 73 65 72 73 5c 76 2d 6c 69 7a 61 67 68 5c 4d 53 5c 57 69 6e 64 6f 77 7 3 31 30 5c 45 64 67 65 5c 56 69 72 67 69 6e 47 61 6c 61 63 74 69 Data Ascii: e C:\Users\lv-lizagh\MS\Windows10_ Templates\Lockscreen_1920x1080_Landscape.psd saved&#xA;2018- 02-13T13:20:18-08:00&#x9;File Lockscreen_1920x1080_Landscape.psd opened&#xA;2018-02-13T13:22:53-08:00&# x9;File C:\Users\lv-lizagh\MS\Windows10\Edge\VirginGalacti

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	1500	IN	Data Raw: 41 46 42 34 39 41 37 31 38 32 33 31 41 46 44 32 41 39 37 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 38 32 38 31 31 45 43 30 35 43 34 42 45 31 39 30 44 36 45 43 37 38 33 44 39 32 31 45 36 37 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 38 33 38 32 33 31 32 34 41 41 46 30 41 31 32 42 37 38 33 42 42 43 36 38 32 31 45 33 30 33 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 38 34 31 37 39 42 31 33 35 44 35 39 30 30 3 7 30 42 43 37 43 46 41 42 44 33 34 34 31 43 31 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 38 35 33 35 41 38 39 44 38 43 46 33 45 42 32 38 38 45 37 36 38 38 33 38 41 44 37 32 38 46 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 34 38 35 39 3c 32 41 42 41 31 39 46 37 44 41 36 Data Ascii: AFB49A718231AFD2A97B</rdf:li> <rdf:li>482811EC05C4BE190D6EC783D921E67E</rdf:li> <rdf:li>483823124AAAF0A12B783BBC6821E3039</rdf:li> <rdf:li>484179B135D590070BC7CFABD3441C1A</rdf:li> <rdf:li>48535A89D8CF3EB288E76883AD728F6</rdf:li> <rdf:li>4859332ABA19F7DA6
2022-04-08 08:02:42 UTC	1516	IN	Data Raw: 3a 6c 69 3e 35 35 37 37 31 33 39 37 36 39 30 35 30 37 30 38 46 37 30 36 37 30 34 35 46 31 34 39 46 38 30 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 35 37 42 31 43 46 45 32 32 44 35 36 37 45 41 30 34 41 36 39 45 34 39 41 34 30 36 43 38 37 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 35 39 35 46 44 36 43 44 3 3 42 32 44 36 34 38 36 32 44 46 31 44 46 31 31 42 45 38 46 33 42 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 35 41 45 33 38 39 46 41 44 36 41 42 30 32 32 30 30 44 33 39 33 34 33 46 36 38 35 38 33 34 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 35 42 32 39 33 31 31 37 34 37 43 36 43 46 34 30 41 33 36 38 45 43 36 37 46 35 35 44 30 46 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 35 Data Ascii: :li>5577139769050708F7067045F149F808</rdf:li> <rdf:li>557B1CFE22D567EA0A469E49A406C872</rdf:li> <rdf:li>5595FD6CD3B2D64862DF1DF11BE8F3B3</rdf:li> <rdf:li>55AE389FAD6AB02200D39343F6858346</rdf:li> <rdf:li>55B29311747C6CF40A368E367F55D0F1</rdf:li> <rdf:li>5
2022-04-08 08:02:42 UTC	1532	IN	Data Raw: 34 31 42 41 39 36 33 35 32 32 32 46 44 33 31 30 42 31 31 33 37 44 37 37 38 46 38 45 37 34 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 34 32 30 31 30 38 46 33 32 38 32 45 44 33 45 43 37 37 38 31 41 31 30 44 35 37 32 38 30 34 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 34 32 31 32 41 33 41 44 41 46 36 45 42 36 33 43 36 37 30 43 37 31 37 35 31 39 46 32 42 37 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 34 33 42 3 5 37 45 43 39 37 33 46 45 30 34 46 38 33 46 38 34 30 30 33 37 30 36 38 38 33 37 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 34 33 46 39 45 41 36 43 44 37 38 44 36 45 43 46 31 46 44 39 43 41 34 44 42 35 32 34 42 33 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 34 34 46 37 37 Data Ascii: 41BA9635222FD310B1137D778F8E742</rdf:li> <rdf:li>6420108F3282ED3EC7781A10D572804B</rdf:li> <rdf:li>64212A3ADAF6EB63C670C717519F2B7E</rdf:li> <rdf:li>643B57EC973FE04F83F8400370688373</rdf:li> <rdf:li>643F9EA6CD78D6ECF1FD9CA4DB524B30</rdf:li> <rdf:li>644F77
2022-04-08 08:02:42 UTC	1539	IN	Data Raw: 35 43 42 35 38 37 35 33 42 45 31 43 45 37 41 34 38 33 41 38 41 35 33 30 46 44 42 43 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 41 35 31 41 46 37 32 32 42 43 44 37 45 39 43 38 38 36 34 43 34 46 33 41 32 30 42 34 43 38 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 41 35 42 34 38 35 42 30 32 42 31 42 45 43 42 34 41 31 44 41 41 35 34 39 38 44 45 41 32 38 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 41 36 39 43 32 3 9 34 45 36 42 46 34 42 46 42 36 41 42 45 43 37 37 46 43 30 42 36 35 46 31 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 41 37 42 34 44 43 36 31 42 37 41 43 45 38 30 42 43 31 37 35 30 42 32 36 30 45 34 36 30 37 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 36 41 38 36 31 44 39 30 Data Ascii: 5CB58753BE1CE7A483A8A530FDBCE</rdf:li> <rdf:li>6A51AF722BCD7E9C8864C4F3A20B4C82</rdf:li> <rdf:li>6A5B485B02B1BECB4A1DAA5498DEA28E</rdf:li> <rdf:li>6A69C294E6BF4BFB6ABEC77FC0B65F19</rdf:li> <rdf:li>6A7B4DC61B7ACE80BC1750B260E46075</rdf:li> <rdf:li>6A861D90
2022-04-08 08:02:42 UTC	1555	IN	Data Raw: 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 38 35 32 42 43 33 41 31 37 42 34 30 36 42 31 31 44 39 42 31 36 38 35 43 36 42 46 45 44 32 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 38 35 34 43 31 30 45 32 32 43 46 33 35 45 41 34 44 34 43 46 46 30 38 37 39 38 42 38 33 32 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 3 7 38 35 42 41 33 38 34 36 46 44 30 32 45 33 31 38 30 39 43 44 39 31 30 42 37 36 32 42 36 32 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 38 36 41 37 35 45 39 43 43 37 34 35 45 33 33 34 33 44 33 43 33 38 39 37 37 38 44 39 34 32 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 37 38 37 37 37 37 45 32 44 36 45 35 30 43 31 43 39 41 34 33 34 34 38 30 46 39 41 41 38 44 33 42 35 41 3c 2f 72 64 66 3a 6c 69 3e 20 Data Ascii: :li> <rdf:li>7852BC3A17B406B11D9B1685C6BFED2D</rdf:li> <rdf:li>7854C10E22CF35EA4D4CFF087 98B8322</rdf:li> <rdf:li>785BA3846FD02E31809CD910B762B625</rdf:li> <rdf:li>786A75E9CC745E3343D3C3897 78D9422</rdf:li> <rdf:li>787E2D6E50C1C9A434480F9AAA8D3B5A</rdf:li>
2022-04-08 08:02:42 UTC	1571	IN	Data Raw: 43 30 37 32 38 46 44 46 36 42 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 36 32 37 45 37 36 32 31 44 39 43 32 41 31 34 39 31 31 37 35 46 34 37 31 42 45 46 41 44 31 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 36 32 38 36 41 31 37 30 32 41 31 30 46 44 30 42 45 46 30 38 41 39 44 43 33 33 32 42 38 32 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 36 32 42 45 33 46 39 32 42 34 30 43 42 38 34 44 45 39 30 46 42 37 35 34 33 42 41 41 43 32 32 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 36 32 44 45 41 30 44 35 44 35 46 36 39 46 37 41 43 36 33 33 45 35 39 32 45 42 36 35 39 41 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 36 33 44 36 42 46 38 34 44 35 39 37 35 45 45 36 33 41 33 43 32 43 31 41 Data Ascii: C0728FDF6B3</rdf:li> <rdf:li>8627E7621D9C2A1491175F471BEFAD11</rdf:li> <rdf:li>86286A170 2A10FD0BEF08A9DC332B827</rdf:li> <rdf:li>862BE3F92C0CB84DE90FB7543BAAC224</rdf:li> <rdf:li>862DEA0D5 D5F69F7AC633E592EB659AF</rdf:li> <rdf:li>863D6BF84D5975EE563A3C2C1A
2022-04-08 08:02:42 UTC	1579	IN	Data Raw: 31 44 34 45 44 38 36 34 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 42 42 36 46 44 35 39 30 30 42 35 42 42 42 41 32 33 36 43 41 36 31 42 39 38 33 35 31 31 33 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 42 43 35 44 45 36 44 36 39 34 34 36 32 39 32 35 35 41 43 46 44 35 44 45 34 44 35 36 32 37 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 42 43 43 34 45 41 41 42 35 37 38 38 46 43 39 42 37 35 31 32 33 31 42 36 41 43 37 45 37 38 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 42 43 44 34 39 31 35 44 37 30 32 43 41 32 39 30 41 39 38 43 31 34 30 33 33 41 37 45 37 41 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 38 42 45 32 42 38 32 32 39 32 36 33 44 38 39 35 36 30 43 32 38 41 31 43 30 46 33 33 Data Ascii: 1D4ED8644</rdf:li> <rdf:li>8BB6FD5900B5BBBA236CA61B9835113A</rdf:li> <rdf:li>8BC5DE6D694 4629255ACFD5DE4D56273</rdf:li> <rdf:li>8BCC4EAAB5788FC9B751231B6AC7E785</rdf:li> <rdf:li>8BCD4915D70 2CA290A98C14033A7E7AF</rdf:li> <rdf:li>8BE2B8229263D89560C28A1C0F33
2022-04-08 08:02:42 UTC	1595	IN	Data Raw: 46 44 34 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 41 34 37 31 38 46 35 46 42 41 42 41 45 30 45 36 39 38 44 34 46 37 43 31 34 41 32 45 39 33 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 41 37 33 43 44 35 45 45 43 33 42 43 42 38 43 39 32 45 44 33 46 32 34 39 37 38 39 30 33 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 41 38 31 33 33 37 35 43 39 41 30 45 34 35 43 34 44 32 36 36 37 41 33 38 32 39 42 31 45 31 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 41 38 35 39 32 38 35 37 30 31 32 44 41 46 44 43 41 39 37 43 32 45 46 34 46 41 33 39 46 36 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 39 41 38 35 46 42 36 30 44 36 42 38 34 30 35 37 30 46 39 31 37 35 41 41 33 33 38 39 37 46 37 36 3c Data Ascii: FD41</rdf:li> <rdf:li>9A4718F5FBABAE0E698D4F7C14A2E93E</rdf:li> <rdf:li>9A73CD5EEC3BCB8C 92ED3F2497897034</rdf:li> <rdf:li>9A813375C9A0E45C4D2667A3829B1E11</rdf:li> <rdf:li>9A8592857012DAFD CA97C2EF4FA39F6F</rdf:li> <rdf:li>9A85FB60D6B840570F9175AA33897F76<

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	1611	IN	Data Raw: 37 42 36 35 46 31 45 31 39 45 38 42 33 34 42 41 41 41 45 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 37 41 31 32 35 35 46 46 33 38 36 36 37 39 35 42 43 42 32 37 30 36 31 30 32 43 37 42 33 43 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 37 41 37 45 45 46 41 35 35 37 32 46 43 45 42 35 44 30 44 35 46 41 34 37 38 43 38 43 41 43 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 37 42 32 45 31 35 37 43 32 45 42 42 33 45 3 4 36 46 35 36 42 31 35 45 31 35 44 36 38 46 33 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 37 42 34 42 36 36 44 43 42 39 45 38 32 33 43 31 41 31 31 42 35 42 35 32 31 44 39 30 35 31 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 37 43 34 46 38 46 42 38 34 45 42 37 31 45 43 44 Data Ascii: 7B65F1E19E8B34BAAE2</rdf:li> <rdf:li>A7A1255FF3866795BCB2706102C7B3C8</rdf:li> <rdf:li>A7A7EEFA5572FCEB5D0D5FA478C8CACF</rdf:li> <rdf:li>A7B2E157C2EBB3E46F56B15E15D68F3B</rdf:li> <rdf:li>A7B4B66DCB9E823C1A11B5B521D90514</rdf:li> <rdf:li>A7C4F8FB84EB71ECD
2022-04-08 08:02:42 UTC	1619	IN	Data Raw: 37 43 42 46 33 36 37 30 31 43 32 46 33 32 35 35 39 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 45 37 31 30 45 39 46 39 43 43 41 43 34 34 31 34 43 44 30 41 43 41 46 46 46 42 46 42 44 31 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 45 38 39 37 32 46 41 46 46 42 44 36 32 38 39 37 44 35 31 42 36 45 32 49 34 45 31 37 35 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 45 38 45 44 33 37 32 43 44 33 46 37 43 44 36 37 3 7 36 46 31 31 36 38 32 43 43 33 45 38 31 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 45 38 46 44 30 42 31 37 43 34 32 46 42 44 31 35 42 36 31 37 41 42 36 44 44 43 46 41 42 41 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 45 39 41 35 36 42 41 44 44 38 44 39 34 33 33 31 35 37 Data Ascii: 7CBF36701C2F325594</rdf:li> <rdf:li>AE710E9F9CCAC4414CD0ACAFFBFBD16</rdf:li> <rdf:li>AE8972FAFFBD62897D51B6B5B94E1758</rdf:li> <rdf:li>AE8ED372CD3F7CD6776F11682CC3E817</rdf:li> <rdf:li>AE8FD0B17C42FBD15B617AB6DDCFABA7</rdf:li> <rdf:li>AE9A56BADD8D9433157
2022-04-08 08:02:42 UTC	1627	IN	Data Raw: 35 34 31 42 46 30 33 46 31 39 42 41 35 31 32 44 43 38 31 35 31 43 44 34 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 41 45 37 31 30 45 39 46 39 43 43 41 43 34 34 31 34 43 44 30 41 43 41 46 46 46 42 46 42 44 31 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 34 46 35 42 36 38 46 38 36 43 41 46 32 46 37 39 32 42 37 38 46 44 35 32 33 30 31 43 45 36 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 34 46 38 42 37 44 37 32 42 34 3 2 45 37 32 31 34 38 38 46 45 36 41 43 43 42 44 36 44 39 34 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 34 46 44 45 42 43 39 44 36 31 46 37 38 38 44 45 37 34 35 36 33 38 36 32 42 41 33 31 39 32 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 42 35 30 31 31 32 35 35 30 35 34 46 46 Data Ascii: 541BF03F19BA512DC8151CD9</rdf:li> <rdf:li>B4E397579B8921AB0A961F1C675F00A6</rdf:li> <rdf:li>B4F5B68F86CAF2F792B78FD52301CE61</rdf:li> <rdf:li>B4F8B7D72B4E2721488FE6ACCBDD6945</rdf:li> <rdf:li>B4FDEBC9D61F788DE74563862BA31924</rdf:li> <rdf:li>B5011255054FF
2022-04-08 08:02:42 UTC	1643	IN	Data Raw: 3c 72 64 66 3a 6c 69 3e 43 33 30 41 46 33 34 31 43 30 32 37 31 33 44 44 42 41 36 30 42 33 44 45 32 34 34 35 39 42 36 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 33 30 42 39 32 30 30 32 45 46 39 42 36 38 34 45 46 38 33 44 30 32 32 33 33 43 46 41 30 44 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 33 32 38 43 3 7 31 30 43 44 30 38 38 34 42 45 44 34 43 41 32 44 33 37 35 36 38 35 47 37 45 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 33 33 35 37 37 45 42 37 43 30 33 41 32 35 43 42 33 31 44 36 46 30 30 30 43 36 43 42 45 34 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 33 34 43 35 46 44 43 41 33 39 30 41 34 44 30 46 46 43 30 32 30 31 41 31 35 42 37 30 31 45 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a Data Ascii: <rdf:li>C30AF341C02713DDBA60B3DE24459B6A</rdf:li> <rdf:li>C30B92002EF9B684EF83D02233CFA0DE</rdf:li> <rdf:li>C328C710CD0884BED4CA2D375685D7E5</rdf:li> <rdf:li>C33577EB7C03A25CB31D6F000C6CBE4E</rdf:li> <rdf:li>C34C5FDCA390A4D0FFC0201A15B701ED</rdf:li> <rdf:li>
2022-04-08 08:02:42 UTC	1659	IN	Data Raw: 6c 69 3e 43 46 33 34 37 44 33 44 46 32 31 35 43 30 39 30 44 37 46 43 30 39 43 34 32 36 42 44 43 36 34 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 46 34 36 36 46 42 44 39 39 39 37 45 35 44 41 35 39 42 35 32 35 34 42 43 45 39 41 38 32 38 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 46 37 31 30 30 41 45 33 34 3 0 36 31 34 37 38 33 32 33 42 31 46 36 38 46 30 39 36 39 31 34 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 46 38 41 44 35 37 33 41 35 41 33 44 42 30 45 39 36 31 37 36 46 46 38 35 44 32 35 44 39 30 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 46 38 43 37 36 32 31 46 38 42 46 37 31 30 45 32 33 43 44 34 34 30 30 39 32 44 39 44 37 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 43 46 Data Ascii: li>CF347D3DF215C090D7FC09C426BDC648</rdf:li> <rdf:li>CF466FBD9997E5DA59B5254BCE9A8281</rdf:li> <rdf:li>CF7100AE34061478323B1F68F096914B</rdf:li> <rdf:li>CF8AD573A5A3DB0E96176FF85D25D905</rdf:li> <rdf:li>CF8C7621F8BF710E23C4C440092D9D75</rdf:li> <rdf:li>CF
2022-04-08 08:02:42 UTC	1667	IN	Data Raw: 3e 44 36 35 33 41 38 44 37 38 38 45 38 36 42 35 32 36 36 32 32 36 41 31 43 34 41 44 41 30 36 43 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 36 35 44 30 32 34 44 41 34 42 41 44 31 37 35 41 43 35 33 32 31 36 44 37 45 37 43 37 34 37 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 36 37 30 45 32 39 33 31 37 43 39 3 9 36 35 30 32 41 39 32 35 31 42 31 39 33 41 42 33 36 43 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 36 38 36 45 41 45 35 44 38 30 44 39 42 45 37 44 32 39 46 33 43 35 45 34 44 33 34 37 30 43 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 36 39 39 33 35 35 33 42 32 44 42 36 46 42 38 39 41 39 38 45 32 42 36 31 35 38 32 43 34 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 44 36 39 45 Data Ascii: >D653A8D788E86B5266226A1C4ADA06C2</rdf:li> <rdf:li>D65D024DA4BAD175AC53216D7E7C7478</rdf:li> <rdf:li>D670E29317C996502A9251B193AB36C2</rdf:li> <rdf:li>D686EAE5D80D9BE7D29F3C5E4D3470CF</rdf:li> <rdf:li>D6993553B2DB6FB89A98E2B61582C41</rdf:li> <rdf:li>D69E
2022-04-08 08:02:42 UTC	1683	IN	Data Raw: 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 33 41 44 34 42 42 32 39 35 45 41 34 32 36 42 31 36 31 36 39 31 35 30 36 39 36 35 31 30 38 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 33 41 46 45 45 44 46 31 39 30 37 39 31 46 32 41 35 42 31 36 42 35 32 32 38 41 37 30 38 36 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 33 43 30 36 43 32 45 37 42 41 30 34 42 33 41 31 33 45 38 30 37 44 32 38 44 44 41 35 32 35 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 33 43 37 33 46 33 44 33 42 42 41 39 33 38 44 45 38 44 45 42 37 43 43 38 39 36 38 39 34 36 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 33 44 43 38 41 45 37 43 30 34 31 32 41 46 45 30 41 33 41 39 37 31 31 31 32 32 30 30 36 31 31 3c 2f 72 64 66 3a Data Ascii: /rdf:li> <rdf:li>E3AD4BB295EA426B1616915069651087</rdf:li> <rdf:li>E3AFEEDF190791F2A5B16B5228A70860</rdf:li> <rdf:li>E3C06C2E7BA04B3A13E807D28DDA5252</rdf:li> <rdf:li>E3C73F3D3BBA938DE8DEB7CC89689467</rdf:li> <rdf:li>E3DC8AE7C0412AFE0A3A971112200611</rdf:li>
2022-04-08 08:02:42 UTC	1699	IN	Data Raw: 41 45 37 43 43 42 46 42 44 42 39 44 34 37 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 46 39 43 30 31 32 44 32 45 45 46 35 45 36 35 45 31 34 39 38 44 41 31 32 42 41 36 36 36 39 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 46 41 46 31 36 34 31 45 36 39 39 46 32 43 36 42 44 38 37 37 35 31 36 41 34 36 34 39 41 41 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 46 42 36 39 32 41 39 38 36 34 34 43 45 45 31 35 33 34 35 3 9 42 31 30 32 44 30 37 35 33 30 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 46 42 44 41 45 42 41 34 33 31 30 45 39 46 38 41 45 32 38 37 44 32 42 30 46 38 41 37 34 31 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 45 46 43 32 44 37 38 45 43 39 30 35 38 46 32 43 32 34 42 34 39 30 Data Ascii: AE7CCBFBD9D477</rdf:li> <rdf:li>EF9C012DEEF5E65E1498DA12BA66692</rdf:li> <rdf:li>EFAF1641E699F2C6BD877516A4649AA4</rdf:li> <rdf:li>EFB692A98644CEE153459B102D075301</rdf:li> <rdf:li>EFBDAEBA4310E9F8AE287D2B0F8A7413</rdf:li> <rdf:li>EFC2D78EC9058F2C24B490

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	1707	IN	Data Raw: 34 32 44 43 39 38 39 31 44 43 31 45 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 35 36 44 37 44 36 30 36 37 46 36 44 30 38 30 37 32 36 41 38 39 37 42 43 35 39 30 39 41 35 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 35 36 45 33 46 31 46 42 43 44 34 37 34 41 35 36 36 35 32 46 37 43 35 31 31 38 41 35 34 36 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 35 36 46 34 39 33 42 34 32 30 45 44 35 46 36 46 42 41 46 43 33 41 45 31 45 33 30 38 46 41 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 46 35 37 33 45 36 37 43 35 39 44 37 38 42 44 45 42 37 38 34 39 39 45 36 34 35 41 Data Ascii: 42DC9891DC1ED</rdf:li> <rdf:li>F56D7D6067F6D080726A897BC5909A59</rdf:li> <rdf:li>F56E3F1FB CD474A56652F7C5118A5464</rdf:li> <rdf:li>F56F493B420ED5F6FB AFC3AE1E308FA9</rdf:li> <rdf:li>F5735FE072BE8068F7C96FECA1DEBB64</rdf:li> <rdf:li>F573C59D78BDEB78499E645A
2022-04-08 08:02:42 UTC	1937	IN	Data Raw: 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 30 63 31 37 31 34 64 34 2d 63 65 30 61 2d 31 31 64 39 2d 62 65 33 62 2d 38 31 65 62 38 38 63 32 34 36 61 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 30 63 31 38 38 66 35 65 2d 32 36 39 61 2d 31 31 65 36 2d 61 33 64 38 2d 66 31 33 32 39 31 33 31 37 62 61 66 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 30 63 39 36 38 62 61 64 2d 32 38 38 65 2d 66 32 34 62 2d 38 33 37 65 2d 61 36 64 66 62 65 39 39 65 36 35 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 6 4 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 30 63 64 33 63 61 Data Ascii: dobe:docid:photoshop:0c1714d4-ce0a-11d9-be3b-81eb88c246a9</rdf:li> <rdf:li>adobe:docid:photoshop:0c188f5e-269a-11e6-a3d8-f13291317baf</rdf:li> <rdf:li>adobe:docid:photoshop:0c968bad-288e-f24b-837e-a6dfbe99e656</rdf:li> <rdf:li>adobe:docid:photoshop:0cd3ca
2022-04-08 08:02:42 UTC	1953	IN	Data Raw: 2d 61 30 61 61 66 35 66 35 31 61 62 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 33 65 34 31 39 37 62 39 2d 61 30 34 64 2d 31 31 65 37 2d 61 35 35 39 2d 62 64 61 30 31 31 34 64 37 38 30 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 33 65 35 38 38 38 36 61 2d 30 30 62 64 2d 31 31 64 38 2d 61 30 61 32 2d 62 62 37 31 62 63 61 32 63 62 35 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 33 65 35 62 33 33 66 34 2d 35 36 36 31 2d 31 31 64 64 2d 39 30 30 32 2d 66 35 37 63 39 66 65 37 61 35 31 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 Data Ascii: -a0aaf5f51ab1</rdf:li> <rdf:li>adobe:docid:photoshop:3e4197b9-a04d-11e7-a559-bda0114d7807</rdf:li> <rdf:li>adobe:docid:photoshop:3e58886a-00bd-11d8-a0a2-bb71bca2cb53</rdf:li> <rdf:li>adobe:docid:photoshop:3e5b33f4-5661-11dd-9002-f57c9fe7a517</rdf:li> <rdf
2022-04-08 08:02:42 UTC	1961	IN	Data Raw: 73 68 6f 70 3a 35 32 62 39 36 62 65 65 2d 33 33 31 30 2d 31 31 37 39 2d 38 37 39 35 2d 66 61 37 38 31 65 62 65 34 37 34 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 35 32 62 64 35 38 37 32 2d 39 39 32 65 2d 31 31 64 39 2d 38 31 64 34 2d 39 62 37 64 30 31 66 39 37 32 32 64 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 35 33 34 32 62 66 36 38 2d 30 66 36 37 2d 31 31 64 65 2d 38 63 38 39 2d 61 62 64 38 36 38 31 35 32 39 30 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 3 5 33 38 63 61 32 38 65 2d 36 36 38 61 2d 31 31 64 61 2d 38 37 62 Data Ascii: shop:52b96bee-3310-1179-8795-fa781ebe4746</rdf:li> <rdf:li>adobe:docid:photoshop:52bd5872-992e-11d9-81d4-9b7d01f9722d</rdf:li> <rdf:li>adobe:docid:photoshop:5342bf68-0f67-11de-8c89-abd868152904</rdf:li> <rdf:li>adobe:docid:photoshop:538ca28e-668a-11da-87b
2022-04-08 08:02:42 UTC	1969	IN	Data Raw: 33 2d 64 64 35 62 2d 31 31 37 38 2d 61 32 30 64 2d 61 66 32 65 66 39 63 31 39 37 64 66 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 36 65 30 31 36 31 39 63 2d 65 63 63 30 2d 31 31 37 38 2d 62 66 37 31 2d 38 38 35 36 64 61 39 64 37 38 36 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 36 65 34 38 64 31 66 66 2d 64 66 61 31 2d 31 31 37 38 2d 61 32 35 33 2d 65 62 62 37 38 32 63 31 66 65 32 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 36 65 35 32 36 36 30 66 2d 35 35 33 38 2d 31 31 65 35 2d 39 64 38 62 2d 65 31 38 39 38 32 62 35 34 32 Data Ascii: 3-dd5b-1178-a20d-af2ef9c197df</rdf:li> <rdf:li>adobe:docid:photoshop:6e01619c-ecc0-1178-bf71-8856da9d7868</rdf:li> <rdf:li>adobe:docid:photoshop:6e48d1ff-dfa1-1178-a253-ebb782c1fe21</rdf:li> <rdf:li>adobe:docid:photoshop:6e52660f-5538-11e5-9d8b-e18982b542
2022-04-08 08:02:42 UTC	1985	IN	Data Raw: 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 39 65 33 34 39 37 66 31 2d 35 66 64 39 2d 31 31 37 38 2d 39 61 35 37 2d 61 62 36 36 65 37 65 66 61 61 38 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 39 65 35 66 62 61 66 38 2d 65 66 30 34 2d 31 31 37 38 2d 39 31 37 33 2d 66 63 65 35 31 62 62 36 32 39 35 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 39 65 37 62 62 64 34 65 2d 31 33 63 30 2d 31 31 37 38 2d 62 34 61 30 2d 66 32 30 30 32 61 36 37 38 61 36 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6 f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 39 65 Data Ascii: li>adobe:docid:photoshop:9e3497f1-5fd9-1178-9a57-ab66e7efaa88</rdf:li> <rdf:li>adobe:docid:photoshop:9e5fbafe-ef04-1178-9173-fce51bb62952</rdf:li> <rdf:li>adobe:docid:photoshop:9e7bbd4e-13c0-1178-b4a0-f2002a678a60</rdf:li> <rdf:li>adobe:docid:photoshop:9e
2022-04-08 08:02:42 UTC	2001	IN	Data Raw: 37 38 2d 61 37 33 36 2d 39 66 35 31 37 33 63 37 32 36 32 64 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 64 33 31 63 65 65 37 2d 64 30 38 31 2d 31 31 37 38 2d 38 35 30 63 2d 63 33 63 31 33 34 39 66 64 31 66 66 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 64 33 33 39 33 64 31 37 2d 33 39 62 65 2d 31 31 65 37 2d 62 33 36 66 2d 66 38 31 66 37 39 39 32 32 33 61 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 64 33 34 38 31 39 39 35 2d 31 62 65 37 2d 31 31 64 61 2d 62 32 34 63 2d 62 65 32 36 64 62 62 34 32 37 64 39 3c 2f 72 64 66 3a 6c Data Ascii: 78-a736-9f5173c7262d</rdf:li> <rdf:li>adobe:docid:photoshop:d31cee78-d081-1178-850c-c3c1349df1ff</rdf:li> <rdf:li>adobe:docid:photoshop:d3393d17-39be-11e7-b36f-f81f799223a6</rdf:li> <rdf:li>adobe:docid:photoshop:d3481995-1be7-11da-b24c-be26dbb427d9</rdf:li>
2022-04-08 08:02:42 UTC	2009	IN	Data Raw: 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 65 62 32 64 34 31 34 31 2d 63 31 34 38 2d 31 31 37 61 2d 38 31 36 62 2d 65 33 33 35 31 30 34 33 30 63 30 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 65 62 33 62 65 66 32 38 2d 30 32 62 36 2d 31 31 64 66 2d 62 64 39 64 2d 39 36 64 61 38 32 30 64 31 34 66 66 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 65 62 36 66 32 66 38 39 2d 64 36 33 35 2d 31 31 65 35 2d 39 63 65 32 2d 39 33 33 37 38 66 30 30 31 35 36 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 61 64 6f 62 65 3a 64 6f 63 69 64 3a 70 68 6f 74 6f 73 68 6f 70 3a 65 62 38 31 30 62 66 38 2d 33 31 34 32 2d 31 Data Ascii: d:photoshop:eb2d4141-c148-117a-816b-e33510430c09</rdf:li> <rdf:li>adobe:docid:photoshop:eb3bef28-02b6-11df-bd9d-96da820d14ff</rdf:li> <rdf:li>adobe:docid:photoshop:eb6f2f89-d635-11e5-9ce2-9337f8001563</rdf:li> <rdf:li>adobe:docid:photoshop:eb810bf8-3142-1

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	2025	IN	Data Raw: 33 31 45 30 31 31 39 37 36 38 44 45 32 46 35 32 31 31 32 46 36 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 32 31 38 32 39 46 39 44 45 44 35 35 44 41 31 31 39 31 38 36 46 46 39 32 37 36 37 44 46 33 43 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 32 31 39 32 45 30 44 33 42 34 46 37 44 43 31 31 42 45 34 33 43 32 33 44 44 45 31 33 44 43 41 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 32 31 41 31 42 32 35 31 46 36 45 46 44 44 31 31 39 33 38 39 38 35 32 42 32 30 37 34 32 42 34 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 32 31 43 41 39 35 42 36 43 46 37 46 44 43 31 31 39 39 30 36 41 43 30 32 35 32 33 44 31 41 43 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 Data Ascii: 31E0119768DE2F52112F6B</rdf:li> <rdf:li>uuid:21829F9DED55DA119186FF92767DF3C7</rdf:li> <rdf:li>uiuid:2192E0D3B4F7DC11BE43C23DDE13DCA8</rdf:li> <rdf:li>uuid:21A1B251F6EFD119389852B20742B49</rdf:li> <rdf:li>uiuid:21CA95B6CF7FDC119906AC02523D1AC1</rdf:li> <rd
2022-04-08 08:02:42 UTC	2041	IN	Data Raw: 72 64 66 3a 6c 69 3e 75 75 69 64 3a 35 36 32 46 35 37 44 45 32 36 45 34 44 45 31 31 41 38 45 46 45 46 38 37 44 39 31 32 33 30 36 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 35 36 42 34 31 37 30 45 35 37 38 34 31 31 44 45 42 45 42 32 46 36 45 39 33 32 44 36 36 41 37 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 35 36 43 46 35 43 30 32 33 46 37 36 44 45 31 31 38 33 43 30 43 31 35 34 37 44 33 32 45 35 37 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 35 37 30 44 31 42 33 34 38 35 30 30 45 31 31 31 38 43 35 35 45 46 36 44 42 38 39 37 31 35 32 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 35 37 31 32 33 44 35 46 41 31 35 31 31 31 44 44 39 35 46 44 45 33 31 Data Ascii: rdf:li>uiuid:562F57DE26E4DE11A8EFEF87D9123063</rdf:li> <rdf:li>uiuid:56B4170E578411DEBEB2F6E932D66A7A</rdf:li> <rdf:li>uiuid:56CF5C023F76DE1183C0C1547D32E578</rdf:li> <rdf:li>uiuid:570D1B348500E1118C55EF6DB8971523</rdf:li> <rdf:li>uiuid:57123D5FA15111DD95FDE31
2022-04-08 08:02:42 UTC	2911	IN	Data Raw: 31 38 31 45 39 41 44 35 36 30 32 35 42 35 46 32 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 36 44 44 37 45 36 38 36 46 42 46 35 44 45 31 31 42 31 42 44 39 44 36 37 43 38 31 38 36 41 42 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 36 45 34 37 45 30 44 30 41 33 43 39 31 31 44 44 39 39 30 45 44 30 32 33 43 41 36 41 44 33 34 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 36 45 37 3 7 38 46 38 35 44 31 43 36 45 37 31 31 41 33 42 39 43 42 39 30 46 34 32 45 30 44 39 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 36 45 42 36 32 45 35 46 43 45 33 36 31 31 44 42 38 46 39 44 46 35 35 43 34 37 43 39 32 32 35 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e Data Ascii: 181E9AD56025B5F22</rdf:li> <rdf:li>uiuid:6DD7E686FBF5DE11B1BD9D67C8186AB3</rdf:li> <rdf:li>uiuid:6E47E0D0A3C911DD990ED023CA6AD342</rdf:li> <rdf:li>uiuid:6E778F85D1C6E711A3B9CB90F42E0D9E</rdf:li> <rdf:li>uiuid:6EB62E5FCE3611DB8F9DF55C47C92251</rdf:li> <rdf:li>
2022-04-08 08:02:42 UTC	2927	IN	Data Raw: 32 43 44 35 45 38 32 45 31 44 43 30 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 39 45 33 33 38 39 36 32 46 44 38 36 45 30 31 31 39 41 37 41 42 41 42 42 31 34 39 42 30 43 31 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 39 45 35 32 41 32 46 45 33 46 45 39 44 31 31 42 38 42 30 38 39 43 44 43 34 31 45 30 41 42 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 39 45 36 37 44 38 4 2 43 37 38 39 31 31 44 44 42 39 46 41 45 43 43 37 33 32 38 42 39 30 37 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 39 45 38 45 46 37 46 43 31 45 31 33 44 46 31 31 42 39 39 38 42 45 37 38 37 33 42 37 44 39 31 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 Data Ascii: 2CD5E82E1DC0F</rdf:li> <rdf:li>uiuid:9E338962FD86E0119A7ABABB149B0C14</rdf:li> <rdf:li>uiuid:9E52A2FE3FE9DD11B8B089CDC41E0AB4</rdf:li> <rdf:li>uiuid:9E667DB8C78911DDB9FAECC7328B9072</rdf:li> <rdf:li>uiuid:9E8EF7FC1E13DF11B998BE7873B7D910</rdf:li> <rdf:li>uiuid
2022-04-08 08:02:42 UTC	2943	IN	Data Raw: 32 44 44 31 31 41 46 36 45 44 46 46 32 38 33 34 46 46 38 37 31 33 33 37 42 33 45 45 46 35 45 44 45 34 38 30 31 31 32 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 44 42 38 30 39 46 35 34 38 43 43 31 44 46 31 31 39 44 34 46 39 41 30 46 38 38 34 35 35 34 32 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 44 42 42 37 38 44 30 38 35 30 39 34 31 31 45 30 41 43 37 39 45 39 34 34 34 37 36 32 33 38 38 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 44 42 42 38 35 30 41 32 44 46 35 34 31 31 44 45 41 45 31 42 42 32 44 33 35 39 33 44 31 43 44 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 Data Ascii: 2DD11AF6EDFF2834FF873</rdf:li> <rdf:li>uiuid:DB7654BDB8CE311B3EEF5EDE4801126</rdf:li> <rdf:li>uiuid:DB809F548CC1DF119D4F9A0F88455424</rdf:li> <rdf:li>uiuid:DBB78D08509411E0AC79E94447623889</rdf:li> <rdf:li>uiuid:DBB850A2DF5411DEAE1BB2D3593D1CDB</rdf:li> <rdf
2022-04-08 08:02:42 UTC	2951	IN	Data Raw: 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 46 37 42 30 35 33 38 39 30 36 35 37 31 31 44 43 39 32 36 46 46 42 34 37 39 38 36 37 34 37 42 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 46 37 44 36 32 32 44 42 30 46 33 35 45 34 31 31 38 45 31 43 42 30 42 31 41 46 43 36 45 41 42 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 46 38 31 45 39 42 43 39 39 37 38 41 44 45 31 31 39 36 41 30 45 46 46 39 35 30 39 36 30 45 31 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 46 38 33 41 30 44 43 34 32 34 33 31 45 30 31 31 39 37 36 38 44 45 32 46 35 32 31 31 32 46 36 42 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 75 75 69 64 3a 46 38 36 34 39 43 36 33 31 43 43 45 30 31 31 42 33 46 Data Ascii: i> <rdf:li>uiuid:F7B05389065711DC926FFB47986747B2</rdf:li> <rdf:li>uiuid:F7D622DB0F35E4118E1CBB01AFC6EAB7</rdf:li> <rdf:li>uiuid:F81E9BC9978ADE1196A0EFF950960E15</rdf:li> <rdf:li>uiuid:F83A0DC42431E0119768DE2F52112F6B</rdf:li> <rdf:li>uiuid:F8649C631CCCE011B3F
2022-04-08 08:02:42 UTC	2959	IN	Data Raw: 37 32 30 36 38 31 31 38 46 36 32 45 45 36 34 43 45 43 33 33 43 45 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 31 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 46 36 32 46 32 46 43 42 36 34 38 32 35 38 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 31 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 46 36 32 46 39 34 35 31 33 33 36 34 36 36 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 31 38 30 31 31 37 34 30 37 32 30 36 38 31 31 39 30 31 46 45 37 44 37 35 42 43 34 32 42 36 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 31 38 30 31 31 37 34 30 37 32 30 36 38 31 31 39 30 32 41 44 33 46 42 37 38 45 46 44 44 46 39 Data Ascii: 72068118F62EE64CEC33CEF</rdf:li> <rdf:li>xmp.did:01801174072068118F62F2FCB6482589</rdf:li> <rdf:li>xmp.did:01801174072068118F62F94513364662</rdf:li> <rdf:li>xmp.did:0180117407206811901FE7D75BC42B61</rdf:li> <rdf:li>xmp.did:0180117407206811902AD3FB78EFDFF9
2022-04-08 08:02:42 UTC	2975	IN	Data Raw: 34 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 30 38 33 44 41 36 34 45 38 41 44 44 41 45 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 34 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 30 38 33 45 46 43 32 32 32 36 38 46 32 33 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 34 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 30 38 33 46 37 36 41 34 38 42 45 35 34 41 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 34 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 32 32 41 39 34 39 44 42 46 46 32 30 45 30 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 34 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 32 32 41 46 36 36 Data Ascii: 4801174072068118083DA64E8ADDAE9</rdf:li> <rdf:li>xmp.did:04801174072068118083EFC22268F23E</rdf:li> <rdf:li>xmp.did:04801174072068118083F76A48BE54AC</rdf:li> <rdf:li>xmp.did:0480117407206811822A949DBFF20E03</rdf:li> <rdf:li>xmp.did:0480117407206811822AAF66

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:42 UTC	2991	IN	Data Raw: 39 42 32 37 36 38 31 31 39 35 46 45 41 32 35 42 42 30 46 43 43 38 45 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 39 36 34 45 41 36 46 36 30 41 35 45 31 31 31 41 30 39 31 41 30 36 32 30 41 36 46 42 39 39 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 39 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 30 38 33 38 32 45 31 35 31 38 31 41 36 31 46 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 39 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 30 38 33 38 43 33 30 35 44 43 41 39 45 38 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 39 38 30 31 31 37 34 30 37 32 30 36 38 31 31 38 30 38 33 38 44 37 43 36 34 31 46 37 38 35 Data Ascii: 9B27681195FEA25BB0FCC8E8</rdf:li> <rdf:li>xmp.did:0964EA6F60A5E111A091A0620A6FB99C</rdf:li> <rdf:li>xmp.did:0980117407206811808382E15181A61F</rdf:li> <rdf:li>xmp.did:098011740720681180838C305DCA9E89</rdf:li> <rdf:li>xmp.did:098011740720681180838D7C641F785
2022-04-08 08:02:42 UTC	2999	IN	Data Raw: 63 66 36 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 62 64 65 37 61 35 35 2d 34 38 35 31 2d 34 35 64 63 2d 39 31 33 38 2d 34 34 37 30 37 62 34 38 61 34 64 61 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 62 65 61 61 64 62 31 2d 64 61 31 33 2d 34 31 37 38 2d 62 30 32 39 2d 65 30 31 36 64 30 31 38 38 66 37 61 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 63 30 36 33 64 63 32 2d 31 66 31 32 2d 34 61 33 31 2d 38 38 38 64 2d 66 30 32 35 63 36 63 64 64 39 64 62 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 30 63 31 64 64 61 33 65 2d 39 35 63 39 2d 63 34 34 63 2d 61 66 33 30 2d 36 30 35 30 63 34 61 66 63 62 31 34 3c 2f 72 Data Ascii: cf61</rdf:li> <rdf:li>xmp.did:0bde7a55-4851-45dc-9138-44707b48a4da</rdf:li> <rdf:li>xmp.did:0beaadb1-da13-4178-b029-e016d0188f7a</rdf:li> <rdf:li>xmp.did:0c063dc2-1f12-4a31-888d-f025c6cdd9db</rdf:li> <rdf:li>xmp.did:0c1dda3e-95c9-c44c-af30-6050c4afcbb14</r
2022-04-08 08:02:42 UTC	3015	IN	Data Raw: 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 63 66 32 32 34 38 37 2d 33 65 33 64 2d 34 62 39 32 2d 38 62 66 62 2d 66 37 65 61 39 36 39 33 32 65 65 62 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 64 38 65 30 66 35 31 2d 65 35 31 64 2d 38 37 34 39 2d 38 35 62 34 2d 35 33 34 64 66 34 37 31 64 39 31 64 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 64 63 33 65 61 38 37 2d 64 35 65 62 2d 34 61 34 30 2d 62 37 36 31 2d 34 35 39 33 36 33 66 64 37 34 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 31 64 65 39 66 31 35 36 2d 37 38 36 32 2d 33 33 34 62 2d 38 34 35 38 2d 38 32 31 31 62 62 61 61 64 32 36 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 Data Ascii: :li>xmp.did:1cf22487-3e3d-4b92-8bfb-f7ea96932eeb</rdf:li> <rdf:li>xmp.did:1d8e0f51-e51d-8749-85b4-534df4719d</rdf:li> <rdf:li>xmp.did:1dc3ea87-d5eb-4a40-b761-4593636f4740</rdf:li> <rdf:li>xmp.did:1de9f156-7862-334b-8458-8211bbaad267</rdf:li> <rdf:li>xmp
2022-04-08 08:02:43 UTC	4472	IN	Data Raw: 42 44 39 38 43 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 61 31 39 32 33 36 34 2d 38 33 32 36 2d 64 64 34 61 2d 61 64 64 31 2d 39 64 34 62 39 31 33 37 64 62 37 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 61 35 65 66 37 61 65 2d 66 38 37 62 2d 34 38 34 65 2d 38 62 38 31 2d 63 39 62 38 36 64 30 34 61 63 64 66 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 61 38 65 66 65 30 37 2d 65 36 66 33 2d 33 65 34 62 2d 61 61 35 38 2d 30 64 33 36 34 35 31 37 65 64 65 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 32 61 61 33 37 30 31 34 2d 38 31 65 66 2d 65 37 34 36 2d 62 37 33 64 2d 36 64 33 37 61 66 61 64 34 37 36 61 3c Data Ascii: BD98C8</rdf:li> <rdf:li>xmp.did:2a192364-8326-dd4a-add1-9d4b9137db72</rdf:li> <rdf:li>xmp.did:2a5ef7ae-f87b-484e-8b81-c9b86d04acdf</rdf:li> <rdf:li>xmp.did:2a8efe07-e6f3-3e4b-aa58-0d364517ede8</rdf:li> <rdf:li>xmp.did:2aa37014-81ef-e746-b73d-6d37afad476a<
2022-04-08 08:02:43 UTC	4480	IN	Data Raw: 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 35 34 39 62 39 38 34 2d 39 38 35 32 2d 34 35 39 62 2d 39 64 36 38 2d 38 61 38 35 39 37 61 65 31 35 37 37 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 35 35 34 33 44 35 33 33 37 32 30 36 38 31 31 38 33 44 31 42 35 32 46 39 35 36 32 43 46 31 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 35 36 30 30 62 37 35 2d 37 65 31 36 2d 34 38 32 66 2d 39 35 38 32 2d 63 66 33 64 61 61 33 35 62 35 66 33 63 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 33 35 36 34 63 63 35 33 2d 66 66 65 36 2d 34 35 34 31 2d 61 35 39 63 2d 35 39 36 66 34 66 30 62 35 37 31 61 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a Data Ascii: f:li> <rdf:li>xmp.did:3549b984-9852-459b-9d68-8a8597ae1577</rdf:li> <rdf:li>xmp.did:35543D533720681183D1B52F9562CF1A</rdf:li> <rdf:li>xmp.did:35600b75-7e16-482f-9582-cf3daa35b56c</rdf:li> <rdf:li>xmp.did:3564cc53-ffe6-4541-a59c-596f4f0b571a</rdf:li> <rdf:
2022-04-08 08:02:43 UTC	4496	IN	Data Raw: 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 33 39 31 31 32 45 42 37 44 32 31 36 38 31 31 38 44 42 42 44 35 38 42 45 31 36 45 39 35 35 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 33 45 30 43 37 45 41 37 37 32 30 36 38 31 31 38 32 32 41 39 35 36 38 31 41 44 34 43 34 35 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 33 45 32 35 30 31 31 34 30 43 38 45 31 31 31 41 46 38 42 41 32 37 33 30 46 46 45 31 32 38 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 34 33 46 37 34 45 30 38 31 44 32 30 36 38 31 31 41 34 38 32 46 37 45 33 32 32 39 42 31 31 30 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 Data Ascii: /rdf:li> <rdf:li>xmp.did:439112EB7D2168118DBBD58BE16E9552</rdf:li> <rdf:li>xmp.did:43E0C7EA77206811822A95681AD4C455</rdf:li> <rdf:li>xmp.did:43E2501140C8E111AF8BA2730FFE128C</rdf:li> <rdf:li>xmp.did:43F74E081D206811A482F7E3229B110C</rdf:li> <rdf:li>xmp.di
2022-04-08 08:02:43 UTC	4512	IN	Data Raw: 45 34 46 35 44 44 46 31 31 41 46 44 45 45 42 36 45 33 43 39 35 37 35 35 32 3f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 32 65 62 37 30 31 39 2d 34 64 64 39 2d 37 31 34 30 2d 61 65 39 35 2d 62 39 63 34 38 37 64 39 65 62 63 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 33 31 45 37 43 32 31 46 33 45 30 44 46 31 31 39 35 38 33 44 31 34 39 39 41 33 36 38 36 46 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 33 34 34 37 33 61 35 2d 35 61 37 30 2d 37 33 34 38 2d 62 30 65 34 2d 33 37 33 35 37 64 32 66 38 36 30 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 33 36 33 39 44 36 30 44 38 33 33 45 32 31 31 39 45 39 36 45 44 Data Ascii: E4F5DDF11AFDEEEB6E3C95755</rdf:li> <rdf:li>xmp.did:52eb7019-4dd9-7140-ae95-b9c487d9ebc2</rdf:li> <rdf:li>xmp.did:531E7C21F3E0DF119583D1499A3686FD</rdf:li> <rdf:li>xmp.did:534473a5-5a70-7348-b0e4-37357d2f8605</rdf:li> <rdf:li>xmp.did:53639D60D833E2119E96ED
2022-04-08 08:02:43 UTC	4520	IN	Data Raw: 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 42 37 36 31 32 44 44 43 38 31 45 45 32 31 31 42 43 33 39 44 42 39 41 41 33 39 42 46 37 42 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 42 37 43 38 44 39 38 31 32 32 30 36 38 31 31 38 38 43 36 42 41 33 36 38 31 45 46 45 44 33 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 42 39 35 42 38 41 35 37 44 32 30 36 38 31 31 39 32 42 30 44 30 41 37 35 38 31 35 46 38 41 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 42 39 41 36 36 35 45 43 33 38 36 31 31 45 35 39 30 39 35 38 30 39 46 34 37 42 34 34 30 41 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 35 42 41 34 37 34 44 41 31 37 Data Ascii: f:li>xmp.did:5B7612DDC81EE211BC39DB9AA39BF7B0</rdf:li> <rdf:li>xmp.did:5B7C8D981220681188C6BA3681EFED35</rdf:li> <rdf:li>xmp.did:5B95B8A57D20681192B0D0A7581F58A6</rdf:li> <rdf:li>xmp.did:5B9A665EC38611E59095809F47B440A2</rdf:li> <rdf:li>xmp.did:5BA474DA17

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:43 UTC	4528	IN	Data Raw: 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 32 43 31 33 44 37 34 43 33 32 30 36 38 31 31 42 45 33 33 45 44 33 44 43 44 31 32 32 39 38 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 32 46 35 35 44 39 46 31 35 30 46 45 30 31 31 41 38 46 43 39 37 43 37 46 38 42 44 31 39 30 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 32 46 44 30 34 32 41 46 41 32 31 36 38 31 31 39 32 37 37 39 35 38 43 42 34 32 45 43 43 36 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 32 62 34 33 39 34 66 2d 39 36 31 34 2d 66 66 34 31 2d 61 32 32 35 2d 30 34 39 61 35 35 35 61 30 33 39 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 36 32 62 63 Data Ascii: rdf:li>xmp.did:62C13D74C3206811BE33ED3DCD122986</rdf:li> <rdf:li>xmp.did:62F55D9F150FE011A8FC97C7F8BD1909</rdf:li> <rdf:li>xmp.did:62FD042AFA2168119277958CB42ECC64</rdf:li> <rdf:li>xmp.did:62b4394f-9614-ff41-a225-049a555a0393</rdf:li> <rdf:li>xmp.did:62bcb
2022-04-08 08:02:43 UTC	4544	IN	Data Raw: 46 31 38 42 46 31 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 31 32 35 44 35 41 33 46 42 44 36 45 32 31 31 39 38 35 31 43 35 35 44 35 33 34 44 42 39 34 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 31 33 37 36 63 30 37 2d 62 33 63 2d 34 37 37 30 2d 38 38 36 30 2d 30 65 63 34 34 34 62 34 37 34 63 32 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 3 7 31 34 46 36 43 30 42 45 32 32 30 36 38 31 31 38 38 43 36 41 38 34 31 45 42 33 39 31 37 45 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 37 31 34 62 35 36 62 61 2d 36 66 64 35 2d 37 34 34 32 2d 62 34 36 65 2d 30 31 33 62 35 30 61 33 31 63 36 33 3c 2f 72 64 66 3a 6c 69 Data Ascii: F18BF1D</rdf:li> <rdf:li>xmp.did:7125D5A3FBD6E2119851C55D534DB94A</rdf:li> <rdf:li>xmp.did:71376c07-b3c8-4770-8860-0ec444b474c2</rdf:li> <rdf:li>xmp.did:714F6C0BE220681188C6A841EB3917E3</rdf:li> <rdf:li>xmp.d id:714b56ba-6fd5-7442-b46e-013b50a31c63</rdf:li>
2022-04-08 08:02:43 UTC	4560	IN	Data Raw: 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 31 41 31 31 41 33 32 32 42 32 30 36 38 31 31 39 31 30 39 44 30 32 42 35 46 42 46 31 44 44 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 31 42 38 33 45 45 33 34 42 32 30 36 38 31 31 39 35 46 45 45 36 33 31 37 42 35 44 41 41 42 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 31 42 42 43 36 36 33 44 44 34 44 46 31 31 39 46 34 33 41 42 35 46 33 35 45 37 39 30 35 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 31 42 44 43 45 44 41 35 32 32 30 36 38 31 31 38 45 42 37 41 33 39 38 38 32 35 38 39 33 35 33 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 31 43 34 37 34 31 39 44 Data Ascii: df:li>xmp.did:81A11A322B2068119109D02B5FBF1DD6</rdf:li> <rdf:li>xmp.did:81B83EE34B20681195FEE6317B5DAABD</rdf:li> <rdf:li>xmp.did:81BBC663DD04DF119F43AB5F35E79051</rdf:li> <rdf:li>xmp.did:81BDCEDA522068118EB7A39882589353</rdf:li> <rdf:li>xmp.did:81C47419D
2022-04-08 08:02:43 UTC	4567	IN	Data Raw: 69 3e 78 6d 70 2e 64 69 64 3a 38 38 33 44 36 39 45 30 31 41 32 30 36 38 31 31 38 32 32 41 43 30 33 41 31 31 41 43 37 31 42 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 38 33 46 39 30 35 38 30 38 32 30 36 38 31 31 38 44 42 42 43 39 35 31 43 32 42 30 33 31 39 45 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 38 34 35 37 65 66 34 2d 39 66 34 35 2d 36 35 34 61 2d 62 33 36 30 2d 61 62 66 62 37 66 63 66 62 34 33 63 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 38 35 30 35 35 32 32 30 44 32 30 36 38 31 31 41 46 46 44 38 36 43 31 32 37 44 41 30 35 31 36 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 38 38 35 39 35 35 36 30 34 Data Ascii: i>xmp.did:883D69E01A206811822AC03A11AC71BC</rdf:li> <rdf:li>xmp.did:883F9058082068118DBB C951C2B0319E</rdf:li> <rdf:li>xmp.did:88457ef4-9fd5-654a-b360-abfb7fcfb43c</rdf:li> <rdf:li>xmp.did:885055220D 206811AFFD86C127DA0516</rdf:li> <rdf:li>xmp.did:885955604
2022-04-08 08:02:43 UTC	4583	IN	Data Raw: 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 39 35 45 35 43 36 32 43 32 34 32 30 36 38 31 31 38 30 38 33 42 46 44 39 41 39 46 38 31 37 33 30 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 39 35 45 39 44 37 44 32 31 33 32 30 36 38 31 31 38 30 38 33 45 44 43 46 30 37 45 34 31 37 31 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 39 35 62 32 34 65 35 39 2d 64 35 33 39 2d 63 31 34 38 2d 62 62 34 38 2d 65 32 31 64 34 62 36 66 31 34 31 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 39 35 62 37 37 32 61 34 2d 61 66 39 33 2d 34 61 31 63 2d 61 38 63 31 2d 64 34 39 32 37 32 30 30 65 38 37 62 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 Data Ascii: li> <rdf:li>xmp.did:95E5C62C242068118083BFD9A9F81730</rdf:li> <rdf:li>xmp.did:95E9D7D2132068118083 EDCF07E41711</rdf:li> <rdf:li>xmp.did:95b24e59-d539-c148-bb48-e21d4b6f1414</rdf:li> <rdf:li>xmp.did:95b772a4-af93-4a1c-a8c1-d4927200e87b</rdf:li> <rdf:li>xmp
2022-04-08 08:02:43 UTC	4599	IN	Data Raw: 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 41 37 45 31 42 44 34 31 45 34 32 30 36 38 31 31 41 36 31 33 44 42 32 36 39 46 45 46 35 32 34 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 41 37 45 32 30 32 43 43 44 31 32 31 36 38 31 31 41 42 30 38 45 41 43 46 43 36 39 44 46 39 43 38 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 41 37 45 46 42 38 44 39 42 32 32 3 1 36 38 31 31 38 41 36 44 45 33 32 44 43 45 37 38 35 34 30 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 41 38 30 37 45 30 43 42 46 44 39 44 45 31 31 31 41 44 44 32 39 42 36 38 34 45 34 35 45 35 38 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 Data Ascii: </rdf:li> <rdf:li>xmp.did:A7E1BD41E4206811A613DB269FEF524D</rdf:li> <rdf:li>xmp.did:A7E202CCD12168 11AB08EACFC69DF9C8</rdf:li> <rdf:li>xmp.did:A7EFB8D9B22168118A6DE32DCE785405</rdf:li> <rdf:li>xmp.di d:A807E0CBFD9DE111ADD29B684E45E581</rdf:li> <rdf:li>xmp.d
2022-04-08 08:02:43 UTC	4607	IN	Data Raw: 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 44 32 45 39 31 41 30 42 36 32 34 36 38 31 31 39 39 34 43 39 43 32 36 34 30 41 41 46 36 46 31 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 34 42 42 33 34 33 33 42 44 32 30 36 38 31 31 38 46 36 32 39 44 45 37 37 36 30 32 38 45 34 44 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 34 42 45 32 37 32 33 39 44 32 31 36 38 31 31 41 39 36 31 39 44 42 31 33 39 36 42 31 43 42 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 34 43 34 38 45 45 41 36 30 32 43 36 38 31 31 38 41 36 44 45 30 42 34 33 44 34 35 35 46 42 39 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 42 34 46 Data Ascii: li> <rdf:li>xmp.did:B4B591A0B6246811994C9C2640AAF6F1</rdf:li> <rdf:li>xmp.did:B4BB3433BD 2068118F629DE776028E4D</rdf:li> <rdf:li>xmp.did:B4BE27239D216811A9619DB1396B1CBC</rdf:li> <rdf:li>xm p.did:B4C48EEA602C68118A6DE0B43D455FB9</rdf:li> <rdf:li>xmp.did:B4F
2022-04-08 08:02:43 UTC	4623	IN	Data Raw: 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 43 43 44 36 44 30 45 32 44 33 32 30 36 38 31 31 41 46 46 44 46 37 30 36 45 37 34 32 36 31 30 41 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 43 43 46 37 37 30 45 37 32 32 32 30 36 38 31 31 39 37 41 35 46 43 37 42 34 41 33 32 36 34 42 35 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 43 43 46 39 30 36 38 31 31 33 32 30 36 38 31 31 38 43 31 34 43 44 31 31 34 32 30 30 31 44 33 34 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 43 44 30 32 37 36 37 39 39 34 46 44 44 46 31 31 39 39 31 45 42 38 45 43 43 36 31 42 43 33 37 43 3c 2f 72 64 66 3a 6c 69 3e 20 3c 72 64 66 3a 6c 69 3e 78 6d 70 2e 64 69 64 3a 43 44 30 39 Data Ascii: f:li>xmp.did:CCD6D0E2D3206811AFFDF706E742610A</rdf:li> <rdf:li>xmp.did:CCF770E7222068119 7A5FC7B4A3264B5</rdf:li> <rdf:li>xmp.did:CCF90685132068118C14CD1142001D34</rdf:li> <rdf:li>xmp.did:C D02767994FDDF11991EB8ECC61BC37C</rdf:li> <rdf:li>xmp.did:CD0B04DC09

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:03 UTC	8021	IN	Data Raw: 86 7f bb f3 67 fa 56 3f 8a 3c 59 1a 69 ab 2e 89 a2 cd 6d 3c 73 85 69 f7 6e 4f 2d ba e4 1e a4 d7 17 79 f0 d5 fc 41 1e fb 79 e4 58 a4 51 b5 a7 93 62 2a 31 c9 04 0e c3 fa d6 b4 a8 46 ab 53 af 2e 5b b3 6a 73 e6 b9 e9 32 78 86 cf 5a 86 e6 de ca e6 39 67 81 43 79 fb b6 a3 29 c7 7f 5a b5 61 18 86 dd a5 b4 b9 83 6c bf 2c ab f7 d7 af 1c 1f e7 58 ba 6f c0 3d 66 df 43 b3 9f 44 d4 6d 96 26 88 6f dd 26 d5 f7 c0 c7 cc bf 5a e3 2e 75 6b cf 0f 47 2c 49 73 1e af 71 b8 c7 2d cd a7 cc 92 60 ff 00 0d 5c 70 b4 6a 5e 38 7a 97 fc fe 7a 58 b5 18 37 ca d9 eb 36 7a 3c 09 6e d2 69 eb 04 8d ca dc c0 cd f7 54 fb 57 94 4d fb 3f bb df 24 af ac c9 f6 7b 95 f9 ad a7 80 ec 65 f7 e7 3d 7a 30 e2 b0 ae 3c 41 ab dc 4d 67 a8 e9 7b 74 cb cb 19 3c c9 16 09 0e d9 94 fd ed de 9f 8d 7a af fc 2d 4d Data Ascii: gV?<Yi.m<sinO-yAyXQb*1FS.[js2xZ9gCy)Zal,Xo=fCDm&o&Z.ukG,lsq-`pj^8zzX76z<niTWM?\$(e=z0<AMg{t<z-M
2022-04-08 08:03:03 UTC	8029	IN	Data Raw: eb c2 e5 67 95 e7 58 92 78 fe 5b 95 53 b9 57 dc 74 15 75 66 dd 66 c9 e7 ac f2 ed 65 6d df c5 fe d1 fa d7 2a 8b 8b 36 e6 e6 56 32 df 58 fb 4a ce 12 05 58 1a 23 e5 37 f7 bf 5a e2 ed 7c bb 1b c8 a3 b8 f3 d9 a7 6d bb 96 4f 95 57 b9 ff 00 1a d1 b8 bc 29 79 04 52 7e e1 f7 48 d2 ed f9 b6 b6 48 1c 56 dd b7 86 46 a1 63 13 f9 ab 3b 46 c5 9a 46 5f 9b 77 e1 5d 89 f2 69 d0 e7 b5 ce 4e ff 00 4f 09 7d 18 b2 58 f6 f9 89 b5 64 5d ad b4 9e 71 ed 5d bd b4 76 fa 5e 93 3c 76 6a b2 df c9 89 76 c7 fc 5d b0 4f b7 35 cf eb 16 69 a3 c8 a2 ed bc f9 64 6f dd ed 6d cc bc fa e6 b6 7c 3f e2 08 6c 2e 27 b3 92 0f b3 2a b0 fd ff 00 f0 c9 9e a7 f0 ad 7e 2d 48 d2 2d dc d5 d3 f5 cb 84 d3 6d be cf 16 d8 27 8b 76 e9 3f 96 0f 7f ce b3 b5 8b 51 ab 5b cf 24 12 c8 d2 c9 98 a3 8f ee ff 00 0f 7f a5 Data Ascii: gX[SWtuffem*6V2XJX#7Z]mOW)yR-HHVFc;FF_wj]NO]Xd]q]v^<vjv]O5idom]?!.^*--H-m'v?Q[\$
2022-04-08 08:03:03 UTC	8045	IN	Data Raw: 8b 4a fb 9a ed 60 0b e4 b7 50 3b 1f 6a a7 aa e9 bf 66 ba b5 93 50 69 23 b2 91 b7 32 cd b2 33 af d7 70 3d 7d 2b a1 4d 4e 4a 33 e8 bd 1b d3 f1 fb ae 54 5f 31 b9 61 75 2c 90 f9 b6 57 8b 3d cc a9 ff 00 2c 5b 67 4f 43 da b9 7d 4a 39 9e 47 b7 d4 74 d9 e5 b8 9e 41 2d b3 43 72 15 63 71 df 07 82 fe d9 ad 6b 7b 5b 2d 26 e3 cf b3 58 20 13 e2 55 dc db 95 94 12 0b 03 e8 7d 05 55 b3 d3 ed b5 b9 a7 d3 af 37 58 a3 29 55 65 53 fb b7 3d 0f bd 45 2b 53 93 97 4f c5 7d dd 8d 95 36 d1 87 73 a6 4b e2 0d 3d 62 99 96 3b ad bb 93 76 36 af 3f c5 b7 96 07 f4 35 cb 27 8c 93 4f b7 5d 1b 59 9e e6 7f 2d 8c 53 41 b5 dd 63 c1 f9 73 91 85 02 bd 07 4b d0 4f 86 21 51 2b 36 af 7e b1 6c 6b 99 98 ef 5c 13 df 38 fd 2b 1a eb 4d d1 f5 2f de fd 9a 3b 3b a9 0f ef 5a 3f 97 f0 60 09 e4 fb d7 ab 46 bd Data Ascii: J'P:jfP#23p=)+MNJ3T_1au,W=,[gOC)J9GtA-Crcqk{[-&X U)U7X)UeS=E+SO)6sK=b;v6?5'O]Y-SAcSKO!Q+6-lkl8+M/;Z?'F
2022-04-08 08:03:03 UTC	8061	IN	Data Raw: 5e 66 e5 b7 39 cf cc 7e 99 ab e5 84 9c 95 27 7e df f0 47 f0 ab 9d 87 84 e6 97 50 b7 92 ee 48 96 28 99 82 6d 5c ab 7b fa d5 bd 7b 41 b1 96 de 71 24 b1 da ee 5f 9a 4f ba cb f8 fb d7 9e 69 fe 2f bb ba 99 8d a4 dd 15 d9 e4 93 0b f3 77 cf a5 3e 6f 11 46 da 0d e1 9e eb ed 32 dc a0 55 f9 b7 2f 5e 7e b5 cb 2c 15 65 5b 9d 3b 6a b4 40 df 32 29 5a e9 f7 9a 5c 73 f9 51 79 8b 3e 76 79 1f 33 f9 60 73 83 e9 5c 60 d5 97 5a 91 60 b8 b3 5b 34 56 0a d2 2b 57 63 a4 ea 36 f6 3a 6b 49 b5 a7 0c bf 3a b3 7c bb 45 45 36 8f 67 e2 79 95 ad 60 5b 30 ff 00 3f 97 1a ed 5e 95 f4 14 aa 2a 72 93 a8 be 7e 84 c7 72 ce 9f a7 e9 71 e9 7e 7c 0d e6 b4 0b b7 6a c7 fc 67 d3 35 56 3d 1e d2 35 bc 8e 68 96 34 97 1b d9 5b 73 6e 1e f5 a5 ac 58 cd 67 63 6f 67 04 7f 2c 6b b9 bf bd 27 19 c6 45 72 1a 86 Data Ascii: ^f9-^-GPH(m\{(Aq\$ _Oi/w>oF2U/^~,e:[j@2)ZlsQy>vy3's\`Z'[4V+Wc6:kl: EE6gy'[0?^*r-rq~ljg5V=5h4[snXgcog ,k'Er
2022-04-08 08:03:03 UTC	8069	IN	Data Raw: 3e 6c 0e 9c 74 e2 b5 97 4f 7b b5 56 75 55 f3 14 c1 2e dc 76 f9 86 e2 79 23 1d 2b d2 94 a5 18 f2 d4 d9 ff 00 56 25 bb e8 6f e9 fe 22 fe dd 56 31 35 dd 8a 2f c8 b2 4f 1e e7 6c 9f ee 8f 94 7f 4a c2 9a 3b 88 f5 48 ae 2e 23 5b 94 8d 4e ed 42 38 f7 4b 1f a4 6d ec 7a e6 a6 f2 de c2 ea 0f bb e4 ac 7b 57 cb c3 36 df 75 38 f9 ab 45 fc 41 6f f6 36 86 46 dd f6 85 dd f3 46 15 97 d8 f6 22 bc ae 55 4a 57 a7 1b a6 47 2a e8 54 8e 7d 07 47 f2 a4 9e 45 fb 39 60 ed 69 e6 3c 7e 71 ff 00 64 74 6f a5 49 65 27 db 35 09 2d af 2c d5 52 f1 76 c5 1e d1 b6 64 27 8d e3 9e 87 bf 53 e9 5c f5 f5 fa 5b 5f 35 bd b6 95 1d cc bf eb 1f 72 97 69 07 63 9e d8 e7 81 5d 17 86 f5 8b 3d 5b cd 26 c6 e5 b5 18 d5 16 48 f7 6d 4e bd 46 0e 72 3d ea ea 53 94 21 cf 66 fe 7f 77 5d 0c f9 59 e1 de 36 d1 53 c3 Data Ascii: >ltO{VuU.vy#+V%o"V15/OIJ;H.#[NB8Kmz[W6u8EAo6FF"UJWG*T]GE9' i<~< qdtol e'5-,Rvd'S\[_5ric]= [&H mNFr=S!fw]Y6S

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49981	23.35.236.56	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:19 UTC	17	OUT	GET /fs/windows/config.json HTTP/1.1 Connection: Keep-Alive Accept: */* Accept-Encoding: identity If-Unmodified-Since: Thu, 20 Apr 2017 16:10:39 GMT User-Agent: Microsoft BITS/7.8 Host: fs.microsoft.com
2022-04-08 08:02:19 UTC	17	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Thu, 20 Apr 2017 16:10:39 GMT ETag: "f9c874a7f0b9d21:0" Server: Microsoft-IIS/10.0 Content-Disposition: attachment; filename=config.json X-Powered-By: ASP.NET Cache-Control: public, max-age=222061 Date: Fri, 08 Apr 2022 08:02:19 GMT Content-Length: 55 Connection: close X-CID: 2
2022-04-08 08:02:19 UTC	17	IN	Data Raw: 7b 22 66 6f 6e 74 53 65 74 55 72 69 22 3a 22 66 6f 6e 74 73 65 74 2d 32 30 31 37 2d 30 34 2e 6a 73 6f 6e 22 2c 22 62 61 73 65 55 72 69 22 3a 22 66 6f 6e 74 73 22 7d Data Ascii: {"fontSetUri":"fontset-2017-04.json","baseUri":"","fonts"}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49999	20.82.210.154	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:05 UTC	8081	OUT	GET /v3/Delivery/Placement?pubid=da63df93-3dbc-42ae-a505-b34988683ac7&pid=310091&adm=2&w=1&h=1&wpx=1&hpx=1&fmt=json&cltp=app&dim=le&rafb=0&nct=1&pm=1&cfmt=text,image,poly&sft=jpeg,png,gif&topt=1&poptin=0&localid=w:472DC600-FEAB-E7F8-720D-1E33F00FD1E7&ctry=US&time=20220408T170305Z&lc=en-US&pl=en-US&idtp=mid&uid=4388269c-b420-4134-ac19-bc7ca8a19ac1&aid=00000000-0000-0000-0000-000000000000&ua=WindowsShellClient%2F9.0.40929.0%20%28Windows%29&asid=d45161c0491847028507c79db5d70c07&ctmode=MultiSession&arch=x64&cdm=1&cdmver=10.0.17134.1&devfam=Windows.Desktop&devform=Unknown&devosver=10.0.17134.1&disp horzres=1280&dispsize=17.1&dispvertres=1024&isu=0&lo=1463022&metered=false&nettype=ethernet&npid=sc-310091&oemName=hsehht%2C%20Inc.&oemid=hsehht%2C%20Inc.&ossku=Professional&rver=2&smBiosDm=hsehht%2C1&tl=2&tsu=1463022&waasBldFlt=1&waasCfgExp=1&waasCfgSet=1&waasRetail=1&waasRing= HTTP/1.1 Accept-Encoding: gzip, deflate X-SDK-CACHE: chs=0&imp=0&chf=0&ds=50583&fs=32319&sc=6 X-SDK-HW-TOKEN: t=EwDYAppeBAAUIAKXDAoFTQM+n+MaRVFKZh/ehWgAAdVW0iu23GlxRyUBGA+V5LMOU/IMaTj obBnQosoTe6w30OZEf3HulBKeYXog3CqxSfjOHeF/J4iLS/gKyhq/ZV/xtrYHZ35PhcBmS2qzlwNBiXp0+I4efq5ns DEEESEQ06VT9dPxHYgWIFLG65LRysydA1IM9dDPzftFvDLM/ickJDFevqkA3hG2mKV46lqHL4CT7eP4Hk0/MorRp8JB 5tew/lJ7o25TIEcXl9Ohbx1KlwUuqQcpj0nfdAUZEjkQqVS2z/wQaH+/fdlFO/AoxQl3Cbc0TeaCp3XlesBJX0bxVN zc22qQqCPfGWQ/Sb52rGvkqBRvdW8DFg8ToMjfqPyDZgAAACE3mODPOPAwVqAFPV53gZzc0aOkGu+jjWn w46hEU9aCKlpEDkH6SywZSj+Z6lyumM/ZCz1/Exb6MZih9PGVRFVdS4rZOFTTsEXw5x6gJoWeqkJZJqul+/LQNZp daM/TGNQWWhUnnbhyzuL3J52vfTsZzAtC6HDHUtfcP567luQfNjw1zOBQG/Pho8+d+FIHWtcPKMXaDH+rX7PpfIRpHT m7bd+I+rsPvLvdstjafDcGAADV0pkaM4oU0n35rzdjzoAWTcazcHXkrs0Gr34gDLPkE96nUwLpeDlXN3LOntP44gHn gFTJAjv4io7zKxVkmOUwHoTarQK7POiXKiwa8x1QRMWrij0xK5k34eIR6Sww4uOhaTcVnkjxlUvC2iz/sxwQS6ZoJu zJ60lCbcq6ptimZGdy/yulx2kCNyCuUG/nBNXbdkf3Kz0nMb3Ry9n0QlM/ncP9d68+s4WiRlc+RuW5MPI3aHMGGT2s nchu87pA34+QQKDXqpJZVZnC+RaoA8mYS8BGPqZ//PidcqGgmzw2vccoT1N6pSAD7mXPmY9QONX68BD3 4uYAk1VCPHrpsKh41QE=&p= Cache-Control: no-cache MS-CV: BYqskdYKuUKf7ZeJ.0 User-Agent: WindowsShellClient/9.0.40929.0 (Windows) X-SDK-HWF: tch0,m301,m751,mA01,mT01 Host: arc.msn.com Connection: Keep-Alive
2022-04-08 08:03:06 UTC	8083	IN	HTTP/1.1 200 OK Cache-Control: no-store, no-cache Pragma: no-cache Content-Length: 167 Content-Type: application/json; charset=utf-8 Expires: Mon, 01 Jan 0001 00:00:00 GMT Server: Microsoft-IIS/10.0 ARC-RSP-DBG: [{"OPTOUTSTATE":"","256"}] X-ARC-SIG: Qh2OeSdX5tk/tt7pk/hBTJmFG6AMjGnSehkZ/mf8Ky+83DmSpp7Ry5J96OQ64WkfBxY36gdi60E4cBd CkMXlZM9Lf2aJ5f1mp7+ciGh3FRc5ErERQRviko4CIUjQnfdPTteZY4wGHeDRlOHyY8mG/m2l4h0ihCwlXct1LW+ 9a0fQlivJuzgPO8TbpMCnCd0ua6yFROAcRfB5q/OaLtXMcKizJ8axi3pqL8+3SSXHz8mNzRG3RY8PmJ2dUu66yiD Zm9Ct46lemDcuacKR5i+HAi0V4WsXqlr6OZ67g6feDqJtHK93yBqbBom5thYpgcnschVvKc9wlsJ2W7tw== Accept-CH: UA, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform, UA-Platform-Version X-AspNet-Version: 4.0.30319 X-Powered-By: ASP.NET Strict-Transport-Security: max-age=31536000; includeSubDomains Date: Fri, 08 Apr 2022 08:03:05 GMT Connection: close
2022-04-08 08:03:06 UTC	8084	IN	Data Raw: 7b 22 62 61 74 63 68 72 73 70 22 3a 7b 22 76 65 72 22 3a 22 31 2e 30 22 2c 22 65 72 72 6f 72 73 22 3a 5b 7b 22 63 6f 64 65 22 3a 32 30 34 30 2c 22 6d 73 67 22 3a 22 44 65 6d 61 6e 64 20 73 6f 75 72 63 65 20 72 65 74 75 72 6e 73 20 65 72 72 6f 72 20 28 4e 61 6d 65 3a 20 47 4e 5f 70 73 2c 20 45 72 72 6f 72 3a 20 4e 6f 20 65 6c 69 67 69 62 6c 65 20 63 6f 6e 74 65 6e 74 2e 29 2e 22 7d 5d 2c 22 72 65 66 72 65 73 68 74 69 6d 65 22 3a 22 32 30 32 32 2d 30 34 2d 30 38 54 31 32 3a 30 33 3a 30 36 22 7d 7d Data Ascii: {"batchrsp":{"ver":"","1.0"},"errors":{"code":"2040","msg":"Demand source returns error (Name: GN_ps, Error: No e ligible content)."},"refreshtime":"2022-04-08T12:03:06"}}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	50000	20.199.120.151	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:15 UTC	8084	OUT	Data Raw: 43 4e 54 20 31 20 43 4f 4e 20 32 34 36 0d 0a 43 6f 6e 74 65 78 74 3a 20 33 63 38 30 61 61 62 34 33 66 61 30 62 30 64 66 0d 0a 0d 0a Data Ascii: CNT 1 CON 246Context: 3c80aab43fa0b0df
2022-04-08 08:03:15 UTC	8084	OUT	Data Raw: 3c 63 6f 6e 6e 65 63 74 3e 3c 76 65 72 3e 32 3c 2f 76 65 72 3e 3c 61 67 65 6e 74 3e 3c 6f 73 3e 57 69 6e 64 6f 77 73 3c 2f 6f 73 3e 3c 6f 73 56 65 72 3e 31 30 2e 30 2e 30 2e 30 2e 31 37 31 33 34 3c 2f 6f 73 56 65 72 3e 3c 70 72 6f 63 3e 78 36 34 3c 2f 70 72 6f 63 3e 3c 6c 63 69 64 3e 65 6e 2d 55 53 3c 2f 6c 63 69 64 3e 3c 67 65 6f 49 64 3e 32 34 34 3c 2f 67 65 6f 49 64 3e 3c 61 6f 61 63 3e 30 3c 2f 61 6f 61 63 3e 3c 64 65 76 69 63 65 54 79 70 65 3e 31 3c 2f 64 65 76 69 63 65 54 79 70 65 3e 3c 64 65 76 69 63 65 4e 61 6d 65 3e 56 4d 77 61 72 65 37 2c 31 3c 2f 64 65 76 69 63 65 4e 61 6d 65 3e 3c 2f 61 67 65 6e 74 3e 3c 2f 63 6f 6e 6e 65 63 74 3e Data Ascii: <connect><ver>2</ver><agent><os>Windows</os><osVer>10.0.0.0.17134</osVer><proc>x64</proc> <lcid>en-US</lcid><geold>244</geold><aoac>0</aoac><deviceType>1</deviceType><deviceName>VMware7.1</ deviceName></agent></connect>

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:15 UTC	8084	OUT	Data Raw: 41 54 48 20 32 20 43 4f 4e 5c 44 45 56 49 43 45 20 31 30 31 34 0d 0a 43 6f 6e 74 65 78 74 3a 20 33 63 38 30 61 61 62 34 33 66 61 30 62 30 64 66 0d 0a 0d 0a 3c 64 65 76 69 63 65 3e 3c 63 6f 6d 70 61 63 74 2d 74 69 63 6b 65 74 3e 74 3d 45 77 43 6f 41 75 70 49 42 41 41 55 31 62 44 47 66 64 61 7a 69 44 66 58 70 6a 4e 35 4e 36 63 59 68 54 31 77 62 6d 51 41 41 51 77 65 75 52 78 64 54 45 52 58 49 34 58 73 61 55 64 61 66 67 57 47 68 6d 46 42 32 63 6a 51 30 2b 6c 52 4d 56 52 66 4d 58 33 46 77 79 4e 35 6e 68 5a 42 49 69 50 59 61 52 4e 51 2f 64 77 71 38 33 2f 58 59 37 5a 42 55 72 6d 54 65 77 44 66 6a 2f 57 6d 4f 6e 51 35 6b 4e 32 56 76 44 35 75 46 4d 37 47 6a 4c 78 56 73 37 55 78 36 70 69 69 71 41 6d 6c 4d 6d 4e 7a 57 34 6d 36 7a 78 2f 52 66 32 38 74 48 6b 4a 46 73 Data Ascii: ATH 2 CON\DEVICE 1014Context: 3c80aab43fa0b0df<device><<compact-ticket>t=EwCoAuplBAAU1bDGfdaziDfXpjN5N6cYhT1wbmQAAQweuRxdTERXI4XsaUdafgWGhmFB2cjQ0+IRMVrFMX3FwyN5nhZBliPYaRNQ/dwq83/XY7ZBUrmTewDfj/WmOnQ5kN2VvD5uFM7GjLxVs7Ux6piiQAmIIMmNzW4m6zx/Rf28tHkJFs
2022-04-08 08:03:15 UTC	8085	OUT	Data Raw: 42 4e 44 20 33 20 43 4f 4e 5c 51 4f 53 20 32 39 0d 0a 43 6f 6e 74 65 78 74 3a 20 33 63 38 30 61 61 62 34 33 66 61 30 62 30 64 66 0d 0a 0d 0a Data Ascii: BND 3 CON\QOS 29Context: 3c80aab43fa0b0df
2022-04-08 08:03:15 UTC	8085	IN	Data Raw: 32 30 32 20 31 20 43 4f 4e 20 35 38 0d 0a Data Ascii: 202 1 CON 58
2022-04-08 08:03:15 UTC	8085	IN	Data Raw: 4d 53 2d 43 56 3a 20 32 66 32 52 39 56 77 72 72 55 2b 51 31 62 41 44 69 62 44 30 61 51 2e 30 0d 0a 0d 0a 50 61 79 6c 6f 61 64 20 70 61 72 73 69 6e 67 20 66 61 69 6c 65 64 2e Data Ascii: MS-CV: 2f2R9VwrrU+Q1bADibD0aQ.0Payload parsing failed.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	50001	52.152.110.14	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:23 UTC	8086	OUT	GET /SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%7D/x64/10.0.17134.1/0?CH=17&L=en-US&P=&PT=0x30&WUA=10.0.17134.1&MK=4MtpozR6MODPIGb&MD=EefvrDUR HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Windows-Update-Agent/10.0.10011.16384 Client-Protocol/1.81 Host: sls.update.microsoft.com
2022-04-08 08:03:24 UTC	8086	IN	HTTP/1.1 200 OK Cache-Control: no-cache Pragma: no-cache Content-Type: application/octet-stream Expires: -1 Last-Modified: Mon, 01 Jan 0001 00:00:00 GMT ETag: "wy8fVV3cy06QIZhZUaOIBEOVMBnt4x8NjH3c50VWOxM= _1440" MS-CorrelationId: 6498898f-c4c8-49f6-967f-2330448e9183 MS-RequestId: c503d6c9-74cf-44b6-bf59-19ecf4a8e19b MS-CV: tLYklXuuWka26piW.0 X-Microsoft-SLSCClientCache: 1440 Content-Disposition: attachment; filename=environment.cab X-Content-Type-Options: nosniff Date: Fri, 08 Apr 2022 08:03:23 GMT Connection: close Content-Length: 30958
2022-04-08 08:03:24 UTC	8086	IN	Data Raw: 4d 53 43 46 00 00 00 00 be 37 00 00 00 00 00 00 44 00 00 00 00 00 00 03 01 01 00 01 00 04 00 20 e0 00 00 14 00 00 00 00 10 00 be 37 00 00 30 41 00 00 00 00 00 00 00 00 64 00 00 00 01 00 01 00 f3 5b 00 00 00 00 00 00 00 00 00 00 80 00 65 6e 76 69 72 6f 6e 6d 65 6e 74 2e 63 61 62 00 27 c3 6c fd 52 37 f3 5b 43 4b ed 7a 05 58 55 dd d6 ee de 9b ee 96 6e 11 e9 b5 e9 52 69 a5 a4 bb 5b a4 bb 6b d3 ad a2 74 77 08 08 08 d2 21 25 dd a0 80 80 48 4a 4a 83 c4 dd e8 17 9e ef d4 7f fe 7b cf 73 fe 7b ef b7 9f 67 ef bd e6 5c 73 ce 35 63 8c f1 8e 77 8c 25 af 22 2e 05 82 7f da c9 40 df 3f 12 3f fe 40 08 60 30 08 0c 42 04 bd f8 08 02 11 7e af c1 fd de 06 10 05 fd fe 31 85 7f af 5b 85 72 83 7e fa f8 83 cc 6c 5d 2d 1d ed 6c 6d cc 6c 9d d9 dd 6d ac 41 f8 7a 2e Data Ascii: MSCF7D 70Ad[environment.cab]IR7[CKzXUnRi[ktw!%HJJ{s(g\s5cw%"._@??@`0B~1[r-]-lmlmAz.
2022-04-08 08:03:24 UTC	8102	IN	Data Raw: b3 49 a2 0d ff f6 07 56 2e e0 cd 9b 1f 2c 88 a2 01 ec 5e 7b 96 ac 79 f1 dc 76 c5 85 50 e5 c7 c8 45 07 64 59 b3 b7 80 da 46 59 e2 3c b1 95 cb ed 18 a0 46 1e 05 b6 ad 0f aa c7 d6 26 8a 7a 17 6e 85 5c 5c 6e b7 9b 98 29 fc 15 9c b1 63 23 9c 27 9a ba 82 04 21 f1 ec 76 cf 7a 3c 9a dc 26 02 a4 4b 13 b7 f5 66 dc 71 d6 12 42 66 da ba 5c 82 4f 0a 63 8b 27 ed ac 5b 4a 30 41 b8 22 8b 2f b7 4c 07 eb 6d 35 30 dd 9f 04 c2 94 77 e9 20 77 b3 ca 0d 58 a9 21 17 bb 64 c6 3c 80 fd e9 00 b3 78 2d 96 fe 20 b6 4c c6 4a 0b e6 fc 7a 35 83 21 a9 5b fb 9f ec fd f1 bd a9 3a 79 0e 3d a3 0c 9a 4f 59 1e be de 85 65 6f ea 2b b7 1c 1f d9 51 fd 01 a2 7c 91 b5 30 82 07 05 30 82 04 ed a0 03 02 01 02 02 13 33 00 00 00 08 59 e3 94 e0 54 c7 17 5d 00 00 00 00 00 08 30 0d 06 09 2a 86 48 86 f7 0d Data Ascii: IV.,^{\yvPEYFY<F&zn\ n)c#'\vz<&KfqBf\Oc'[J0A"/Lm50w wXld<x- LJz5[;y=OYeo+Q[003YT]0*H

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	50003	20.82.210.154	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:25 UTC	8117	OUT	POST /v3/Delivery/Events/Impression HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Content-Length: 2786 Content-Type: text/plain; charset=UTF-8 Host: arc.msn.com Connection: Keep-Alive Cache-Control: no-cache
2022-04-08 08:03:25 UTC	8117	OUT	Data Raw: 50 49 44 3d 34 32 35 31 30 36 35 35 38 26 54 49 44 3d 37 30 30 33 34 32 30 38 35 26 43 49 44 3d 31 32 38 30 30 30 30 30 30 31 33 39 32 37 32 39 26 42 49 44 3d 31 30 32 30 37 37 33 30 37 35 26 50 47 3d 50 43 30 30 30 50 30 46 52 35 2e 30 30 30 30 30 30 49 51 38 26 54 50 49 44 3d 34 32 35 31 30 36 35 35 38 26 52 45 51 41 53 49 44 3d 37 35 31 38 35 39 36 37 38 38 43 42 34 36 44 39 42 44 41 41 36 37 46 42 30 37 36 35 37 37 37 45 26 41 53 49 44 3d 65 34 38 39 36 33 36 38 62 36 61 36 34 65 64 62 39 35 34 37 39 36 32 63 30 35 34 65 31 64 37 63 26 54 49 4d 45 3d 32 30 32 32 30 34 30 38 54 31 37 30 32 34 39 5a 26 53 4c 4f 54 3d 32 26 52 45 51 54 3d 32 30 32 32 30 34 30 38 54 30 38 30 31 32 32 26 4d 41 5f 53 63 6f 72 65 3d 32 26 4c 4f 43 41 4c 49 44 3d 77 Data Ascii: PID=425106558&TID=700342085&CID=128000000001392729&BID=1020773075&PG=PC000P0FR 5.0000000IQ8&TPID=425106558&REQASID=7518596788CB46D9BDAA67FB0765777E&ASID=e4896368b6a64edb 9547962c054e1d7c&TIME=20220408T170249Z&SLOT=2&REQT=20220408T080123&MA_Score=2&LOCALID=w
2022-04-08 08:03:25 UTC	8120	IN	HTTP/1.1 200 OK Cache-Control: no-store, no-cache Pragma: no-cache Content-Type: application/xml; charset=utf-8 Expires: Mon, 01 Jan 0001 00:00:00 GMT Server: Microsoft-IIS/10.0 ARC-RSP-DBG: [] X-AspNet-Version: 4.0.30319 X-Powered-By: ASP.NET Strict-Transport-Security: max-age=31536000; includeSubDomains Date: Fri, 08 Apr 2022 08:03:24 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	50002	52.242.101.226	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:25 UTC	8120	OUT	GET /SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%7D/x64/10.0.17134.1/0?CH=17&L=en-US&P=&PT=0x30&WUA=10.0.17134.1&MK=4MtpozR6MODPIGb&MD=EefvrDUR HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Windows-Update-Agent/10.0.10011.16384 Client-Protocol/1.81 Host: sls.update.microsoft.com
2022-04-08 08:03:25 UTC	8120	IN	HTTP/1.1 200 OK Cache-Control: no-cache Pragma: no-cache Content-Type: application/octet-stream Expires: -1 Last-Modified: Mon, 01 Jan 0001 00:00:00 GMT ETag: "wy8fVV3cy06QIZhZUaOIBEoVMBnt4x8NjH3c50VWOxM=_1440" MS-CorrelationId: a278de06-a581-49c0-a954-23dccab326d0 MS-RequestId: 3fb01cc2-3d79-4c14-8852-141ee9df3a6a MS-CV: gmbPxqUvkUS4g0On.0 X-Microsoft-SLSCClientCache: 1440 Content-Disposition: attachment; filename=environment.cab X-Content-Type-Options: nosniff Date: Fri, 08 Apr 2022 08:03:24 GMT Connection: close Content-Length: 30958
2022-04-08 08:03:25 UTC	8121	IN	Data Raw: 4d 53 43 46 00 00 00 00 be 37 00 00 00 00 00 44 00 00 00 00 00 00 00 03 01 01 00 01 00 04 00 20 e0 00 00 14 00 00 00 00 10 00 be 37 00 00 30 41 00 00 00 00 00 00 00 00 64 00 00 00 01 00 01 00 00 f3 5b 00 00 00 00 00 00 00 00 00 00 80 00 65 6e 76 69 72 6f 6e 6d 65 6e 74 2e 63 61 62 00 27 c3 6c fd 52 37 f3 5b 43 4b ed 7a 05 58 55 dd d6 ee de 9b ee 96 6e 11 e9 b5 e9 52 69 a5 a4 bb 5b a4 bb 6b d3 ad a2 74 77 08 08 08 d2 21 25 dd a0 80 80 48 4a 4a 83 c4 dd e8 17 9e ef d4 7f fe 7b cf 73 fe 7b ef b7 9f 67 ef bd e6 5c 73 ce 35 63 8c f1 8e 77 8c 25 af 22 2e 05 82 7f da c9 40 df 3f 12 3f fe 40 08 60 30 08 0c 42 04 bd f8 08 02 11 7e af c1 fd de 06 10 05 fd fe 31 85 7f af 5b 85 72 83 7e fa f8 83 cc 6c 5d 2d 1d ed 6c 6d cc 6c 9d d9 dd 6d ac 41 f8 7a 2e Data Ascii: MSCF7D 70Ad[environment.cab]IR7[CKzXUnRi[ktw!%HJJ{s[g]s5cw%"._@??@`0B-1[r-]-lmlmAz.
2022-04-08 08:03:25 UTC	8136	IN	Data Raw: b3 49 a2 0d ff f6 07 56 2e e0 cd 9b 1f 2c 88 a2 01 ec 5e 7b 96 ac 79 f1 dc 76 c5 85 50 e5 c7 c8 45 07 64 59 b3 b7 80 da 46 59 e2 3c b1 95 cb ed 18 a0 46 1e 05 b6 ad 0f aa c7 d6 26 8a 7a 17 6e 85 5c 5c 6e b7 9b 98 29 fc 15 9c b1 63 23 9c 27 9a ba 82 04 21 f1 ec 76 cf 7a 3c 9a dc 26 02 a4 4b 13 b7 f5 66 dc 71 d6 12 42 66 da ba 5c 82 4f 0a 63 8b 27 ed ac 5b 4a 30 41 b8 22 8b 2f b7 4c 07 eb 6d 35 30 dd 9f 04 c2 94 77 e9 20 77 b3 ca 0d 58 a9 21 17 bb 64 c6 3c 80 fd e9 00 b3 78 2d 96 fe 20 b6 4c c6 4a 0b e6 fc 7a 35 83 21 a9 5b fb 9f ec fd f1 bd a9 3a 79 0e 3d a3 0c 9a 4f 59 1e be de 85 65 6f ea 2b b7 1c 1f d9 51 fd 01 a2 7c 91 b5 30 82 07 05 30 82 04 ed a0 03 02 01 02 02 13 33 00 00 00 08 59 e3 94 e0 54 c7 17 5d 00 00 00 00 00 00 30 0d 06 09 2a 86 48 86 f7 0d Data Ascii: IV.,^jyvPEYFY<F&znl\n)c#!vz<&KfqBfOc[J0A]/Lm50w wXId<x- LJz5I[;y=OYeo+Q[003YT]0*H

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	50004	52.152.110.14	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:25 UTC	8151	OUT	GET /SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%7D/x64/10.0.17134.1/0?CH=17&L=en-US&P=&PT=0x30&WUA=10.0.17134.1&MK=4MtpozR6MODPIGb&MD=EefvrDUR HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Windows-Update-Agent/10.0.10011.16384 Client-Protocol/1.81 Host: sls.update.microsoft.com
2022-04-08 08:03:26 UTC	8151	IN	HTTP/1.1 200 OK Cache-Control: no-cache Pragma: no-cache Content-Type: application/octet-stream Expires: -1 Last-Modified: Mon, 01 Jan 0001 00:00:00 GMT ETag: "wy8fVV3cy06QlZhZUaOlBEoVMBnt4x8NJH3c50VWOxM= _1440" MS-CorrelationId: 14f0036d-4d32-4abb-a094-f581bfe67ef7 MS-RequestId: 10b06799-e3d0-4850-8593-25c027d206bc MS-CV: sRJVG35YWkShSH1h.0 X-Microsoft-SLSCClientCache: 1440 Content-Disposition: attachment; filename=environment.cab X-Content-Type-Options: nosniff Date: Fri, 08 Apr 2022 08:03:25 GMT Connection: close Content-Length: 30958
2022-04-08 08:03:26 UTC	8152	IN	Data Raw: 4d 53 43 46 00 00 00 00 be 37 00 00 00 00 00 00 44 00 00 00 00 00 00 03 01 01 00 01 00 04 00 20 e0 00 00 14 00 00 00 00 00 10 00 be 37 00 00 30 41 00 00 00 00 00 00 00 00 00 64 00 00 00 01 00 01 00 f3 5b 00 00 00 00 00 00 00 00 00 00 80 00 65 6e 76 69 72 6f 6e 6d 65 6e 74 2e 63 61 62 00 27 c3 6c fd 52 37 f3 5b 43 4b ed 7a 05 58 55 dd d6 ee de 9b ee 96 6e 11 e9 b5 e9 52 69 a5 a4 bb 5b a4 bb 6b d3 ad a2 74 77 08 08 08 d2 21 25 dd a0 80 80 48 4a 4a 83 c4 dd e8 17 9e ef d4 7f fe 7b cf 73 fe 7b ef b7 9f 67 ef bd e6 5c 73 ce 35 63 8c f1 8e 77 8c 25 af 22 2e 05 82 7f da c9 40 df 3f 12 3f fe 40 08 60 30 08 0c 42 04 bd f8 08 02 11 7e af c1 fd de 06 10 05 fd f6 31 85 7f af 5b 85 72 83 7e fa f8 83 cc 6c 5d 2d 1d ed 6c 6d cc 6c 9d d9 dd 6d ac 41 f8 7a 2e Data Ascii: MSCF7D 70Ad[environment.cab\IR7[CKzXUnRi[ktwl%hJJj[s[gs5cw%".@@?@'0B~1[r-l]~lmlmAz.
2022-04-08 08:03:26 UTC	8167	IN	Data Raw: b3 49 a2 0d ff f6 07 56 2e e0 cd 9b 1f 2c 88 a2 01 ec 5e 7b 96 ac 79 f1 dc 76 c5 85 50 e5 c7 c8 45 07 64 59 b3 b7 80 da 46 59 e2 3c b1 95 cb ed 18 a0 46 1e 05 b6 ad 0f aa c7 d6 26 8a 7a 17 6e 85 5c 5c 6e b7 9b 98 29 fc 15 9c b1 63 23 9c 27 9a ba 82 04 21 f1 ec 76 cf 7a 3c 9a dc 26 02 a4 4b 13 b7 f5 66 dc 71 d6 12 42 66 da ba 5c 82 4f 0a 63 8b 27 ed ac 5b 4a 30 41 b8 22 8b 2f b7 4c 07 eb 6d 35 30 dd 9f 04 c2 94 77 e9 20 77 b3 ca 0d 58 a9 21 17 bb 64 c6 3c 80 fd e9 00 b3 78 2d 96 fe 20 b6 4c c6 4a 0b e6 fc 7a 35 83 21 a9 5b fb 9f ec fd f1 bd a9 3a 79 0e 3d a3 0c 9a 4f 59 1e be de 85 65 6f ea 2b b7 1c 1f d9 51 fd 01 a2 7c 91 b5 30 82 07 05 30 82 04 ed a0 03 02 01 02 02 13 33 00 00 00 08 59 e3 94 e0 54 c7 17 5d 00 00 00 00 00 08 30 0d 06 09 2a 86 48 86 f7 0d Data Ascii: IV.,^f{vPEdYFY<F&zr\\n)c#f!vz<&KfqBfOc[J0A"/Lm50w wXld<x- LJz5f[:y=OYeo+Q 003YT 0"H

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	50005	52.152.110.14	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:26 UTC	8182	OUT	GET /SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%7D/x64/10.0.17134.1/0?CH=17&L=en-US&P=&PT=0x30&WUA=10.0.17134.1&MK=4MtpozR6MODPIGb&MD=EefvrDUR HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Windows-Update-Agent/10.0.10011.16384 Client-Protocol/1.81 Host: sls.update.microsoft.com
2022-04-08 08:03:26 UTC	8182	IN	HTTP/1.1 200 OK Cache-Control: no-cache Pragma: no-cache Content-Type: application/octet-stream Expires: -1 Last-Modified: Mon, 01 Jan 0001 00:00:00 GMT ETag: "wy8fVV3cy06QlZhZUaOlBEoVMBnt4x8NJH3c50VWOxM= _1440" MS-CorrelationId: ac2ec315-b527-4b2a-85fc-7054edcb6117 MS-RequestId: 5dd8dd25-ac33-47ad-9348-a63cd0a67a52 MS-CV: i4CCqt7CUkOjNsUb.0 X-Microsoft-SLSCClientCache: 1440 Content-Disposition: attachment; filename=environment.cab X-Content-Type-Options: nosniff Date: Fri, 08 Apr 2022 08:03:25 GMT Connection: close Content-Length: 30958

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:26 UTC	8183	IN	Data Raw: 4d 53 43 46 00 00 00 00 be 37 00 00 00 00 00 00 44 00 00 00 00 00 00 03 01 01 00 01 00 04 00 20 e0 00 00 14 00 00 00 00 00 10 00 be 37 00 00 30 41 00 00 00 00 00 00 00 00 00 64 00 00 00 01 00 01 00 f3 5b 00 00 00 00 00 00 00 00 00 00 00 80 00 65 6e 76 69 72 6f 6e 6d 65 6e 74 2e 63 61 62 00 27 c3 6c fd 52 37 f3 5b 43 4b ed 7a 05 58 55 dd d6 ee de 9b ee 96 6e 11 e9 b5 e9 52 69 a5 a4 bb 5b a4 bb 6b d3 ad a2 74 77 08 08 08 d2 21 25 dd a0 80 80 48 4a 4a 83 c4 dd e8 17 9e ef d4 7f fe 7b cf 73 fe 7b ef b7 9f 67 ef bd e6 5c 73 ce 35 63 8c f1 8e 77 8c 25 af 22 2e 05 82 7f da c9 40 df 3f 12 3f fe 40 08 60 30 08 0c 42 04 bd f8 08 02 11 7e af c1 fd de 06 10 05 fd f6 31 85 7f af 5b 85 72 83 7e fa f8 83 cc 6c 5d 2d 1d ed 6c 6d cc 6c 9d d9 dd 6d ac 41 f8 7a 2e Data Ascii: MSCF7D 70Ad[environment.cab!R7[CKzXUnRi[ktw!%HJJ{s[gs5cw%".@??@ '0B~[!r-]!lmAz.
2022-04-08 08:03:26 UTC	8198	IN	Data Raw: b3 49 a2 0d ff f6 07 56 2e e0 cd 9b 1f 2c 88 a2 01 ec 5e 7b 96 ac 79 f1 dc 76 c5 85 50 e5 c7 c8 45 07 64 59 b3 b7 80 da 46 59 e2 3c b1 95 cb ed 18 a0 46 1e 05 b6 ad 0f aa c7 d6 26 8a 7a 17 6e 85 5c 5c 6e b7 9b 98 29 fc 15 9c b1 63 23 9c 27 9a ba 82 04 21 f1 ec 76 cf 7a 3c 9a dc 26 02 a4 4b 13 b7 f5 66 dc 71 d6 12 42 66 da ba 5c 82 4f 0a 63 8b 27 ed ac 5b 4a 30 41 b8 22 8b 2f b7 4c 07 eb 6d 35 30 dd 9f 04 c2 94 77 e9 20 77 b3 ca 0d 58 a9 21 17 bb 64 c6 3c 80 fd e9 00 b3 78 2d 96 fe 20 b6 4c c6 4a 0b e6 fc 7a 35 83 21 a9 5b fb 9f ec fd f1 bd a9 3a 79 0e 3d a3 0c 9a 4f 59 1e be de 85 65 6f ea 2b b7 1c 1f d9 51 fd 01 a2 7c 91 b5 30 82 07 05 30 82 04 ed a0 03 02 01 02 02 13 33 00 00 00 08 59 e3 94 e0 54 c7 17 5d 00 00 00 00 00 08 30 0d 06 09 2a 86 48 86 f7 0d Data Ascii: IV.,^{yPEdYFY<F&zn\\n)c#!vz<&KfqBfOc'[J0A"/Lm50w wXld<x- LJz5![:y=OYeo+Q]003YT]0*H

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.3	50006	40.112.88.60	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:27 UTC	8213	OUT	GET /v1/a/installComplete?pg=PC000P0FR5.0000000IQ8&unid=&placementType=PostOOBE&app=&pid=425106558&c id=128000000001392729&tid=700342085&reqasid=8d771849a7234e0ab71c2ac9a71f46b4®ion=US&lang=EN-US&oe m=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.17134.1&mo=&cap=&aid=&anid=&muid =&persid=&itemId=9WZDNCRFHWD2&skuld=0010&installKind=RedirectTile&ctid=store-curated-postoobe&bSrc=i .t&asid=e4896368b6a64edb9547962c054e1d7c&time=20220408T170223Z HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Host: ris.api.iris.microsoft.com Connection: Keep-Alive
2022-04-08 08:03:27 UTC	8214	IN	HTTP/1.1 204 No Content Content-Length: 0 Server: Microsoft-HTTPAPI/2.0 request-id: c9123693-df0e-4591-b4e2-ff48357bb11e Date: Fri, 08 Apr 2022 08:03:26 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	50008	40.112.88.60	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:27 UTC	8214	OUT	GET /v1/a/opportunity?pg=PC000P0FR5.0000000IQ8&unid=&placementType=PostOOBE&app=&pid=425106558&cid=1 28000000001392729&tid=700342085&reqasid=8d771849a7234e0ab71c2ac9a71f46b4®ion=US&lang=EN- US&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.17134.1&mo=&cap=&aid=&anid =&muid=&persid=&itemId=9NBLGGZM6WM&skuld=0010&installKind=RedirectTile&ctid=store-curated-postoobe& bSrc=i.t&asid=e4896368b6a64edb9547962c054e1d7c&time=20220408T170227Z HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Host: ris.api.iris.microsoft.com Connection: Keep-Alive
2022-04-08 08:03:27 UTC	8215	IN	HTTP/1.1 204 No Content Content-Length: 0 Server: Microsoft-HTTPAPI/2.0 request-id: 2a88f5d5-8fc6-4301-84ac-052aae501d7b Date: Fri, 08 Apr 2022 08:03:27 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.3	50007	20.54.110.249	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:27 UTC	8215	OUT	GET /v7.0/products/lookup?alternateId=PackageFamilyName&value=SpotifyAB.SpotifyMusic_zpdnekdrzrea0&m arket=US&languages=en-US%2Cen%2Cneutral&fieldsTemplate=InstallAgent&mold=Public&oemId=Public&scmid=Public HTTP/1.1 Connection: Keep-Alive Content-Type: application/json User-Agent: Install Service MS-CV: kkb781LL8EaQlxCb.0.2.4 Host: displaycatalog.mp.microsoft.com
2022-04-08 08:03:27 UTC	8215	IN	HTTP/1.1 200 OK Connection: close Date: Fri, 08 Apr 2022 08:03:27 GMT Content-Type: application/json; charset=utf-8 Server: Kestrel Transfer-Encoding: chunked Vary: Authorization MS-CorrelationId: 614a84eb-b694-42d7-bb19-26139ba6d0d5 MS-RequestId: aa6caf41-8fbd-4074-b5d3-4fbcd221fafd MS-CV: kkb781LL8EaQlxCb.0.2.4.422986582.0.1.422986582.0.0 X-Content-Type-Options: nosniff MS-ServerId: 6 Region: neu Node: aks-systempool-37630073-vmss000034 MS-DocumentVersions: 9NCBCSZSJRSB 3985
2022-04-08 08:03:27 UTC	8216	IN	Data Raw: 36 66 33 62 0d 0a 7b 22 42 69 67 49 64 73 22 3a 5b 22 39 4e 43 42 43 53 5a 53 4a 52 53 42 22 5d 2c 22 48 61 73 4d 6f 72 65 50 61 67 65 73 22 3a 66 61 6c 73 65 2c 22 50 72 6f 64 75 63 74 73 22 3a 5b 7b 22 4c 61 73 74 4d 6f 64 69 66 69 65 64 44 61 74 65 22 3a 22 32 30 32 32 2d 30 34 2d 30 31 54 31 32 3a 32 31 3a 31 32 2e 36 39 39 36 33 35 36 5a 22 2c 22 4c 6f 63 61 6c 69 7a 65 64 50 72 6f 70 65 72 74 69 65 73 22 3a 5b 7b 22 46 72 61 6e 63 68 69 73 65 73 22 3a 5b 5d 2c 22 49 6d 61 67 65 73 22 3a 5b 7b 22 46 69 6c 65 49 64 22 3a 22 33 30 32 39 34 34 30 38 30 32 33 38 33 35 34 38 32 31 37 22 2c 22 45 49 53 4c 69 73 74 69 6e 67 49 64 65 6e 74 69 66 69 65 72 22 3a 6e 75 6c 6c 2c 22 42 61 63 6b 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 23 31 65 64 37 36 30 22 2c Data Ascii: 6f3b[{"BigIds":["9NCBCSZSJRSB"],"HasMorePages":false,"Products":[{"LastModifiedDate":"2022-04-01T12 :21:12.6996356Z","LocalizedProperties":{"Franchises":[],"Images":{"FileId":"3029440802383548217","EISListingIdentifier ":null,"BackgroundColor":"#1ed760",
2022-04-08 08:03:27 UTC	8219	IN	Data Raw: 31 36 34 39 34 38 30 2e 64 30 38 35 39 36 63 36 2d 65 36 62 36 2d 34 38 62 33 2d 38 66 63 39 2d 39 35 39 36 38 35 63 30 34 66 30 31 22 2c 22 57 69 64 74 68 22 3a 33 31 30 7d 2c 7b 22 46 69 6c 65 49 64 22 3a 22 33 30 34 30 38 39 35 35 31 30 33 39 33 37 31 35 39 30 35 22 2c 22 45 49 53 4c 69 73 74 69 6e 67 49 64 65 6e 74 69 66 69 65 72 22 3a 6e 75 6c 6c 2c 22 42 61 63 6b 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 23 31 65 64 37 36 30 22 2c 22 43 61 70 74 69 6f 6e 22 3a 22 22 2c 22 46 69 6c 65 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 31 32 37 30 35 2c 22 46 6f 72 65 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 22 2c 22 48 65 69 67 68 74 22 3a 34 36 35 2c 22 49 6d 61 67 65 50 6f 73 69 74 69 6f 6e 49 6e 66 6f 22 3a 22 22 2c 22 49 6d 61 67 65 50 75 72 70 6f 73 65 22 Data Ascii: 1649480.d08596c6-e6b6-48b3-8fc9-959685c04f01","Width":310},{"FileId":"3040895510393715905","EISLis tingIdentifier":null,"BackgroundColor":"#1ed760","Caption":"","FileSizeInBytes":12705,"ForegroundColor":"","Height":465, "ImagePositionInfo":"","ImagePurpose"
2022-04-08 08:03:27 UTC	8223	IN	Data Raw: 43 61 70 74 69 6f 6e 22 3a 22 22 2c 22 46 69 6c 65 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 33 35 30 36 38 33 2c 22 46 6f 72 65 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 22 2c 22 48 65 69 67 68 74 22 3a 37 36 38 2c 22 49 6d 61 67 65 50 6f 73 69 74 69 6f 6e 49 6e 66 6f 22 3a 22 44 65 73 6b 74 6f 70 2f 32 22 2c 22 49 6d 61 67 65 50 75 72 70 6f 73 65 22 3a 22 53 63 72 65 65 6e 73 68 6f 74 22 2c 22 55 6e 73 63 61 6c 65 64 49 6d 61 67 65 53 48 41 32 35 36 48 61 73 68 22 3a 22 59 4c 4e 66 68 57 66 7a 4c 68 2f 4b 39 4a 71 70 4c 67 37 7a 6e 79 48 56 67 59 4d 4f 66 34 7a 66 56 75 77 78 5a 70 61 32 6b 4e 59 3d 22 2c 22 55 72 69 22 3a 22 2f 2f 73 74 6f 72 65 2d 69 6d 61 67 65 73 2e 73 2d 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 69 6d 61 67 65 2f 61 70 70 73 2e 34 35 Data Ascii: Caption":"","FileSizeInBytes":350683,"ForegroundColor":"","Height":768,"ImagePositionInfo":"Desktop/2","Imag ePurpose":"Screenshot","UnscaledImageSHA256Hash":"YLNfhWfzLh/K9JqplGzngYVgYMO4zfVuwXZpa2kNY-","Uri ":"//store-images.s-microsoft.com/image/apps.45
2022-04-08 08:03:27 UTC	8228	IN	Data Raw: 22 54 46 22 2c 22 47 41 22 2c 22 47 4d 22 2c 22 47 45 22 2c 22 47 48 22 2c 22 47 49 22 2c 22 47 4c 22 2c 22 47 44 22 2c 22 47 50 22 2c 22 47 55 22 2c 22 47 47 22 2c 22 47 4e 22 2c 22 47 57 22 2c 22 47 59 22 2c 22 48 54 22 2c 22 48 4d 22 2c 22 48 4e 22 2c 22 41 5a 22 2c 22 42 53 22 2c 22 42 42 22 2c 22 42 59 22 2c 22 42 5a 22 2c 22 42 4a 22 2c 22 42 4d 22 2c 22 42 54 22 2c 22 4b 4d 22 2c 22 43 47 22 2c 22 43 44 22 2c 22 43 4b 22 2c 22 43 58 22 2c 22 43 43 2 2 2c 22 43 49 22 2c 22 43 57 22 2c 22 4a 4d 22 2c 22 53 4a 22 2c 22 4a 45 22 2c 22 4b 4d 22 2c 22 4b 47 22 2c 22 4b 47 22 2c 22 4c 41 22 2c 22 4c 53 22 2c 22 4c 52 22 2c 22 4d 4f 22 2c 22 4d 4b 22 2c 22 4d 47 22 2c 22 4d 57 22 2c 22 49 4d 22 2c 22 4d 48 22 2c 22 4d 51 22 2c 22 4d 55 22 2c 22 59 54 22 2c 22 46 4d 22 2c Data Ascii: "TF","GA","GM","GE","GH","GI","GL","GD","GP","GU","GG","GN","GW","GY","HT","HM","HN","AZ","BS","BB ","BY","BZ","BJ","BM","BT","KM","CG","CD","CK","CX","CC","CI","CW","JM","SJ","JE","KI","KG","LA","LS","LR","MO ","MK","MG","MW","IM","MH","MQ","MU","YT","FM",
2022-04-08 08:03:27 UTC	8232	IN	Data Raw: 22 56 43 22 2c 22 54 4a 22 2c 22 54 5a 22 2c 22 54 47 22 2c 22 54 4b 22 2c 22 54 4f 22 2c 22 54 4d 22 2c 22 54 43 22 2c 22 54 56 22 2c 22 55 4d 22 2c 22 55 47 22 2c 22 56 49 22 2c 22 56 47 22 2c 22 57 46 22 2c 22 45 48 22 2c 22 5a 4d 22 2c 22 5a 57 22 2c 22 55 5a 22 2c 22 56 55 22 2c 22 53 52 22 2c 22 53 5a 22 2c 22 41 44 22 2c 22 4d 43 22 2c 22 53 4d 22 2c 22 4d 45 22 2c 22 56 41 22 2c 22 4e 45 55 54 52 41 4c 22 5d 7d 5d 2c 22 50 72 6f 64 75 63 74 49 64 2 2 3a 22 39 4e 43 42 43 53 5a 53 4a 52 53 42 22 2c 22 50 72 6f 70 65 72 74 69 65 73 22 3a 7b 22 46 75 6c 66 69 6c 6c 6d 65 6e 74 44 61 74 61 22 3a 7b 22 50 72 6f 64 75 63 74 49 64 22 3a 22 39 4e 43 42 43 53 5a 53 4a 52 53 42 22 2c 22 57 75 43 61 74 65 67 6f 72 79 49 64 22 3a 22 35 63 33 35 33 62 39 63 2d Data Ascii: "VC","TJ","TZ","TG","TK","TO","TM","TC","TV","UM","UG","VI","VG","WF","EH","ZM","ZW","UZ","VU","SR ","SZ","AD","MC","SM","ME","VA","NEUTRAL"]}]","ProductId":"9NCBCSZSJRSB","Properties":{"FulfillmentData":{"Prod uctId":"9NCBCSZSJRSB","WuCategoryId":"5c353b9c-
2022-04-08 08:03:27 UTC	8236	IN	Data Raw: 39 61 36 37 2d 37 36 64 39 31 30 38 63 37 63 62 35 3a 46 75 6c 6c 22 5d 2c 22 4c 69 63 65 6e 73 69 6e 67 4b 65 79 49 64 73 22 3a 5b 22 31 22 5d 7d 2c 7b 22 45 6e 74 69 74 6c 65 6d 65 6e 74 4b 65 79 73 22 3a 5b 22 62 69 67 3a 39 4e 43 42 43 53 5a 53 4a 52 53 42 3a 30 30 30 31 22 5d 2c 22 4c 69 63 65 6e 73 69 6e 67 4b 65 79 49 64 73 22 3a 5b 22 31 22 5d 7d 2c 7b 22 45 6e 74 69 74 6c 65 6d 65 6e 74 4b 65 79 73 22 3a 5b 22 62 69 67 3a 39 4e 43 42 43 53 5a 53 4a 52 53 42 3a 30 30 30 32 2d 5d 2c 22 4c 69 63 65 6e 73 69 6e 67 4b 65 79 49 64 73 22 3a 5b 22 31 22 5d 7d 5d 7d 2c 22 4d 61 72 6b 65 74 73 22 3a 5b 22 55 53 22 5d 2c 22 4f 72 64 65 72 4d 61 6e 61 67 65 6d 65 6e 74 44 61 74 61 22 3a 7b 22 47 72 61 6e 74 65 64 45 6e 74 69 74 6c 65 6d 65 6e 74 4b 65 79 73 Data Ascii: 9a67-76d9108c7cb5-Full"},"LicensingKeyIds":["1"]},{"EntitlementKeys":{"big:9NCBCSZSJRSB:0001"},"Li censingKeyIds":["1"]},{"EntitlementKeys":{"big:9NCBCSZSJRSB:0002"},"LicensingKeyIds":["1"]}],{"Markets":{"US"] ","OrderManagementData":{"GrantedEntitlementKeys

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:27 UTC	8240	IN	Data Raw: 2c 22 4d 57 22 2c 22 49 4d 22 2c 22 4d 48 22 2c 22 4d 51 22 2c 22 4d 55 22 2c 22 59 54 22 2c 22 46 4d 22 2c 22 4d 44 22 2c 22 4d 4e 22 2c 22 4d 53 22 2c 22 4d 5a 22 2c 22 4d 4d 22 2c 22 4e 41 22 2c 22 4e 52 22 2c 22 4e 50 22 2c 22 4d 56 22 2c 22 4d 4c 22 2c 22 4e 43 22 2c 22 4e 49 22 2c 22 4e 45 22 2c 22 4e 55 22 2c 22 4e 46 22 2c 22 50 57 22 2c 22 50 53 22 2c 22 50 41 22 2c 22 50 47 22 2c 22 50 59 22 2c 22 52 45 22 2c 22 52 57 22 2c 22 42 4c 22 2c 22 4d 46 22 2c 22 57 53 22 2c 22 53 54 22 2c 22 53 4e 22 2c 22 4d 50 22 2c 22 50 4e 22 2c 22 53 58 22 2c 22 53 42 22 2c 22 53 4f 22 2c 22 53 43 22 2c 22 53 4c 22 2c 22 47 53 22 2c 22 53 48 22 2c 22 4b 4e 22 2c 22 4c 43 22 2c 22 50 4d 22 2c 22 56 43 22 2c 22 54 4a 22 2c 22 54 5a 22 2c 22 54 47 22 2c 22 54 4b 22 Data Ascii: ", "MW", "IM", "MH", "MQ", "MU", "YT", "FM", "MD", "MN", "MS", "MZ", "MM", "NA", "NR", "NP", "MV", "ML", "NC", "NI", "NE", "NU", "NF", "PW", "PS", "PA", "PG", "PY", "RE", "RW", "BL", "MF", "WS", "ST", "SN", "MP", "PN", "SX", "SB", "SO", "SC", "SL", "GS", "SH", "KN", "LC", "PM", "VC", "TJ", "TZ", "TG", "TK"
2022-04-08 08:03:27 UTC	8244	IN	Data Raw: 32 3a 32 31 3a 31 32 2e 37 36 38 36 31 35 31 5a 22 2c 22 4d 61 72 6b 65 74 73 22 3a 5b 22 55 53 22 5d 2c 22 4f 72 64 65 72 4d 61 6e 61 67 65 6d 65 6e 74 44 61 74 61 22 3a 7b 22 47 72 61 6e 74 65 64 45 6e 74 69 74 6c 65 6d 65 6e 74 4b 65 79 73 22 3a 5b 5d 2c 22 50 72 69 63 65 22 3a 7b 22 43 75 72 72 65 6e 63 79 43 6f 64 65 22 3a 22 55 53 44 22 2c 22 49 73 50 49 52 65 71 75 69 72 65 64 22 3a 66 61 6c 73 65 2c 22 4c 69 73 74 50 72 69 63 65 22 3a 30 2e 30 2c 22 4d 53 52 50 22 3a 30 2e 30 2c 22 54 61 78 54 79 70 65 22 3a 22 22 2c 22 57 68 6f 6c 65 73 61 6c 65 43 75 72 72 65 6e 63 79 43 6f 64 65 22 3a 22 22 7d 7d 2c 22 50 72 6f 70 65 72 74 69 65 73 22 3a 7b 7d 2c 22 53 6b 75 49 64 22 3a 22 30 30 31 31 22 2c 22 44 69 73 70 6c 61 79 52 61 6e 6b 22 3a 31 2c 22 52 Data Ascii: 2:21:12.7686151Z", "Markets":["US"], "OrderManagementData":{"GrantedEntitlementKeys":[], "Price":{"CurrencyCode":"USD", "IsPIRequired":false, "ListPrice":0.0, "MSRP":0.0, "TaxType":""," WholesaleCurrencyCode":""}}, "Properties":{"Skuld":"0011", "DisplayRank":1, "R
2022-04-08 08:03:27 UTC	8244	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49978	20.82.210.154	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:20 UTC	17	OUT	GET /v3/Delivery/Placement?pubid=da63df93-3dbc-42ae-a505-b34988683ac7&pid=280815&adm=2&w=1&h=1&wpix=1&hpx=1&fmt=json&cltp=app&dim=le&rafb=0&nct=1&pm=1&cfmt=text,image,poly&sft=jpeg,png,gif&topt=1&poptin=0&localid=w:472DC600-FEAB-E7F8-720D-1E33F00FD1E7&ctry=US&time=20220408T170212Z&lc=en-US&pl=en-US&idtp=mid&uid=4388269c-b420-4134-ac19-bc7ca8a19ac1&aid=00000000-0000-0000-0000-000000000000&ua=WindowsShellClient%2F9.0.40929.0%20Windows%29&asid=492dae31b56c4c9eae7feff7513297e&ctmode=MultiSession&arch=x64&cdm=1&cdmver=10.0.17134.1&devfam=Windows.Desktop&devform=Unknown&devosver=10.0.17134.1&disphorzzres=1280&dispsize=17.1&dispvertres=1024&isu=0&lo=1463022&metered=false&nettype=ethernet&npid=sc-280815&oemName=hseht%2C%20Inc.&oemid=hseht%2C%20Inc.&ossku=Professional&smBiosDm=hseht7%2C1&tl=2&tsu=1463022&waasBldFlt=1&waasCfgExp=1&waasCfgSet=1&waasRetail=1&waasRing= HTTP/1.1 Accept-Encoding: gzip, deflate X-SDK-CACHE: chs=0&imp=0&chf=0&ds=50583&fs=32319&sc=6 X-SDK-HW-TOKEN: t=EwDYAppeBAAUIAKXDAofTQM+n+MaRVFKzH/ehWgAAdVW0iu23GlxjRyUBGA+V5LMOu/IMaTj obBnQosoTe6w30OZEf3HuIBKeYXog3CqxSfjOHeF/J4iLS/gKyhq/ZV/xtryHZ35PhcBmS2qzlwNBiXp0+4efq5ns DEEESQ06VT9dPxHYgWIFLG65LRysydA1IM9dDPzftFvDLM/ickJDFevqkA3hG2mKV46qlHL4CT7eP4Hk0/MORp8JB 5tew/jl7o25TIEcX9Ohbx1KlwUuqQcpj0nfDAUZEjkQqVS2z/lwQaH+/fdlFO/AoxQI3CbcoTeaCp3XlesBJX0bxVN zc22qQqCPiGWWQ/Sb52rGvkgBRvdW8DFg8ToMjfqPYDZgAAcE3mODPOPawVqAFPV53gZZc0aOkGu+jJWN w46hEU9aCKlpEDkH6SywZSQj+Z6lyumM/ZCz1/Exb6MZih9PGVRFV0dS4rZOfTtsEXw5x6gJoWeqkJZJqul+/LQNZp daM/TGNQWhUnnbhyzuL3J52vfTsZzAtC6HDHUtfcP567luQfNjw1zOBQG/Pho8+d+FIHWtcPKMXaDH+rX7PpfIRpHT m7bdH++rsPvLvdstjafDcGAADV0pkaM4oU0n35rzdzjoAWTcazcHXkrs0Gr34gDLPkE96nUwLpeDIXN3LOntP44gHn gFTJAvt4io7zKxVkmOUwHoTarQK7POiXKiwa8x1QRMWjr0xK5k34eIR6SWW4uOhaTkCvnxjxlUvc2iz/sxwQS6Z0Ju zJ60lCbq6ptimZGdy/yulx2kCNYcUG/nBNXbdKtF3Kz0nMb3Ry9n0QIm/ncP9d68+s4WiRlc+RuW5MPI3aHMGGT2s nchu87pA34+QQKDxQpJZVZnC+RaoA8mYS8BGPqZ//PidcQGgmzw2vcc0T1N6pSAD7mXPYm9QONX68BD3 4uYAk1VCPHrpsKh41QE=&p= Cache-Control: no-cache MS-CV: BYqskdYKuUKf7ZeJ.0 User-Agent: WindowsShellClient/9.0.40929.0 (Windows) X-SDK-HWF: tch0,m301,m751,mA01,mT01 Host: arc.msn.com Connection: Keep-Alive
2022-04-08 08:02:20 UTC	21	IN	HTTP/1.1 200 OK Cache-Control: no-store, no-cache Pragma: no-cache Content-Length: 3040 Content-Type: application/json; charset=utf-8 Expires: Mon, 01 Jan 0001 00:00:00 GMT Server: Microsoft-IIS/10.0 ARC-RSP-DBG: [{"RADIDS":"","1,P425116123-T700333390-C128000000001627409+B+P20+S1"}],{"OPTOUTST ATE":"256"}] X-ARC-SIG: jYg3qLjL9Y7DWzBRHX/+PyS9UJXd6jECnibQpLQst2MdB7YiU51XCLeBBRHBb9vImkerL9wZdwBzS4+ HP5SweUxO6M4NtQxTUoSktHWe4tlzvNOOQIGs+/O0qhFZ2IN17EHNuOZcaR8iMIPemwxRssGzeba+XC7 MABxD+HPDINCQv7acrDYMG+z49gtd6ztDjnbbe+9uYj8FA4qVYjMbch1Jk+iUpTMcUhBp13q+4/7m160jsoylzvX G348EYRWrNkTKcQp7PJJ6dEx8/FhoVSKcMKcwFkFGBW8V5Z6yV607yTuNd42Cnff5qDIWEHVMb2ariX3fnupTPyNmXp eZA== Accept-CH: UA, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform, UA-Platform-Version X-AspNet-Version: 4.0.30319 X-Powered-By: ASP.NET Strict-Transport-Security: max-age=31536000; includeSubDomains Date: Fri, 08 Apr 2022 08:02:19 GMT Connection: close

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:20 UTC	22	IN	Data Raw: 7b 22 62 61 74 63 68 72 73 70 22 3a 7b 22 76 65 72 22 3a 22 31 2e 30 22 2c 22 69 74 65 6d 73 22 3a 5b 7b 22 69 74 65 6d 22 3a 22 7b 5c 22 66 5c 22 3a 5c 22 72 61 66 5c 22 2c 5c 22 76 5c 22 3a 5c 22 31 2e 30 5c 22 2c 5c 22 72 64 72 5c 22 3a 5b 7b 5c 22 63 5c 22 3a 5c 22 43 44 4d 5c 22 2c 5c 22 75 5c 22 3a 5c 22 53 75 62 73 63 72 69 62 65 6 4 43 6f 6e 74 65 6e 74 5c 22 7d 5d 2c 5c 22 61 64 5c 22 3a 7b 5c 22 63 6c 61 73 73 5c 22 3a 5c 22 63 6f 6e 74 65 6e 74 5c 22 2c 5c 22 63 6f 6c 6c 65 63 74 69 6f 6e 73 5c 22 3a 5b 5d 2c 5c 22 69 74 65 6d 50 72 6f 70 65 72 74 79 4d 61 6e 69 66 65 73 74 5c 22 3a 7b 5c 22 6e 6f 4f 70 5c 22 3a 7b 5c 22 74 79 70 65 5c 22 3a 5c 22 61 63 74 69 6f 6e 5c 22 7d 7d 2c 5c 22 69 74 65 6d 73 5c 22 3a 5b 7b 5c 22 70 72 6f 70 65 72 74 69 Data Ascii: {"batchrsp":{"ver":"1.0","items":[{"item":{"f":"raf","v":"1.0"},"rd":{"c":"CDM","ul":"SubscribedCont ent"}}, {"ad":{"class":"content","collections":[""],"itemPropertyManifest":{"noOp":{"type":"action"}},"items":{"properti

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	50009	40.112.88.60	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:27 UTC	8227	OUT	GET /v1/a/opportunity?pg=PC000P0FR5.0000000IQ8&unid=&placementType=PostOOBE&app=&pid=425106558&cid=128000000001392729&tid=700342085&reqasid=8d771849a7234e0ab71c2ac9a71f46b4®ion=US&lang=EN-US&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.17134.1&mo=&cap=&aid=&anid=&muid=&persid=&itemId=9WZDNCRFHWD2&skuld=0010&installKind=RedirectTile&ctid=store-curated-postoobe&bSrc=i.t&asid=e4896368b6a64edb9547962c054e1d7c&time=20220408T170230Z HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Host: ris.api.iris.microsoft.com Connection: Keep-Alive
2022-04-08 08:03:27 UTC	8244	IN	HTTP/1.1 204 No Content Content-Length: 0 Server: Microsoft-HTTPAPI/2.0 request-id: 107e50e4-a74e-491d-b8c0-a91805046893 Date: Fri, 08 Apr 2022 08:03:27 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	50010	40.112.88.60	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:27 UTC	8244	OUT	GET /v1/a/opportunity?pg=PC000P0FR5.0000000IQ8&unid=&placementType=PostOOBE&app=&pid=425106558&cid=128000000001392729&tid=700342085&reqasid=8d771849a7234e0ab71c2ac9a71f46b4®ion=US&lang=EN-US&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.17134.1&mo=&cap=&aid=&anid=&muid=&persid=&itemId=9NH2GPH4JZS4&skuld=0010&installKind=Install&ctid=store-curated-postoobe&bSrc=i.t&asid=e4896368b6a64edb9547962c054e1d7c&time=20220408T170232Z HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Host: ris.api.iris.microsoft.com Connection: Keep-Alive
2022-04-08 08:03:27 UTC	8245	IN	HTTP/1.1 204 No Content Content-Length: 0 Server: Microsoft-HTTPAPI/2.0 request-id: 85d1895f-4158-4a57-b45c-4de3b9f46e5c Date: Fri, 08 Apr 2022 08:03:27 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.3	50011	20.54.89.106	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:27 UTC	8245	OUT	GET /SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%7D/x64/10.0.17134.1/0?CH=17&L=en-US&P=&PT=0x30&WUA=10.0.17134.1&MK=4MtpozR6MODPIGb&MD=EefvrDUR HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Windows-Update-Agent/10.0.10011.16384 Client-Protocol/1.81 Host: sls.update.microsoft.com

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:27 UTC	8245	IN	HTTP/1.1 200 OK Cache-Control: no-cache Pragma: no-cache Content-Type: application/octet-stream Expires: -1 Last-Modified: Mon, 01 Jan 0001 00:00:00 GMT ETag: "wy8fVV3cy06QlZhZUaOlBEoVMBnt4x8NjH3c50VWOxM=_1440" MS-CorrelationId: c06878f6-0b4a-49cf-add5-70a9a8627c00 MS-RequestId: 3aa854ad-016a-4aa9-a94c-5c4cdc8d88eb MS-CV: 7pM+pa80hUGSJ0uF.0 X-Microsoft-SLSCClientCache: 1440 Content-Disposition: attachment; filename=environment.cab X-Content-Type-Options: nosniff Date: Fri, 08 Apr 2022 08:03:27 GMT Connection: close Content-Length: 30958
2022-04-08 08:03:27 UTC	8246	IN	Data Raw: 4d 53 43 46 00 00 00 00 be 37 00 00 00 00 00 00 44 00 00 00 00 00 00 03 01 01 00 01 00 04 00 20 e0 00 00 14 00 00 00 00 00 10 00 be 37 00 00 30 41 00 00 00 00 00 00 00 00 00 64 00 00 00 01 00 01 00 f3 5b 00 00 00 00 00 00 00 00 00 00 80 00 65 6e 76 69 72 6f 6e 6d 65 6e 74 2e 63 61 62 00 27 c3 6c fd 52 37 f3 5b 43 4b ed 7a 05 58 55 dd d6 ee de 9b ee 96 6e 11 e9 b5 e9 52 69 a5 a4 bb 5b a4 bb 6b d3 ad a2 74 77 08 08 08 d2 21 25 dd a0 80 80 48 4a 4a 83 c4 dd e8 17 9e ef d4 7f fe 7b cf 73 fe 7b ef b7 9f 67 ef bd e6 5c 73 ce 35 63 8c f1 8e 77 8c 25 af 22 2e 05 82 7f da c9 40 df 3f 12 3f fe 40 08 60 30 08 0c 42 04 bd f8 08 02 11 7e af c1 fd de 06 10 05 fd fe f6 31 85 7f af 5b 85 72 83 7e fa f8 83 cc 6c 5d 2d 1d ed 6c 6d cc 6c 9d d9 dd 6d ac 41 f8 7a 2e Data Ascii: MSCF7D 70Adj[environment.cab\lR7[CKzXUnRi[kw/%HJJ[s[gl's5cw%".@??@`0B~1[~l]-lmlmAz.
2022-04-08 08:03:27 UTC	8261	IN	Data Raw: b3 49 a2 0d ff f6 07 56 2e e0 cd 9b 1f 2c 88 a2 01 ec 5e 7b 96 ac 79 f1 dc 76 c5 85 50 e5 c7 c8 45 07 64 59 b3 b7 80 da 46 59 e2 3c b1 95 cb ed 18 a0 46 1e 05 b6 ad 0f aa c7 d6 26 8a 7a 17 6e 85 5c 5c 6e b7 9b 98 29 fc 15 9c b1 63 23 9c 27 9a ba 82 04 21 f1 ec 76 cf 7a 3c 9a dc 26 02 a4 4b 13 b7 f5 66 dc 71 d6 12 42 66 da ba 5c 82 4f 0a 63 8b 27 ed ac 5b 4a 30 41 b8 22 8b 2f b7 4c 07 eb 6d 35 30 dd 9f 04 c2 94 77 e9 20 77 b3 ca 0d 58 a9 21 17 bb 64 c6 3c 80 fd e9 00 b3 78 2d 96 fe 20 b6 4c c6 4a 0b e6 fc 7a 35 83 21 a9 5b fb 9f ec fd f1 bd a9 3a 79 0e 3d a3 0c 9a 4f 59 1e be de 85 65 6f ea 2b b7 1c 1f d9 51 fd 01 a2 7c 91 b5 30 82 07 05 30 82 04 ed a0 03 02 01 02 02 13 33 00 00 00 08 59 e3 94 e0 54 c7 17 5d 00 00 00 00 00 08 30 0d 06 09 2a 86 48 86 f7 0d Data Ascii: IV.,^{\yvPEdYFY<F&znl\n)c#'\vz<&KfqBfOc'[J0A"/Lm50w wXld<x- Lj35l[:y=OYeo+Q[003YT]J0*H

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.3	50012	40.112.88.60	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:28 UTC	8276	OUT	GET /v1/a/opportunity?pg=PC000P0FR5.0000000IQ8&unid=&placementType=PostOOBE&app=&pid=425106558&cid=128000000001392729&tid=700342085&reqasid=8d771849a7234e0ab71c2ac9a71f46b4®ion=US&lang=EN-US&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.17134.1&mo=&cap=&aid=&anid=&muid=&persid=&itemId=9NBLGGH6J6VK&skuld=0010&installKind=RedirectTile&ctid=store-curated-postoobe&bSrc=i.t&asid=e4896368b6a64edb9547962c054e1d7c&time=20220408T170234Z HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Host: ris.api.iris.microsoft.com Connection: Keep-Alive
2022-04-08 08:03:28 UTC	8277	IN	HTTP/1.1 204 No Content Content-Length: 0 Server: Microsoft-HTTPAPI/2.0 request-id: f687a791-4332-4b7d-88c0-9e30220332b3 Date: Fri, 08 Apr 2022 08:03:27 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.3	50014	40.112.88.60	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:28 UTC	8277	OUT	GET /v1/a/opportunity?pg=PC000P0FR5.0000000IQ8&unid=&placementType=PostOOBE&app=&pid=425106558&cid=128000000001392729&tid=700342085&reqasid=8d771849a7234e0ab71c2ac9a71f46b4®ion=US&lang=EN-US&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.17134.1&mo=&cap=&aid=&anid=&muid=&persid=&itemId=9P6RC76MSMMJ&skuld=0010&installKind=Install&ctid=store-curated-postoobe&bSrc=i.t&asid=e4896368b6a64edb9547962c054e1d7c&time=20220408T170235Z HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Host: ris.api.iris.microsoft.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:28 UTC	8277	IN	HTTP/1.1 204 No Content Content-Length: 0 Server: Microsoft-HTTPAPI/2.0 request-id: d889c692-b237-4be7-b6e6-e0087306f391 Date: Fri, 08 Apr 2022 08:03:28 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.3	50013	52.152.110.14	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:28 UTC	8277	OUT	GET /SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%7D/x64/10.0.17134.1/0?CH=17&L=en-US&P=&PT=0x30&WUA=10.0.17134.1&MK=4MtpozR6MODPIGb&MD=EefvrDUR HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Windows-Update-Agent/10.0.10011.16384 Client-Protocol/1.81 Host: sls.update.microsoft.com
2022-04-08 08:03:28 UTC	8279	IN	HTTP/1.1 200 OK Cache-Control: no-cache Pragma: no-cache Content-Type: application/octet-stream Expires: -1 Last-Modified: Mon, 01 Jan 0001 00:00:00 GMT ETag: "wy8fVV3cy06QlZhZUaOlBEoVMBnt4x8NJH3c50VWOxM=_1440" MS-CorrelationId: fae81dd2-0c1c-4dc9-89fd-60720e91a771 MS-RequestId: 2ace8fcc-b675-412a-96fb-73939cfd22f MS-CV: iuBsxsxsfk6hf1t5.0 X-Microsoft-SLSCClientCache: 1440 Content-Disposition: attachment; filename=environment.cab X-Content-Type-Options: nosniff Date: Fri, 08 Apr 2022 08:03:28 GMT Connection: close Content-Length: 30958
2022-04-08 08:03:28 UTC	8279	IN	Data Raw: 4d 53 43 46 00 00 00 00 be 37 00 00 00 00 00 00 44 00 00 00 00 00 00 03 01 01 00 01 00 04 00 20 e0 00 00 14 00 00 00 00 00 10 00 be 37 00 00 30 41 00 00 00 00 00 00 00 00 00 64 00 00 00 01 00 01 00 f3 5b 00 00 00 00 00 00 00 00 00 00 80 00 65 6e 76 69 72 6f 6e 6d 65 6e 74 2e 63 61 62 00 27 c3 6c fd 52 37 f3 5b 43 4b ed 7a 05 58 55 dd d6 ee de 9b ee 96 6e 11 e9 b5 e9 52 69 a5 a4 bb 5b a4 bb 6b d3 ad a2 74 77 08 08 08 d2 21 25 dd a0 80 80 48 4a 4a 83 c4 dd e8 17 9e ef d4 7f fe 7b cf 73 fe 7b ef b7 9f 67 ef bd e6 5c 73 ce 35 63 8c f1 8e 77 8c 25 af 22 2e 05 82 7f da c9 40 df 3f 12 3f fe 40 08 60 30 08 0c 42 04 bd f8 08 02 11 7e af c1 fd de 06 10 05 fd f6 31 85 7f af 5b 85 72 83 7e fa f8 83 cc 6c 5d 2d 1d ed 6c 6d cc 6c 9d d9 dd 6d ac 41 f8 7a 2e Data Ascii: MSCF7D 70Ad[environment.cab\IR7[CKzXUnRi[ktw!%HJJ[s[gs5cw%".@@?@'0B~1[r~l]~lmlmAz.
2022-04-08 08:03:28 UTC	8295	IN	Data Raw: b3 49 a2 0d ff f6 07 56 2e e0 cd 9b 1f 2c 88 a2 01 ec 5e 7b 96 ac 79 f1 dc 76 c5 85 50 e5 c7 c8 45 07 64 59 b3 b7 80 da 46 59 e2 3c b1 95 cb ed 18 a0 46 1e 05 b6 ad 0f aa c7 d6 26 8a 7a 17 6e 85 5c 5c 6e b7 9b 98 29 fc 15 9c b1 63 23 9c 27 9a ba 82 04 21 f1 ec 76 cf 7a 3c 9a dc 26 02 a4 4b 13 b7 f5 66 dc 71 d6 12 42 66 da ba 5c 82 4f 0a 63 8b 27 ed ac 5b 4a 30 41 b8 22 8b 2f b7 4c 07 eb 6d 35 30 dd 9f 04 c2 94 77 e9 20 77 b3 ca 0d 58 a9 21 17 bb 64 c6 3c 80 fd e9 00 b3 78 2d 96 fe 20 b6 4c c6 4a 0b e6 fc 7a 35 83 21 a9 5b fb 9f ec fd f1 bd a9 3a 79 0e 3d a3 0c 9a 4f 59 1e be de 85 65 6f ea 2b b7 1c 1f d9 51 fd 01 a2 7c 91 b5 30 82 07 05 30 82 04 ed a0 03 02 01 02 02 13 33 00 00 00 08 59 e3 94 e0 54 c7 17 5d 00 00 00 00 08 30 0d 06 09 2a 86 48 86 f7 0d Data Ascii: IV.,^f{yPEdYFY<F&zn\\n)c#f!vz<&KfqBfOc'[J0A"/Lm50w wXld<x- LJz5f[;y=OYeo+Q[003YT]0*H

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.3	50015	40.112.88.60	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:28 UTC	8278	OUT	GET /v1/a/opportunity?pg=PC000P0FR5.0000000IQ8&unid=&placementType=PostOOBE&app=&pid=425106558&cid=128000000001392729&tid=700342085&reqasid=8d771849a7234e0ab71c2ac9a71f46b4®ion=US&lang=EN-US&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.17134.1&mo=&cap=&aid=&anid=&muid=&persid=&itemId=9WZDNCRFJ27N&skuId=0010&installKind=Install&ctid=store-curated-postoobe&bSrc=i.t&asid=e4896368b6a64edb9547962c054e1d7c&time=20220408T170237Z HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Host: ris.api.iris.microsoft.com Connection: Keep-Alive
2022-04-08 08:03:28 UTC	8278	IN	HTTP/1.1 204 No Content Content-Length: 0 Server: Microsoft-HTTPAPI/2.0 request-id: 08f9cd8f-f4a0-4be0-b43b-e154675ddee4 Date: Fri, 08 Apr 2022 08:03:28 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.3	50017	20.54.110.249	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:28 UTC	8309	OUT	GET /v7.0/products/lookup?alternateId=PackageFamilyName&value=Microsoft.YourPhone_8wekyb3d8bbwe&mark et=US&languages=en-US%2Cen%2Cneutral&fieldsTemplate=InstallAgent&mold=Public&oemId=Public&scmlId=Public HTTP/1.1 Connection: Keep-Alive Content-Type: application/json User-Agent: Install Service MS-CV: 6bD/MunolEWqHDEG.0.2.4 Host: displaycatalog.mp.microsoft.com
2022-04-08 08:03:29 UTC	8310	IN	HTTP/1.1 200 OK Connection: close Date: Fri, 08 Apr 2022 08:03:28 GMT Content-Type: application/json; charset=utf-8 Server: Kestrel Transfer-Encoding: chunked Vary: Authorization MS-CorrelationId: dbff4310-b40d-4478-99bf-c61cef6d2b81 MS-RequestId: d3a9bd45-587f-45a4-9e2d-a6b7df223484 MS-CV: 6bD/MunolEWqHDEG.0.2.4.422986805.0.1.422986805.0.0 X-Content-Type-Options: nosniff MS-ServerId: 65db49-5khkq Region: neu Node: aks-systempool-37630073-vmss000007 MS-DocumentVersions: 9NMPJ99VJBWVJ3160
2022-04-08 08:03:29 UTC	8311	IN	Data Raw: 31 32 34 63 63 0d 0a 7b 22 42 69 67 49 64 73 22 3a 5b 22 39 4e 4d 50 4a 39 39 56 4a 42 57 56 22 5d 2c 22 48 61 73 4d 6f 72 65 50 61 67 65 73 22 3a 66 61 6c 73 65 2c 22 50 72 6f 64 75 63 74 73 22 3a 5b 7b 22 4c 61 73 74 4d 6f 64 69 66 69 65 64 44 61 74 65 22 3a 22 32 30 32 32 2d 30 34 2d 30 36 54 32 31 3a 33 31 3a 32 32 2e 37 30 39 32 38 38 34 5a 22 2c 22 4c 6f 63 61 6c 69 7a 65 64 50 72 6f 70 65 72 74 69 65 73 22 3a 5b 7b 22 46 72 61 6e 63 68 69 73 65 73 2 2 3a 5b 5d 2c 22 49 6d 61 67 65 73 22 3a 5b 7b 22 46 69 6c 65 49 64 22 3a 22 33 30 35 36 36 34 32 31 33 30 34 32 34 33 34 39 34 38 36 22 2c 22 45 49 53 4c 69 73 74 69 6e 67 49 64 65 6e 74 69 66 69 65 72 22 3a 6e 75 6c 6c 2c 22 42 61 63 6b 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 23 30 30 37 38 44 37 22 Data Ascii: 124cc{"BigIds":["9NMPJ99VJBWV"],"HasMorePages":false,"Products":[{"LastModifiedDate":"2022-04-06T2 1:31:22.7092884Z","LocalizedProperties":{"Franchises":[],"Images":{"FileId":"3056642130424349486","EISListingIdentifie r":null,"BackgroundColor":"#0078D7"
2022-04-08 08:03:29 UTC	8314	IN	Data Raw: 2d 38 30 37 33 2d 34 31 64 63 64 38 33 65 64 64 62 65 2e 63 30 65 36 64 32 65 38 2d 32 64 34 30 2d 34 61 37 38 2d 39 31 62 38 2d 35 30 30 35 35 35 38 36 66 34 35 33 22 2c 22 57 69 64 74 68 22 3a 36 36 7d 2c 7b 22 46 69 6c 65 49 64 22 3a 22 33 30 34 31 38 31 32 33 31 32 30 33 39 36 37 39 30 39 36 22 2c 22 45 49 53 4c 69 73 74 69 6e 67 49 64 65 6e 74 69 66 69 65 72 22 3a 6e 75 6c 6c 2c 22 42 61 63 6b 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 23 30 30 37 38 44 37 22 2c 22 43 61 70 74 69 6f 6e 22 3a 22 22 2c 22 46 69 6c 65 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 33 35 36 32 2c 22 46 6f 72 65 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 22 2c 22 48 65 69 67 68 74 22 3a 38 38 2c 22 49 6d 61 67 65 50 6f 73 69 74 69 6f 6e 49 6e 66 6f 22 3a 22 22 2c 22 49 6d 61 67 65 Data Ascii: -8073-41dcd83eddb.e0e6d2e8-2d40-4a78-91b8-50055586f453","Width":66},{"FileId":"304181231203967909 6","EISListingIdentifier":null,"BackgroundColor":"#0078D7","Caption":"","FileSizeInBytes":3562,"ForegroundColor":"","Hei ght":88,"ImagePositionInfo":"","Image
2022-04-08 08:03:29 UTC	8318	IN	Data Raw: 22 22 2c 22 46 69 6c 65 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 38 38 39 35 2c 22 46 6f 72 65 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 22 2c 22 48 65 69 67 68 74 22 3a 33 30 30 2c 22 49 6d 61 67 65 50 6f 73 69 74 69 6f 6e 49 6e 66 6f 22 3a 22 22 2c 22 49 6d 61 67 65 50 75 72 70 6f 73 65 22 3a 22 54 69 6c 65 22 2c 22 55 6e 73 63 61 6c 65 64 49 6d 61 67 65 53 48 41 32 35 36 48 61 73 68 22 3a 22 6e 37 68 41 59 52 4b 4b 51 34 5a 31 56 4f 35 45 74 73 2f 35 2f 55 2f 2b 67 34 62 32 7a 4f 44 5a 65 33 55 4e 66 2b 69 47 59 36 45 3d 22 2c 22 55 72 69 22 3a 22 2f 2f 73 74 6f 72 65 2d 69 6d 61 67 65 73 2e 73 2d 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 69 6d 61 67 65 2f 61 70 70 73 2e 34 37 32 36 33 2e 31 33 37 35 33 38 39 31 35 31 39 33 39 37 30 36 37 2e 38 30 31 31 Data Ascii: "", "FileSizeInBytes":8895, "ForegroundColor":""," "Height":300, "ImagePositionInfo":""," "ImagePurpose":"Tile", "Un scaledImageSHA256Hash":"n7hAYRKKQ4Z1VO5Ets/5/U/+g4b2zODZe3UNf+iGY6E=", "Uri":"//store-images.s-micros oft.com/image/apps.47263.13753891519397067.8011
2022-04-08 08:03:29 UTC	8322	IN	Data Raw: 2c 22 49 6d 61 67 65 50 6f 73 69 74 69 6f 6e 49 6e 66 6f 22 3a 22 44 65 73 6b 74 6f 70 2f 36 22 2c 22 49 6d 61 67 65 50 75 72 70 6f 73 65 22 3a 22 53 63 72 65 65 6e 73 68 6f 74 22 2c 22 55 6e 73 63 61 6c 65 64 49 6d 61 67 65 53 48 41 32 35 36 48 61 73 68 22 3a 22 42 5a 6b 4f 6a 6c 77 2b 4b 49 54 52 36 42 6f 45 42 42 79 6f 63 30 73 63 46 49 56 47 63 36 6e 4f 36 74 44 54 39 73 72 71 6e 4b 59 3d 22 2c 22 55 72 69 22 3a 22 2f 2f 73 74 6f 72 65 2d 69 6d 61 67 65 73 2e 73 2d 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 69 6d 61 67 65 2f 61 70 70 73 2e 33 39 31 37 33 2e 31 33 37 35 33 38 39 31 35 31 39 33 39 37 30 36 37 2e 65 38 61 30 36 64 37 64 2d 66 66 62 32 2d 34 35 34 32 2d 39 65 66 61 2d 34 36 30 30 36 63 62 39 37 30 36 39 2e 66 30 62 36 36 64 35 36 2d 33 33 Data Ascii: , "ImagePositionInfo":"Desktop/6", "ImagePurpose":"Screenshot", "UnscaledImageSHA256Hash":"BZkOjIw+KI TR6BoEBByoc0scFIVGc6nO6tDT9srqnKY=", "Uri":"//store-images.s-microsoft.com/image/apps.39173.137538915 19397067.e8a06d7d-ffb2-4542-9efa-46006cb97069.f0b66d56-33
2022-04-08 08:03:29 UTC	8326	IN	Data Raw: 74 50 72 6f 64 75 63 74 22 3a 7a 72 75 65 2c 22 50 72 65 66 65 72 72 65 64 53 6b 75 49 64 22 3a 22 30 30 31 30 22 2c 22 50 72 6f 64 75 63 74 54 79 70 65 22 3a 22 41 70 70 6c 69 63 61 74 69 6f 6e 22 2c 22 56 61 6c 69 64 61 74 69 6f 6e 44 61 74 61 22 3a 7b 22 50 61 73 73 65 64 56 61 6c 69 64 61 74 69 6f 6e 22 3a 66 61 6c 73 65 2c 22 52 65 7 6 69 73 69 6f 6e 49 64 22 3a 22 32 30 32 32 2d 30 34 2d 30 36 54 32 31 3a 33 33 3a 31 36 2e 32 36 30 33 39 36 35 5a 7c 7c 2e 7c 7c 62 33 35 36 66 63 36 30 2d 38 34 35 36 2d 34 63 66 37 2d 61 39 31 63 2d 39 63 34 39 36 62 62 61 38 34 36 33 7c 7c 31 31 35 32 39 32 31 35 30 35 36 39 34 37 30 36 34 36 31 7c 7c 4e 75 6c 6c 7c 7c 66 75 6c 6c 72 65 6c 65 61 73 65 22 2c 22 56 61 6c 69 64 61 74 69 6f 6e 52 65 73 75 6c 74 55 72 69 Data Ascii: tProduct":true,"PreferredSkuld":"","0010","ProductType":"Application","ValidationData":{"PassedValidation":fals e,"RevisionId":"","2022-04-06T21:33:16.2603965Z"},"b356fc60-8456-4cf7-a91c-9c496bba8463 1152921505694706461 Nu ll fullrelease", "ValidationResultUri

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:29 UTC	8330	IN	Data Raw: 72 73 69 6f 6e 22 2a 32 38 31 34 37 35 30 38 39 30 30 30 33 38 34 2c 22 50 6c 61 74 66 6f 72 6d 4e 61 6d 65 22 3a 22 57 69 6e 64 6f 77 73 2e 55 6e 69 76 65 72 73 61 6c 22 7d 5d 2c 22 50 6c 61 74 66 6f 72 6d 44 65 70 65 6e 64 65 6e 63 79 58 6d 6c 42 6c 6f 62 22 3a 22 7b 5c 22 62 6c 6f 62 2e 76 65 72 73 69 6f 6e 5c 22 3a 31 36 38 38 38 36 37 30 34 30 35 32 36 33 33 36 2c 5c 22 63 6f 6e 74 65 6e 74 2e 62 75 6e 64 6c 65 64 50 61 63 6b 61 67 65 73 5c 22 3a 5b 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 59 6f 75 72 50 68 6f 6e 65 5f 31 2e 32 30 30 31 32 2e 31 33 35 2e 30 5f 78 38 36 5f 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 5c 22 2c 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 59 6f 75 72 50 68 6f 6e 65 5f 31 2e 32 30 30 31 32 2e 31 33 35 2e 30 5f 61 72 6d 36 34 5f 5f 38 Data Ascii: rsion":2814750890000384,"PlatformName":"","Windows.Universal"},"PlatformDependencyXmlBlob":"","{\blob.version":1688867040526336,\"content.bundledPackages\":{\"[\"Microsoft.YourPhone_1.20012.135.0_x86__8wekyb3d8bbwe\", \"Microsoft.YourPhone_1.20012.135.0_arm64__8
2022-04-08 08:03:29 UTC	8334	IN	Data Raw: 65 22 2c 22 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 2e 59 6f 75 72 50 68 6f 6e 65 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 2c 22 4d 61 69 6e 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 46 6f 72 44 6c 63 22 3a 6e 75 6c 6c 2c 22 50 61 63 6b 61 67 65 46 75 6c 6c 4e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 2e 59 6f 75 72 50 68 6f 6e 65 5f 32 30 32 30 2e 34 31 36 2e 32 30 32 2e 30 5f 6e 65 75 74 72 61 6c 5f 7e 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 2c 22 50 61 63 6b 61 67 65 49 64 22 3a 22 35 30 65 35 32 65 31 3 5 2d 63 63 61 32 2d 34 38 32 35 2d 33 66 66 33 2d 36 64 66 39 31 62 32 34 66 65 64 34 2d 58 38 36 2d 58 36 34 2d 41 72 6d 2d 41 72 6d 36 34 22 2c 22 50 61 63 6b 61 67 65 52 61 6e 6b 22 Data Ascii: e","PackageFamilyName":"","Microsoft.YourPhone_8wekyb3d8bbwe","MainPackageFamilyNameForDlc":null,"PackageFullName":"","Microsoft.YourPhone_2020.416.202.0_neutral_~_8wekyb3d8bbwe","PackageId":"","50e52e15-cca2-4825-3ff3-6df91b24fed4-X86-X64-Arm-Arm64","PackageRank"
2022-04-08 08:03:29 UTC	8338	IN	Data Raw: 6f 72 6b 43 6c 69 65 6e 74 53 65 72 76 65 72 22 2c 22 72 65 6d 6f 74 65 53 79 73 74 65 6d 22 2c 22 70 68 6f 6e 65 43 61 6c 6c 22 2c 22 63 6f 6e 66 69 72 6d 41 70 70 43 6c 6f 73 65 22 2c 22 70 68 6f 6e 65 4c 69 6e 65 54 72 61 6e 73 70 6f 72 74 4d 61 6e 61 67 65 6d 65 6e 74 22 2c 22 70 68 6f 6e 65 43 61 6c 6c 53 79 73 74 65 6d 22 2c 22 74 61 72 67 65 74 65 64 43 6f 6e 74 65 6e 74 22 2c 22 72 75 6e 46 75 6c 6c 54 72 75 73 74 22 2c 22 70 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 22 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 75 6e 73 69 67 6e 65 64 50 61 63 6b 61 67 65 4d 61 6e 6 1 67 65 6d 65 6e 74 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 73 74 6f 72 65 46 69 6c 74 65 72 2e 63 6f 72 65 2e 6e 6f 74 53 75 70 70 6f 72 74 65 Data Ascii: orkClientServer","remoteSystem","phoneCall","confirmAppClose","phoneLineTransportManagement","phoneCallSystem","targetedContent","runFullTrust","packageManagement","Microsoft.unsignedPackageManageme nt_8wekyb3d8bbwe","Microsoft.storeFilter.core.notSupporte
2022-04-08 08:03:29 UTC	8342	IN	Data Raw: 35 2d 33 66 39 62 2d 34 64 31 33 2d 61 30 30 31 2d 66 35 33 61 38 32 62 31 33 30 65 32 22 2c 22 57 75 43 61 74 65 67 6f 72 79 49 64 22 3a 22 62 39 39 61 65 66 39 61 2d 31 36 38 35 2d 34 37 39 38 2d 62 34 62 31 2d 33 64 39 34 65 65 36 64 37 31 38 34 22 2c 22 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 6 6 74 2e 59 6f 75 72 50 68 6f 6e 65 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 2c 22 53 6b 75 49 64 22 30 30 31 30 22 2c 22 43 6f 6e 74 65 6e 74 22 3a 6e 75 6c 6c 2c 22 50 61 63 6b 61 67 65 46 65 61 74 75 72 65 73 22 3a 6e 75 6c 6c 7d 7d 2c 7b 22 41 70 70 6c 69 63 61 74 69 6f 6e 73 22 3a 5b 7b 22 41 70 70 6c 69 63 61 74 69 6f 6e 49 64 22 3a 22 41 70 70 22 7d 5d 2c 22 41 72 63 68 69 74 65 63 74 75 72 65 73 22 3a 5b Data Ascii: 5-3f9b-4d13-a001-f53a82b130e2","WuCategoryId":"","b99aef9a-1685-4798-b4b1-3d94ee6d7184","PackageFamilyName":"","Microsoft.YourPhone_8wekyb3d8bbwe","Skuld":"","0010","Content":null,"PackageFeatures":null},{\"Applications\":{\"[\"ApplicationId\":\"App\"],\"Architectures\":[
2022-04-08 08:03:29 UTC	8346	IN	Data Raw: 6c 65 76 65 6c 5c 22 3a 37 36 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 35 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 35 34 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 33 7d 5d 7d 7d 22 2c 22 50 61 63 6b 61 67 65 44 6f 77 6e 6c 6f 61 64 55 72 69 73 22 3a 6e 75 6c 6c 2c 22 46 75 6c 66 69 6c 6c 6d 65 6e 74 44 61 74 61 22 3a 7b 22 50 72 6f 64 75 63 74 49 64 22 3a 22 3 9 4e 4d 50 4a 39 39 56 4a 42 57 56 22 2c 22 57 75 42 75 6e 64 6c 65 49 64 22 3a 22 35 37 30 30 61 31 35 35 2d 33 66 39 62 2d 34 64 31 33 2d 61 30 30 31 2d 66 35 33 61 38 32 62 31 33 30 65 32 22 2c 22 57 75 43 61 74 65 67 6f 72 79 49 64 22 3a 22 62 39 39 61 65 66 39 61 2d 31 36 38 35 2d 34 37 39 38 2d 62 Data Ascii: level\":76,\"systemId\":16},{\"level\":68,\"systemId\":15},{\"level\":54,\"systemId\":13}}]\",\"PackageDownlo adUris\":null,\"FulfillmentData\":{\"\"ProductId\":\"9NMPJ39VJJBWV\",\"WuBundleid\":\"5700a155-3f9b-4d13-a001-f53a82b130e2\",\"WuCategoryId\":\"b99aef9a-1685-4798-b
2022-04-08 08:03:29 UTC	8350	IN	Data Raw: 38 36 2d 58 36 34 2d 58 36 34 22 2c 22 50 61 63 6b 61 67 65 52 61 6e 6b 22 3a 33 30 30 38 32 2c 22 50 6c 61 74 66 6f 72 6d 44 65 70 65 6e 64 65 6e 63 69 65 73 22 3a 5b 7b 22 4d 61 78 54 65 73 74 65 64 22 3a 32 38 31 34 37 35 31 31 36 33 30 38 38 38 39 36 2c 22 4d 69 6e 56 65 72 73 69 6f 6e 22 3a 32 38 31 34 37 35 30 39 37 30 34 37 38 35 39 32 2c 22 50 6c 61 74 66 6f 72 6d 4e 61 6d 65 22 3a 22 57 69 6e 64 6f 77 73 2e 55 6e 69 76 65 73 61 6c 22 7d 5d 2c 22 50 6c 61 74 66 6f 72 6d 44 65 70 65 6e 64 65 6e 63 79 58 6d 6c 42 6c 6f 62 22 3a 22 7b 5c 22 62 6c 6f 62 2e 76 65 72 73 69 6f 6e 5c 22 3a 31 36 38 38 38 36 37 30 34 30 35 32 36 33 33 36 2c 5c 22 63 6f 6e 74 65 6e 74 2e 62 75 6e 64 6c 65 64 50 61 63 6b 61 67 65 73 5c 22 3a 5b 5c 22 4d 69 63 72 6f 73 6f Data Ascii: 86-X64-X64\",\"PackageRank\":30082,\"PlatformDependencies\":{\"[\"MaxTested\":2814751163088896,\"MinVersion\":2814750970478592,\"PlatformName\":\"Windows.Universal\"}],\"PlatformDependencyXmlBlob\":\"({\"blob.version\":16888670 40526336,\"content.bundledPackages\":{\"[\"Microso
2022-04-08 08:03:29 UTC	8354	IN	Data Raw: 22 5d 2c 22 4c 69 63 65 6e 73 69 6e 67 4b 65 79 49 64 73 22 3a 5b 22 31 22 5d 7d 2c 7b 22 45 6e 74 69 74 6c 65 6d 65 6e 74 4b 65 79 73 22 3a 5b 22 77 65 73 3a 41 70 70 3a 64 30 39 33 32 63 37 33 2d 65 37 33 30 2d 34 36 38 30 2d 62 63 34 34 2d 61 35 39 30 38 66 65 63 62 66 38 62 3a 46 75 6c 6c 22 5d 2c 22 4c 69 63 65 6e 73 69 6e 67 4b 65 79 49 64 73 22 3a 5b 22 31 22 5d 7d 2c 7b 22 45 6e 74 69 74 6c 65 6d 65 6e 74 69 74 6c 65 6d 65 6e 74 4b 65 79 73 22 3a 5b 22 62 69 67 3a 39 4e 4d 50 4a 39 Data Ascii: \"],\"LicensingKeyIds\":\"[\"1\"]\",\"EntitlementKeys\":{\"wes:App:d0932c73-e730-4680-bc44-a5908fecbf8b:Full \"],\"LicensingKeyIds\":\"[\"1\"]\",\"EntitlementKeys\":{\"wes:App:6ead4a77-d076-4866-9188-621a5b1f414f:Full\"],\"Licensin gKeyIds\":\"[\"1\"]\",\"EntitlementKeys\":{\"big:9NMPJ9
2022-04-08 08:03:29 UTC	8358	IN	Data Raw: 22 47 4d 22 2c 22 47 45 22 2c 22 47 48 22 2c 22 47 49 22 2c 22 47 4c 22 2c 22 47 44 22 2c 22 47 50 22 2c 22 47 55 22 2c 22 47 47 22 2c 22 47 4e 22 2c 22 47 57 22 2c 22 47 59 22 2c 22 48 54 22 2c 22 48 4d 22 2c 22 48 4e 22 2c 22 41 5a 22 2c 22 42 53 22 2c 22 42 42 22 2c 22 42 59 22 2c 22 42 5a 22 2c 22 42 4a 22 2c 22 42 4d 22 2c 22 42 54 22 2c 22 4b 4d 22 2c 22 43 47 22 2c 22 43 44 22 2c 22 43 4b 22 2c 22 43 58 22 2c 22 43 4d 22 2c 22 43 49 22 2c 22 43 57 2 2 2c 22 4a 4d 22 2c 22 53 4a 22 2c 22 4a 45 22 2c 22 4b 49 22 2c 22 4b 47 22 2c 22 4c 41 22 2c 22 4c 53 22 2c 22 4c 52 22 2c 22 4d 4f 22 2c 22 4d 4b 22 2c 22 4d 47 22 2c 22 4d 57 22 2c 22 49 4d 22 2c 22 4d 48 22 2c 22 4d 51 22 2c 22 4d 55 22 2c 22 59 54 22 2c 22 46 4d 22 2c 22 4d 44 22 2c 22 4d 4e 22 2c Data Ascii: \"GM\",\"GE\",\"GH\",\"GI\",\"GL\",\"GD\",\"GP\",\"GU\",\"GG\",\"GN\",\"GW\",\"GY\",\"HT\",\"HM\",\"HN\",\"AZ\",\"BS\",\"BB\",\"BY\",\"BZ \"\",\"BJ\",\"BM\",\"BT\",\"KM\",\"CG\",\"CD\",\"CK\",\"CX\",\"CC\",\"CI\",\"CW\",\"JM\",\"SJ\",\"JE\",\"KI\",\"KG\",\"LA\",\"LS\",\"LR\",\"MO\",\"MK\",\"MG \"\",\"MW\",\"IM\",\"MH\",\"MQ\",\"MU\",\"YT\",\"FM\",\"MD\",\"MN\",

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:29 UTC	8362	IN	Data Raw: 5f 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 5c 22 2c 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 59 6f 75 72 50 68 6f 6e 65 5f 31 2e 32 30 30 31 32 2e 31 33 35 2e 37 30 5f 61 72 6d 5f 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 5c 22 2c 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 59 6f 75 72 50 68 6f 6e 65 5f 31 2e 32 30 30 31 32 2e 31 33 35 2e 37 30 5f 78 36 34 5f 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 5c 22 5d 2c 5c 22 63 6f 6e 74 65 6e 74 2e 69 73 4d 61 69 6e 5c 22 3a 66 61 6c 73 65 2c 5c 22 63 6f 6e 74 65 6e 74 2e 70 61 63 6b 61 67 65 49 64 5c 22 3a 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 59 6f 75 72 50 68 6f 6e 65 5f 32 30 32 30 2e 33 30 35 2e 32 33 33 31 2e 37 30 5f 6e 65 75 74 72 61 6c 5f 7e 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 5c 22 2c 5c 22 63 6f 6e 74 65 6e Data Ascii: __8wekyb3d8bbwe"],"Microsoft.YourPhone_1.20012.135.70_arm__8wekyb3d8bbwe"],"Microsoft.YourPhone_1.20012.135.70_x64__8wekyb3d8bbwe"],"content.isMain":false,"content.packageId":"Microsoft.YourPhone_2020.305.2331.70_neutral~__8wekyb3d8bbwe"],"conten
2022-04-08 08:03:29 UTC	8366	IN	Data Raw: 61 6e 6b 22 3a 33 30 30 33 35 2c 22 50 6c 61 74 66 6f 72 6d 44 65 70 65 6e 64 65 6e 63 69 65 73 22 3a 5b 7b 22 4d 61 78 54 65 73 74 65 64 22 3a 32 38 31 34 37 35 30 39 37 30 34 37 38 35 39 32 2c 22 4d 69 6e 56 65 72 73 69 6f 6e 22 3a 32 38 31 34 37 35 30 38 39 30 30 30 33 38 34 2c 22 50 6c 61 74 66 6f 72 6d 4e 61 6d 65 22 3a 22 7f 69 6e 64 6f 77 73 2e 58 62 6f 78 22 7d 5d 2c 22 50 6c 61 74 66 6f 72 6d 44 65 70 65 6e 64 65 6e 63 79 58 6d 6c 42 6c 6f 62 2 2 3a 22 7b 5c 22 62 6c 6f 62 2e 76 65 72 73 69 6f 6e 5c 22 3a 31 36 38 38 38 36 37 30 34 30 35 32 36 33 33 36 2c 5c 22 63 6f 6e 74 65 6e 74 2e 62 75 6e 64 6c 65 64 50 61 63 6b 61 67 65 73 5c 22 3a 5b 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 59 6f 75 72 50 68 6f 6e 65 5f 31 2e 32 30 30 33 32 2e 31 31 31 2e 37 Data Ascii: ank":.30035,"PlatformDependencies":[{"MaxTested":.2814750970478592,"MinVersion":.2814750890000384,"PlatformName":"Windows.Xbox"}],"PlatformDependencyXmlBlob":"{"blob.version":.1688867040526336,"content.bundledPackages":["Microsoft.YourPhone_1.20032.111.7
2022-04-08 08:03:29 UTC	8370	IN	Data Raw: 6f 72 74 65 64 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 5d 2c 22 45 78 70 65 72 69 65 6e 63 65 49 64 73 22 3a 5b 5d 2c 22 4d 61 78 44 6f 77 6e 6c 6f 61 64 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 32 39 37 30 39 33 35 32 32 2c 22 4d 61 78 49 6e 73 74 61 6c 6c 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 32 36 36 34 37 37 35 36 38 2c 22 50 61 63 6b 61 67 65 46 6f 72 6d 61 74 22 3a 22 41 70 70 78 42 75 6e 64 6c 65 22 2c 22 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 2e 59 6f 75 72 50 68 6f 6e 65 5f 38 6f 72 65 6b 79 62 33 64 38 62 62 77 65 2 2 2c 22 4d 61 69 6e 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 46 6f 72 44 6c 63 22 3a 6e 75 6c 6c 2c 22 50 61 63 6b 61 67 65 46 75 6c 6c 4e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 Data Ascii: orted_8wekyb3d8bbwe"],"ExperienceIds":[],"MaxDownloadSizeInBytes":.297093522,"MaxInstallSizeInBytes":.266477568,"PackageFormat":"AppxBundle","PackageFamilyName":"Microsoft.YourPhone_8wekyb3d8bbwe","MainPackageFamilyNameForDlc":null,"PackageFullName":"Micros
2022-04-08 08:03:29 UTC	8374	IN	Data Raw: 69 65 6e 74 53 65 72 76 65 72 22 2c 22 72 65 6d 6f 74 65 53 79 73 74 65 6d 22 2c 22 70 68 6f 6e 65 43 61 6c 6c 22 2c 22 63 6f 6e 66 69 72 6d 41 70 70 43 6c 6f 73 65 22 2c 22 70 68 6f 6e 65 4c 69 6e 65 54 72 61 6e 73 70 6f 72 74 4d 61 6e 61 67 65 6d 65 6e 74 22 2c 22 70 68 6f 6e 65 43 61 6c 6c 53 79 73 74 65 6d 22 2c 22 74 61 72 67 65 74 65 64 43 6f 6e 74 65 6e 74 22 2c 22 72 75 6e 46 75 6c 6c 54 72 75 73 74 22 2c 22 70 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 22 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 75 6e 73 69 67 6e 65 64 50 61 63 6b 61 67 65 4d 61 6e 61 67 65 6d 65 6e 74 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 73 74 6f 72 65 46 69 6c 74 65 72 2e 63 6f 72 65 2e 6e 6f 74 53 75 70 70 6f 72 74 65 64 5f 38 77 65 Data Ascii: ientServer","remoteSystem","phoneCall","confirmAppClose","phoneLineTransportManagement","phoneCallSystem","targetedContent","runFullTrust","packageManagement","Microsoft.unsignedPackageManagement_8wekyb3d8bbwe","Microsoft.storeFilter.core.notSupported_8we
2022-04-08 08:03:29 UTC	8378	IN	Data Raw: 5c 22 3a 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 59 6f 75 72 50 68 6f 6e 65 5f 30 2e 32 32 30 32 32 2e 31 38 30 2e 30 5f 78 38 36 5f 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 5c 22 2c 5c 22 73 74 75 62 5c 22 3a 74 72 75 65 2c 5c 22 74 64 66 73 5c 22 3a 5b 7b 5c 22 6e 61 6d 65 5c 22 3a 5c 22 57 69 6e 64 6f 77 73 2e 55 6e 69 76 65 72 73 61 6c 5c 22 2c 5c 22 76 6d 61 78 5c 22 3a 32 38 31 34 37 35 31 30 31 33 30 31 31 34 35 36 2c 5c 22 76 6d 69 6e 5c 22 3a 32 38 31 34 37 35 31 30 31 33 30 31 31 34 35 36 7d 5d 7d 5d 2c 5c 22 70 6f 6c 69 63 79 5c 22 3a 7b 5c 22 63 61 74 65 67 6f 72 7 9 2e 66 69 72 73 74 5c 22 3a 5c 22 61 70 70 5c 22 2c 5c 22 63 61 74 65 67 6f 72 79 2e 73 65 63 6f 6e 64 5c 22 3a 5c 22 50 72 6f 64 75 63 74 69 76 69 74 79 5c 22 2c 5c 22 6f 70 74 4f 75 Data Ascii: \":"Microsoft.YourPhone_0.22022.180.0_x86__8wekyb3d8bbwe"],"stub":true,"tdfs":{"name":"Windows.Universal"},"vmax":".2814751013011456","vmin":".2814751013011456}}},"policy":{"category.first":"app"},"category.second":"Productivity"},"optOu
2022-04-08 08:03:29 UTC	8382	IN	Data Raw: 22 41 76 61 69 6c 61 62 69 6c 69 74 79 3b 33 22 2c 22 41 76 61 69 6c 61 62 69 6c 69 74 79 42 53 63 68 65 6d 61 22 3a 22 41 76 61 69 6c 61 62 69 6c 69 74 79 55 6e 69 66 69 65 64 41 70 70 3b 33 22 2c 22 41 76 61 69 6c 61 62 69 6c 69 74 79 49 64 22 3a 22 39 5a 33 52 50 4b 48 48 30 46 33 4c 22 2c 22 43 6f 6e 64 69 74 69 6f 6e 73 22 3a 7b 22 43 6c 69 65 6e 74 43 6f 6e 64 69 74 69 6f 6e 73 22 3a 7b 22 41 6c 6c 6f 77 65 64 50 6c 61 74 66 6f 72 6d 73 22 3a 5b 7b 22 4d 61 78 56 65 72 73 69 6f 6e 22 3a 32 31 34 37 34 38 33 36 34 37 2c 22 4d 69 6e 56 65 72 73 69 6f 6e 22 3a 30 2c 22 5 0 6c 61 74 66 6f 72 6d 4e 61 6d 65 22 3a 22 57 69 6e 64 6f 77 73 2e 44 65 73 6b 74 6f 70 22 7d 2c 7b 22 4d 61 78 56 65 72 73 69 6f 6e 22 3a 32 31 34 37 34 38 33 36 34 37 2c 22 4d 69 6e Data Ascii: "Availability;3","AvailabilityBSchema":"AvailabilityUnifiedApp;3","AvailabilityId":"9Z3RPKHH0F3L","Conditions":{"ClientConditions":{"AllowedPlatforms":[{"MaxVersion":.2147483647,"MinVersion":0,"PlatformName":"Windows.Desktop"}],"MaxVersion":.2147483647,"Min
2022-04-08 08:03:29 UTC	8384	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.3	50016	40.112.88.60	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:28 UTC	8310	OUT	GET /v1/a/opportunity?pg=PC000P0FR5.0000000IQ8&unid=&placementType=PostOOBE&app=&pid=425106558&cid=128000000001392729&tid=700342085&reqasid=8d771849a7234e0ab71c2ac9a71f46b4®ion=US&lang=EN-US&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.17134.1&mo~&cap=&aid=&anid=&muid=&persid=&itemId=9N0866F504W8&skuld=0010&installKind=Install&ctid=store-curated-posttoobe&bSrc=i.t&asid=e4896368b6a64edb9547962c054e1d7c&time=20220408T170238Z HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Host: ris.api.iris.microsoft.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:29 UTC	8310	IN	HTTP/1.1 204 No Content Content-Length: 0 Server: Microsoft-HTTPAPI/2.0 request-id: 3b39271d-dbd6-4eb2-a65c-936a6d90daba Date: Fri, 08 Apr 2022 08:03:28 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.3	50018	40.112.88.60	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:29 UTC	8384	OUT	GET /v1/a/opportunity?pg=PC000P0FR5.0000000IQ8&unid=&placementType=PostOOBE&app=&pid=425106558&cid=128000000001392729&tid=700342085&reqasid=8d771849a7234e0ab71c2ac9a71f46b4®ion=US&lang=EN-US&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.17134.1&mo=&cap=&aid=&anid=&muid=&persid=&itemId=9WZDNCRFJ10M&skuld=0010&installKind=Install&ctid=store-curated-postoobe&bSrc=i.t&asid=e4896368b6a64edb9547962c054e1d7c&time=20220408T170240Z HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Host: ris.api.iris.microsoft.com Connection: Keep-Alive
2022-04-08 08:03:29 UTC	8385	IN	HTTP/1.1 204 No Content Content-Length: 0 Server: Microsoft-HTTPAPI/2.0 request-id: 16d561b9-4b64-46a5-9095-8f774241a94a Date: Fri, 08 Apr 2022 08:03:29 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49979	20.82.210.154	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:20 UTC	19	OUT	GET /v3/Delivery/Placement?pubid=da63df93-3dbc-42ae-a505-b34988683ac7&pid=338389&adm=2&w=1&h=1&wpw=1&hpx=1&fmt=json&cltp=app&dim=le&rafb=0&nct=1&pm=1&cfmt=text,image,poly&sft=jpeg,png,gif&topt=1&poptin=0&localid=w.472DC600-FEAB-E7F8-720D-1E33F00FD1E7&ctry=US&time=20220408T170212Z&lc=en-US&pl=en-US&idtp=mid&uid=4388269c-b420-4134-ac19-bc7ca8a19ac1&aid=00000000-0000-0000-0000-000000000000&ua=WindowsShellClient%2F9.0.40929.0%20%28Windows%29&asid=3382b3df4d44412c80bfa0684fe70791&ctmode=MultiSession&arch=x64&cdm=1&cdmver=10.0.17134.1&devfam=Windows.Desktop&devform=Unknown&devosver=10.0.17134.1&disp horzres=1280&dispsize=17.1&dispvertres=1024&isu=0&lo=1463022&metered=false&nettype=ethernet&npid=sc-338389&oemName=hsehht%2C%20Inc.&oemid=hsehht%2C%20Inc.&ossku=Professional&smBiosDm=hsehht7%2C1&tl=2&tsu=1463022&waasBldFlt=1&waasCfgExp=1&waasCfgSet=1&waasRetail=1&waasRing= HTTP/1.1 Accept-Encoding: gzip, deflate X-SDK-CACHE: chs=0&imp=0&chf=0&ds=50583&fs=32319&sc=6 X-SDK-HW-TOKEN: t=EwDYAppeBAAUIAKXDAofTQM+n+MaRVFKzH/ehWgAAdVW0iu23GlXjRyUBGA+V5LMoU/IMaTj obBnQosoTe6w30OZEf3HulBKeYXog3CqxSfjOHeF/J4iLS/gKyhq/ZV/xtrYHZ35PhcBmS2qzlwNBiXp0+I4efq5ns DEEESQ06VT9dPxHYgWIFLG65LRysydA1IM9dDPzftFvDLM/ickJDFevqkA3hG2mKV46lqHL4CT7eP4Hk0/MOrRp8JB 5tew/jl7o25TIEcXI9Ohbx1KlwUuqQcpj0nfDAUZEjkQqVS2z/wQaH+/fdlFO/AoxQl3CbcoTeaCp3XlesBJX0bxVN zc22qQqCPfGWQ/Sb52rGvkgBRvdW8DFg8ToMjfqPyYDZgAAACE3mODPOPAwVqAFPV53gZZc0aOkGu+jjWn w46hEU9aCKlpEDkH6SywZSJq+Z6lyumM/ZCz1/Exb6MZih9PGVRFV0dS4rZOFTTSEXw5x6gJoWeqkJZJqul+/LQNZp daM/TGNQWhUnnbhyzuL3J52vfTsZzATC6HDHUtCP567luQfNjw1zOBQG/Pho8+d+FIHWtCPKMxAdH+rX7PpflRpHT m7bd+H+rsPvLvdstjafDCGAADV0pkaM4oU0n35rzdzjoAWTcazcHXkrs0Gr34gDLPkE96nUwLpeDIXN3LontP44gHn gfTJA4vz4io7zKxVkmOUwHoTarQK7POiXKiwa8x1QRMWjr0xK5k34eIR6SWW4uOhaTkCvnxjxlUvc2iz/sxwQS6ZoJu zJ60lcBcq6ptimZGdy/yulx2kCNYcUG/nBNXbdKtF3Kz0nMb3Ry9n0QIm/ncP9d68+s4WiRlc+RuW5MPI3aHMGGT2s nchu87pA34+QqKDXqpJZVZnC+RaoA8mYs8BGPqZ//PidcqGGmzw2vccoT1N6pSAD7mXPYm9QONX68BD3 4uYAk1VCPPhRpsKh41QE=&p= Cache-Control: no-cache MS-CV: BYqskdYKuUKf7ZeJ.0 User-Agent: WindowsShellClient/9.0.40929.0 (Windows) X-SDK-HWF: tch0,m301,m751,mA01,mT01 Host: arc.msn.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:29 UTC	8387	IN	HTTP/1.1 200 OK Cache-Control: no-cache Pragma: no-cache Content-Type: application/octet-stream Expires: -1 Last-Modified: Mon, 01 Jan 0001 00:00:00 GMT ETag: "wy8fVV3cy06QlZhZUaOlBEoVMBnt4x8NjH3c50VWOxM=_1440" MS-CorrelationId: 90bb4944-6ad9-4afc-a150-a1d991f9a0c5 MS-RequestId: 6463b563-ca83-4b92-b11c-ccc435dc7307 MS-CV: ul/zKTnn50mW3R1i.0 X-Microsoft-SLSCClientCache: 1440 Content-Disposition: attachment; filename=environment.cab X-Content-Type-Options: nosniff Date: Fri, 08 Apr 2022 08:03:29 GMT Connection: close Content-Length: 30958
2022-04-08 08:03:29 UTC	8387	IN	Data Raw: 4d 53 43 46 00 00 00 00 be 37 00 00 00 00 00 00 44 00 00 00 00 00 00 03 01 01 00 01 00 04 00 20 e0 00 00 14 00 00 00 00 00 10 00 be 37 00 00 30 41 00 00 00 00 00 00 00 00 00 64 00 00 00 01 00 01 00 f3 5b 00 00 00 00 00 00 00 00 00 00 80 00 65 6e 76 69 72 6f 6e 6d 65 6e 74 2e 63 61 62 00 27 c3 6c fd 52 37 f3 5b 43 4b ed 7a 05 58 55 dd d6 ee de 9b ee 96 6e 11 e9 b5 e9 52 69 a5 a4 bb 5b a4 bb 6b d3 ad a2 74 77 08 08 08 d2 21 25 dd a0 80 80 48 4a 4a 83 c4 dd e8 17 9e ef d4 7f fe 7b cf 73 fe 7b ef b7 9f 67 ef bd e6 5c 73 ce 35 63 8c f1 8e 77 8c 25 af 22 2e 05 82 7f da c9 40 df 3f 12 3f fe 40 08 60 30 08 0c 42 04 bd f8 08 02 11 7e af c1 fd de 06 10 05 fd f6 31 85 7f af 5b 85 72 83 7e fa f8 83 cc 6c 5d 2d 1d ed 6c 6d cc 6c 9d d9 dd 6d ac 41 f8 7a 2e Data Ascii: MSCF7D 70Adj[environment.cab\lR7[CKzXUnRi[ktwl%HJJ[s[gl5cw%".@@?@`0B~1[~l]-lmlmAz.
2022-04-08 08:03:29 UTC	8403	IN	Data Raw: b3 49 a2 0d ff f6 07 56 2e e0 cd 9b 1f 2c 88 a2 01 ec 5e 7b 96 ac 79 f1 dc 76 c5 85 50 e5 c7 c8 45 07 64 59 b3 b7 80 da 46 59 e2 3c b1 95 cb ed 18 a0 46 1e 05 b6 ad 0f aa c7 d6 26 8a 7a 17 6e 85 5c 5c 6e b7 9b 98 29 fc 15 9c b1 63 23 9c 27 9a ba 82 04 21 f1 ec 76 cf 7a 3c 9a dc 26 02 a4 4b 13 b7 f5 66 dc 71 d6 12 42 66 da ba 5c 82 4f 0a 63 8b 27 ed ac 5b 4a 30 41 b8 22 8b 2f b7 4c 07 eb 6d 35 30 dd 9f 04 c2 94 77 e9 20 77 b3 ca 0d 58 a9 21 17 bb 64 c6 3c 80 fd e9 00 b3 78 2d 96 fe 20 b6 4c c6 4a 0b e6 fc 7a 35 83 21 a9 5b fb 9f ec fd f1 bd a9 3a 79 0e 3d a3 0c 9a 4f 59 1e be de 85 65 6f ea 2b b7 1c 1f d9 51 fd 01 a2 7c 91 b5 30 82 07 05 30 82 04 ed a0 03 02 01 02 02 13 33 00 00 00 08 59 e3 94 e0 54 c7 17 5d 00 00 00 00 00 08 30 0d 06 09 2a 86 48 86 f7 0d Data Ascii: IV.,^jvPEdYFY<F&znl\nc#`lvz<&KfqBfOc[J0A"/Lm50w wXld<x- Lj5z[;y=OYeo+Q[003YT]T0*H

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.3	50021	40.112.88.60	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:29 UTC	8386	OUT	GET /v1/a/opportunity?pg=PC000P0FR5.0000000IQ8&unid=&placementType=PostOOBE&app=&pid=425106558&cid=128000000001392729&tid=700342085&reqasid=8d771849a7234e0ab71c2ac9a71f46b4®ion=US&lang=EN-US&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.17134.1&mo=&cap=&aid=&anid=&muid=&persid=&itemId=9NC2FBTHCJV8&skuld=0010&installKind=RedirectTile&ctid=store-curated-postoobe&bSrc=i.t&asid=e4896368b6a64edb9547962c054e1d7c&time=20220408T170243Z HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Host: ris.api.iris.microsoft.com Connection: Keep-Alive
2022-04-08 08:03:29 UTC	8387	IN	HTTP/1.1 204 No Content Content-Length: 0 Server: Microsoft-HTTPAPI/2.0 request-id: 15ce020e-8099-43ec-9769-a05c49540657 Date: Fri, 08 Apr 2022 08:03:29 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.3	50022	40.112.88.60	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:29 UTC	8418	OUT	GET /v1/a/opportunity?pg=PC000P0FR5.0000000IQ8&unid=&placementType=PostOOBE&app=&pid=425106558&cid=128000000001392729&tid=700342085&reqasid=8d771849a7234e0ab71c2ac9a71f46b4®ion=US&lang=EN-US&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.17134.1&mo=&cap=&aid=&anid=&muid=&persid=&itemId=9NBLGGH1CQ7L&skuld=0010&installKind=RedirectTile&ctid=store-curated-postoobe&bSrc=i.t&asid=e4896368b6a64edb9547962c054e1d7c&time=20220408T170245Z HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Host: ris.api.iris.microsoft.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:29 UTC	8418	IN	HTTP/1.1 204 No Content Content-Length: 0 Server: Microsoft-HTTPAPI/2.0 request-id: a378e3ca-3722-47f6-be97-76d9ef742d76 Date: Fri, 08 Apr 2022 08:03:29 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.3	50024	40.112.88.60	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:30 UTC	8418	OUT	GET /v1/a/impression?pg=PC000P0FR5.0000000IQ8&unid=&placementType=PostOOBE&app=&pid=425106558&cid=128000000001392729&tid=700342085&reqasid=8d771849a7234e0ab71c2ac9a71f46b4®ion=US&lang=EN-US&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.17134.1&mo=&cap=&aid=&anid=&muid=&persid=&bSrc=i.t&time=20220408T170247Z&asid=e4896368b6a64edb9547962c054e1d7c&eid= HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Host: ris.api.iris.microsoft.com Connection: Keep-Alive
2022-04-08 08:03:30 UTC	8419	IN	HTTP/1.1 204 No Content Content-Length: 0 Server: Microsoft-HTTPAPI/2.0 request-id: df9c344e-6ed5-4e51-b955-8a22664191fe Date: Fri, 08 Apr 2022 08:03:29 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.3	50023	52.152.110.14	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:30 UTC	8419	OUT	GET /SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%D/x64/10.0.17134.1/0?CH=17&L=en-US&P=&PT=0x30&WUA=10.0.17134.1&MK=4MtpozR6MODPIGb&MD=EefvrDUR HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Windows-Update-Agent/10.0.10011.16384 Client-Protocol/1.81 Host: sls.update.microsoft.com
2022-04-08 08:03:30 UTC	8420	IN	HTTP/1.1 200 OK Cache-Control: no-cache Pragma: no-cache Content-Type: application/octet-stream Expires: -1 Last-Modified: Mon, 01 Jan 0001 00:00:00 GMT ETag: "wy8fVV3cy06QIZhZUaOlBEoVMBnt4x8NJH3c50VWOxM= _1440" MS-CorrelationId: 50a0abe1-c847-462e-b060-4c273913643d MS-RequestId: d8bf9f39-83d5-4d69-997b-8181ebe00294 MS-CV: 69kH4xewCEieSR9K.0 X-Microsoft-SLSCClientCache: 1440 Content-Disposition: attachment; filename=environment.cab X-Content-Type-Options: nosniff Date: Fri, 08 Apr 2022 08:03:29 GMT Connection: close Content-Length: 30958
2022-04-08 08:03:30 UTC	8421	IN	Data Raw: 4d 53 43 46 00 00 00 00 be 37 00 00 00 00 00 00 44 00 00 00 00 00 00 03 01 01 00 01 00 04 00 20 e0 00 00 14 00 00 00 00 00 10 00 be 37 00 00 30 41 00 00 00 00 00 00 00 00 64 00 00 00 01 00 01 00 f3 5b 00 00 00 00 00 00 00 00 00 00 65 6e 76 69 72 6f 6e 6d 65 6e 74 2e 63 61 62 00 27 c3 6c fd 52 37 f3 5b 43 4b ed 7a 05 58 55 dd d6 ee de 9b ee 96 6e 11 e9 b5 e9 52 69 a5 a4 bb 5b a4 bb 6b d3 ad a2 74 77 08 08 08 d2 21 25 dd a0 80 80 48 4a 4a 83 c4 dd e8 17 9e ef d4 7f fe 7b cf 73 fe 7b ef b7 9f 67 ef bd e6 5c 73 ce 35 63 8c f1 8e 77 8c 25 af 22 2e 05 82 7f da c9 40 df 3f 12 3f fe 40 08 60 30 08 0c 42 04 bd f8 08 02 11 7e af c1 fd de 06 10 05 fd f6 31 85 7f af 5b 85 72 83 7e fa f8 83 cc 6c 5d 2d 1d ed 6c 6d cc 6c 9d d9 dd 6d ac 41 f8 7a 2e Data Ascii: MSCF7D 70Ad[environment.cab'IR7[CKzXUnRi[ktw!%HJJ[s[gl5cw%".@@??@ '0B-1[r-l]mImAz.
2022-04-08 08:03:30 UTC	8436	IN	Data Raw: b3 49 a2 0d ff f6 07 56 2e e0 cd 9b 1f 2c 88 a2 01 ec 5e 7b 96 ac 79 f1 dc 76 c5 85 50 e5 c7 c8 45 07 64 59 b3 b7 80 da 46 59 e2 3c b1 95 cb ed 18 a0 46 1e 05 b6 ad 0f aa c7 d6 26 8a 7a 17 6e 85 5c 5c 6e b7 9b 98 29 fc 15 9c b1 63 23 9c 27 9a ba 82 04 21 f1 ec 76 cf 7a 3c 9a dc 26 02 a4 4b 13 b7 f5 66 dc 71 d6 12 42 66 da ba 5c 82 4f 0a 63 8b 27 ed ac 5b 4a 30 41 b8 22 8b 2f b7 4c 07 eb 6d 35 30 dd 9f 04 c2 94 77 e9 20 77 b3 ca 0d 58 a9 21 17 bb 64 c6 3c 80 fd e9 00 b3 78 2d 96 fe 20 b6 4c c6 4a 0b e6 fc 7a 35 83 21 a9 5b fb 9f ec fd f1 bd a9 3a 79 0e 3d a3 0c 9a 4f 59 1e be de 85 65 6f ea 2b b7 1c 1f d9 51 fd 01 a2 7c 91 b5 30 82 07 05 30 82 04 ed a0 03 02 01 02 02 13 33 00 00 00 08 59 e3 94 e0 54 c7 17 5d 00 00 00 00 08 30 0d 06 09 2a 86 48 86 f7 0d Data Ascii: IV.,^[yvPEdYFY<F&znl\n)c#'\vz<&KfqBfOc'[J0A"/Lm50w wXld<x- LJz5I[.y=OYeo+Q[003YT]0"H

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.3	50025	40.112.88.60	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:30 UTC	8419	OUT	GET /v1/a/installComplete?pg=PC000P0FR5.0000000IQ8&unid=&placementType=PostOOBE&app=&pid=425106554&c id=128000000001392709&tid=700342084&reqasid=cbed9efce7f24d8b9b00c27d1eebe749®ion=US&lang=EN-US&oe m=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.17134.1&mo=&cap=&aid=&anid=&muid =&persid=&itemId=9WZDNCRFJ3P2&skuld=0010&installKind=Install&ctid=store-curated-postoobe&bSrc=i.t&as id=ac8063a32da047dabe6fd5f6a689fb6c&time=20220408T170253Z HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Host: ris.api.iris.microsoft.com Connection: Keep-Alive
2022-04-08 08:03:30 UTC	8420	IN	HTTP/1.1 204 No Content Content-Length: 0 Server: Microsoft-HTTPAPI/2.0 request-id: 6f879072-0c31-40c0-ae82-41d816b3588f Date: Fri, 08 Apr 2022 08:03:30 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.3	50026	40.112.88.60	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:30 UTC	8451	OUT	GET /v1/a/installComplete?pg=PC000P0FR5.0000000IQ8&unid=&placementType=PostOOBE&app=&pid=425106554&c id=128000000001392709&tid=700342084&reqasid=cbed9efce7f24d8b9b00c27d1eebe749®ion=US&lang=EN-US&oe m=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.17134.1&mo=&cap=&aid=&anid=&muid =&persid=&itemId=9NBLGGH5FV99&skuld=0010&installKind=Install&ctid=store-curated-postoobe&bSrc=i.t&as id=ac8063a32da047dabe6fd5f6a689fb6c&time=20220408T170257Z HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Host: ris.api.iris.microsoft.com Connection: Keep-Alive
2022-04-08 08:03:30 UTC	8451	IN	HTTP/1.1 204 No Content Content-Length: 0 Server: Microsoft-HTTPAPI/2.0 request-id: a8e39c7d-a013-4108-b3f8-4982f6f6a8d3 Date: Fri, 08 Apr 2022 08:03:30 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.3	50027	20.54.110.249	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:30 UTC	8452	OUT	GET /v7.0/products/lookup?alternateId=PackageFamilyName&value=Microsoft.BingNews_8wekyb3d8bbwe&marke t=US&languages=en-US%2Cen%2Cneutral&fieldsTemplate=InstallAgent&mold=Public&oemId=Public&scmId=Public HTTP/1.1 Connection: Keep-Alive Content-Type: application/json User-Agent: Install Service MS-CV: t1Ts4111nkyKVrtC.0.2.4 Host: displaycatalog.mp.microsoft.com
2022-04-08 08:03:30 UTC	8453	IN	HTTP/1.1 200 OK Connection: close Date: Fri, 08 Apr 2022 08:03:30 GMT Content-Type: application/json; charset=utf-8 Server: Kestrel Transfer-Encoding: chunked Vary: Authorization MS-CorrelationId: ac521aff-b4cb-423d-807f-ab051d3e9d41 MS-RequestId: e461c70b-5ca0-44e2-a071-65dde1cce5c0 MS-CV: t1Ts4111nkyKVrtC.0.2.4.422987100.0.1.422987100.4131967894.0 X-Content-Type-Options: nosniff MS-ServerId: 65db49-ldvIm Region: neu Node: aks-systempool-37630073-vmss00003a MS-DocumentVersions: 9WZDNCRFHVFWJ4011

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:30 UTC	8453	IN	Data Raw: 32 66 64 35 66 0d 0a 7b 22 42 69 67 49 64 73 22 3a 5b 22 39 57 5a 44 4e 43 52 46 48 56 46 57 22 5d 2c 22 48 61 73 4d 6f 72 65 50 61 67 65 73 22 3a 66 61 6c 73 65 2c 22 50 72 6f 64 75 63 74 73 22 3a 5b 7b 22 4c 61 73 74 4d 6f 64 69 66 69 65 64 44 61 74 65 22 3a 22 32 30 32 32 2d 30 33 2d 31 30 54 32 32 3a 30 39 3a 33 37 2e 35 39 30 37 36 38 31 5a 22 2c 22 4c 6f 63 61 6c 69 7a 65 64 50 72 6f 70 65 72 74 69 65 73 22 3a 5b 7b 22 46 72 61 6e 63 68 69 73 65 73 2 2 3a 5b 5d 2c 22 49 6d 61 67 65 73 22 3a 5b 7b 22 46 69 6c 65 49 64 22 3a 22 32 30 30 30 30 30 30 30 30 38 31 37 31 39 32 31 31 22 2c 22 45 49 53 4c 69 73 74 69 6e 67 49 64 65 6e 74 69 66 69 65 72 22 3a 6e 75 6c 6c 2c 22 42 61 63 6b 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 23 32 36 32 46 33 38 22 Data Ascii: 2fd5f{"BigIds":["9WZDNCRFHFW"],"HasMorePages":false,"Products":[{"LastModifiedDate":"2022-03-10T2 2:09:37.5907681Z","LocalizedProperties":{"Franchises":"","Images":{"Fileid":"2000000000081719211","EISListingIdentifier":null,"BackgroundColor":"#262F38"}}
2022-04-08 08:03:30 UTC	8457	IN	Data Raw: 38 65 34 2d 30 65 32 32 33 65 64 36 63 35 61 31 2e 64 66 39 63 34 35 65 66 2d 35 61 63 36 2d 34 64 32 66 2d 62 35 32 39 2d 38 64 65 66 65 64 37 30 34 64 31 63 22 2c 22 57 69 64 74 68 22 3a 36 36 7d 2c 7b 22 46 69 6c 65 49 64 22 3a 22 32 30 30 30 30 30 30 30 30 38 31 37 31 38 39 32 38 22 2c 22 45 49 53 4c 69 73 74 69 6e 67 49 64 65 6e 74 69 66 69 65 72 22 3a 6e 75 6c 6c 2c 22 42 61 63 6b 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 23 32 36 32 46 33 38 22 2c 22 43 61 70 74 69 6f 6e 22 3a 22 22 2c 22 46 69 6c 65 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 31 37 32 38 2c 22 46 6f 72 65 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 22 2c 22 48 65 69 67 68 74 22 3a 38 38 2c 22 49 6d 61 67 65 50 6f 73 69 74 69 6f 6e 49 6e 66 6f 22 3a 22 22 2c 22 49 6d 61 67 65 50 75 Data Ascii: 8e4-0e223ed6c5a1.df9c45ef-5ac6-4d2f-b529-8defed704d1c","Width":66},{Fileid":"2000000000081718928","EISListingIdentifier":null,"BackgroundColor":"#262F38","Caption":"","FileSizeInBytes":1728,"ForegroundColor":"","Height":88,"ImagePositionInfo":"","ImagePu
2022-04-08 08:03:30 UTC	8461	IN	Data Raw: 65 49 6e 42 79 74 65 73 22 3a 35 34 32 34 2c 22 46 6f 72 65 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 22 2c 22 48 65 69 67 68 74 22 3a 33 30 30 2c 22 49 6d 61 67 65 50 6f 73 69 74 69 6f 6e 49 6e 66 6f 22 3a 22 22 2c 22 49 6d 61 67 65 50 75 72 70 6f 73 65 22 3a 22 54 69 6c 65 22 2c 22 55 6e 73 63 61 6c 65 64 49 6d 61 67 65 53 48 41 32 35 36 48 61 73 68 22 3a 22 41 4a 6b 79 42 55 41 30 37 6e 63 46 2b 53 6c 36 76 7a 61 65 5a 74 33 74 41 4a 45 32 2f 35 31 65 66 34 2b 41 58 51 54 45 59 67 59 3d 22 2c 22 55 72 69 22 3a 22 2f 2f 73 74 6f 72 65 2d 69 6d 61 67 65 73 2e 73 2d 49 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 69 6d 61 67 65 2f 61 70 70 73 2e 33 39 31 36 38 2e 39 30 30 37 31 39 39 32 36 36 32 34 37 38 34 36 2e 62 35 63 34 39 39 35 35 2d 65 30 35 30 2d 34 35 Data Ascii: elnBytes":5424,"ForegroundColor":"","Height":300,"ImagePositionInfo":"","ImagePurpose":"Tile","UnscaldedImageSHA256Hash":"","AJkyBUA07ncF+Sl6vzaeZt3tAJE2/51ef4+AXQTEYgY=","Uri":"","store-images.s-microso
2022-04-08 08:03:31 UTC	8465	IN	Data Raw: 42 49 22 2c 22 4b 48 22 2c 22 43 4d 22 2c 22 43 56 22 2c 22 4b 59 22 2c 22 43 46 22 2c 22 54 44 22 2c 22 54 4c 22 2c 22 44 4a 22 2c 22 44 4d 22 2c 22 44 4f 22 2c 22 45 43 22 2c 22 53 56 22 2c 22 47 51 22 2c 22 45 52 22 2c 22 45 54 22 2c 22 46 4b 22 2c 22 46 4f 22 2c 22 46 4a 22 2c 22 47 46 22 2c 22 50 46 22 2c 22 54 46 22 2c 22 47 41 22 2c 22 47 4d 22 2c 22 47 45 22 2c 22 47 48 22 2c 22 47 49 22 2c 22 47 4a 22 2c 22 47 44 22 2c 22 47 50 22 2c 22 47 52 2c 22 47 55 22 2c 22 47 47 22 2c 22 47 4e 22 2c 22 47 57 22 2c 22 47 59 22 2c 22 48 54 22 2c 22 48 4d 22 2c 22 48 4e 22 2c 22 41 5a 22 2c 22 42 53 22 2c 22 42 42 22 2c 22 42 59 22 2c 22 42 5a 22 2c 22 42 4a 22 2c 22 42 4d 22 2c 22 42 54 22 2c 22 4b 4d 22 2c 22 43 47 22 2c 22 43 44 22 2c 22 43 4b 22 2c 22 43 58 22 2c 22 Data Ascii: BI","KH","CM","CV","KY","CF","TD","TL","DJ","DM","DO","EC","SV","GQ","ER","ET","FK","FO","FJ","GF","PF","TF","GA","GM","GE","GH","GI","GL","GD","GP","GU","GG","GN","GW","GY","HT","HM","HN","AZ","BS","BB","BY","BZ","BJ","BM","BT","KM","CG","CD","CK","CX","
2022-04-08 08:03:31 UTC	8469	IN	Data Raw: 48 22 2c 22 50 4c 22 2c 22 50 54 22 2c 22 51 41 22 2c 22 52 4f 22 2c 22 52 55 22 2c 22 53 41 22 2c 22 52 53 22 2c 22 53 47 22 2c 22 53 4b 22 2c 22 53 49 22 2c 22 5a 41 22 2c 22 4b 52 22 2c 22 45 53 22 2c 22 53 45 22 2c 22 43 48 22 2c 22 54 57 22 2c 22 54 48 22 2c 22 54 54 22 2c 22 54 4e 22 2c 22 54 52 22 2c 22 55 41 22 2c 22 41 45 22 2c 22 47 42 22 2c 22 56 4e 22 2c 22 59 45 22 2c 22 4c 59 22 2c 22 4c 4b 22 2c 22 55 59 22 2c 22 56 45 22 2c 22 41 46 22 2c 2 2 41 58 22 2c 22 41 4c 22 2c 22 41 53 22 2c 22 41 4f 22 2c 22 41 49 22 2c 22 41 51 22 2c 22 41 47 22 2c 22 41 4d 22 2c 22 41 57 22 2c 22 42 4f 22 2c 22 42 51 22 2c 22 42 41 22 2c 22 42 57 22 2c 22 42 56 22 2c 22 49 4f 22 2c 22 42 4e 22 2c 22 42 46 22 2c 22 42 49 22 2c 22 4b 48 22 2c 22 43 4d 22 2c 22 43 Data Ascii: H","PL","PT","QA","RO","RU","SA","RS","SG","SK","SI","ZA","KR","ES","SE","CH","TW","TH","TT","TN","TR","UA","AE","GB","VN","YE","LY","LK","UY","VE","AF","AX","AL","AS","AO","AI","AQ","AG","AM","AW","BO","BQ","BA","BW","BV","IO","BN","BF","BI","KH","CM","C
2022-04-08 08:03:31 UTC	8473	IN	Data Raw: 34 2e 33 31 2e 31 32 31 32 34 2e 37 30 5f 6e 65 75 74 72 61 6c 5f 7e 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 5c 22 2c 5c 22 63 6f 6e 74 65 6e 74 2e 70 72 6f 64 75 63 74 49 64 5c 22 3a 5c 22 39 63 33 65 38 63 61 64 2d 36 37 30 32 2d 34 38 34 32 2d 38 66 36 31 2d 62 38 62 33 33 63 63 39 63 61 66 31 5c 22 2c 5c 22 63 6f 6e 74 65 6e 74 2e 74 61 72 67 65 74 50 6c 61 74 66 6f 72 6d 73 5c 22 3a 5b 7b 5c 22 70 6c 61 74 66 6f 72 6d 2e 6d 61 78 56 65 72 69 6f 6e 54 65 73 74 65 64 5c 22 3a 32 38 31 34 37 35 30 38 39 30 30 30 30 33 38 34 2c 5c 22 70 6c 61 74 66 6f 72 6d 2e 6d 69 6e 56 65 72 73 69 6f 6e 5c 22 3a 32 38 31 34 37 35 30 37 35 34 32 37 35 33 32 38 2c 5c 22 70 6c 61 74 66 6f 72 6d 2e 74 61 72 67 65 74 5c 22 3a 35 7d 5d 2c 5c 22 63 6f 6e 74 65 6e 74 2e Data Ascii: 4.31.12124.70_neutral_~_8wekyb3d8bbwe","content.productId":"9c3e8cad-6702-4842-8f61-b8b33cc9ca f1","content.targetPlatforms":{"platform.maxVersionTested":"2814750890000384","platform.minVersion":"2814 750754275328","platform.target":5},"content.
2022-04-08 08:03:31 UTC	8477	IN	Data Raw: 35 30 38 33 35 32 37 37 38 32 34 2c 5c 22 70 6c 61 74 66 6f 72 6d 2e 74 61 72 67 65 74 5c 22 3a 30 7d 5d 2c 5c 22 63 6f 6e 74 65 6e 74 2e 74 79 70 65 5c 22 3a 37 2c 5c 22 70 6f 6c 69 63 69 5c 22 3a 7b 5c 22 63 61 74 65 67 6f 72 79 2e 66 69 72 73 74 5c 22 3a 5c 22 61 70 70 5c 22 2c 5c 22 63 61 74 65 67 6f 72 79 2e 74 68 69 72 64 5c 22 3a 5c 22 4e 65 77 73 20 26 20 77 65 61 74 68 65 72 5c 22 2c 5c 22 63 61 74 65 67 6f 72 79 2e 74 68 69 72 64 5c 22 3a 5c 22 4e 65 77 73 5c 22 2c 5c 22 6f 70 74 4f 75 74 2e 62 61 63 6b 75 70 52 65 73 74 6f 72 65 5c 22 3a 74 72 75 65 2c 5c 22 6f 70 74 4f 75 74 2e 72 65 6d 6f 76 65 61 62 6c 65 4d 65 64 69 61 5c 22 3a 66 61 6c 73 65 7d 2c 5c 22 70 6f 6c 69 63 79 32 5c 22 3a 7b 5c 22 61 67 65 52 61 74 69 6e 67 5c 22 3a 31 2c 5c Data Ascii: 50835277824,"platform.target":0},"content.type":"7","policy":{"category.first":"app"},"category.secon d":{"News & weather"},"category.third":{"News"},"optOut.backupRestore":true,"optOut.removeableMedia":false},"p olicy2":{"ageRating":1,}
2022-04-08 08:03:31 UTC	8481	IN	Data Raw: 69 61 5c 22 3a 66 61 6c 73 65 7d 2c 5c 22 70 6f 6c 69 63 79 32 5c 22 3a 7b 5c 22 61 67 65 52 61 74 69 6e 67 5c 22 3a 31 2c 5c 22 6f 70 74 4f 75 74 2e 44 56 52 5c 22 3a 66 61 6c 73 65 2c 5c 22 74 68 69 72 64 50 61 72 74 79 41 70 70 52 61 74 69 6e 67 73 5c 22 3a 5b 7b 5c 22 6c 65 76 65 6c 5c 22 3a 37 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 33 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 34 38 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 32 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 32 37 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 39 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 37 36 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 36 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 36 38 2c 5c 22 Data Ascii: ial":false},"policy2":{"ageRating":1,"optOut.DVR":false,"thirdPartyAppRatings":{"level":"7","systemId":"3,{ \level":"12","systemId":"5","level":"48","systemId":"12","level":"27","systemId":"9","level":"76","systemId":"16","level "":68,}

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:31 UTC	8485	IN	Data Raw: 76 65 6c 5c 22 3a 37 36 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 36 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 35 34 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 33 7d 5d 7d 7d 22 2c 22 50 61 63 6b 61 67 65 44 6f 77 6e 6c 6f 61 64 55 72 69 73 22 3a 6e 75 6c 6c 2c 22 46 75 6c 66 69 6c 6c 6d 65 6e 74 44 61 74 61 22 3a 7b 22 50 72 6f 64 75 63 74 49 64 22 3a 22 39 57 5 a 44 4e 43 52 46 48 56 46 57 22 2c 22 57 75 42 75 6e 64 6c 65 49 64 22 3a 65 62 63 67 61 62 36 35 32 2d 63 32 32 37 2d 34 35 39 36 2d 62 61 37 37 2d 34 36 37 62 63 38 64 61 65 33 33 32 22 2c 22 57 75 43 61 74 65 67 6f 72 79 49 64 22 3a 22 65 61 61 66 32 63 65 33 2d 64 35 61 33 2d 34 61 35 39 2d 61 65 33 Data Ascii: vel\":"76,\"systemId\":"16},{\"level\":"68,\"systemId\":"15},{\"level\":"54,\"systemId\":"13}}]]","PackageDownload Uris":null,"FulfillmentData":{"ProductId":"9WZDNCRFHVFw","WuBundId":"eb7ab652-c227-4596-ba77-467bc8dae332","WuCategoryId":"eaaaf2ce3-d5a3-4a59-ae3
2022-04-08 08:03:31 UTC	8489	IN	Data Raw: 64 61 65 33 33 32 22 2c 22 57 75 43 61 74 65 67 6f 72 79 49 64 22 3a 22 65 61 61 66 32 63 65 33 2d 64 35 61 33 2d 34 61 35 39 2d 61 65 33 31 2d 32 37 36 66 62 63 34 34 61 37 63 64 22 2c 22 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 2c 22 53 6b 75 49 64 22 3a 22 30 30 31 30 22 2c 22 43 6f 6e 74 65 6e 74 22 3a 6e 75 6c 6c 2c 22 50 61 63 6b 61 6 7 65 46 65 61 74 75 72 65 73 22 3a 6e 75 6c 6c 7d 7d 2c 7b 22 41 70 70 6c 69 63 61 74 69 6f 6e 73 22 3a 5b 7b 22 41 70 70 6c 69 63 61 74 69 6f 6e 49 64 22 3a 22 41 70 70 65 78 4e 65 77 73 22 7d 5d 2c 2c 22 41 72 63 68 69 74 65 63 74 75 72 65 73 22 3a 5b 22 61 72 6d 22 2c 22 78 38 36 22 2c 22 78 36 34 22 5d Data Ascii: dae332","WuCategoryId":"eaaaf2ce3-d5a3-4a59-ae31-276fbc44a7cd","PackageFamilyName":"Microsoft.BingNews_8wekyb3d8bbwe","Skuld":"0010","Content":null,"PackageFeatures":null},{\"Applications\":{\"ApplicationId\":\"AppxNews\"}},\"Architectures\":{\"arm\",\"x86\",\"x64\"]
2022-04-08 08:03:31 UTC	8493	IN	Data Raw: 70 65 78 4e 65 77 73 22 7d 5d 2c 22 41 72 63 68 69 74 65 63 74 75 72 65 73 22 3a 5b 22 61 72 6d 22 2c 22 78 38 36 22 2c 22 78 36 34 22 5d 2c 22 43 61 70 61 62 69 6c 69 74 69 65 73 22 3a 5b 22 69 6e 74 65 72 6e 65 74 43 6c 69 65 6e 74 22 5d 2c 22 45 78 70 65 72 69 65 6e 63 65 49 64 73 22 3a 5b 5d 2c 22 4d 61 78 44 6f 77 6e 6c 6f 61 64 53 6 9 7a 65 49 6e 42 79 74 65 73 22 3a 39 35 35 32 36 34 30 34 2c 22 4d 61 78 49 6e 73 74 61 6c 6c 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 33 35 37 30 30 37 33 36 2c 22 50 61 63 6b 61 67 65 46 6f 61 6d 69 6c 79 4e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 2c 22 4d 61 Data Ascii: pexNews\"}},\"Architectures\":{\"arm\",\"x86\",\"x64\"},\"Capabilities\":{\"internetClient\"},\"ExperienceIds\":[],\"MaxDownloadSizeInBytes\":95526404,\"MaxInstallSizeInBytes\":35700736,\"PackageFormat\":\"EAppxBundle\",\"PackageFamilyName\":\"Microsoft.BingNews_8wekyb3d8bbwe\",\"Ma
2022-04-08 08:03:31 UTC	8497	IN	Data Raw: 6c 79 4e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 2c 22 4d 61 69 6e 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 46 6f 72 44 6c 63 22 3a 6e 75 6c 6c 2c 22 50 61 63 6b 61 67 65 46 75 6c 6c 4e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 34 2e 37 2e 32 32 30 30 32 2e 37 30 5f 6e 65 75 74 72 61 6c 5f 7e 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 2c 22 50 61 63 6b 61 67 65 49 64 22 3a 22 66 38 32 31 33 36 37 38 2d 64 65 37 33 2d 34 38 31 64 2d 66 31 35 33 2d 37 65 32 39 30 63 33 30 34 33 64 37 2d 58 38 36 2d 58 36 34 2d 41 72 6d 22 2c 22 50 61 63 6b 61 67 65 52 61 6e 6b 22 3a 33 30 31 35 33 3c 22 50 6c 61 74 66 6f 72 6d 44 65 70 65 6e 64 65 6e 63 Data Ascii: lyName\":\"Microsoft.BingNews_8wekyb3d8bbwe\",\"MainPackageFamilyNameForDlc\":null,\"PackageFullName\":\"Microsoft.BingNews_4.7.22002.70_neutral_~_8wekyb3d8bbwe\",\"PackageId\":\"f8213678-de73-481d-f153-7e290c3043d7-X86-X64-Arm\",\"PackageRank\":30163,\"PlatformDependenc
2022-04-08 08:03:31 UTC	8501	IN	Data Raw: 2d 41 72 6d 22 2c 22 50 61 63 6b 61 67 65 52 61 6e 6b 22 3a 33 30 31 36 33 2c 22 50 6c 61 74 66 6f 72 6d 44 65 70 65 6e 64 65 6e 63 69 65 73 22 3a 5b 7b 22 4d 61 78 54 65 73 22 64 22 3a 32 38 31 34 37 35 30 39 33 31 32 32 32 35 32 38 2c 22 4d 69 6e 56 65 72 73 69 6f 6e 22 3a 32 38 31 34 37 35 30 38 33 35 32 37 37 38 32 34 2c 22 50 6c 61 74 66 6f 72 6d 4e 61 6d 65 22 3a 22 57 69 6e 64 6f 77 73 2e 55 6e 69 76 65 72 73 61 6c 22 7d 5d 2c 22 50 6c 61 74 66 6f 72 6d 44 65 70 65 6e 64 65 6e 63 79 58 6d 6c 42 6c 6f 62 22 3a 22 7b 5c 22 62 6c 6f 62 2e 76 65 72 73 69 6f 6e 5c 22 3a 31 36 38 38 38 36 37 30 34 30 35 32 36 33 33 36 2c 5c 22 63 6f 6e 74 65 6e 74 2e 62 75 6e 64 6c 65 64 50 61 63 6b 61 6 7 65 73 5c 22 3a 5b 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e Data Ascii: -Arm\",\"PackageRank\":30163,\"PlatformDependencies\":{\"MaxTested\":2814750931222528,\"MinVersion\":2814750835277824,\"PlatformName\":\"Windows.Universal\"}},\"PlatformDependencyXmlBlob\":\"(\\\"blob.version\\\":1688867040526336,\"content.bundledPackages\":[\\\"Microsoft.Bin
2022-04-08 08:03:31 UTC	8505	IN	Data Raw: 63 6f 6e 74 65 6e 74 2e 62 75 6e 64 6c 65 64 50 61 63 6b 61 67 65 73 5c 22 3a 5b 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 34 2e 34 37 2e 32 32 31 38 31 2e 37 30 5f 61 72 6d 5f 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 5c 22 2c 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 34 2e 34 37 2e 32 32 31 38 31 2e 37 30 5f 78 36 34 5f 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 5c 22 2c 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 34 2e 34 37 2e 32 32 31 38 31 2e 37 30 5f 78 38 36 5f 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 5c 22 5d 2c 5c 22 63 6f 6e 74 65 6e 74 2e 69 73 4d 61 69 6e 5c 22 3a 66 61 6c 73 65 2c 5c 22 63 6f 6e 74 65 6e 74 2e 70 61 63 6b 61 67 65 49 64 5c 22 3a 5c 22 4d 69 63 72 6f 73 6f 66 74 2e Data Ascii: content.bundledPackages\":[\\\"Microsoft.BingNews_4.47.22181.70_arm_8wekyb3d8bbwe\\\",\\\"Microsoft.BingNews_4.47.22181.70_x64_8wekyb3d8bbwe\\\",\\\"Microsoft.BingNews_4.47.22181.70_x86_8wekyb3d8bbwe\\\"],\"content.isMain\":false,\"content.packageId\":\"Microsoft.
2022-04-08 08:03:31 UTC	8509	IN	Data Raw: 22 3a 66 61 6c 73 65 2c 5c 22 63 6f 6e 74 65 6e 74 2e 70 61 63 6b 61 67 65 49 64 5c 22 3a 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 34 2e 38 2e 36 30 30 31 2e 30 5f 6e 65 75 74 72 61 6c 5f 7e 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 5c 22 2c 5c 22 63 6f 6e 74 65 6e 74 2e 70 72 6f 64 75 63 74 49 64 5c 22 3a 5c 22 39 63 33 65 38 63 61 64 2d 36 37 30 32 2d 34 38 34 32 2d 38 66 36 31 2d 62 38 62 33 63 63 39 63 61 66 31 5c 22 2c 5c 22 63 6f 6e 74 65 6e 74 2e 74 61 72 67 65 74 50 6c 61 74 66 6f 72 6d 73 5c 22 3a 5b 7b 5c 22 70 6c 61 74 66 6f 72 6d 2e 6d 61 78 56 65 72 73 69 6f 6e 54 65 73 74 65 64 5c 22 3a 32 38 31 34 37 35 30 39 33 31 32 32 32 35 32 38 2c 5c 22 70 6c 61 7 4 66 6f 72 6d 2e 6d 69 6e 56 65 72 73 69 6f 6e 5c 22 3a 32 38 31 Data Ascii: \":false,\"content.packageId\":\"Microsoft.BingNews_4.8.6001.0_neutral_~_8wekyb3d8bbwe\\\",\"content.productId\":\"9c3e8cad-6702-4842-8f61-b8b33cc9caf1\\\",\"content.targetPlatforms\":[\\\"platform.maxVersionTested\\\":2814750931222528,\"platform.minVersion\":281
2022-04-08 08:03:31 UTC	8513	IN	Data Raw: 31 34 37 35 30 39 33 31 32 32 32 35 32 38 2c 5c 22 70 6c 61 74 66 6f 72 6d 2e 6d 69 6e 56 65 72 73 69 6f 6e 5c 22 3a 32 38 31 34 37 35 30 38 33 35 32 37 37 38 32 34 2c 5c 22 70 6c 61 74 66 6f 72 6d 2e 74 61 72 67 65 74 5c 22 3a 30 7d 5d 2c 5c 22 63 6f 6e 74 65 6e 74 2e 74 79 70 65 5c 22 3a 37 2c 5c 22 70 6f 6c 69 63 79 5c 22 3a 7b 5c 22 63 61 74 65 67 6f 72 79 2e 66 69 72 73 74 5c 22 61 70 70 5c 22 2c 5c 22 63 61 74 65 67 6f 72 79 2e 73 65 63 6f 6e 64 5c 22 3a 5c 22 4e 65 77 73 20 26 20 77 65 61 74 68 65 72 5c 22 2c 5c 22 63 61 74 65 67 6f 72 79 2e 74 68 69 72 64 5c 22 3a 5c 22 4e 65 77 73 5c 22 2c 5c 22 6f 70 74 4f 75 74 2e 62 61 63 6b 75 70 52 65 73 74 6f 72 65 5c 22 3a 74 72 75 65 2c 5c 22 6f 70 74 4f 75 74 2e 72 65 6d 6f 76 65 61 62 6c 65 4d Data Ascii: 14750931222528,\"platform.minVersion\":2814750835277824,\"platform.target\":[0],\"content.type\":[7,\"policy\":[\\\"category.first\\\":\\\"app\\\",\\\"category.second\\\":\\\"News & weather\\\",\\\"category.third\\\":\\\"News\\\",\\\"optOut.backupRestore\\\":true,\"optOut.removeableM

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:31 UTC	8517	IN	Data Raw: 75 74 2e 62 61 63 6b 75 70 52 65 73 74 6f 72 65 5c 22 3a 74 72 75 65 2c 5c 22 6f 70 74 4f 75 74 2e 72 65 6d 6f 76 65 61 62 6c 65 4d 65 64 69 61 5c 22 3a 66 61 6c 73 65 7d 2c 5c 22 70 6f 6c 69 63 79 32 5c 22 3a 7b 5c 22 61 67 65 52 61 74 69 6e 67 5c 22 3a 31 2c 5c 22 6f 70 74 4f 75 74 2e 44 56 52 5c 22 3a 66 61 6c 73 65 2c 5c 22 74 68 69 72 64 50 61 72 74 79 41 70 70 52 61 74 69 6e 67 73 5c 22 3a 5b 7b 5c 22 6c 65 76 65 6c 5c 22 3a 37 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 33 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 31 32 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 35 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 34 38 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 32 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 2 2 3a 32 37 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 39 7d 2c 7b Data Ascii: ut.backupRestore!":true,"optOut.removeableMedia!":false},"policy2!":{"\ageRating!":1,"optOut.DVR!":false, \"thirdPartyAppRatings!":{"!level!":7,\"systemId!":3},{!level!":12,\"systemId!":5},{!level!":48,\"systemId!":12},{!level!":27, \"systemId!":9},{
2022-04-08 08:03:31 UTC	8521	IN	Data Raw: 73 79 73 74 65 6d 49 64 5c 22 3a 31 32 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 32 37 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 36 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 36 38 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 35 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 35 34 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 33 7d 5d 7d 7d 22 2c 22 50 61 63 6b 61 67 65 44 6f 77 6 e 6c 6f 61 64 55 72 69 73 22 3a 6e 75 6c 6c 2c 22 46 75 6c 66 69 6c 6c 6d 65 6e 74 44 61 74 61 22 3a 7b 22 50 72 6f 64 75 63 74 49 64 22 3a 22 39 57 5a 44 4e 43 52 46 48 56 46 57 22 2c 22 57 75 42 75 6e 64 6c 65 49 64 22 3a 2a 26 62 37 61 62 36 35 32 2d 63 32 32 37 2d 34 35 39 36 2d 62 61 37 37 2d 34 36 Data Ascii: systemId!":12},{!level!":27,\"systemId!":9},{!level!":76,\"systemId!":16},{!level!":68,\"systemId!":15},{!level!": 54,\"systemId!":13}}},"PackageDownloadUris!":null,\"FulfillmentData!":{"ProductId!":\"9WZDNCRFHVF\", \"WuBundId!\": \"eb7ab652-c227-4596-ba77-46
2022-04-08 08:03:31 UTC	8525	IN	Data Raw: 46 48 56 46 57 22 2c 22 57 75 42 75 6e 64 6c 65 49 64 22 3a 22 65 62 37 61 62 36 35 32 2d 63 32 32 37 2d 34 35 39 36 2d 62 61 37 37 2d 34 36 37 62 63 38 64 61 65 33 33 32 22 2c 22 57 75 43 61 74 65 67 6f 72 79 49 64 22 3a 22 65 61 61 66 32 63 65 33 2d 64 35 61 33 2d 34 61 35 39 2d 61 65 33 31 2d 32 37 36 66 62 63 34 34 61 37 63 64 22 2c 22 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 2c 22 53 6b 75 49 64 22 3a 22 30 30 31 30 22 2c 22 43 6f 6e 74 65 6e 74 22 3a 6e 75 6c 6c 2c 22 50 61 63 6b 61 67 65 46 65 61 74 75 72 65 73 22 3a 6e 75 6c 6c 7d 7d 2c 7b 22 41 70 70 6c 69 63 61 74 69 6f 6e 49 64 Data Ascii: FHVF\", \"WuBundId!\": \"eb7ab652-c227-4596-ba77-467bc8dae332\", \"WuCategoryId!\": \"eaaf2ce3-d5a3-4a59- ae31-276fbc44a7cd\", \"PackageFamilyName!\": \"Microsoft.BingNews_8wekyb3d8bbwe\", \"Skuld!\": \"0010\", \"Content!\": null, \"PackageFeatures!\": null}}, {\"Applications!\": [{\"ApplicationId
2022-04-08 08:03:31 UTC	8529	IN	Data Raw: 74 75 72 65 73 22 3a 6e 75 6c 6c 7d 7d 2c 7b 22 41 70 70 6c 69 63 61 74 69 6f 6e 73 22 3a 5b 7b 22 41 70 70 6c 69 63 61 74 69 6f 6e 49 64 22 3a 22 41 70 70 65 78 4e 65 77 73 22 7d 5d 2c 22 41 72 63 68 69 74 65 63 74 75 72 65 73 22 3a 5b 22 78 36 34 22 2c 22 61 72 6d 22 2c 22 78 38 36 22 5d 2c 22 43 61 70 61 62 69 6c 69 74 69 65 73 22 3a 5b 22 69 6e 74 65 72 6e 65 74 43 6c 69 65 6e 74 22 5d 2c 22 45 78 70 65 72 69 65 6e 63 65 49 64 73 22 3a 5b 5d 2c 22 4d 61 78 44 6f 77 6e 6c 6f 61 64 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 33 35 31 37 32 33 35 32 2c 22 50 61 63 6b 61 67 65 46 6f 72 6d 61 74 22 3a 22 41 70 70 78 42 75 6e 64 6c 65 22 2c 22 50 61 63 6b 61 67 65 Data Ascii: tures!\":null}}, {\"Applications!\": [{\"ApplicationId!\": \"AppexNews\"}], \"Architectures!\": [\"x64\", \"arm\", \"x86\"], \"Capabilities!\": [\"internetClient\"], \"ExperienceIds!\": [], \"MaxDownloadSizeInBytes!\": 39928934, \"MaxInstallSizeInBytes!\": 35172352, \"PackageFo rmat!\": \"AppxBundle\", \"Package
2022-04-08 08:03:31 UTC	8533	IN	Data Raw: 35 31 37 36 34 34 38 2c 22 50 61 63 6b 61 67 65 46 6f 72 6d 61 74 22 3a 22 45 41 70 70 78 42 75 6e 64 6c 6c 65 22 2c 22 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 2c 22 4d 61 69 6e 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 46 6f 72 44 6c 63 22 3a 6e 75 6c 6c 2c 22 50 61 63 6b 61 67 65 46 75 6c 6c 4e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 34 2e 39 2e 33 31 30 30 31 2e 37 30 5f 6e 65 75 74 72 61 6c 5f 7e 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 2c 22 50 61 63 6b 61 67 65 49 64 22 3a 22 32 65 36 34 63 36 35 62 2d 64 61 32 30 2d 61 32 39 35 2d 34 63 33 64 2d 66 31 66 31 36 38 62 35 34 66 32 36 2d 58 Data Ascii: 5176448, \"PackageFormat!\": \"EAppxBundle\", \"PackageFamilyName!\": \"Microsoft.BingNews_8wekyb3d8b bwe\", \"MainPackageFamilyNameForDlc!\": null, \"PackageFullName!\": \"Microsoft.BingNews_4.9.31001.70_neutral_~ _8wekyb3d8bbwe\", \"PackageId!\": \"2e64c65b-da20-a295-4c3d-f1f168b54f26-X
2022-04-08 08:03:31 UTC	8537	IN	Data Raw: 67 65 49 64 22 3a 22 61 33 31 66 35 37 30 62 2d 39 63 32 65 2d 36 65 32 38 2d 37 61 35 64 2d 39 35 30 35 63 30 61 37 33 33 35 64 2d 58 38 36 2d 58 36 34 2d 41 72 6d 22 2c 22 50 61 63 6b 61 67 65 52 61 6e 6b 22 3a 33 30 33 34 33 2c 22 50 6c 61 74 66 6f 72 6d 44 65 70 65 6e 64 65 6e 63 69 65 73 22 3a 5b 7b 22 4d 61 78 54 65 73 74 65 64 22 3a 32 38 31 34 37 35 30 39 33 31 32 32 32 35 32 38 2c 22 4d 69 6e 56 65 72 73 69 6f 6e 22 3a 32 38 31 34 37 35 30 38 33 35 32 37 37 38 32 34 2c 22 50 6c 61 74 66 6f 72 6d 4e 61 6d 65 22 3a 22 57 69 6e 64 6f 77 73 2e 55 6e 69 76 65 72 73 61 6c 22 7d 5d 2c 22 50 6c 61 74 66 6f 72 6d 44 65 70 65 6e 64 65 6e 63 79 58 6d 6c 42 6c 6f 62 22 3a 22 7b 5c 22 62 6c 6f 62 2e 76 65 72 73 69 6f 6e 5c 22 3a 31 36 38 38 38 36 37 30 34 30 Data Ascii: geld!\": \"a31f570b-9c2e-6e28-7a5d-9505c0a7335d-X86-X64-Arm\", \"PackageRank!\": 30343, \"PlatformDe pendencies!\": [{\"MaxTested!\": 2814750931222528, \"MinVersion!\": 2814750835277824, \"PlatformName!\": \"Windows.Universal\"}], \"PlatformDependencyXmlBlob!\": \"{!blob.version!\": 1688867040
2022-04-08 08:03:31 UTC	8541	IN	Data Raw: 65 6e 63 79 58 6d 6c 42 6c 6f 62 22 3a 22 7b 5c 22 62 6c 6f 62 2e 76 65 72 73 69 6f 6e 5c 22 3a 31 36 38 38 38 36 37 30 34 30 35 32 36 33 33 36 2c 5c 22 63 6f 6e 74 65 6e 74 2e 62 75 6e 64 6c 65 64 50 61 63 6b 61 67 65 73 5c 22 3a 5b 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 34 2e 35 34 2e 32 32 37 34 31 2e 37 30 5f 78 38 36 5f 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 5c 22 2c 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 34 2e 35 34 2e 32 32 37 34 31 2e 37 30 5f 78 36 34 5f 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 5c 22 2c 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 34 2e 35 34 2e 32 32 37 34 31 2e 37 30 5f 78 36 34 5f 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 5c 22 5d 2c 5c 22 63 6f 6e 74 65 6e Data Ascii: encyXmlBlob!\": \"{!blob.version!\": 1688867040526336, !content.bundledPackages!\": [!Microsoft.BingNews _4.54.22741.70_x86__8wekyb3d8bbwe!\", !Microsoft.BingNews_4.54.22741.70_x64__8wekyb3d8bbwe!\", !Micros oft.BingNews_4.54.22741.70_arm__8wekyb3d8bbwe!\", !conten
2022-04-08 08:03:31 UTC	8545	IN	Data Raw: 6b 61 67 65 46 75 6c 6c 4e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 33 2e 31 2e 36 2e 30 5f 61 72 6d 5f 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 2c 22 50 61 63 6b 61 67 65 49 64 22 3a 22 64 66 64 33 31 39 31 62 2d 38 64 38 34 2d 34 39 31 37 2d 61 37 30 38 2d 30 37 38 30 39 39 36 62 36 62 62 61 22 2c 22 50 61 63 6b 61 67 65 52 61 6e 6b 22 3a 31 34 30 30 30 2c 22 50 6c 61 74 66 6f 72 6d 44 65 70 65 6e 64 65 6e 63 69 65 73 22 3a 5b 7b 22 4d 61 78 54 65 73 74 65 64 22 3a 32 32 35 31 38 30 34 31 30 38 36 35 32 35 34 34 2c 22 4d 69 6e 56 65 72 73 69 6f 6e 22 3a 32 32 35 31 38 30 34 31 30 38 36 35 32 35 34 34 2c 22 50 6c 61 74 66 6f 72 6d 4e 61 6d 65 22 3a 22 57 69 6e 64 6f 77 73 2e 57 69 6e 64 6f 77 73 50 68 6f 6e 65 38 78 Data Ascii: kageFullName!\": \"Microsoft.BingNews_3.1.6.0_arm__8wekyb3d8bbwe\", \"PackageId!\": \"dfd3191b-8d84-4917- a708-0780996b6bba\", \"PackageRank!\": 14000, \"PlatformDependencies!\": [{\"MaxTested!\": 2251804108652544, \"MinVersion !\": 2251804108652544, \"PlatformName!\": \"Windows.WindowsPhone8x

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:31 UTC	8549	IN	Data Raw: 22 3a 31 2c 5c 22 6f 70 74 4f 75 74 2e 44 56 52 5c 22 3a 66 61 6c 73 65 2c 5c 22 74 68 69 72 64 50 61 72 74 79 41 70 70 52 61 74 69 6e 67 73 5c 22 3a 5b 7b 5c 22 6c 65 76 65 6c 5c 22 3a 37 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 33 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 31 32 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 35 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 34 38 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 32 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 32 3 7 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 39 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 37 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 36 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 36 38 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 35 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 35 34 2c 5c 22 73 79 73 74 65 6d Data Ascii: ".1,\"optOut.DVR\":false,\"thirdPartyAppRatings\":{\"level\":\"7,\"systemId\":\"3,\"level\":\"12,\"systemId\":\"5,\"level\":\"48,\"systemId\":\"12,\"level\":\"27,\"systemId\":\"9,\"level\":\"76,\"systemId\":\"16,\"level\":\"68,\"systemId\":\"15,\"level\":\"54,\"system
2022-04-08 08:03:31 UTC	8553	IN	Data Raw: 69 74 69 65 73 22 3a 5b 7b 22 41 63 74 69 6f 6e 73 22 3a 5b 22 44 65 74 61 69 6c 73 22 2c 22 46 75 6c 66 69 6c 6c 22 2c 22 50 75 72 63 68 61 73 65 22 2c 22 42 72 6f 77 73 65 22 2c 22 43 75 72 61 74 65 22 2c 22 52 65 64 65 65 6d 22 5d 2c 22 41 76 61 69 6c 61 62 69 6c 69 74 79 41 53 63 68 65 6d 61 22 3a 5c 22 41 76 61 69 6c 61 62 69 6c 69 74 79 3b 33 22 2c 22 41 76 61 69 6c 61 62 69 6c 69 74 79 42 53 63 68 65 6d 61 22 3a 22 41 76 61 69 6c 61 62 69 6c 69 74 79 55 6e 69 66 69 65 64 41 70 70 3b 33 22 2c 22 41 76 61 69 6c 61 62 69 6c 69 74 79 49 64 22 3a 22 42 30 35 4b 39 56 38 42 5a 53 4a 30 22 2c 22 43 6f 6e 64 69 74 69 6f 6e 73 22 3a 7b 22 43 6c 69 65 6e 74 43 6f 6e 64 69 74 69 6f 6e 73 22 3a 7b 22 41 6c 6c 6f 77 65 64 50 6c 61 74 66 6f 72 6d 73 22 3a 5b 7b 22 Data Ascii: ities\":\"Actions\":\"Details\",\"Fulfill\",\"Purchase\",\"Browse\",\"Curate\",\"Redeem\",\"AvailabilityASchema\":\"Availa bility;3\",\"AvailabilityBSchema\":\"AvailabilityUnifiedApp;3\",\"AvailabilityId\":\"B05K9V8BZSJ0\",\"Conditions\":{\"ClientConditions\": {\"AllowedPlatforms\":{\"
2022-04-08 08:03:31 UTC	8557	IN	Data Raw: 64 65 70 74 68 20 72 65 70 6f 72 74 69 6e 67 20 66 72 6f 6d 20 74 68 65 20 77 6f 72 6c 64 27 73 20 62 65 73 74 20 6a 6f 75 72 6e 61 6c 69 73 74 73 2e 5c 6e c2 a0 5c 6e 2d 20 4f 75 72 20 65 64 69 74 6f 72 73 20 63 75 72 61 74 65 20 74 68 65 20 6d 6f 73 74 20 74 72 75 73 74 65 64 2c 20 69 6d 70 6f 72 74 61 6e 74 2c 20 69 6e 74 65 72 65 73 74 69 6e 67 20 61 6e 64 20 74 72 65 6e 64 69 6e 67 20 6e 65 77 73 5c 6e 2d 20 59 6f 75 20 63 68 6f 6f 73 65 20 77 68 69 63 68 20 74 6f 70 69 63 73 20 6d 61 74 74 65 72 20 6d 6f 73 74 20 74 6f 20 65 6e 2d 20 4d 69 63 72 6f 73 6f 66 74 20 4e 65 77 73 20 75 70 64 61 74 65 73 20 79 6f 75 20 77 69 74 68 20 6e 6f 74 69 66 69 63 61 74 69 6f 6e 73 20 6f 66 20 62 72 65 61 6b 69 6e 67 20 6e 65 77 73 2c 20 71 75 69 63 6b Data Ascii: depth reporting from the world's best journalists.\n\n- Our editors curate the most trusted, important, interesting and trending news\n- You choose which topics matter most to you.\n- Microsoft News updates you with notifications of breaking news, quick
2022-04-08 08:03:31 UTC	8561	IN	Data Raw: 62 77 65 5c 22 2c 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 34 2e 33 31 2e 31 32 31 32 34 2e 30 5f 78 38 36 5f 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 5c 22 2c 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 34 2e 33 31 2e 31 32 31 32 34 2e 30 5f 61 72 6d 5f 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 5c 22 5d 2c 5c 22 63 6f 6e 74 65 6e 74 2e 69 73 4d 61 69 6e 5c 22 3a 66 61 6c 73 65 2c 5c 22 3a 66 61 6c 74 65 6e 74 2e 70 61 63 6b 61 67 65 49 64 5c 22 3a 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 34 2e 33 31 2e 31 32 31 32 34 2e 30 5f 6e 65 75 74 72 61 6c 5f 7e 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 5c 22 2c 5c 22 63 6f 6e 74 65 6e 74 2e 70 72 6f 64 75 63 74 49 64 5c 22 3a 5c 22 39 63 33 65 38 63 61 Data Ascii: bwel\",\"Microsoft.BingNews_4.31.12124.0_x86__8wekyb3d8bbwel\",\"Microsoft.BingNews_4.31.12124.0_arm __8wekyb3d8bbwel\",\"content.isMain\":false,\"content.packageId\":\"Microsoft.BingNews_4.31.12124.0_neutral_~__8wekyb3d8bbwel\",\"content.productId\":\"9c3e8ca
2022-04-08 08:03:31 UTC	8565	IN	Data Raw: 7e 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 5c 22 2c 5c 22 63 6f 6e 74 65 6e 74 2e 70 72 6f 64 75 63 74 49 64 5c 22 3a 5c 22 39 63 33 65 38 63 61 64 2d 36 37 30 32 2d 34 38 34 32 2d 38 66 36 31 2d 62 38 62 33 33 63 39 63 61 66 31 5c 22 2c 5c 22 63 6f 6e 74 65 6e 74 2e 74 61 72 67 65 74 50 6c 61 74 66 6f 72 6d 73 5c 22 3a 5b 7b 5c 22 70 6c 61 74 66 6f 72 6d 2e 6d 61 78 56 65 72 73 69 6f 6e 54 65 73 74 65 64 5c 22 3a 32 38 31 34 37 35 30 39 33 31 32 32 32 35 32 38 2c 5c 22 70 6c 61 74 66 6f 72 6d 2e 6d 69 6e 56 65 72 73 69 6f 6e 5c 22 3a 32 38 31 34 37 35 30 38 33 35 32 3 7 37 38 32 34 2c 5c 22 70 6c 61 74 66 6f 72 6d 2e 74 61 72 67 65 74 5c 22 3a 35 7d 5d 2c 5c 22 63 6f 6e 74 65 6e 74 2e 74 79 70 65 5c 22 3a 37 2c 5c 22 70 6f 6c 69 63 79 5c 22 3a 7b 5c Data Ascii: ~__8wekyb3d8bbwel\",\"content.productId\":\"9c3e8cad-6702-4842-8f61-b8b33cc9caf1\",\"content.targetP latforms\":{\"platform.maxVersionTested\":\"281475093122528,\"platform.minVersion\":\"2814750835277824,\"platfor m.target\":\"5\",\"content.type\":\"7,\"policy\":{\
2022-04-08 08:03:31 UTC	8569	IN	Data Raw: 61 72 67 65 74 5c 22 3a 35 7d 5d 2c 5c 22 63 6f 6e 74 65 6e 74 2e 74 79 70 65 5c 22 3a 37 2c 5c 22 70 6f 6c 69 63 79 5c 22 3a 7b 5c 22 63 61 74 65 67 6f 72 79 2e 66 69 72 73 74 5c 22 3a 5c 22 61 70 70 5c 22 2c 5c 22 63 61 74 65 67 6f 72 79 2e 73 65 63 6f 6e 64 5c 22 3a 5c 22 4e 65 77 73 20 26 20 77 65 61 74 68 65 72 5c 22 2c 5c 22 63 61 74 65 67 6f 72 79 2e 74 68 69 72 64 5c 22 3a 5c 22 4e 65 77 73 5c 22 2c 5c 22 6f 70 74 4f 75 74 2e 62 61 63 6b 75 70 52 65 73 74 6f 72 65 5c 22 3a 74 72 75 65 2c 5c 22 6f 70 74 4f 75 74 2e 72 65 6d 6f 76 65 61 62 6c 65 4d 65 64 69 61 5c 22 3a 66 61 6c 73 65 7d 2c 5c 22 70 6f 6c 69 63 79 32 5c 22 3a 7b 5c 22 61 67 65 52 61 74 69 6e 67 5c 22 3a 31 2c 5c 22 6f 70 74 4f 75 74 2e 44 56 52 5c 22 3a 66 61 6c 73 65 2c 5c 22 74 68 Data Ascii: arget\":\"5\",\"content.type\":\"7,\"policy\":{\"category.first\":\"appl\",\"category.second\":\"News & weather\",\"categor y.third\":\"News\",\"optOut.backupRestore\":true,\"optOut.removeableMedia\":false,\"policy2\":{\"ageRating\":1,\"optOut .DVR\":false,\"th
2022-04-08 08:03:31 UTC	8573	IN	Data Raw: 5c 22 61 67 65 52 61 74 69 6e 67 5c 22 3a 31 2c 5c 22 6f 70 74 4f 75 74 2e 44 56 52 5c 22 3a 66 61 6c 73 65 2c 5c 22 74 68 69 72 64 50 61 72 74 79 41 70 70 52 61 74 69 6e 67 73 5c 22 3a 5b 7b 5c 22 6c 65 76 65 6c 5c 22 3a 37 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 33 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 31 32 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 35 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 34 38 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 32 7d 2c 7 b 5c 22 6c 65 76 65 6c 5c 22 3a 32 37 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 39 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 37 36 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 36 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 36 38 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 35 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 Data Ascii: \"ageRating\":1,\"optOut.DVR\":false,\"thirdPartyAppRatings\":{\"level\":\"7,\"systemId\":\"3,\"level\":\"12,\" systemId\":\"5,\"level\":\"48,\"systemId\":\"12,\"level\":\"27,\"systemId\":\"9,\"level\":\"76,\"systemId\":\"16,\"level\":\"68,\"systemId \":\"15,\"level\"
2022-04-08 08:03:31 UTC	8577	IN	Data Raw: 36 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 36 38 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 35 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 35 34 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 33 7d 5d 7d 7d 22 2c 22 50 61 63 6b 61 67 65 44 6f 77 6e 6c 6f 61 64 55 72 69 73 22 3a 6e 75 6c 6c 2c 22 46 75 6c 66 69 6c 6c 6d 65 6e 74 44 61 74 61 22 3a 7b 22 50 72 6f 64 75 63 74 49 64 22 3a 22 39 57 5a 44 4e 43 52 46 48 56 46 57 22 2c 22 57 75 42 75 6e 64 6c 65 49 64 22 3a 22 65 62 37 61 62 36 35 32 2d 63 32 32 37 2d 34 35 39 36 2d 62 61 37 37 2d 34 36 37 62 63 38 64 61 65 33 33 32 22 2c 22 57 75 43 61 74 65 67 6f 72 79 49 64 22 3a 22 65 61 61 66 32 63 65 33 2d 64 35 61 33 2d 34 61 35 39 2d 61 65 33 31 2d 32 37 36 66 62 63 34 61 37 63 64 22 2c 22 50 61 63 6b 61 67 Data Ascii: 6j,\"level\":\"68,\"systemId\":\"15,\"level\":\"54,\"systemId\":\"13\"}}\",\"PackageDownloadUris\":null,\"FulfillmentData\": {\"ProductId\":\"9WZDNCRFHFW\",\"WuBundleId\":\"eb7ab652-c227-4596-ba77-467bc8dae332\",\"WuCategoryId\":\"eaa2ce3-d5a3-4a59-ae31-276fbc44a7cd\",\"Packag

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:31 UTC	8581	IN	Data Raw: 22 65 61 61 66 32 63 65 33 2d 64 35 61 33 2d 34 61 35 39 2d 61 65 33 31 2d 32 37 36 66 62 63 34 34 61 37 63 64 22 2c 22 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 2c 22 53 6b 75 49 64 22 3a 22 30 30 31 31 22 2c 22 43 6f 6e 7 4 65 6e 74 22 3a 6e 75 6c 6c 2c 22 50 61 63 6b 61 67 65 46 65 61 74 75 72 65 73 22 3a 6e 75 6c 6c 7d 7d 2c 7b 22 41 70 70 6c 69 63 61 74 69 6f 6e 73 22 3a 5b 7b 22 41 70 70 6c 69 63 61 74 69 6f 6e 49 64 22 3a 22 41 70 70 65 78 4e 65 77 73 22 7d 5d 2c 22 41 72 63 68 69 74 65 63 74 75 72 65 73 22 3a 5b 22 61 72 6d 22 2c 22 78 38 36 22 2c 22 78 36 34 22 5d 2c 22 43 61 70 61 62 69 6c 69 74 69 65 73 22 3a 5b 22 69 6e 74 65 72 Data Ascii: "eaa2ce3-d5a3-4a59-ae31-276fbc44a7cd","PackageFamilyName":"","Microsoft.BingNews_8wekyb3d8bbwe","Skuld":"","0011","Content":null,"PackageFeatures":null},{("Applications":[{"ApplicationId":"","AppexNews"}]),("Architectures":["arm","x86","x64"],"Capabilities":["inter
2022-04-08 08:03:31 UTC	8585	IN	Data Raw: 72 65 73 22 3a 5b 22 61 72 6d 22 2c 22 78 38 36 22 2c 22 78 36 34 22 5d 2c 22 43 61 70 61 62 69 6c 69 74 69 65 73 22 3a 5b 22 69 6e 74 65 72 6e 65 74 43 6c 69 65 6e 74 22 5d 2c 22 45 78 70 65 72 69 65 6e 63 65 49 64 73 22 3a 5b 5d 2c 22 4d 61 78 44 6f 77 6e 6c 6f 61 64 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 23 39 32 36 34 35 34 31 2c 22 4d 61 78 49 6e 73 74 61 6c 6c 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 33 35 37 30 30 37 33 36 2c 22 50 61 63 6b 61 67 65 46 6f 72 6d 61 74 22 3a 22 41 70 70 78 42 75 6e 64 6c 65 22 2c 22 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 2c 22 4d 61 69 6e 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 46 6f 72 44 Data Ascii: res":["arm","x86","x64"],"Capabilities":["internetClient"],"ExperienceIds":[],"MaxDownloadSizeInBytes":39264541,"MaxInstallSizeInBytes":35700736,"PackageFormat":"","AppxBundle","PackageFamilyName":"","Microsoft.BingNews_8wekyb3d8bbwe","MainPackageFamilyNameForD
2022-04-08 08:03:31 UTC	8589	IN	Data Raw: 4e 65 77 73 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 2c 22 4d 61 69 6e 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 46 6f 72 44 6c 63 22 3a 6e 75 6c 6c 2c 22 50 61 63 6b 61 67 65 46 75 6c 6c 4e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 34 2e 37 2e 32 32 30 30 32 2e 30 5f 6e 65 75 74 72 61 6c 5f 7e 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 2c 22 50 61 63 6b 61 67 65 49 64 22 3a 22 31 61 62 31 37 65 34 66 2d 63 64 66 6e 2d 39 35 31 64 2d 34 64 66 61 2d 35 32 65 61 63 37 36 61 64 33 63 2d 58 38 36 2d 58 36 34 2d 41 72 6d 22 2c 22 50 61 63 6b 61 67 65 52 61 6e 6b 22 3a 33 30 31 34 33 2c 22 50 6c 61 74 66 6f 72 6d 44 65 70 65 6e 64 65 6e 63 69 65 73 22 3a 5b 7b 22 4d 61 78 54 65 73 74 65 64 22 3a 32 38 31 34 37 Data Ascii: News_8wekyb3d8bbwe","MainPackageFamilyNameForDlc":"","PackageFullName":"","Microsoft.BingNews_4.7.22002.0_neutral_~_8wekyb3d8bbwe","Packageld":"","1ab17e4f-cdff-951d-4dfa-52eac76add3c-X86-X64-Arm","PackageRank":30143,"PlatformDependencies":["("MaxTested":28147
2022-04-08 08:03:31 UTC	8593	IN	Data Raw: 30 31 37 33 2c 22 50 6c 61 74 66 6f 72 6d 44 65 70 65 6e 64 65 6e 63 69 65 73 22 3a 5b 7b 22 4d 61 78 54 65 73 74 65 64 22 3a 32 38 31 34 37 35 30 39 33 31 32 32 32 35 32 38 2c 22 4d 69 6e 56 65 72 73 69 6f 6e 22 3a 32 38 31 34 37 35 30 38 33 35 32 37 38 32 34 2c 22 50 6c 61 74 66 6f 72 6d 4e 63 79 65 65 22 3a 22 57 69 6e 64 6f 77 73 2e 58 62 6f 78 22 7d 5d 2c 22 50 6c 61 74 66 6f 72 6d 44 65 70 65 6e 64 65 6e 63 79 68 6d 6c 42 6f 62 62 22 3a 22 7b 5c 22 62 6c 6f 62 2e 76 65 72 73 69 6f 6e 5c 22 3a 31 36 38 38 38 36 37 30 34 30 35 32 36 33 33 36 2c 5c 22 63 6f 6e 74 65 6e 74 2e 62 75 6e 64 6c 65 64 50 61 63 6b 61 67 65 73 5c 22 3a 5b 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 7 3 5f 34 2e 34 35 2e 32 32 30 35 33 2e 37 30 5f 78 38 36 5f 5f 38 Data Ascii: 0173,"PlatformDependencies":["("MaxTested":2814750931222528,"MinVersion":2814750835277824,"PlatformName":"","Windows.Xbox"}]),("PlatformDependencyXmlBlob":["("blob.version":1688867040526336,"content.bundledPackages":["("Microsoft.BingNews_4.45.22053.70_x86__8
2022-04-08 08:03:31 UTC	8597	IN	Data Raw: 65 73 5c 22 3a 5b 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 34 2e 34 37 2e 32 32 31 38 31 2e 30 5f 61 72 6d 5f 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 5c 22 2c 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 34 2e 34 37 2e 32 32 31 38 31 2e 30 5f 78 38 36 5f 5f 38 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 34 2e 34 37 2e 32 32 31 38 31 2e 30 5f 78 38 36 5f 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 5c 22 5d 2c 5c 22 63 6f 6e 74 65 6e 74 2e 69 73 4d 61 69 6e 5c 22 3a 66 61 6c 73 65 2c 5c 22 63 6f 6e 74 65 6e 74 2e 70 61 63 6b 61 67 65 49 64 5c 22 3a 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 34 2e 38 2e 35 30 30 31 2e 30 5f 6e 65 75 74 Data Ascii: es":["("Microsoft.BingNews_4.47.22181.0_arm__8wekyb3d8bbwe"],["("Microsoft.BingNews_4.47.22181.0_x64__8wekyb3d8bbwe"],["("Microsoft.BingNews_4.47.22181.0_x86__8wekyb3d8bbwe"],["content.isMain":false,"content.packageld":"","("Microsoft.BingNews_4.8.5001.0_neut
2022-04-08 08:03:31 UTC	8601	IN	Data Raw: 49 64 5c 22 3a 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 34 2e 38 2e 36 30 30 31 2e 37 30 5f 6e 65 75 74 72 61 6c 5f 7e 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 5c 22 2c 5c 22 63 6f 6e 74 65 6e 74 2e 70 72 6f 64 75 63 74 49 64 5c 22 3a 5c 22 39 63 33 65 38 63 61 64 2d 36 37 30 32 2d 34 38 34 32 2d 38 66 36 31 2d 62 38 62 33 33 63 63 39 63 61 66 31 5c 22 2c 5c 22 63 6f 6e 74 65 6e 74 2e 74 61 72 67 65 74 50 6c 61 74 66 6f 72 6d 73 5c 22 3a 5b 7b 5c 22 70 6c 61 74 66 6f 72 6d 2e 6d 61 78 56 65 72 73 69 6f 6e 54 65 73 74 65 64 5c 22 3a 32 38 31 34 37 35 3 0 39 33 31 32 32 32 35 32 38 2c 5c 22 70 6c 61 74 66 6f 72 6d 2e 6d 69 6e 56 65 72 73 69 6f 6e 5c 22 3a 32 38 31 34 37 35 30 38 33 35 32 37 37 38 32 34 2c 5c 22 70 6c 61 74 66 6f 72 6d Data Ascii: Id":["("Microsoft.BingNews_4.8.6001.70_neutral_~_8wekyb3d8bbwe"],["content.productId":["("9c3e8cad-6702-4842-8f61-b8b33cc9caf1"],["content.targetPlatforms":["("platform.maxVersionTested":2814750931222528,"platform.minVersion":2814750835277824,"platform
2022-04-08 08:03:31 UTC	8605	IN	Data Raw: 6d 2e 6d 69 6e 56 65 72 73 69 6f 6e 5c 22 3a 32 38 31 34 37 35 30 38 33 35 32 37 38 32 34 2c 5c 22 70 6c 61 74 66 6f 72 6d 2e 74 61 72 67 65 74 5c 22 3a 35 7d 5d 2c 5c 22 63 6f 6e 74 65 6e 74 2e 74 70 65 5c 22 3a 37 2c 5c 22 70 6f 6c 69 63 79 5c 22 3a 7b 5c 22 63 61 74 65 67 6f 72 79 2e 66 69 72 73 74 5c 22 3a 5c 22 61 70 70 5c 22 2c 5c 22 63 61 74 65 67 6f 72 79 2e 73 65 63 6f 6e 64 5c 22 3a 5c 22 4e 65 77 73 20 26 20 77 65 61 74 68 65 72 5c 22 2c 5c 22 63 61 74 65 67 6f 72 79 2e 74 68 69 72 64 5c 22 3a 5c 22 4e 65 77 73 5c 22 2c 5c 22 6f 70 74 4f 75 74 2e 62 61 63 6b 75 70 52 65 73 74 6f 72 65 5c 22 3a 74 72 75 65 2c 5c 22 6f 70 74 4f 75 74 2e 72 65 6d 6f 76 65 61 62 6c 65 64 65 64 69 61 5c 22 3a 66 61 6c 73 65 7d 2c 5c 22 70 6f 6c 69 63 79 32 5c Data Ascii: m.minVersion("2814750835277824,"platform.target["5]),("content.type["7],"policy":["("category.first":["("app"],["category.second":["("News & weather"],["category.third":["("News"],["optOut.backupRestore":true,"optOut.removeableMedia":["false)],("policy2["
2022-04-08 08:03:31 UTC	8609	IN	Data Raw: 65 2c 5c 22 6f 70 74 4f 75 74 2e 72 65 6d 6f 76 65 61 62 6c 65 4d 65 64 69 61 5c 22 3a 66 61 6c 73 65 7d 2c 5c 22 70 6f 6c 69 63 79 32 5c 22 3a 7b 5c 22 61 67 65 52 61 74 69 6e 67 5c 22 3a 31 2c 5c 22 6f 70 74 4f 75 74 2e 44 56 52 5c 22 3a 66 61 6c 73 65 2c 5c 22 74 68 69 72 64 50 61 72 74 79 41 70 52 61 74 69 6e 67 73 5c 22 3a 5b 7b 5c 22 6c 65 76 65 6c 5c 22 3a 37 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 33 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 31 32 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 35 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 34 38 2c 5c 22 73 79 73 74 65 6d 4 9 64 5c 22 3a 31 32 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 32 37 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 39 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 37 36 2c 5c 22 73 79 73 74 65 6d 49 Data Ascii: e,("optOut.removeableMedia":["false)],("policy2":["("ageRating":["1,"optOut.DVR":["false,"thirdPartyAppRatings":["("level":["7,"systemId":["3]),("level":["12,"systemId":["5]),("level":["48,"systemId":["12]),("level":["27,"systemId":["9]),("level":["76,"systemId

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:31 UTC	8613	IN	Data Raw: 6c 5c 22 3a 32 37 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 39 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 37 36 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 36 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 35 34 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 33 7d 5d 7d 7d 22 2c 22 50 61 63 6b 61 67 65 44 6f 77 6e 6c 6f 61 64 55 72 69 73 22 3a 6e 75 6c 6c 2c 22 46 75 6c 66 69 6 c 6c 6d 65 6e 74 44 61 74 61 22 3a 7b 22 50 72 6f 64 75 63 74 49 64 22 3a 22 39 57 5a 44 4e 43 52 46 48 56 46 57 22 2c 22 57 75 42 75 6e 64 6c 65 49 64 22 3a 22 65 62 37 61 62 36 35 32 2d 63 32 32 37 2d 34 35 39 36 2d 62 61 37 37 2d 34 36 37 62 63 38 64 61 65 33 33 32 22 2c 22 57 75 43 61 74 65 67 6f 72 Data Ascii: l\":27,\"systemId\":\"9},{\"level\":\"76,\"systemId\":\"16},{\"level\":\"68,\"systemId\":\"15},{\"level\":\"54,\"systemId\":\"13}}} \", \"PackageDownloadUri\":null, \"FulfillmentData\":{ \"ProductId\":\"9WZDNCRFHVFW\", \"WuBundId\":\"eb7ab652-c227-4596-ba77-467bc8dae332\", \"WuCategor
2022-04-08 08:03:31 UTC	8617	IN	Data Raw: 37 61 62 36 35 32 2d 63 32 32 37 2d 34 35 39 36 2d 62 61 37 37 2d 34 36 37 62 63 38 64 61 65 33 33 32 22 2c 22 57 75 43 61 74 65 67 6f 72 79 49 64 22 3a 22 65 61 61 66 32 63 65 33 2d 64 35 61 33 2d 34 61 35 39 2d 61 65 33 31 2d 32 37 36 66 62 63 34 34 61 37 63 64 22 2c 22 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 2c 22 53 6b 75 49 64 22 3a 22 30 30 31 31 22 2c 22 43 6f 6e 74 65 6e 74 22 3a 6e 75 6c 6c 2c 22 50 61 63 6b 61 67 65 46 65 61 74 75 72 65 73 22 3a 6e 75 6c 6c 7d 7d 2c 7b 22 41 70 70 6c 69 63 61 74 69 6f 6e 73 22 3a 5b 7b 22 41 70 70 6c 69 63 61 74 69 6f 6e 49 64 22 3a 22 41 70 70 65 78 4e 65 77 73 22 7d 5d 2c 22 41 72 63 68 69 74 Data Ascii: 7ab652-c227-4596-ba77-467bc8dae332\", \"WuCategoryId\":\"eaaef2ce3-d5a3-4a59-ae31-276bfc44a7cd \", \"PackageFamilyName\":\"Microsoft.BingNews_8wekyb3d8bbwe\", \"Skuld\":\"0011\", \"Content\":null, \"PackageFeatures\":null}}, { \"Applications\":[{ \"ApplicationId\":\"AppexNews\"}], \"Archit
2022-04-08 08:03:31 UTC	8621	IN	Data Raw: 74 69 6f 6e 73 22 3a 5b 7b 22 41 70 70 6c 69 63 61 74 69 6f 6e 49 64 22 3a 22 41 70 70 65 78 4e 65 77 73 22 7d 5d 2c 22 41 72 63 68 69 74 65 63 74 75 72 65 73 22 3a 5b 22 78 38 36 22 2c 22 61 72 6d 22 2c 22 78 36 34 22 5d 2c 22 43 61 70 61 62 69 6c 69 74 69 65 73 22 3a 5b 22 69 6e 74 65 72 6e 65 74 43 6c 69 65 6e 74 22 5d 2c 22 45 78 70 65 72 69 65 6e 63 65 49 64 73 22 3a 5b 5d 2c 22 4d 61 78 44 6f 77 6e 6c 6f 61 64 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 3 3 39 39 33 30 38 36 35 2c 22 4d 61 78 49 6e 73 74 61 6c 6c 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 35 31 37 36 34 34 38 2c 22 50 61 63 6b 61 67 65 46 6f 72 6d 61 74 22 3a 22 41 70 70 78 42 75 6e 64 6c 65 22 2c 22 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 2e Data Ascii: tions\":[{ \"ApplicationId\":\"AppexNews\"}], \"Architectures\":[\"x86\", \"arm\", \"x64\"], \"Capabilities\":[\"internetClient\"] \", \"ExperiencesIds\":[], \"MaxDownloadSizeInBytes\":39930865, \"MaxInstallSizeInBytes\":35176448, \"PackageFormat\":\"AppxBu ndle\", \"PackageFamilyName\":\"Microsoft.
2022-04-08 08:03:31 UTC	8625	IN	Data Raw: 22 3a 22 45 41 70 70 78 42 75 6e 64 6c 65 22 2c 22 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 2c 22 2d 4d 61 69 6e 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 46 6f 72 44 6c 63 22 3a 6e 75 6c 6c 2c 22 50 61 63 6b 61 67 6 5 46 75 6c 6c 4e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 73 6f 34 2e 39 2e 31 30 30 30 31 2e 37 30 5f 6e 65 75 74 72 61 6c 5f 7e 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 2c 22 50 61 63 6b 61 67 65 49 64 22 3a 22 64 39 37 34 65 31 61 34 2d 31 35 32 63 2d 63 38 33 37 2d 36 32 34 63 2d 35 36 36 32 39 39 39 63 64 65 34 38 2d 58 38 36 2d 58 36 34 2d 41 72 6d 22 2c 22 50 61 63 6b 61 67 65 52 61 Data Ascii: \": \"EAppxBundle\", \"PackageFamilyName\":\"Microsoft.BingNews_8wekyb3d8bbwe\", \"MainPackageFamili yNameForDlc\":null, \"PackageFullName\":\"Microsoft.BingNews_4.9.10001.70_neutral_~_8wekyb3d8bbwe\", \"Packa gId\":\"d974e1a4-152c-c837-624c-5662999cde48-X86-X64-Arm\", \"PackageRa
2022-04-08 08:03:31 UTC	8629	IN	Data Raw: 33 39 2d 66 31 63 33 2d 65 62 31 34 32 36 63 63 38 33 35 63 2d 58 38 36 2d 58 36 34 2d 41 72 6d 22 2c 22 50 61 63 6b 61 67 65 52 61 6e 6b 22 3a 33 30 33 36 33 2c 22 50 6c 61 74 66 6f 72 6d 44 65 70 65 6e 64 65 6e 63 69 65 73 22 3a 5b 7b 22 4d 61 78 54 65 73 74 65 64 22 3a 32 38 31 34 37 35 30 39 33 31 32 32 32 35 32 38 2c 22 4d 69 6e 56 65 72 73 69 6f 6e 22 3a 32 38 31 34 37 35 30 38 33 35 32 37 37 38 32 34 2c 22 50 6c 61 74 66 6f 72 6d 4e 61 6d 65 22 3a 22 57 69 6e 64 6f 77 73 2e 55 6e 69 76 65 72 73 61 6c 22 7d 5d 2c 22 50 6c 61 74 66 6f 72 6d 44 65 70 65 6e 64 65 6e 63 79 58 6d 6c 42 6c 6f 62 22 3a 22 7b 5c 22 62 6c 6f 62 2e 76 65 72 73 69 6f 6e 5c 22 3a 31 36 38 38 36 37 30 34 30 35 32 36 33 33 36 2c 5c 22 63 6f 6e 74 65 6e 74 2e 62 75 6e 64 6c 65 Data Ascii: 39-f1c3-eb1426cc835c-X86-X64-Arm\", \"PackageRank\":30363, \"PlatformDependencies\":[{ \"MaxTested\":2814750 931222528, \"MinVersion\":2814750835277824, \"PlatformName\":\"Windows.Universal\"}], \"PlatformDependencyXmlBlob\":\"{ \"b lob.version\":1688867040526336, \"content.bundle
2022-04-08 08:03:31 UTC	8633	IN	Data Raw: 6c 6f 61 64 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 37 35 34 33 37 30 36 2c 22 4d 61 78 49 6e 73 74 61 6c 6c 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 6e 75 6c 6c 2c 22 50 61 63 6b 61 67 65 46 6f 72 6d 61 74 22 3a 22 58 61 70 22 2c 22 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 2c 22 4d 61 69 6e 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 65 46 6f 72 44 6c 63 22 3a 6e 75 6c 6c 2c 22 50 61 63 6b 61 67 65 46 75 6c 6c 4e 61 6d 65 22 3a 22 22 2c 22 50 61 63 6b 61 67 65 49 64 22 3a 22 64 64 36 35 31 35 39 30 2d 61 30 61 35 2d 34 62 61 31 2d 62 30 64 37 2d 64 33 64 30 62 65 32 34 30 39 35 61 22 2c 22 50 61 63 6b 61 67 65 52 61 6e 6b 22 3a 31 31 30 Data Ascii: loadSizeInBytes\":7543706, \"MaxInstallSizeInBytes\":null, \"PackageFormat\":\"Xap\", \"PackageFamilyName\":\"M icrosoft.BingNews_8wekyb3d8bbwe\", \"MainPackageFamilyNameForDlc\":null, \"PackageFullName\":\"\", \"PackageId\" :\"dd651590-a0a5-4ba1-b0d7-d3d0be24095a\", \"PackageRank\":110
2022-04-08 08:03:31 UTC	8637	IN	Data Raw: 34 35 30 32 36 34 30 36 34 2c 22 50 6c 61 74 66 6f 72 6d 4e 61 6d 65 22 3a 22 57 69 6e 64 6f 77 73 2e 57 69 6e 64 6f 77 73 38 78 22 7d 5d 2c 22 50 6c 61 74 66 6f 72 6d 44 65 70 65 6e 64 65 6e 63 79 58 6d 6c 42 6c 6f 62 22 3a 22 7b 5c 22 62 6c 6f 62 2e 76 65 72 73 69 6f 6e 5c 22 3a 31 36 38 38 38 36 37 30 34 30 35 32 36 33 33 36 2c 5c 22 63 6f 6e 74 65 6e 74 2e 69 73 4d 61 69 6e 5c 22 3a 66 61 6c 73 65 2c 5c 22 63 6f 6e 74 65 6e 74 2e 6d 61 78 4f 53 54 65 73 74 65 64 5c 22 3a 31 36 38 38 38 35 38 34 35 30 32 36 34 30 36 34 2c 5c 22 63 6f 6e 74 65 6e 74 2e 6d 69 6e 4f 53 5c 22 3a 31 36 38 38 38 35 38 34 35 30 32 36 34 30 36 34 2c 5c 22 63 6f 6e 74 65 6e 74 2e 70 61 63 6b 61 67 65 49 64 5c 22 3 a 5c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f Data Ascii: 450264064, \"PlatformName\":\"Windows.Windows8x\"}], \"PlatformDependencyXmlBlob\":\"{ \"blob.version\":1688 867040526336, \"content.isMain\":false, \"content.maxOSTested\":1688858450264064, \"content.minOS\":1688858450264 064, \"content.packageId\":\"Microsoft.BingNews_
2022-04-08 08:03:31 UTC	8641	IN	Data Raw: 56 46 57 22 2c 22 57 75 42 75 6e 64 6c 65 49 64 22 3a 22 65 62 37 61 62 36 35 32 2d 63 32 32 37 2d 34 35 39 36 2d 62 61 37 37 2d 34 36 37 62 63 38 64 61 65 33 33 32 22 2c 22 57 75 43 61 74 65 67 6f 72 79 49 64 22 3a 22 65 61 61 66 32 63 65 33 2d 64 35 61 33 2d 34 61 35 39 2d 61 65 33 31 2d 32 37 36 66 62 63 34 61 37 63 64 22 2c 22 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 2e 42 69 6e 67 4e 65 77 73 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 2c 22 53 6b 75 49 64 22 3a 22 30 30 31 31 22 2c 22 43 6f 6e 74 65 6e 74 22 3a 6e 75 6c 6c 2c 22 50 61 63 6b 61 67 65 46 65 61 74 75 72 65 73 22 3a 6e 75 6c 6c 7d 7d 2c 7b 22 41 70 70 6c 69 63 61 74 69 6f 6e 73 22 3a 5b 7b 22 41 70 70 6c 69 63 61 74 69 6f 6e 49 64 22 3a Data Ascii: VFVW\", \"WuBundId\":\"eb7ab652-c227-4596-ba77-467bc8dae332\", \"WuCategoryId\":\"eaaef2ce3-d5a3-4a59-ae31- 276bfc44a7cd\", \"PackageFamilyName\":\"Microsoft.BingNews_8wekyb3d8bbwe\", \"Skuld\":\"0011\", \"Content\":null, \"P ackageFeatures\":null}}, { \"Applications\":[{ \"ApplicationId\":
2022-04-08 08:03:31 UTC	8645	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.3	50028	40.112.88.60	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:30 UTC	8452	OUT	GET /v1/a/opportunity?pg=PC000P0FR5.0000000IQ8&unid=&placementType=PostOOBE&app=&pid=425106554&cid=128000000001392709&tid=700342084&reqasid=cbed9efce7f24d8b9b00c27d1eebe749®ion=US&lang=EN-US&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.17134.1&mo=&cap=&auid=&anid=&muid=&persid=&itemId=9NXQXXLFST89&skuld=0010&installKind=Install&ctid=store-curated-postoobe&bSrc=i.t&asid=ac8063a32da047dabe6fd5f6a689fb6c&time=20220408T170259Z HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Host: ris.api.iris.microsoft.com Connection: Keep-Alive
2022-04-08 08:03:30 UTC	8453	IN	HTTP/1.1 204 No Content Content-Length: 0 Server: Microsoft-HTTPAPI/2.0 request-id: 3f387025-5740-4024-bf27-9c1f02572ede Date: Fri, 08 Apr 2022 08:03:30 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49982	20.199.120.85	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:24 UTC	29	OUT	Data Raw: 43 4e 54 20 31 20 43 4f 4e 20 32 34 36 0d 0a 43 6f 6e 74 65 78 74 3a 20 39 34 66 33 32 30 66 39 39 33 64 36 64 62 63 64 0d 0a 0d 0a Data Ascii: CNT 1 CON 246Context: 94f320f993d6dbcd
2022-04-08 08:02:24 UTC	29	OUT	Data Raw: 3c 63 6f 6e 6e 65 63 74 3e 3c 76 65 72 3e 32 3c 2f 76 65 72 3e 3c 61 67 65 6e 74 3e 3c 6f 73 3e 57 69 6e 64 6f 77 73 3c 2f 6f 73 3e 3c 6f 73 56 65 72 3e 31 30 2e 30 2e 30 2e 30 2e 31 37 31 33 34 3c 2f 6f 73 56 65 72 3e 3c 70 72 6f 63 3e 78 36 34 3c 2f 70 72 6f 63 3e 3c 6c 63 69 64 3e 65 6e 2d 55 53 3c 2f 6c 63 69 64 3e 3c 67 65 6f 49 64 3e 32 34 34 3c 2f 67 65 6f 49 64 3e 3c 61 6f 61 63 3e 30 3c 2f 61 6f 61 63 3e 3c 64 65 76 69 63 65 54 79 70 65 3e 31 3c 2f 64 65 76 69 63 65 54 79 70 65 3e 3c 64 65 76 69 63 65 4e 61 6d 65 3e 56 4d 77 61 72 65 37 2c 31 3c 2f 64 65 76 69 63 65 4e 61 6d 65 3e 3c 2f 61 67 65 6e 74 3e 3c 2f 63 6f 6e 6e 65 63 74 3e Data Ascii: <connect><ver>2</ver><agent><os>Windows</os><osVer>10.0.0.0.17134</osVer><proc>x64</proc><lcid>en-US</lcid><geold>244</geold><aoac>0</aoac><deviceType>1</deviceType><deviceName>VMware7,1</deviceName></agent></connect>
2022-04-08 08:02:24 UTC	29	OUT	Data Raw: 41 54 48 20 32 20 43 4f 4e 5c 44 45 56 49 43 45 20 31 30 31 34 0d 0a 43 6f 6e 74 65 78 74 3a 20 39 34 66 33 32 30 66 39 39 33 64 36 64 62 63 64 0d 0a 0d 0a 3c 64 65 76 69 63 65 3e 3c 63 6f 6d 70 61 63 74 2d 74 69 63 6b 65 74 3e 74 3d 45 77 43 6f 41 75 70 49 42 41 41 55 31 62 44 47 66 64 61 7a 69 44 66 58 70 6a 4e 35 4e 36 63 59 68 54 31 77 62 6d 51 41 41 51 77 65 75 52 78 64 54 45 52 58 49 34 58 73 61 55 64 61 66 67 57 47 68 6d 46 42 32 63 6a 51 30 2b 6c 52 4d 56 52 66 4d 58 33 46 77 79 4e 35 6e 68 5a 42 49 69 50 59 61 52 4e 51 2f 64 77 71 38 33 2f 58 59 37 5a 42 55 72 6d 54 65 77 44 66 6a 2f 57 6d 4f 6e 51 35 6b 4e 32 56 76 44 35 75 46 4d 37 47 6a 4c 78 56 73 37 55 78 36 70 69 69 71 41 6d 6c 4d 6d 4e 7a 57 34 6d 36 7a 78 2f 52 66 32 38 74 48 6b 4a 46 73 Data Ascii: ATH 2 CON\DEVICE 1014Context: 94f320f993d6dbcd<device><compact-ticket>t=EwCoAup\BAAU1bDGfdaziDfXpjN5N6cYhT1wbmQAAQweuRxdTERXl4XsaUdafgWGhmFB2cjQ0+IRMVRFmX3FwyN5nhZBliPYaRNQ\dwq83/XY7ZBUrmTewDfj/WmOnQ5kN2VvD5uFM7GjLxVs7Ux6piiqAmI MmNzW4m6zx/Rf28tHkJfS
2022-04-08 08:02:24 UTC	30	OUT	Data Raw: 42 4e 44 20 33 20 43 4f 4e 5c 51 4f 53 20 32 39 0d 0a 43 6f 6e 74 65 78 74 3a 20 39 34 66 33 32 30 66 39 39 33 64 36 64 62 63 64 0d 0a 0d 0a Data Ascii: BND 3 CON\QOS 29Context: 94f320f993d6dbcd
2022-04-08 08:02:24 UTC	30	IN	Data Raw: 32 30 32 20 31 20 43 4f 4e 20 35 38 0d 0a Data Ascii: 202 1 CON 58
2022-04-08 08:02:24 UTC	30	IN	Data Raw: 4d 53 2d 43 56 3a 20 56 50 52 67 72 6b 5a 38 4b 6b 32 78 46 78 58 49 4d 5a 41 4f 53 67 2e 30 0d 0a 0d 0a 50 61 79 6c 6f 61 64 20 70 61 72 73 69 6e 67 20 66 61 69 6c 65 64 2e Data Ascii: MS-CV: VPRgrkZ8Kk2xFxXIMZAOSg.0Payload parsing failed.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.3	50029	40.112.88.60	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:31 UTC	8489	OUT	GET /v1/a/opportunity?pg=PC000P0FR5.0000000IQ8&unid=&placementType=PostOOBE&app=&pid=425106554&cid=128000000001392709&tid=700342084&reqasid=cbed9efce7f24d8b9b00c27d1eebe749®ion=US&lang=EN-US&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.17134.1&mo=&cap=&aid=&anid=&muid=&persid=&itemId=9WZDNCRFHVFW&skuld=0010&installKind=Install&ctid=store-curated-postoobe&bSrc=i.t&asid=ac8063a32da047dabe6fd5f6a689fb6c&time=20220408T170302Z HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Host: ris.api.iris.microsoft.com Connection: Keep-Alive
2022-04-08 08:03:31 UTC	8633	IN	HTTP/1.1 204 No Content Content-Length: 0 Server: Microsoft-HTTPAPI/2.0 request-id: 91c9d4d7-18ff-4c90-8c17-defbb9c947b6 Date: Fri, 08 Apr 2022 08:03:30 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.3	50030	40.112.88.60	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:31 UTC	8645	OUT	GET /v1/a/opportunity?pg=PC000P0FR5.0000000IQ8&unid=&placementType=PostOOBE&app=&pid=425106554&cid=128000000001392709&tid=700342084&reqasid=cbed9efce7f24d8b9b00c27d1eebe749®ion=US&lang=EN-US&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.17134.1&mo=&cap=&aid=&anid=&muid=&persid=&itemId=9NCBCSZSJRSB&skuld=0010&installKind=Install&ctid=store-curated-postoobe&bSrc=i.t&asid=ac8063a32da047dabe6fd5f6a689fb6c&time=20220408T170304Z HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Host: ris.api.iris.microsoft.com Connection: Keep-Alive
2022-04-08 08:03:31 UTC	8646	IN	HTTP/1.1 204 No Content Content-Length: 0 Server: Microsoft-HTTPAPI/2.0 request-id: c9c90fae-862a-4a37-99c9-9622ef344dd3 Date: Fri, 08 Apr 2022 08:03:30 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.3	50031	40.112.88.60	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:31 UTC	8646	OUT	GET /v1/a/opportunity?pg=PC000P0FR5.0000000IQ8&unid=&placementType=PostOOBE&app=&pid=425106554&cid=128000000001392709&tid=700342084&reqasid=cbed9efce7f24d8b9b00c27d1eebe749®ion=US&lang=EN-US&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.17134.1&mo=&cap=&aid=&anid=&muid=&persid=&itemId=9NMPJ99VJBWV&skuld=0010&installKind=Install&ctid=store-curated-postoobe&bSrc=i.t&asid=ac8063a32da047dabe6fd5f6a689fb6c&time=20220408T170306Z HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Host: ris.api.iris.microsoft.com Connection: Keep-Alive
2022-04-08 08:03:31 UTC	8647	IN	HTTP/1.1 204 No Content Content-Length: 0 Server: Microsoft-HTTPAPI/2.0 request-id: 5d8ea45e-299a-4a22-af28-03e930484d4b Date: Fri, 08 Apr 2022 08:03:30 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.3	50033	40.112.88.60	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:31 UTC	8647	OUT	GET /v1/a/opportunity?pg=PC000P0FR5.0000000IQ8&unid=&placementType=PostOOBE&app=&pid=425106554&cid=128000000001392709&tid=700342084&reqasid=cbed9efce7f24d8b9b00c27d1eebe749®ion=US&lang=EN-US&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.17134.1&mo=&cap=&aid=&anid=&muid=&persid=&itemId=9NBLGGH5FV99&skuld=0010&installKind=Install&ctid=store-curated-postoobe&bSrc=i.t&asid=ac8063a32da047dabe6fd5f6a689fb6c&time=20220408T170308Z HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Host: ris.api.iris.microsoft.com Connection: Keep-Alive
2022-04-08 08:03:31 UTC	8648	IN	HTTP/1.1 204 No Content Content-Length: 0 Server: Microsoft-HTTPAPI/2.0 request-id: 54067007-297a-415b-8711-dd21af9739af Date: Fri, 08 Apr 2022 08:03:30 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.3	50032	52.242.101.226	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:31 UTC	8647	OUT	GET /SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%7D/x64/10.0.17134.1/0?CH=17&L=en-US&P=&PT=0x30&WUA=10.0.17134.1&MK=4MtpozR6MODPIGb&MD=EefvrDUR HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Windows-Update-Agent/10.0.10011.16384 Client-Protocol/1.81 Host: sls.update.microsoft.com
2022-04-08 08:03:31 UTC	8648	IN	HTTP/1.1 200 OK Cache-Control: no-cache Pragma: no-cache Content-Type: application/octet-stream Expires: -1 Last-Modified: Mon, 01 Jan 0001 00:00:00 GMT ETag: "wy8fVV3cy06QIZhZUaOIBeoVMBnt4x8NjH3c50VWOxM=_1440" MS-CorrelationId: b4313648-4220-4ed9-a885-e514253cdc77 MS-RequestId: fcaca677-3cfd-4cc3-b4b7-736ce3b74dd5 MS-CV: FMcLht1YPU6BgFde.0 X-Microsoft-SLSCClientCache: 1440 Content-Disposition: attachment; filename=environment.cab X-Content-Type-Options: nosniff Date: Fri, 08 Apr 2022 08:03:31 GMT Connection: close Content-Length: 30958
2022-04-08 08:03:31 UTC	8648	IN	Data Raw: 4d 53 43 46 00 00 00 00 be 37 00 00 00 00 00 44 00 00 00 00 00 00 03 01 01 00 01 00 04 00 20 e0 00 00 14 00 00 00 00 00 10 00 be 37 00 00 30 41 00 00 00 00 00 00 00 00 64 00 00 01 00 01 00 f3 5b 00 00 00 00 00 00 00 00 00 80 00 65 6e 76 69 72 6f 6e 6d 65 6e 74 2e 63 61 62 00 27 c3 6c fd 52 37 f3 5b 43 4b ed 7a 05 58 55 dd d6 ee de 9b ee 96 6e 11 e9 b5 e9 52 69 a5 a4 bb 5b a4 bb 6b d3 ad a2 74 77 08 08 08 d2 21 25 dd a0 80 80 48 4a 4a 83 c4 dd e8 17 9e ef d4 7f fe 7b cf 73 fe 7b ef b7 9f 67 ef bd e6 5c 73 ce 35 63 8c f1 8e 77 8c 25 af 22 2e 05 82 7f da c9 40 df 3f 12 3f fe 40 08 60 30 08 0c 42 04 bd f8 08 02 11 7e af c1 fd de 06 10 05 fd f6 31 85 7f af 5b 85 72 83 7e fa f8 83 cc 6c 5d 2d 1d ed 6c 6d cc 6c 9d d9 dd 6d ac 41 f8 7a 2e Data Ascii: MSCF7D 70Adj[environment.cab\IR7[CKzXUnRi[ktw!%HJJ[s{gls5cw%".@??@`0B~1[r-]-lmlmAz.
2022-04-08 08:03:31 UTC	8664	IN	Data Raw: b3 49 a2 0d ff f6 07 56 2e e0 cd 9b 1f 2c 88 a2 01 ec 5e 7b 96 ac 79 f1 dc 76 c5 85 50 e5 c7 c8 45 07 64 59 b3 b7 80 da 46 59 e2 3c b1 95 cb ed 18 a0 46 1e 05 b6 ad 0f aa c7 d6 26 8a 7a 17 6e 85 5c 5c 6e b7 9b 98 29 fc 15 9c b1 63 23 9c 27 9a ba 82 04 21 f1 ec 76 cf 7a 3c 9a dc 26 02 a4 4b 13 b7 f5 66 dc 71 d6 12 42 66 da ba 5c 82 4f 0a 63 8b 27 ed ac 5b 4a 30 41 b8 22 8b 2f b7 4c 07 eb 6d 35 30 dd 9f 04 c2 94 77 e9 20 77 b3 ca 0d 58 a9 21 17 bb 64 c6 3c 80 fd e9 00 b3 78 2d 96 fe 20 b6 4c c6 4a 0b e6 fc 7a 35 83 21 a9 5b fb 9f ec fd f1 bd a9 3a 79 0e 3d a3 0c 9a 4f 59 1e be de 85 65 6f ea 2b b7 1c 1f d9 51 fd 01 a2 7c 91 b5 30 82 07 05 30 82 04 ed a0 03 02 01 02 02 13 33 00 00 00 08 59 e3 94 e0 54 c7 17 5d 00 00 00 00 08 30 0d 06 09 2a 86 48 86 f7 0d Data Ascii: IV.,^{\yvPEdYFY<F&zn\n)c#:\vz<&KfqBfOc'[J0A"/Lm50w wXld<- Ljz5l[-y=OYeo+Q[003YT]0*H

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.3	50034	40.112.88.60	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:32 UTC	8679	OUT	GET /v1/a/opportunity?pg=PC000P0FR5.0000000IQ8&unid=&placementType=PostOOBE&app=&pid=425106554&cid=128000000001392709&tid=700342084&reqasid=cbed9efce7f24d8b9b00c27d1eebe749®ion=US&lang=EN-US&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.17134.1&mo=&cap=&aid=&anid=&muid=&persid=&itemId=9WZDNCRDFNG7&skuld=0010&installKind=Install&ctid=store-curated-postoobe&bSrc=i.t&asid=ac8063a32da047dabe6fd5f6a689fb6c&time=20220408T170310Z HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Host: ris.api.iris.microsoft.com Connection: Keep-Alive
2022-04-08 08:03:32 UTC	8679	IN	HTTP/1.1 204 No Content Content-Length: 0 Server: Microsoft-HTTPAPI/2.0 request-id: b59b680a-b553-4946-a69c-2f900c677fff Date: Fri, 08 Apr 2022 08:03:31 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.3	50036	40.112.88.60	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:32 UTC	8679	OUT	GET /v1/a/impression?pg=PC000P0FR5.0000000IQ8&unid=&placementType=PostOOBE&app=&pid=425106554&cid=128000000001392709&tid=700342084&reqasid=cbed9efce7f24d8b9b00c27d1eebe749®ion=US&lang=EN-US&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.17134.1&mo=&cap=&aid=&anid=&muid=&persid=&bSrc=i.t&time=20220408T170315Z&asid=ac8063a32da047dabe6fd5f6a689fb6c&eid= HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Host: ris.api.iris.microsoft.com Connection: Keep-Alive
2022-04-08 08:03:32 UTC	8680	IN	HTTP/1.1 204 No Content Content-Length: 0 Server: Microsoft-HTTPAPI/2.0 request-id: 3b6886b1-063b-4d50-8e6f-fe9952815c4d Date: Fri, 08 Apr 2022 08:03:31 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.3	50035	52.242.101.226	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:32 UTC	8680	OUT	GET /SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%7D/x64/10.0.17134.1/0?CH=17&L=en-US&P=&PT=0x30&WUA=10.0.17134.1&MK=4MtpozR6MODPIGb&MD=EefvrDUR HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Windows-Update-Agent/10.0.10011.16384 Client-Protocol/1.81 Host: sls.update.microsoft.com
2022-04-08 08:03:32 UTC	8680	IN	HTTP/1.1 200 OK Cache-Control: no-cache Pragma: no-cache Content-Type: application/octet-stream Expires: -1 Last-Modified: Mon, 01 Jan 0001 00:00:00 GMT ETag: "wy8fV3cy06QlZhZUaOlBEoVMBnt4x8NjH3c50VWOxM=_1440" MS-CorrelationId: cf9cbf41-0e86-4d38-87e1-9c1e3a1b088d MS-RequestId: 7c1f90d0-9446-4bae-b4b4-b2111b170b1e MS-CV: 0aN2V3D8CU6Zk+pX.0 X-Microsoft-SLSClietCache: 1440 Content-Disposition: attachment; filename=environment.cab X-Content-Type-Options: nosniff Date: Fri, 08 Apr 2022 08:03:32 GMT Connection: close Content-Length: 30958
2022-04-08 08:03:32 UTC	8681	IN	Data Raw: 4d 53 43 46 00 00 00 00 be 37 00 00 00 00 00 44 00 00 00 00 00 00 00 03 01 01 00 01 00 04 00 20 e0 00 00 14 00 00 00 00 00 10 00 be 37 00 00 30 41 00 00 00 00 00 00 00 00 64 00 00 01 00 01 00 f3 5b 00 00 00 00 00 00 00 00 00 00 80 00 65 6e 76 69 72 6f 6e 6d 65 6e 74 2e 63 61 62 00 27 c3 6c fd 52 37 f3 5b 43 4b ed 7a 05 58 55 dd d6 ee de 9b ee 96 6e 11 e9 b5 e9 52 69 a5 a4 bb 5b a4 bb 6b d3 ad a2 74 77 08 08 08 d2 21 25 dd a0 80 80 48 4a 4a 83 c4 dd e8 17 9e ef d4 7f fe 7b cf 73 fe 7b ef b7 9f 67 ef bd e6 5c 73 ce 35 63 8c f1 8e 77 8c 25 af 22 2e 05 82 7f da c9 40 df 3f 12 3f fe 40 08 60 30 08 0c 42 04 bd f8 08 02 11 7e af c1 fd de 06 10 05 fd f6 31 85 7f af 5b 85 72 83 7e fa f8 83 cc 6c 5d 2d 1d ed 6c 6d cc 6c 9d d9 dd 6d ac 41 f8 7a 2e Data Ascii: MSCF7D 70Adj[environment.cab\IR7[CKzXUnRi[ktw\%HJJ[s[gs5cw%".@??@`0B-1[r-l]-lmlmAz.

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:32 UTC	8696	IN	Data Raw: b3 49 a2 0d ff f6 07 56 2e e0 cd 9b 1f 2c 88 a2 01 ec 5e 7b 96 ac 79 f1 dc 76 c5 85 50 e5 c7 c8 45 07 64 59 b3 b7 80 da 46 59 e2 3c b1 95 cb ed 18 a0 46 1e 05 b6 ad 0f aa c7 d6 26 8a 7a 17 6e 85 5c 5c 6e b7 9b 98 29 fc 15 9c b1 63 23 9c 27 9a ba 82 04 21 f1 ec 76 cf 7a 3c 9a dc 26 02 a4 4b 13 b7 f5 66 dc 71 d6 12 42 66 da ba 5c 82 4f 0a 63 8b 27 ed ac 5b 4a 30 41 b8 22 8b 2f b7 4c 07 eb 6d 35 30 dd 9f 04 c2 94 77 e9 20 77 b3 ca 0d 58 a9 21 17 bb 64 c6 3c 80 fd e9 00 b3 78 2d 96 fe 20 b6 4c c6 4a 0b e6 fc 7a 35 83 21 a9 5b fb 9f ec fd f1 bd a9 3a 79 0e 3d a3 0c 9a 4f 59 1e be de 85 65 6f ea 2b b7 1c 1f d9 51 fd 01 a2 7c 91 b5 30 82 07 05 30 82 04 ed a0 03 02 01 02 02 13 33 00 00 00 08 59 e3 94 e0 54 c7 17 5d 00 00 00 00 08 30 0d 06 09 2a 86 48 86 f7 0d Data Ascii: IV.,^{\yPEdYFY<F&z\n\nc#^lvz<&KfqBfOc"[J0A"/Lm50w wXld<x- Lj5z[:y=OYeo+Q[003YT]J0*H

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.3	50037	20.54.110.249	443	C:\Users\user\l\Desktop\l.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:32 UTC	8711	OUT	GET /v7.0/products/lookup?alternateId=PackageFamilyName&value=6F71D7A7.HotspotShieldFreeVPN_nsbqstbb9qxb6&market=US&languages=en-US%2Cen%2Cneutral&fieldsTemplate=InstallAgent&mold=Public&oemId=Public&scmlId=Public HTTP/1.1 Connection: Keep-Alive Content-Type: application/json User-Agent: Install Service MS-CV: ADE0AlIAz0+Cj5BW.0.2.4 Host: displaycatalog.mp.microsoft.com
2022-04-08 08:03:32 UTC	8712	IN	HTTP/1.1 200 OK Connection: close Date: Fri, 08 Apr 2022 08:03:32 GMT Content-Type: application/json; charset=utf-8 Server: Kestrel Transfer-Encoding: chunked Vary: Authorization MS-CorrelationId: f33b8a5f-ac14-456a-a88f-7ca633628ddb MS-RequestId: b67ca5ba-689f-4deb-adca-85f7d2e12110 MS-CV: ADE0AlIAz0+Cj5BW.0.2.4.422987403.0.1.422987403.1502015328.0 X-Content-Type-Options: nosniff MS-ServerId: 74 Region: neu Node: aks-systempool-37630073-vmss00002m MS-DocumentVersions: 9WZDNCRDFNG7J3613
2022-04-08 08:03:32 UTC	8712	IN	Data Raw: 63 33 34 32 0d 0a 7b 22 42 69 67 49 64 73 22 3a 5b 22 39 57 5a 44 4e 43 52 44 46 4e 47 37 22 5d 2c 22 48 61 73 4d 6f 72 65 50 61 67 65 73 22 3a 66 61 6c 73 65 2c 22 50 72 6f 64 75 63 74 73 22 3a 5b 7b 22 4c 61 73 74 4d 6f 64 69 66 69 65 64 44 61 74 65 22 3a 22 32 30 32 32 2d 30 33 2d 30 32 54 30 31 3a 31 37 3a 35 30 2e 36 32 30 32 30 30 30 5a 22 2c 22 4c 6f 63 61 6c 69 7a 65 64 50 72 6f 70 65 72 74 69 65 73 22 3a 5b 7b 22 46 72 61 6e 63 68 69 73 65 73 22 3a 5b 5d 2c 22 49 6d 61 67 65 73 22 3a 5b 7b 22 46 69 6c 65 49 64 22 3a 22 33 30 36 37 35 35 37 30 30 32 39 37 33 30 31 31 35 32 30 22 2c 22 45 49 53 4c 69 73 74 69 6e 67 49 64 65 6e 74 69 66 69 65 72 22 3a 6e 75 6c 6c 2c 22 42 61 63 6b 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 23 30 33 31 38 33 37 22 2c Data Ascii: c342{"BigIds":["9WZDNCRDFNG7"],"HasMorePages":false,"Products":[{"LastModifiedDate":"2022-03-02T01:17:50.6202000Z","LocalizedProperties":[{"Franchises":[],"Images":[{"FileId":"3067557002973011520","EISListingIdentifier":"","null","BackgroundColor":"#031837",
2022-04-08 08:03:32 UTC	8716	IN	Data Raw: 65 30 2d 65 34 34 38 37 38 37 65 39 37 32 65 2e 37 33 35 61 62 39 30 64 2d 35 38 31 37 2d 34 35 36 38 2d 39 64 62 64 2d 31 65 31 31 61 66 33 62 62 61 39 31 22 2c 22 57 69 64 74 68 22 3a 32 31 36 30 7d 2c 7b 22 46 69 6c 65 49 64 22 3a 22 32 30 30 30 30 30 30 30 30 35 36 35 36 39 38 34 33 22 2c 22 45 49 53 4c 69 73 74 69 6e 67 49 64 65 6e 74 69 66 69 65 72 22 3a 6e 75 6c 6c 2c 22 42 61 63 6b 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 23 30 33 31 38 33 37 22 2c 22 43 61 70 74 69 6f 6e 22 3a 22 22 2c 22 46 69 6c 65 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 31 32 37 35 31 2c 22 46 6f 72 65 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 22 2c 22 48 65 69 67 68 74 22 3a 33 30 30 2c 22 49 6d 61 67 65 50 6f 73 69 74 69 6f 6e 49 6e 66 6f 22 3a 22 22 2c 22 49 6d 61 67 Data Ascii: e0-e448787e972e.735ab90d-5817-4568-9dbd-1e11af3bba91","Width":2160},{"FileId":"2000000000056569843","EISListingIdentifier":null,"BackgroundColor":"#031837","Caption":"","FileSizelnBytes":12751,"ForegroundColor":"","Height":300,"ImagePositionInfo":"","Imag
2022-04-08 08:03:32 UTC	8720	IN	Data Raw: 5c 72 5c 6e 48 6f 74 73 70 6f 74 20 53 68 69 65 6c 64 20 56 50 4e 20 50 72 65 6d 69 75 6d 20 73 65 72 76 69 63 65 20 69 6e 63 6c 75 64 65 73 3a 5c 72 5c 6e 5c 72 5c 6e 2d 20 37 2d 64 61 79 20 66 72 65 65 20 74 72 69 61 6c 3a 20 66 72 65 65 20 6f 66 20 63 68 61 72 67 65 3b 20 6e 6f 20 63 6f 6d 6d 69 74 6d 65 6e 74 3b 20 63 61 6e 63 65 6c 20 61 6e 79 74 69 6d 65 2e 5c 72 5c 6e 2d 20 50 61 79 6d 65 6e 74 20 77 69 6c 6c 20 62 65 20 63 68 61 72 67 65 64 20 74 6f 20 79 6f 75 72 20 4d 69 63 72 6f 73 6f 66 74 20 53 74 6f 72 65 20 61 63 63 6f 75 6e 74 20 61 74 20 63 6f 6e 66 69 72 6d 61 74 69 6f 6e 20 6f 66 20 70 75 72 63 68 61 73 65 2e 5c 72 5c 6e 2d 20 53 75 62 73 63 72 69 70 74 69 6f 6e 20 61 75 74 6f 6d 61 74 69 63 61 6c 6c 79 20 72 65 6e 65 77 73 20 75 6e 6c Data Ascii: \r\nHotspot Shield VPN Premium service includes:\r\n\r\n- 7-day free trial: free of charge; no commitment; cancel anytime.\r\n- Payment will be charged to your Microsoft Store account at confirmation of purchase.\r\n- Subscription automatically renews unl
2022-04-08 08:03:32 UTC	8724	IN	Data Raw: 75 63 74 54 79 70 65 22 3a 22 41 70 70 6c 69 63 61 74 69 6f 6e 22 2c 22 56 61 6c 69 64 61 74 69 6f 6e 44 61 74 61 22 3a 7b 22 50 61 73 73 65 64 56 61 6c 69 64 61 74 69 6f 6e 22 3a 66 61 6c 73 65 2c 22 52 65 76 69 73 69 6f 6e 49 64 22 3a 22 32 30 32 32 2d 30 33 2d 30 32 54 30 31 3a 31 38 3a 34 31 2e 34 30 32 37 37 36 30 5a 7c 7c 2e 7c 7c 36 32 64 36 34 30 31 31 2d 62 34 38 63 2d 34 31 33 31 2d 62 36 36 36 2d 61 37 33 64 30 39 35 32 62 62 66 37 7c 7c 31 31 35 32 39 32 31 35 30 35 36 39 34 33 38 30 31 37 39 7c 7c 4e 75 6c 6c 7c 7c 66 75 6c 6c 72 65 6c 65 61 73 65 22 2c 22 56 61 6c 69 64 61 74 69 6f 6e 52 65 73 75 6c 74 55 72 69 22 3a 22 22 7d 2c 22 4d 65 72 63 68 61 6e 64 69 7a 69 6e 67 54 61 67 73 22 3a 5b 5d 2c 22 50 61 72 74 44 22 3a 22 22 2c 22 50 72 6f Data Ascii: uctType":"","Application","ValidationData":{"PassedValidation":false,"RevisionId":"","2022-03-02T01:18:41.4027760Z"},"62d64011-b48c-4131-b666-a73d0952bbf7 1152921505694380179 Null fullrelease","ValidationResult Uri":"","MerchandizingTags":[],"PartD":"","Pro

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:32 UTC	8728	IN	Data Raw: 43 4b 22 2c 22 43 58 22 2c 22 43 43 22 2c 22 43 49 22 2c 22 43 57 22 2c 22 4a 4d 22 2c 22 53 4a 22 2c 22 4a 45 22 2c 22 4b 49 22 2c 22 4b 47 22 2c 22 4c 41 22 2c 22 4c 53 22 2c 22 4c 52 22 2c 22 4d 4f 22 2c 22 4d 4b 22 2c 22 4d 47 22 2c 22 4d 57 22 2c 22 49 4d 22 2c 22 4d 48 22 2c 22 4d 51 22 2c 22 4d 55 22 2c 22 59 54 22 2c 22 46 4d 22 2c 22 4d 44 22 2c 22 4d 4e 22 2c 22 4d 53 22 2c 22 4d 5a 22 2c 22 4d 4d 22 2c 22 4e 41 22 2c 22 4e 52 22 2c 22 4e 50 22 2c 22 4d 56 22 2c 22 4d 4c 22 2c 22 4e 43 22 2c 22 4e 49 22 2c 22 4e 55 22 2c 22 4e 52 2c 22 4e 46 22 2c 22 50 57 22 2c 22 50 53 22 2c 22 50 41 22 2c 22 50 47 22 2c 22 50 59 22 2c 22 52 45 22 2c 22 52 57 22 2c 22 42 4c 22 2c 22 4d 46 22 2c 22 57 53 22 2c 22 53 54 22 2c 22 53 4e 22 2c 22 4d 50 22 2c 22 Data Ascii: CK","CX","CC","CI","CW","JM","SJ","JE","KI","KG","LA","LS","LR","MO","MK","MG","MW","IM","MH","MQ","MU","YT","FM","MD","MN","MS","MZ","MM","NA","NR","NP","MV","ML","NC","NI","NE","NU","NF","PW","PS","PA","PG","PY","RE","RW","BL","MF","WS","ST","SN","MP","
2022-04-08 08:03:32 UTC	8732	IN	Data Raw: 6c 66 69 6c 6c 6d 65 6e 74 44 61 74 61 22 3a 7b 22 50 72 6f 64 75 63 74 49 64 22 3a 22 39 57 5a 44 4e 43 52 44 46 4e 47 37 22 2c 22 57 75 42 75 6e 64 6c 65 49 64 22 3a 22 62 35 61 34 64 39 35 64 2d 61 39 61 66 2d 34 38 62 34 2d 62 35 37 62 2d 64 66 61 36 39 66 38 31 37 39 62 31 22 2c 22 57 75 43 61 74 65 67 6f 72 79 49 64 22 3a 22 31 37 36 30 37 33 30 66 2d 66 37 37 31 2d 34 64 33 66 2d 62 65 34 36 2d 66 61 66 62 65 31 35 66 62 39 37 65 22 2c 22 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 22 3a 22 36 46 37 31 44 37 41 37 2e 48 6f 74 73 70 6f 74 53 68 69 65 6c 64 46 72 65 65 56 50 4e 5f 6e 73 62 71 73 74 62 62 39 71 78 62 36 22 2c 22 53 6b 75 49 64 22 3a 22 30 30 31 30 22 2c 22 43 6f 6e 74 65 6e 74 22 3a 6e 75 6c 6c 2c 22 50 61 63 6b 61 67 65 46 65 Data Ascii: lfillmentData":{"ProductId":"9WZDNCRDFNG7","WuBundleId":"b5a4d95d-a9af-48b4-b57b-dfa69f8179b1","WuCategoryId":"a760730f-f771-4d3f-be46-fafbe15fb97e","PackageFamilyName":"6F71D7A7.HotspotShieldFreeVPN_N_nsbqstbb9qxb6","Skuld":"0010","Content":null,"PackageFe
2022-04-08 08:03:32 UTC	8736	IN	Data Raw: 73 22 3a 5b 5d 2c 22 4d 61 78 44 6f 77 6e 6c 6f 61 64 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 32 32 31 34 32 37 39 34 2c 22 4d 61 78 49 6e 73 74 61 6c 6c 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 35 30 33 39 37 31 38 34 2c 22 50 61 63 6b 61 67 65 46 6f 72 6d 61 74 22 3a 22 4d 73 69 78 22 2c 22 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 22 3a 22 36 46 37 31 44 37 41 37 2e 48 6f 74 73 70 6f 74 53 68 69 65 6c 64 46 72 65 65 56 50 4e 5f 6e 73 62 71 73 74 62 62 39 71 78 62 36 22 2c 22 4d 61 69 6e 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 22 3a 22 36 46 37 31 44 37 41 37 2e 48 6f 74 73 70 6f 74 53 68 69 65 6c 64 46 72 65 65 56 50 4e 5f 32 2e 31 30 2e 35 2e 30 5f Data Ascii: s":["","MaxDownloadSizeInBytes":22142794,"MaxInstallSizeInBytes":50397184,"PackageFormat":"Msix","PackageFamilyName":"6F71D7A7.HotspotShieldFreeVPN_nsbqstbb9qxb6","MainPackageFamilyNameForDlc":null,"PackageFullName":"6F71D7A7.HotspotShieldFreeVPN_2.10.5.0_
2022-04-08 08:03:32 UTC	8740	IN	Data Raw: 22 3a 22 57 69 6e 64 6f 77 73 2e 48 6f 6c 6f 67 72 61 70 68 69 63 22 7d 2c 7b 22 4d 61 78 56 65 72 73 69 6f 6e 22 3a 32 31 34 37 34 38 33 36 34 37 2c 22 4d 69 6e 56 65 72 73 69 6f 6e 22 3a 30 2c 22 50 6c 61 74 66 6f 72 6d 4e 61 6d 65 22 3a 22 57 69 6e 64 6f 77 73 2e 43 6f 72 65 22 7d 2c 7b 22 4d 61 78 56 65 72 73 69 6f 6e 22 3a 32 31 34 37 34 38 33 36 34 37 2c 22 4d 69 6e 56 65 72 73 69 6f 6e 22 3a 30 2c 22 50 6c 61 74 66 6f 72 6d 4e 61 6d 65 22 3a 22 57 69 6e 64 6f 77 73 2e 38 38 32 38 30 38 30 22 7d 5d 7d 2c 22 45 6e 64 44 61 74 65 22 3a 22 39 39 39 38 2d 31 32 2d 33 30 54 30 30 3a 30 30 3a 30 30 2e 30 30 30 30 30 30 5a 22 2c 22 52 65 73 6f 75 72 63 65 53 65 74 49 64 73 22 3a 5b 22 31 22 5d 2c 22 53 74 61 72 74 44 61 74 65 22 3a 22 31 37 35 33 6d 30 Data Ascii: ":"Windows.Holographic"),{"MaxVersion":2147483647,"MinVersion":0,"PlatformName":"Windows.Core"},{"MaxVersion":2147483647,"MinVersion":0,"PlatformName":"Windows.8828080"}]],"EndDate":"9998-12-30T00:00:00.000000Z","ResourceSetIds":["1"],"StartDate":"1753-0
2022-04-08 08:03:32 UTC	8744	IN	Data Raw: 72 5c 6e 5c 72 5c 6e e2 96 ba 20 42 52 4f 57 53 45 20 53 45 43 55 52 45 4c 59 5c 72 5c 6e 53 74 61 79 20 73 65 63 75 72 65 20 77 69 74 68 20 6d 69 6c 69 74 61 72 79 2d 67 72 61 64 65 20 65 6e 63 72 79 70 6e 65 64 20 74 72 61 66 66 69 63 20 62 65 74 77 65 65 6e 20 79 6f 75 72 20 64 65 76 69 63 65 20 61 6e 64 20 6f 75 72 20 73 65 72 76 65 72 73 20 77 68 69 6c 65 20 63 6f 6e 6e 65 63 74 65 64 20 77 69 74 68 20 48 6f 74 73 70 6f 74 20 53 68 69 65 6c 64 20 56 50 4e 2e 5c 72 5c 6e 5c 72 5c 6e e2 96 ba 20 53 54 41 59 20 50 52 49 56 41 54 45 5c 72 5c 6e 59 6f 75 72 20 70 72 69 76 61 63 79 20 69 73 20 6f 75 72 20 6d 69 73 73 69 6f 6e 2e 20 43 6f 6e 6e 65 63 74 20 74 6f 61 6e 79 20 6f 66 20 6f 75 72 20 72 65 6c 69 61 62 6c 65 20 56 50 4e 20 73 65 72 76 65 72 73 Data Ascii: \r\n\r\n BROWSE SECURELY\r\n\r\nStay secure with military-grade encrypted traffic between your device and our servers while connected with Hotspot Shield VPN.\r\n\r\n\r\n STAY PRIVATE\r\n\r\nYour privacy is our mission. Connect to any of our reliable VPN servers
2022-04-08 08:03:32 UTC	8748	IN	Data Raw: 69 7a 65 49 6e 42 79 74 65 73 22 3a 34 39 37 36 32 33 30 34 2c 22 50 61 63 6b 61 67 65 46 6f 72 6d 61 74 22 3a 22 45 4d 73 69 78 22 2c 22 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 22 3a 22 36 46 37 31 44 37 41 37 2e 48 6f 74 73 70 6f 74 53 68 69 65 6c 64 46 72 65 65 56 50 4e 5f 6e 73 62 71 73 74 62 62 39 71 78 62 36 22 2c 22 4d 61 69 6e 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 46 6f 72 4d 6c 63 22 3a 6e 75 6c 6c 2c 22 50 61 63 6b 61 67 65 46 75 6c 6c 4e 61 6d 65 22 3a 22 36 46 37 31 44 37 41 37 2e 48 6f 74 73 70 6f 74 53 68 69 65 6c 64 46 72 65 65 56 50 4e 5f 32 2e 31 30 2e 35 2e 37 30 5f 61 72 6d 5f 5f 6e 73 62 71 73 74 62 62 39 71 78 62 36 22 2c 22 50 61 63 6b 61 67 65 49 64 22 3a 22 33 35 64 34 65 65 63 61 2d 33 61 31 34 2d 61 64 33 Data Ascii: izelnBytes":49762304,"PackageFormat":"EMsix","PackageFamilyName":"6F71D7A7.HotspotShieldFreeVPN_nsbqstbb9qxb6","MainPackageFamilyNameForDlc":null,"PackageFullName":"6F71D7A7.HotspotShieldFreeVPN_2.10.5.70_arm__nsbqstbb9qxb6","Packageld":"35d4eeca-3a14-ad3
2022-04-08 08:03:33 UTC	8752	IN	Data Raw: 36 2c 5c 22 63 6f 6e 74 65 6e 74 2e 69 73 4d 61 69 6e 5c 22 3a 66 61 6c 73 65 2c 5c 22 63 6f 6e 74 65 6e 74 2e 70 61 63 6b 61 67 65 49 64 5c 22 3a 5c 22 36 46 37 31 44 37 41 37 2e 48 6f 74 73 70 6f 74 53 68 69 65 6c 64 46 72 65 65 56 50 4e 5f 32 2e 31 30 2e 35 2e 37 30 5f 78 38 36 5f 5f 6e 73 62 71 73 74 62 62 39 71 78 62 36 5c 22 2c 5c 22 63 6f 6e 74 65 6e 74 2e 70 72 6f 64 75 63 74 49 64 5c 22 3a 5c 22 39 64 30 64 30 63 66 35 2d 66 32 32 62 2d 34 37 36 31 2d 61 62 65 65 2d 66 37 30 66 38 30 34 62 37 30 61 62 5c 22 2c 5c 22 63 6f 6e 74 65 6e 74 2e 74 61 72 67 65 74 50 6c 61 74 66 6f 72 6d 73 5c 22 3a 5b 7b 5c 22 70 6c 61 74 66 6f 72 6d 2e 6d 61 78 56 65 72 73 69 6f 6e 54 65 73 74 65 64 5c 22 3a 32 38 31 34 37 35 30 39 37 30 34 37 38 35 39 32 2c 5c 22 70 Data Ascii: 6,\,\"content.isMain\":false,\"content.packageld\":\"6F71D7A7.HotspotShieldFreeVPN_2.10.5.70_x86__nsbqstbb9qxb6\", \"content.productld\":\"9d0d0cf5-f22b-4761-abee-f70f804b70ab\", \"content.targetPlatforms\":{[\"platform.maxVersionTested\":2814750970478592,\"p
2022-04-08 08:03:33 UTC	8756	IN	Data Raw: 2c 5c 22 70 6f 6c 69 63 79 32 5c 22 3a 7b 5c 22 61 67 65 52 61 74 69 6e 67 5c 22 3a 31 2c 5c 22 6f 70 74 4f 75 74 2e 44 56 52 5c 22 3a 66 61 6c 73 65 2c 5c 22 74 68 69 72 64 50 61 72 74 79 41 70 70 52 61 74 69 6e 67 73 5c 22 3a 5b 7b 5c 22 6c 65 76 65 6c 5c 22 3a 37 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 33 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 31 32 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 35 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 38 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 32 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 32 37 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 39 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 37 36 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 36 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 36 38 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a Data Ascii: ,,\"policy2\":{\"ageRating\":1,\"optOut.DVR\":false,\"thirdPartyAppRatings\":{\"[\"level\":7,\"systemId\":3},{\"level\":12,\"systemId\":5},{\"level\":48,\"systemId\":12},{\"level\":27,\"systemId\":9},{\"level\":76,\"systemId\":16},{\"level\":68,\"systemId\":

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:33 UTC	8760	IN	Data Raw: 4d 69 6e 56 65 72 73 69 6f 6e 22 3a 30 2c 22 50 6c 61 74 66 6f 72 6d 4e 61 6d 65 22 3a 22 57 69 6e 64 6f 77 73 2e 48 6f 6c 6f 67 72 61 70 68 69 63 22 7d 2c 7b 22 4d 61 78 56 65 72 73 69 6f 6e 22 3a 32 31 34 37 34 38 33 36 34 37 2c 22 4d 69 6e 56 65 72 73 69 6f 6e 22 3a 30 2c 22 50 6c 61 74 66 6f 72 6d 4e 61 6d 65 22 3a 22 57 69 6e 64 6f 77 73 2e 43 6f 72 65 22 7d 2c 7b 22 4d 61 78 56 65 72 73 69 6f 6e 22 3a 32 31 34 37 34 38 33 36 34 37 2c 22 4d 69 6e 56 65 72 73 69 6f 6e 22 3a 30 2c 22 50 6c 61 74 66 6f 72 6d 4e 61 6d 65 22 3a 22 57 69 6e 64 6f 77 73 2e 38 38 32 38 30 38 30 22 7d 5d 7d 2c 22 45 6e 64 44 61 74 65 22 3a 22 39 39 39 38 2d 31 32 2d 33 30 54 30 30 3a 30 30 3a 30 30 2e 30 30 30 30 30 30 5a 22 2c 22 52 65 73 6f 75 72 63 65 53 65 74 49 64 73 Data Ascii: MinVersion":0,"PlatformName":"Windows.Holographic"},{"MaxVersion":2147483647,"MinVersion":0,"PlatformName":"Windows.Core"},{"MaxVersion":2147483647,"MinVersion":0,"PlatformName":"Windows.8828080"}]],{"EndDate":"9998-12-30T00:00:00.000000Z"},"ResourceSetIds
2022-04-08 08:03:33 UTC	8761	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.3	50038	52.242.101.226	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:33 UTC	8761	OUT	GET /SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%7D/x64/10.0.17134.1/0?CH=17&L=en-US&P=&PT=0x30&WUA=10.0.17134.1&MK=4MtpozR6MODPIGb&MD=EefvrDUR HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Windows-Update-Agent/10.0.10011.16384 Client-Protocol/1.81 Host: sls.update.microsoft.com
2022-04-08 08:03:33 UTC	8761	IN	HTTP/1.1 200 OK Cache-Control: no-cache Pragma: no-cache Content-Type: application/octet-stream Expires: -1 Last-Modified: Mon, 01 Jan 0001 00:00:00 GMT ETag: "wy8fVV3cy06QIZhZUaOIBeOvMBnt4x8NjH3c50VWOxM=_1440" MS-CorrelationId: 447b1056-43ba-4fda-a9d4-198642dceea3 MS-RequestId: 5b655adf-9175-4a0c-b604-d59e55bd55c4 MS-CV: AvdqEEZnEUO+0blf.0 X-Microsoft-SLSCClientCache: 1440 Content-Disposition: attachment; filename=environment.cab X-Content-Type-Options: nosniff Date: Fri, 08 Apr 2022 08:03:32 GMT Connection: close Content-Length: 30958
2022-04-08 08:03:33 UTC	8762	IN	Data Raw: 4d 53 43 46 00 00 00 00 be 37 00 00 00 00 00 00 44 00 00 00 00 00 00 03 01 01 00 01 00 04 00 20 e0 00 00 14 00 00 00 00 10 00 be 37 00 00 30 41 00 00 00 00 00 00 00 00 64 00 00 01 00 01 00 f3 5b 00 00 00 00 00 00 00 00 00 00 80 00 65 6e 76 69 72 6f 6e 6d 65 6e 74 2e 63 61 62 00 27 c3 6c fd 52 37 f3 5b 43 4b ed 7a 05 58 55 dd d6 ee de 9b ee 96 6e 11 e9 b5 e9 52 69 a5 a4 bb 5b a4 bb 6b d3 ad a2 74 77 08 08 08 d2 21 25 dd a0 80 80 48 4a 4a 83 c4 dd e8 17 9e ef d4 7f fe 7b cf 73 fe 7b ef b7 9f 67 ef bd e6 5c 73 ce 35 63 8c f1 8e 77 8c 25 af 22 2e 05 82 7f da c9 40 df 3f 12 3f fe 40 08 60 30 08 0c 42 04 bd f8 08 02 11 7e af c1 fd de 06 10 05 fd f6 31 85 7f af 5b 85 72 83 7e fa f8 83 cc 6c 5d 2d 1d ed 6c 6d cc 6c 9d d9 dd 6d ac 41 f8 7a 2e Data Ascii: MSCF7D 70Ad[environment.cab]IR7[CKzXUnRi[ktw!%HJJ{s(gls5cw%"_@??@`0B-[r-l]-lmlmAz.
2022-04-08 08:03:33 UTC	8777	IN	Data Raw: b3 49 a2 0d ff f6 07 56 2e e0 cd 9b 1f 2c 88 a2 01 ec 5e 7b 96 ac 79 f1 dc 76 c5 85 50 e5 c7 c8 45 07 64 59 b3 b7 80 da 46 59 e2 3c b1 95 cb ed 18 a0 46 1e 05 b6 ad 0f aa c7 d6 26 8a 7a 17 6e 85 5c 5c 6e b7 9b 98 29 fc 15 9c b1 63 23 9c 27 9a ba 82 04 21 f1 ec 76 cf 7a 3c 9a dc 26 02 a4 4b 13 b7 f5 66 dc 71 d6 12 42 66 da ba 5c 82 4f 0a 63 8b 27 ed ac 5b 4a 30 41 b8 22 8b 2f b7 4c 07 eb 6d 35 30 dd 9f 04 c2 94 77 e9 20 77 b3 ca 0d 58 a9 21 17 bb 64 c6 3c 80 fd e9 00 b3 78 2d 96 fe 20 b6 4c c6 4a 0b e6 fc 7a 35 83 21 a9 5b fb 9f ec fd f1 bd a9 3a 79 0e 3d a3 0c 9a 4f 59 1e be de 85 65 6f ea 2b b7 1c 1f d9 51 fd 01 a2 7c 91 b5 30 82 07 05 30 82 04 ed a0 03 02 01 02 02 13 33 00 00 00 08 59 e3 94 e0 54 c7 17 5d 00 00 00 00 08 30 0d 06 09 2a 86 48 86 7f 0d Data Ascii: IV.,^{\yvPEDYFY<F&zn\ n)c#`!vz<&KfqBfOc[J0A"/Lm50w wX!d<x- LJz5l[:y=OYeo+Qj003YTj]0*H

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49985	20.199.120.85	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:27 UTC	30	OUT	Data Raw: 43 4e 54 20 31 20 43 4f 4e 20 32 34 36 0d 0a 04 43 6f 6e 74 65 78 74 3a 20 38 37 30 62 37 62 34 30 33 30 65 35 35 36 65 34 0d 0a 0d 0a Data Ascii: CNT 1 CON 246Context: 870b7b4030e556e4

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:27 UTC	31	OUT	Data Raw: 3c 63 6f 6e 6e 65 63 74 3e 3c 76 65 72 3e 32 3c 2f 76 65 72 3e 3c 61 67 65 6e 74 3e 3c 6f 73 3e 57 69 6e 64 6f 77 73 3c 2f 6f 73 3e 3c 6f 73 56 65 72 3e 31 30 2e 30 2e 30 2e 31 37 31 33 34 3c 2f 6f 73 56 65 72 3e 3c 70 72 6f 63 3e 78 36 34 3c 2f 70 72 6f 63 3e 3c 6c 63 69 64 3e 65 6e 2d 55 53 3c 2f 6c 63 69 64 3e 3c 67 65 6f 49 64 3e 32 34 34 3c 2f 67 65 6f 49 64 3e 3c 61 6f 61 63 3e 30 3c 2f 61 6f 61 63 3e 3c 64 65 76 69 63 65 54 79 70 65 3e 31 3c 2f 64 65 76 69 63 65 54 79 70 65 3e 3c 64 65 76 69 63 65 4e 61 6d 65 3e 56 4d 77 61 72 65 37 2c 31 3c 2f 64 65 76 69 63 65 4e 61 6d 65 3e 3c 2f 61 67 65 6e 74 3e 3c 2f 63 6f 6e 6e 65 63 74 3e Data Ascii: <connect><ver>2</ver><agent><os>Windows</os><osVer>10.0.0.0.17134</osVer><proc>x64</proc><lcid>en-US</lcid><geold>244</geold><aoc>0</aoc><deviceType>1</deviceType><deviceName>VMware7,1</deviceName></agent></connect>
2022-04-08 08:02:27 UTC	31	OUT	Data Raw: 41 54 48 20 32 20 43 4f 4e 5c 44 45 56 49 43 45 20 31 30 31 34 0d 0a 43 6f 6e 74 65 78 74 3a 20 38 37 30 62 37 62 34 30 33 30 65 35 35 36 65 34 0d 0a 0d 0a 3c 64 65 76 69 63 65 3e 3c 63 6f 6d 70 61 63 74 2d 74 69 63 6b 65 74 3e 74 3d 45 77 43 6f 41 75 70 49 42 41 41 55 31 62 44 47 66 64 61 7a 69 44 66 58 70 6a 4e 35 4e 36 63 59 68 54 31 77 62 6d 51 41 41 51 77 65 75 52 78 64 54 45 52 58 49 34 58 73 61 55 64 61 66 67 57 47 68 6d 46 42 32 63 6a 51 30 2b 6c 52 4d 56 52 66 4d 58 33 46 77 79 4e 35 6e 68 5a 42 49 69 50 59 61 52 4e 51 2f 64 77 71 38 33 2f 58 59 37 5a 42 55 72 6d 54 65 77 44 66 6a 2f 57 6d 4f 6e 51 35 6b 4e 32 56 76 44 35 75 46 4d 37 47 6a 4c 78 56 73 37 55 78 36 70 69 69 71 41 6d 6c 4d 6d 4e 7a 57 34 6d 36 7a 78 2f 52 66 32 38 74 48 6b 4a 46 73 Data Ascii: ATH 2 CON\DEVICE 1014Context: 870b7b4030e556e4<device><compact-ticket>t=EwCoAup\BAAU1bDGfdaziDfXpjN5N6cYhT1wbmQAAQweuRxdTERXI4XsaUdafgWGHmFB2cjQ0+IRMVrFMX3FwyN5nhZBlIPYaRNQ\dwq83/XY7ZBUrmTewDfj/WmOnQ5kN2vVD5uFM7GjLxVs7Ux6piiqAmlMmNzW4m6zx\RF28thkJFs
2022-04-08 08:02:27 UTC	32	OUT	Data Raw: 42 4e 44 20 33 20 43 4f 4e 5c 51 4f 53 20 32 39 0d 0a 43 6f 6e 74 65 78 74 3a 20 38 37 30 62 37 62 34 30 33 30 65 35 35 36 65 34 0d 0a 0d 0a Data Ascii: BND 3 CON\QOS 29Context: 870b7b4030e556e4
2022-04-08 08:02:27 UTC	32	IN	Data Raw: 32 30 32 20 31 20 43 4f 4e 20 35 38 0d 0a Data Ascii: 202 1 CON 58
2022-04-08 08:02:27 UTC	32	IN	Data Raw: 4d 53 2d 43 56 3a 20 72 4c 56 74 36 68 68 66 66 30 57 70 71 4e 43 70 56 6b 34 68 74 51 2e 30 0d 0a 0d 0a 50 61 79 6c 6f 61 64 20 70 61 72 73 69 6e 67 20 66 61 69 6c 65 64 2e Data Ascii: MS-CV: rLVt6hhf0WpqNCpVvk4htQ.0Payload parsing failed.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.3	50039	20.54.89.106	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:33 UTC	8792	OUT	GET /SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%7D/x64/10.0.17134.1/0?CH=17&L=en-US&P=&PT=0x30&WUA=10.0.17134.1&MK=4MtpozR6MODPIGb&MD=EefvrDUR HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Windows-Update-Agent/10.0.10011.16384 Client-Protocol/1.81 Host: sls.update.microsoft.com
2022-04-08 08:03:34 UTC	8792	IN	HTTP/1.1 200 OK Cache-Control: no-cache Pragma: no-cache Content-Type: application/octet-stream Expires: -1 Last-Modified: Mon, 01 Jan 0001 00:00:00 GMT ETag: "wy8fVV3cy06QlZhZUaOlBEoVMBnt4x8NjH3c50VWOxM=_1440" MS-CorrelationId: cbc61937-96fe-4744-b40e-de157ba7038b MS-RequestId: 3c9c07ae-5521-439a-8893-318597c8a1f6 MS-CV: Zlzn9UWA+ESHZ4XX.0 X-Microsoft-SLSCClientCache: 1440 Content-Disposition: attachment; filename=environment.cab X-Content-Type-Options: nosniff Date: Fri, 08 Apr 2022 08:03:33 GMT Connection: close Content-Length: 30958
2022-04-08 08:03:34 UTC	8793	IN	Data Raw: 00 14 00 00 00 00 10 00 be 37 00 00 30 41 00 00 00 00 00 00 00 00 00 03 01 01 00 01 00 04 00 20 e0 00 00 00 00 00 00 00 80 00 65 6e 76 69 72 6f 6e 6d 65 6e 74 2e 63 61 62 00 27 c3 6c fd 52 37 f3 5b 43 4b ed 7a 05 58 55 dd d6 ee de 9b ee 96 6e 11 e9 b5 e9 52 69 a5 a4 bb 5b a4 bb 6b d3 ad a2 74 77 08 08 08 d2 21 25 dd a0 80 80 48 4a 4a 83 c4 dd e8 17 9e ef d4 7f fe 7b cf 73 fe 7b ef b7 9f 67 ef bd e6 5c 73 ce 35 63 8c f1 8e 77 8c 25 af 22 2e 05 82 7f da c9 40 df 3f 12 3f fe 40 08 60 30 08 0c 42 04 bd f8 08 02 11 7e af c1 fd de 06 10 05 fd f6 31 85 7f af 5b 85 72 83 7e fa f8 83 cc 6c 5d 2d 1d ed 6c 6d cc 6c 9d d9 dd 6d ac 41 f8 7a 2e Data Ascii: MSCF7D 70Ad[environment.cab\IR7[CKzXUnRi[ktw!%HJJ[s{g5scw%".@@?@ '0B~1[r-]lmlmAz.
2022-04-08 08:03:34 UTC	8808	IN	Data Raw: b3 49 a2 0d ff f6 07 56 2e e0 cd 9b 1f 2c 88 a2 01 ec 5e 7b 96 ac 79 f1 dc 76 c5 85 50 e5 c7 c8 45 07 64 59 b3 b7 80 da 46 59 e2 3c b1 95 cb ed 18 a0 46 1e 05 b6 ad 0f aa c7 d6 26 8a 7a 17 6e 85 5c 5c 6e b7 9b 98 29 fc 15 9c b1 63 23 9c 27 9a ba 82 04 21 f1 ec 76 cf 7a 3c 9a dc 26 02 a4 4b 13 b7 f5 66 dc 71 d6 12 42 66 da ba 5c 82 4f 0a 63 8b 27 ed ac 5b 4a 30 41 b8 22 8b 2f b7 4c 07 eb 6d 35 30 dd 9f 04 c2 94 77 e9 20 77 b3 ca 0d 58 a9 21 17 bb 64 c6 3c 80 fd e9 00 b3 78 2d 96 fe 20 b6 4c c6 4a 0b e6 fc 7a 35 83 21 a9 5b fb 9f ec fd f1 bd a9 3a 79 0e 3d a3 0c 9a 4f 59 1e be de 85 65 6f ea 2b b7 1c 1f d9 51 fd 01 a2 7c 91 b5 30 82 07 05 30 82 04 ed a0 03 02 01 02 02 13 33 00 00 00 59 e3 94 e0 54 c7 17 5d 00 00 00 00 00 08 30 0d 06 09 2a 86 48 86 f7 0d Data Ascii: IV.,^{yVPedYFY<F&zn\\n)c#^!vz<&KfqBfOc'[J0A"/Lm50w wXld<x- Ljz5[:y=OYeo+Q 003YT 0"H

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.3	50040	20.54.110.249	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:34 UTC	8823	OUT	GET /v7.0/products/lookup?alternateId=PackageFamilyName&value=Disney.37853FC22B2CE_6rarf9sa4v8jt&market=US&languages=en-US%2Cen%2Cneutral&fieldsTemplate=InstallAgent&mold=Public&oemId=Public&scmId=Public HTTP/1.1 Connection: Keep-Alive Content-Type: application/json User-Agent: Install Service MS-CV: RETjtPaEwECyiDEt.0.2.4 Host: displaycatalog.mp.microsoft.com
2022-04-08 08:03:34 UTC	8823	IN	HTTP/1.1 200 OK Connection: close Date: Fri, 08 Apr 2022 08:03:33 GMT Content-Type: application/json; charset=utf-8 Server: Kestrel Transfer-Encoding: chunked Vary: Authorization MS-CorrelationId: 8a3250f2-6033-446a-bfbb-807ad1f7b2a8 MS-RequestId: 55cb43bc-6837-42c6-baa4-ea215988a21a MS-CV: RETjtPaEwECyiDEt.0.2.4.422987627.0.1.422987627.4070804641.0 X-Content-Type-Options: nosniff MS-ServerId: 65db49-pn5ph Region: neu Node: aks-systempool-37630073-vmss000003 MS-DocumentsVersions: 9NXQXXLFST89 1942
2022-04-08 08:03:34 UTC	8824	IN	Data Raw: 66 62 36 30 0d 0a 7b 22 42 69 67 49 64 73 22 3a 5b 22 39 4e 58 51 58 58 4c 46 53 54 38 39 22 5d 2c 22 48 61 73 4d 6f 72 65 50 61 67 65 73 22 3a 66 61 6c 73 65 2c 22 50 72 6f 64 75 63 74 73 22 3a 5b 7b 22 4c 61 73 74 4d 6f 64 69 66 69 65 64 44 61 74 65 22 3a 22 32 30 32 32 2d 30 34 2d 30 36 54 31 35 3a 35 34 3a 32 39 2e 30 35 30 39 36 39 38 5a 22 2c 22 4c 6f 63 61 6c 69 7a 65 64 50 72 6f 70 65 72 74 69 65 73 22 3a 5b 7b 22 46 72 61 6e 63 68 69 73 65 73 22 3a 5b 5d 2c 22 49 6d 61 67 65 73 22 3a 5b 7b 22 46 69 6c 65 49 64 22 3a 22 33 30 35 36 36 31 37 39 32 30 30 39 34 30 39 39 31 39 30 22 2c 22 45 49 53 4c 69 73 74 69 6e 67 49 64 65 6e 74 69 66 69 65 72 22 3a 6e 75 6c 6c 2c 22 42 61 63 6b 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 74 72 61 6e 73 70 61 72 65 Data Ascii: fb60["BigIds":["9NXQXXLFST89"],"HasMorePages":false,"Products":{"LastModifiedDate":"2022-04-06T15:54:29.0509698Z","LocalizedProperties":{"Franchises":[],"Images":{"FileId":"3056617920094099190","EISListingIdentifier":"","null","BackgroundColor":"transpare
2022-04-08 08:03:34 UTC	8827	IN	Data Raw: 2e 36 35 30 30 34 2e 31 34 34 39 35 33 31 31 38 34 37 31 32 34 31 37 30 2e 65 38 39 61 34 64 63 65 2d 66 64 39 61 2d 34 61 31 30 2d 62 38 65 34 2d 61 36 63 33 61 61 31 63 30 35 35 65 2e 31 33 35 32 66 66 62 62 2d 36 65 36 61 2d 34 30 38 37 2d 38 39 34 32 2d 36 33 66 31 39 35 62 33 34 32 38 66 22 2c 22 57 69 64 74 68 22 3a 36 36 7d 2c 7b 22 46 69 6c 65 49 64 22 3a 22 33 30 33 34 39 33 32 35 33 31 31 33 39 32 38 38 37 33 33 22 2c 22 45 49 53 4c 69 73 74 69 6e 67 49 64 65 6e 74 69 66 69 65 72 22 3a 6e 75 6c 6c 2c 22 42 61 63 6b 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 74 72 61 6e 73 70 61 72 65 6e 74 22 2c 22 43 61 70 74 69 6f 6e 22 3a 22 22 2c 22 46 69 6c 65 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 36 30 32 34 2c 22 46 6f 72 65 67 72 6f 75 6e 64 43 6f 6c 6f Data Ascii: .65004.14495311847124170.e89a4dce-fd9a-4a10-b8e4-a6c3aa1c055e.1352ffb6-6e6a-4087-8942-63f195b3428f","Width":66},{"FileId":"3034932531139288733","EISListingIdentifier":null,"BackgroundColor":"transparent","Caption":"","FileSizeInBytes":6024,"ForegroundColo
2022-04-08 08:03:34 UTC	8831	IN	Data Raw: 37 34 39 37 36 35 34 31 30 32 34 34 36 31 22 2c 22 45 49 53 4c 69 73 74 69 6e 67 49 64 65 6e 74 69 66 69 65 72 22 3a 6e 75 6c 6c 2c 22 42 61 63 6b 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 74 72 61 6e 73 70 61 72 65 6e 74 22 2c 22 43 61 70 74 69 6f 6e 22 3a 22 22 2c 22 46 69 6c 65 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 37 39 35 34 31 2c 22 46 6f 72 65 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 22 2c 22 48 65 69 67 68 74 22 3a 33 30 30 2c 22 49 6d 61 67 65 50 6f 73 69 74 69 6f 6e 49 6e 66 6f 22 3a 22 22 2c 22 49 6d 61 67 65 50 75 72 70 6f 73 65 22 3a 22 54 69 6c 65 22 2c 22 55 6e 73 63 61 6c 65 64 49 6d 61 67 65 53 48 41 32 35 36 48 61 73 68 22 3a 22 33 38 30 6c 77 36 43 53 43 31 58 33 69 45 42 72 4c 4e 75 71 66 68 35 2b 4c 63 41 43 74 2f 70 37 46 72 42 52 Data Ascii: 74976541024461","EISListingIdentifier":null,"BackgroundColor":"transparent","Caption":"","FileSizeInBytes":79541,"ForegroundColor":"","Height":300,"ImagePositionInfo":"","ImagePurpose":"Tile","UnscaledImageSHA256Hash":"380lw6CSC1X3iEBRlNuqfh5+LcACUp7FrBR
2022-04-08 08:03:34 UTC	8835	IN	Data Raw: 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 74 72 61 6e 73 70 61 72 65 6e 74 22 2c 22 43 61 70 74 69 6f 6e 22 3a 22 22 2c 22 46 69 6c 65 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 31 39 30 33 35 39 35 2c 22 46 6f 72 65 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 22 2c 22 48 65 69 67 68 74 22 3a 31 30 38 30 2c 22 49 6d 61 67 65 50 6f 73 69 74 69 6f 6e 49 6e 66 6f 22 3a 22 44 65 73 6b 74 6f 70 2f 35 22 2c 22 49 6d 61 67 65 50 75 72 70 6f 73 65 22 3a 22 53 63 72 65 65 6e 73 68 6f 74 22 2c 22 55 6e 73 63 61 6c 65 64 49 6d 61 67 65 53 48 41 32 35 36 48 61 73 68 22 3a 22 54 4d 70 39 37 77 6b 63 53 51 6c 45 33 43 78 68 34 71 73 4c 61 42 46 62 62 42 4b 4e 48 41 32 48 39 36 4e 6f 6a 4b 6a 2f 30 7a 34 3d 22 2c 22 5 5 72 69 22 3a 22 2f 2f 73 74 6f 72 65 2d 69 6d 61 67 65 73 2e 73 Data Ascii: oundColor":"transparent","Caption":"","FileSizeInBytes":1903595,"ForegroundColor":"","Height":1080,"ImagePositionInfo":"Desktop/5","ImagePurpose":"Screenshot","UnscaledImageSHA256Hash":"TmP97wkcSQIE3Cxb4qslLaBFbbBKNHA2H96NjKj/Oz4=", "Uri":"//store-images.s
2022-04-08 08:03:34 UTC	8839	IN	Data Raw: 2c 22 45 49 53 4c 69 73 74 69 6e 67 49 64 65 6e 74 69 66 69 65 72 22 3a 6e 75 6c 6c 2c 22 42 61 63 6b 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 74 72 61 6e 73 70 61 72 65 6e 74 22 2c 22 43 61 70 74 69 6f 6e 22 3a 22 22 2c 22 46 69 6c 65 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 33 30 35 37 31 39 35 2c 22 46 6f 72 65 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 22 2c 22 48 65 69 67 68 74 22 3a 32 31 36 30 2c 22 49 6d 61 67 65 50 6f 73 69 74 69 6f 6e 49 6e 66 6f 22 3a 22 58 62 6f 78 2f 36 22 2c 22 49 6d 61 67 65 50 75 72 70 6f 73 65 22 3a 22 53 63 72 65 65 6e 73 68 6f 74 22 2c 22 55 6e 73 63 61 6c 65 64 49 6d 61 67 65 53 48 41 32 35 36 48 61 73 68 22 3a 22 4e 32 77 69 45 4a 51 4c 61 71 73 69 53 55 45 43 42 54 54 50 46 35 79 70 57 69 43 32 41 33 45 6f 77 2b 43 41 Data Ascii: ,"EISListingIdentifier":null,"BackgroundColor":"transparent","Caption":"","FileSizeInBytes":3057195,"Foregro undColor":"","Height":2160,"ImagePositionInfo":"Xbox/6","ImagePurpose":"Screenshot","UnscaledImageSHA256Hash":"N2wiEJQLaqsiSUECBTTPF5ypWiC2A3Eow+CA

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:34 UTC	8843	IN	Data Raw: 49 22 2c 22 41 51 22 2c 22 41 47 22 2c 22 41 4d 22 2c 22 41 57 22 2c 22 42 4f 22 2c 22 42 51 22 2c 22 42 41 22 2c 22 42 57 22 2c 22 42 56 22 2c 22 49 4f 22 2c 22 42 4e 22 2c 22 42 46 22 2c 22 42 49 22 2c 22 4b 48 22 2c 22 43 4d 22 2c 22 43 56 22 2c 22 4b 59 22 2c 22 43 46 22 2c 22 54 44 22 2c 22 54 4c 22 2c 22 44 4a 22 2c 22 44 4d 22 2c 22 44 4f 22 2c 22 45 43 22 2c 22 53 56 22 2c 22 47 51 22 2c 22 45 52 22 2c 22 45 54 22 2c 22 46 4b 22 2c 22 46 4f 22 2c 22 46 4a 22 2c 22 47 46 22 2c 22 50 46 22 2c 22 54 46 22 2c 22 47 41 22 2c 22 47 4d 22 2c 22 47 45 22 2c 22 47 48 22 2c 2 2 47 49 22 2c 22 47 4c 22 2c 22 47 44 22 2c 22 47 50 22 2c 22 47 55 22 2c 22 47 47 22 2c 22 47 4e 22 2c 22 47 57 22 2c 22 47 59 22 2c 22 48 54 22 2c 22 48 4d 22 2c 22 48 4e 22 2c 22 41 Data Ascii: I","AQ","AG","AM","AW","BO","BQ","BA","BW","BV","IO","BN","BF","BI","KH","CM","CV","KY","CF","TD","TL","DJ","DM","DO","EC","SV","GQ","ER","ET","FK","FO","FJ","GF","PF","TF","GA","GM","GE","GH","GI","GL","GD","GP","GU","GG","GN","GW","GY","HT","HM","HN","A
2022-04-08 08:03:34 UTC	8847	IN	Data Raw: 48 22 2c 22 42 44 22 2c 22 42 45 22 2c 22 42 52 22 2c 22 42 47 22 2c 22 43 41 22 2c 22 43 4c 22 2c 22 43 4e 22 2c 22 43 4f 22 2c 22 43 52 22 2c 22 48 52 22 2c 22 43 59 22 2c 22 43 5a 22 2c 22 44 4b 22 2c 22 45 47 22 2c 22 45 45 22 2c 22 46 49 22 2c 22 46 52 22 2c 22 44 45 22 2c 22 47 52 22 2c 22 47 54 22 2c 22 48 4b 22 2c 22 48 55 22 2c 22 49 53 22 2c 22 49 4e 22 2c 22 49 44 22 2c 22 49 51 22 2c 22 49 45 22 2c 22 49 4c 22 2c 22 49 54 22 2c 22 4a 50 22 2c 2 2 4a 4f 22 2c 22 4b 5a 22 2c 22 4b 45 22 2c 22 4b 57 22 2c 22 4c 56 22 2c 22 4c 42 22 2c 22 4c 49 22 2c 22 4c 54 22 2c 22 4c 55 22 2c 22 4d 59 22 2c 22 4d 54 22 2c 22 4d 52 22 2c 22 4d 58 22 2c 22 4d 41 22 2c 22 4e 4c 22 2c 22 4e 5a 22 2c 22 4e 47 22 2c 22 4e 4f 22 2c 22 4f 4d 22 2c 22 50 4b 22 2c 22 50 Data Ascii: H","BD","BE","BR","BG","CA","CL","CN","CO","CR","HR","CY","CZ","DK","EG","EE","FI","FR","DE","GR","GT","HK","HU","IS","IN","ID","IQ","IE","IL","IT","JP","JO","KZ","KE","KW","LV","LB","LI","LT","LU","MY","MT","MR","MX","MA","NL","NZ","NG","NO","OM","PK","P
2022-04-08 08:03:34 UTC	8851	IN	Data Raw: 37 32 33 32 33 32 2d 37 62 36 30 2d 34 66 37 32 2d 39 39 32 35 2d 39 30 32 66 37 35 36 61 38 33 62 32 5c 22 2c 5c 22 63 6f 6e 74 65 6e 74 2e 74 61 72 67 65 74 50 6c 61 74 66 6f 72 6d 73 5c 22 3a 5b 7b 5c 22 70 6c 61 74 66 6f 72 6d 2e 6d 61 78 56 65 72 73 69 6f 6e 54 65 73 74 65 64 5c 22 3a 32 38 31 34 37 35 31 30 31 34 39 37 37 35 33 36 2c 5c 22 70 6c 61 74 66 6f 72 6d 2e 6d 69 6e 56 65 72 73 69 6f 6e 5c 22 3a 32 38 31 34 37 35 31 30 31 34 39 37 37 35 33 3 6 2c 5c 22 70 6c 61 74 66 6f 72 6d 2e 74 61 72 67 65 74 5c 22 3a 35 7d 2c 7b 5c 22 30 6c 61 74 66 6f 72 6d 2e 6d 61 78 56 65 72 73 69 6f 6e 54 65 73 74 65 64 5c 22 3a 32 38 31 34 37 35 31 30 31 34 39 37 37 35 33 36 2c 5c 22 70 6c 61 74 66 6f 72 6d 2e 6d 69 6e 56 65 72 73 69 6f 6e 5c 22 3a 32 38 31 34 37 Data Ascii: 723232-7b60-4f72-9925-902f756a83b2\","content.targetPlatforms":[{"platform.maxVersionTested":2814751014977536,"platform.minVersion":2814751014977536,"platform.target":5},{"platform.maxVersionTested":2814751014977536,"platform.minVersion":28147
2022-04-08 08:03:34 UTC	8855	IN	Data Raw: 73 65 7d 2c 5c 22 70 6f 6c 69 63 79 32 5c 22 3a 7b 5c 22 61 67 65 52 61 74 69 6e 67 5c 22 3a 33 2c 5c 22 6f 70 74 4f 75 74 2e 44 56 52 5c 22 3a 74 72 75 65 2c 5c 22 74 68 69 72 64 50 61 72 74 79 41 70 70 52 61 74 69 6e 67 73 5c 22 3a 5b 7b 5c 22 6c 65 76 65 6c 5c 22 3a 39 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 35 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 32 39 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 32 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 32 39 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 39 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 37 38 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 36 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 37 32 2c 5c 22 73 79 73 74 65 6d 49 64 5c Data Ascii: se},"policy2":{"ageRating":3,"optOut.DVR":true,"thirdPartyAppRatings":[{"level":9,"systemId":3},{"level":81,"systemId":5},{"level":51,"systemId":12},{"level":29,"systemId":9},{"level":78,"systemId":16},{"level":72,"systemId}
2022-04-08 08:03:34 UTC	8859	IN	Data Raw: 49 64 22 3a 22 32 32 65 30 63 65 37 66 2d 34 32 37 61 2d 34 30 66 61 2d 62 66 61 36 2d 30 64 65 37 62 38 35 35 34 38 34 30 22 2c 22 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 22 3a 22 44 69 73 6e 65 79 2e 33 37 38 35 33 46 43 32 32 42 32 43 45 5f 36 72 61 72 66 39 73 61 34 76 38 6a 74 22 2c 22 53 6b 75 49 64 22 3a 22 30 30 31 30 22 2c 22 43 6f 6e 74 65 6e 74 22 3a 6e 75 6c 6c 2c 22 50 61 63 6b 61 67 65 46 65 61 74 75 72 65 73 22 3a 6e 75 6c 6c 7d 7d 2c 7b 22 41 70 70 6c 69 63 61 74 69 6f 6e 73 22 3a 5b 7b 22 41 70 70 6c 69 63 61 74 69 6f 6e 49 64 22 3a 22 41 70 70 22 7d 5d 2c 22 41 72 63 68 69 74 65 63 74 75 72 65 73 22 3a 5b 22 78 36 34 22 5d 2c 22 43 61 70 61 62 69 6c 69 74 69 65 73 22 3a 5b 22 69 6e 74 65 72 6e 65 74 43 6c 69 65 6e 74 22 2c 22 Data Ascii: Id":"22e0ce7f-427a-40fa-bfa6-0de7b8554840","PackageFamilyName":"Disney.37853FC22B2CE_6rarf9sa4v8jt","Skuld":"0010","Content":null,"PackageFeatures":null},"Applications":[{"ApplicationId":"App"}],"Architectures":["x64"],"Capabilities":["internetClient",
2022-04-08 08:03:34 UTC	8863	IN	Data Raw: 42 53 63 68 65 6d 61 22 3a 22 41 76 61 69 6c 61 62 69 6c 69 74 79 55 6e 69 66 69 65 64 41 70 70 3b 33 22 2c 22 41 76 61 69 6c 61 62 69 6c 69 74 79 49 64 22 3a 22 42 31 38 4c 48 58 38 34 50 34 52 39 22 2c 22 43 6f 6e 64 69 74 69 6f 6e 73 22 3a 7b 22 43 6c 69 65 6e 74 43 6f 6e 64 69 74 69 6f 6e 73 22 3a 7b 22 41 6c 6c 6f 77 65 64 50 6c 61 74 66 6f 72 6d 73 22 3a 5b 7b 22 4d 61 78 56 65 72 73 69 6f 6e 22 3a 32 31 34 37 34 38 33 36 34 37 2c 22 4d 69 6e 65 65 7 2 73 69 6f 6e 22 3a 30 2c 22 50 6c 61 74 66 6f 72 6d 4e 61 6d 65 22 3a 22 57 69 6e 64 6f 77 73 2e 44 65 73 6b 74 6f 70 2 2 7d 2c 7b 22 4d 61 78 56 65 72 73 69 6f 6e 22 3a 32 31 34 37 34 38 33 36 34 37 2c 22 4d 69 6e 56 65 72 73 69 6f 6e 22 3a 30 2c 22 50 6c 61 74 66 6f 72 6d 4e 61 6d 65 22 3a 22 57 69 6e Data Ascii: BSchema":"AvailabilityUnifiedApp;3","AvailabilityId":"B18LHX84P4R9","Conditions":["ClientConditions":["AllowedPlatforms":[{"MaxVersion":2147483647,"MinVersion":0,"PlatformName":"Windows.Desktop"}],"MaxVersion":2147483647,"MinVersion":0,"PlatformName":"Win
2022-04-08 08:03:34 UTC	8867	IN	Data Raw: 65 20 70 72 6f 6d 70 74 65 64 20 74 6f 20 75 70 64 61 74 65 20 74 68 65 69 72 20 50 61 72 65 6e 74 61 6c 20 43 6f 6e 74 72 6f 6c 73 2e 20 54 68 69 73 20 69 6e 63 6c 75 64 65 73 20 74 68 65 20 6f 70 74 69 6f 6e 20 74 6f 20 73 65 6c 65 63 74 20 63 6f 6e 74 65 6e 74 20 72 61 74 69 6e 67 73 20 72 65 73 74 72 69 63 74 69 6f 6e 73 20 66 6f 72 20 65 61 63 68 20 70 72 6f 66 69 6c 65 20 61 73 20 77 65 6c 6c 20 61 73 20 74 6f 20 61 64 64 20 61 20 50 49 4e 20 74 6f 20 6c 6f 63 6b 20 70 72 6f 66 69 6c 65 73 2e 20 54 68 6f 73 65 20 74 68 61 74 20 63 68 6f 6f 73 65 20 74 6f 20 6b 65 65 70 20 74 68 65 69 72 20 73 65 74 74 69 6e 67 73 20 74 68 65 20 73 61 6d 65 20 77 69 6c 6c 20 63 6f 6e 74 69 6e 75 65 20 74 6f 20 65 6e 6a 6f 79 20 44 69 73 6e 65 79 2b 20 61 73 20 74 68 Data Ascii: e prompted to update their Parental Controls. This includes the option to select content ratings restrictions for each profile as well as to add a PIN to lock profiles. Those that choose to keep their settings the same will continue to enjoy Disney+ as th
2022-04-08 08:03:34 UTC	8871	IN	Data Raw: 3a 5b 7b 5c 22 70 6c 61 74 66 6f 72 6d 2e 6d 61 78 56 65 72 73 69 6f 6e 54 65 73 74 65 64 5c 22 3a 32 38 31 34 37 35 31 30 31 34 39 37 37 35 33 36 2c 5c 22 70 6c 61 74 66 6f 72 6d 2e 6d 69 6e 56 65 72 73 69 6f 6e 5c 22 3a 32 38 31 34 37 35 31 30 31 34 39 37 37 35 33 36 2c 5c 22 70 6c 61 74 66 6f 72 6d 2e 74 61 72 67 65 74 5c 22 3a 35 7d 5d 2c 5c 22 63 6f 6e 74 65 6e 74 2e 74 79 70 65 5c 22 3a 37 2c 5c 22 70 6f 6c 69 63 79 5c 22 3a 7b 5c 22 63 61 74 65 67 6f 72 79 2e 66 69 72 73 74 5c 22 3a 5c 22 61 70 70 5c 22 2c 5c 22 63 61 74 65 67 6f 72 79 2e 73 65 63 6f 6e 64 5c 22 3a 5 c 22 45 6e 74 65 72 74 61 69 6e 6d 65 6e 74 5c 22 2c 5c 22 6f 70 74 4f 75 74 2e 62 61 63 6b 75 70 52 65 73 74 6f 72 65 5c 22 3a 66 61 6c 73 65 2c 5c 22 6f 70 74 4f 75 74 2e 72 65 6d 6f Data Ascii: [{"platform.maxVersionTested":2814751014977536,"platform.minVersion":2814751014977536,"platform.target":5}],"content.type":7,"policy":{"category.first":"app","category.second":"Entertainment"},"optOut.backupRestore":false,"optOut.remo

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:34 UTC	8875	IN	Data Raw: 74 4f 75 74 2e 72 65 6d 6f 76 65 61 62 6c 65 4d 65 64 69 61 5c 22 3a 66 61 6c 73 65 7d 2c 5c 22 70 6f 6c 69 63 79 32 5c 22 3a 7b 5c 22 61 67 65 52 61 74 69 6e 67 5c 22 3a 33 2c 5c 22 6f 70 74 4f 75 74 2e 44 56 52 5c 22 3a 74 72 75 65 2c 5c 22 74 68 69 72 64 50 61 72 74 79 41 70 70 52 61 74 69 6e 67 73 5c 22 3a 5b 7b 5c 22 6c 65 76 65 6c 5c 22 3a 39 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 33 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 38 31 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 35 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 35 31 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 32 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 32 39 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 39 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 37 38 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 36 7d Data Ascii: tOut.removeableMedia":false},{"policy2":{"ageRating":3,"optOut.DVR":true,"thirdPartyAppRatings":{"level":9,"systemId":3},{"level":81,"systemId":5},{"level":51,"systemId":12},{"level":29,"systemId":9},{"level":78,"systemId":16}
2022-04-08 08:03:34 UTC	8879	IN	Data Raw: 61 30 37 30 36 22 2c 22 57 75 43 61 74 65 67 6f 72 79 49 64 22 3a 22 32 32 65 30 63 65 37 66 2d 34 32 37 61 2d 34 30 66 61 2d 62 66 61 36 2d 30 64 65 37 62 38 35 35 34 38 34 30 22 2c 22 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 22 3a 22 44 69 73 6e 65 79 2e 33 37 38 35 33 46 43 32 32 42 32 43 45 5f 36 72 61 72 66 39 73 61 34 76 38 6a 74 22 2c 22 53 6b 75 49 64 22 3a 22 30 30 31 31 22 2c 22 43 6f 6e 74 65 6e 74 22 3a 6e 75 6c 6c 2c 22 50 61 63 6b 61 67 65 46 65 61 74 75 72 65 73 22 3a 6e 75 6c 6c 7d 7d 2c 7b 22 41 70 70 6c 69 63 61 74 69 6f 6e 73 22 3a 5b 7b 22 41 70 70 6c 69 63 61 74 69 6f 6e 49 64 22 3a 22 41 70 70 22 7d 5d 2c 22 41 72 63 68 69 74 65 63 74 75 72 65 73 22 3a 5b 22 61 72 6d 36 34 22 5d 2c 22 43 61 70 61 62 69 6c 69 74 69 65 73 22 Data Ascii: a0706","WuCategoryId":"22e0ce7f-427a-40fa-bfa6-0de7b8554840","PackageFamilyName":"Disney.37853FC22B2CE_6rarf9sa4v8jt","Skuld":"0011","Content":null,"PackageFeatures":null},{Applications":[{"ApplicationId":"App"}],"Architectures":["arm64"],"Capabilities"
2022-04-08 08:03:34 UTC	8883	IN	Data Raw: 69 6c 79 4e 61 6d 65 22 3a 22 44 69 73 6e 65 79 2e 33 37 38 35 33 46 43 32 32 42 32 43 45 5f 36 72 61 72 66 39 73 61 34 76 38 6a 74 22 2c 22 4d 61 69 6e 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 46 6f 72 44 6c 63 22 3a 6e 75 6c 6c 2c 22 50 61 63 6b 61 67 65 46 75 6c 6c 4e 61 6d 65 22 3a 22 44 69 73 6e 65 79 2e 33 37 38 35 33 46 43 32 32 42 32 43 45 5f 31 2e 32 36 2e 32 2e 37 30 5f 78 36 34 5f 5f 36 72 61 72 66 39 73 61 34 76 38 6a 74 22 2c 22 50 61 63 6b 61 67 65 49 64 22 3a 22 65 66 64 39 61 31 35 38 2d 33 34 32 38 2d 31 35 64 66 2d 33 30 66 37 2d 63 30 66 38 61 39 38 66 65 38 35 65 2d 58 36 34 22 2c 22 50 61 63 6b 61 67 65 52 61 6e 6b 22 3a 33 30 30 31 32 2c 22 50 6c 61 74 66 6f 72 6d 44 65 70 65 6e 64 65 6e 63 69 65 73 22 3a 5b 7b 22 4d 61 78 Data Ascii: ilyName":"Disney.37853FC22B2CE_6rarf9sa4v8jt","MainPackageFamilyNameForDlc":null,"PackageFullName":"Disney.37853FC22B2CE_1.26.2.70_x64_6rarf9sa4v8jt","PackageId":"ef9a158-3428-15df-30f7-c0f8a98fe85e-X64","PackageRank":30012,"PlatformDependencies":{"Max
2022-04-08 08:03:34 UTC	8887	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.3	50041	20.199.120.85	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:34 UTC	8887	OUT	Data Raw: 43 4e 54 20 31 20 43 4f 4e 20 32 34 36 0d 0a 43 6f 6e 74 65 78 74 3a 20 37 63 31 34 36 33 61 37 38 30 62 37 64 32 66 61 0d 0a 0d 0a Data Ascii: CNT 1 CON 246Context: 7c1463a780b7d2fa
2022-04-08 08:03:34 UTC	8887	OUT	Data Raw: 3c 63 6f 6e 6e 65 63 74 3e 3c 76 65 72 3e 32 3c 2f 76 65 72 3e 3c 61 67 65 6e 74 3e 3c 6f 73 3e 57 69 6e 64 6f 77 73 3c 2f 6f 73 3e 3c 6f 73 56 65 72 3e 31 30 2e 30 2e 30 2e 31 37 31 33 34 3c 2f 6f 73 56 65 72 3e 3c 70 72 6f 63 3e 78 36 34 3c 2f 70 72 6f 63 3e 3c 6c 63 69 64 3e 65 6e 2d 55 53 3c 2f 6c 63 69 64 3e 3c 67 65 6f 49 64 3e 32 34 34 3c 2f 67 65 6f 49 64 3e 3c 61 6f 61 63 3e 30 3c 2f 61 6f 61 63 3e 3c 64 65 76 69 63 65 54 79 70 65 3e 31 3c 2f 64 65 76 69 63 65 54 79 70 65 3e 3c 64 65 76 69 63 65 4e 61 6d 65 3e 56 4d 77 61 72 65 37 2c 31 3c 2f 64 65 76 69 63 65 4e 61 6d 65 3e 3c 2f 61 67 65 6e 74 3e 3c 2f 63 6f 6e 6e 65 63 74 3e Data Ascii: <connect><ver>2</ver><agent><os>Windows</os><osVer>10.0.0.0.17134</osVer><proc>x64</proc><lcid>en-US</lcid><geoid>244</geoid><aoac>0</aoac><deviceType>1</deviceType><deviceName>VMware7,1</deviceName></agent></connect>
2022-04-08 08:03:34 UTC	8887	OUT	Data Raw: 41 54 48 20 32 20 43 4f 4e 5c 44 45 56 49 43 45 20 31 30 31 34 0d 0a 43 6f 6e 74 65 78 74 3a 20 37 63 31 34 36 33 61 37 38 30 62 37 64 32 66 61 0d 0a 0d 0a 0d 0a 3c 64 65 76 69 63 65 3e 3c 63 6f 6d 70 61 63 74 2d 74 69 63 6b 65 74 3e 74 3d 45 77 43 6f 41 75 70 49 42 41 41 55 31 62 44 47 66 64 61 7a 69 44 66 58 70 6a 4e 35 4e 36 63 59 68 54 31 77 62 6d 51 41 41 51 77 65 75 52 78 64 54 45 52 58 49 34 58 73 61 55 64 61 66 67 57 47 68 6d 46 42 32 63 6a 51 30 2b 6c 52 4d 56 52 66 4d 58 33 46 77 79 4e 35 6e 68 5a 42 49 69 50 59 61 52 4e 51 2f 64 77 71 38 33 2f 58 59 37 5a 42 55 72 6d 54 65 77 44 66 6a 2f 57 6d 4f 6e 51 35 6b 4e 32 56 76 44 35 75 46 4d 37 47 6a 4c 78 56 73 37 55 78 36 70 69 69 71 41 6d 6c 4d 6d 4e 7a 57 34 6d 36 7a 78 2f 52 66 32 38 74 48 6b 4a 46 73 Data Ascii: ATH 2 CON\DEVICE 1014Context: 7c1463a780b7d2fa<device><compact-ticket>t=EwCoAupIBAAU1bDGfdaziDfXpjN5N6cYHT1wbmQAAQweuRxdTERXl4XsaUdafgWGhmFB2cjQ0+IRMVrIMX3FwyN5nhZBliPYaRNQ/dwq83/XYZBUrlmTewDfj/WmOnQ5kN2VvD5uFM7GjLxVs7Ux6piiQAmIMmNzW4m6zx/Rf28tHkJFs
2022-04-08 08:03:34 UTC	8888	OUT	Data Raw: 42 4e 44 20 33 20 43 4f 4e 5c 51 4f 53 20 32 39 0d 0a 43 6f 6e 74 65 78 74 3a 20 37 63 31 34 36 33 61 37 38 30 62 37 64 32 66 61 0d 0a 0d 0a Data Ascii: BND 3 CON\QOS 29Context: 7c1463a780b7d2fa
2022-04-08 08:03:34 UTC	8888	IN	Data Raw: 32 30 32 20 31 20 43 4f 4e 20 35 38 0d 0a Data Ascii: 202 1 CON 58
2022-04-08 08:03:34 UTC	8888	IN	Data Raw: 4d 53 2d 43 56 3a 20 6b 73 71 4c 51 2b 71 4b 46 30 4f 30 33 4c 78 36 57 42 56 64 42 51 2e 30 0d 0a 0d 0a 50 61 79 6c 6f 61 64 20 70 61 72 73 69 6e 67 20 66 61 69 6c 65 64 2e Data Ascii: MS-CV: ksLQ+qKF003Lx6WBVdBQ.0Payload parsing failed.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.3	50042	52.152.110.14	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:35 UTC	8888	OUT	GET /SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%D/x64/10.0.17134.1/0?CH=17&L=en-US&P=&PT=0x30&WUA=10.0.17134.1&MK=4MtpozR6MODPIGb&MD=EefvrDUR HTTP/1.1 Connection: Keep-Alive Accept: /* User-Agent: Windows-Update-Agent/10.0.10011.16384 Client-Protocol/1.81 Host: sls.update.microsoft.com
2022-04-08 08:03:35 UTC	8888	IN	HTTP/1.1 200 OK Cache-Control: no-cache Pragma: no-cache Content-Type: application/octet-stream Expires: -1 Last-Modified: Mon, 01 Jan 0001 00:00:00 GMT ETag: "wy8fVV3cy06QlZhZUaOlBEoVMBnt4x8NjH3c50VWOxM= _1440" MS-CorrelationId: e54c863e-970c-448e-a66a-a78fd66cea92 MS-RequestId: b86f83a6-0ead-4f2e-ae45-b047fa4c7b3b MS-CV: rF01JHrdLUaPusa6.0 X-Microsoft-SLSCClientCache: 1440 Content-Disposition: attachment; filename=environment.cab X-Content-Type-Options: nosniff Date: Fri, 08 Apr 2022 08:03:34 GMT Connection: close Content-Length: 30958
2022-04-08 08:03:35 UTC	8889	IN	Data Raw: 4d 53 43 46 00 00 00 00 be 37 00 00 00 00 00 00 44 00 00 00 00 00 00 03 01 01 00 01 00 04 00 20 e0 00 00 14 00 00 00 00 00 10 00 be 37 00 00 30 41 00 00 00 00 00 00 00 00 00 64 00 00 00 01 00 01 00 f3 5b 00 00 00 00 00 00 00 00 00 00 80 00 65 6e 76 69 72 6f 6e 6d 65 6e 74 2e 63 61 62 00 27 c3 6c fd 52 37 f3 5b 43 4b ed 7a 05 58 55 dd d6 ee de 9b ee 96 6e 11 e9 b5 e9 52 69 a5 a4 bb 5b a4 bb 6b d3 ad a2 74 77 08 08 08 d2 21 25 dd a0 80 80 48 4a 4a 83 c4 dd e8 17 9e ef d4 7f fe 7b cf 73 fe 7b ef b7 9f 67 ef bd e6 5c 73 ce 35 63 8c f1 8e 77 8c 25 af 22 2e 05 82 7f da c9 40 df 3f 12 3f fe 40 08 60 30 08 0c 42 04 bd f8 08 02 11 7e af c1 fd de 06 10 05 fd f6 31 85 7f af 5b 85 72 83 7e fa f8 83 cc 6c 5d 2d 1d ed 6c 6d cc 6c 9d d9 dd 6d ac 41 f8 7a 2e Data Ascii: MSCF7D 70Ad[environment.cab'IR7[CKzXUnRi[ktw!%HJJ[s{gls5cw%".@??@ '0B~1[r-l]~lmlmAz.
2022-04-08 08:03:35 UTC	8904	IN	Data Raw: b3 49 a2 0d ff f6 07 56 2e e0 cd 9b 1f 2c 88 a2 01 ec 5e 7b 96 ac 79 f1 dc 76 c5 85 50 e5 c7 c8 45 07 64 59 b3 b7 80 da 46 59 e2 3c b1 95 cb ed 18 a0 46 1e 05 b6 ad 0f aa c7 d6 26 8a 7a 17 6e 85 5c 5c 6e b7 9b 98 29 fc 15 9c b1 63 23 9c 27 9a ba 82 04 21 f1 ec 76 cf 7a 3c 9a dc 26 02 a4 4b 13 b7 f5 66 dc 71 d6 12 42 66 da ba 5c 82 4f 0a 63 8b 27 ed ac 5b 4a 30 41 b8 22 8b 2f b7 4c 07 eb 6d 35 30 dd 9f 04 c2 94 77 e9 20 77 b3 ca 0d 58 a9 21 17 bb 64 c6 3c 80 fd e9 00 b3 78 2d 96 fe 20 b6 4c c6 4a 0b e6 fc 7a 35 83 21 a9 5b fb 9f ec fd f1 bd a9 3a 79 0e 3d a3 0c 9a 4f 59 1e be de 85 65 6f ea 2b b7 1c 1f d9 51 fd 01 a2 7c 91 b5 30 82 07 05 30 82 04 ed a0 03 02 01 02 02 13 33 00 00 00 08 59 e3 94 e0 54 c7 17 5d 00 00 00 00 00 08 30 0d 06 09 2a 86 48 86 f7 0d Data Ascii: IV.,^[yvPEdYFY<F&zn\\n)c#\\vz<&KfqBfOc[J0A"/Lm50w wX!d<x- LJz5I:[y=OYeo+Q[003YT]0*H

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
64	192.168.2.3	50043	40.125.122.176	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:35 UTC	8919	OUT	GET /SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%D/x64/10.0.17134.1/0?CH=17&L=en-US&P=&PT=0x30&WUA=10.0.17134.1&MK=4MtpozR6MODPIGb&MD=EefvrDUR HTTP/1.1 Connection: Keep-Alive Accept: /* User-Agent: Windows-Update-Agent/10.0.10011.16384 Client-Protocol/1.81 Host: sls.update.microsoft.com
2022-04-08 08:03:36 UTC	8920	IN	HTTP/1.1 200 OK Cache-Control: no-cache Pragma: no-cache Content-Type: application/octet-stream Expires: -1 Last-Modified: Mon, 01 Jan 0001 00:00:00 GMT ETag: "wy8fVV3cy06QlZhZUaOlBEoVMBnt4x8NjH3c50VWOxM= _1440" MS-CorrelationId: 0daa6949-6414-45d1-b395-2d8b1f3869d4 MS-RequestId: 4ed057c6-e554-44b3-b940-798b4a761336 MS-CV: 3kYZeqXyfka3rJbV.0 X-Microsoft-SLSCClientCache: 1440 Content-Disposition: attachment; filename=environment.cab X-Content-Type-Options: nosniff Date: Fri, 08 Apr 2022 08:03:35 GMT Connection: close Content-Length: 30958
2022-04-08 08:03:36 UTC	8920	IN	Data Raw: 4d 53 43 46 00 00 00 00 be 37 00 00 00 00 00 00 44 00 00 00 00 00 00 03 01 01 00 01 00 04 00 20 e0 00 00 14 00 00 00 00 00 10 00 be 37 00 00 30 41 00 00 00 00 00 00 00 00 00 64 00 00 00 01 00 01 00 f3 5b 00 00 00 00 00 00 00 00 00 00 80 00 65 6e 76 69 72 6f 6e 6d 65 6e 74 2e 63 61 62 00 27 c3 6c fd 52 37 f3 5b 43 4b ed 7a 05 58 55 dd d6 ee de 9b ee 96 6e 11 e9 b5 e9 52 69 a5 a4 bb 5b a4 bb 6b d3 ad a2 74 77 08 08 08 d2 21 25 dd a0 80 80 48 4a 4a 83 c4 dd e8 17 9e ef d4 7f fe 7b cf 73 fe 7b ef b7 9f 67 ef bd e6 5c 73 ce 35 63 8c f1 8e 77 8c 25 af 22 2e 05 82 7f da c9 40 df 3f 12 3f fe 40 08 60 30 08 0c 42 04 bd f8 08 02 11 7e af c1 fd de 06 10 05 fd f6 31 85 7f af 5b 85 72 83 7e fa f8 83 cc 6c 5d 2d 1d ed 6c 6d cc 6c 9d d9 dd 6d ac 41 f8 7a 2e Data Ascii: MSCF7D 70Ad[environment.cab'IR7[CKzXUnRi[ktw!%HJJ[s{gls5cw%".@??@ '0B~1[r-l]~lmlmAz.

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:36 UTC	8936	IN	Data Raw: b3 49 a2 0d ff f6 07 56 2e e0 cd 9b 1f 2c 88 a2 01 ec 5e 7b 96 ac 79 f1 dc 76 c5 85 50 e5 c7 c8 45 07 64 59 b3 b7 80 da 46 59 e2 3c b1 95 cb ed 18 a0 46 1e 05 b6 ad 0f aa c7 d6 26 8a 7a 17 6e 85 5c 5c 6e b7 9b 98 29 fc 15 9c b1 63 23 9c 27 9a ba 82 04 21 f1 ec 76 cf 7a 3c 9a dc 26 02 a4 4b 13 b7 f5 66 dc 71 d6 12 42 66 da ba 5c 82 4f 0a 63 8b 27 ed ac 5b 4a 30 41 b8 22 8b 2f b7 4c 07 eb 6d 35 30 dd 9f 04 c2 94 77 e9 20 77 b3 ca 0d 58 a9 21 17 bb 64 c6 3c 80 fd e9 00 b3 78 2d 96 fe 20 b6 4c c6 4a 0b e6 fc 7a 35 83 21 a9 5b fb 9f ec fd f1 bd a9 3a 79 0e 3d a3 0c 9a 4f 59 1e be de 85 65 6f ea 2b b7 1c 1f d9 51 fd 01 a2 7c 91 b5 30 82 07 05 30 82 04 ed a0 03 02 01 02 02 13 33 00 00 00 08 59 e3 94 e0 54 c7 17 5d 00 00 00 00 08 30 0d 06 09 2a 86 48 86 f7 0d Data Ascii: IV.,^{\yVPeDYFY<F&z\n\nc#\lvz<&KfqBfOc"[J0A"/Lm50w wXld<x- Ljz5l[:y=OYeo+Q[003YT]0*H

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
65	192.168.2.3	50044	20.54.110.249	443	C:\Users\user\l\Desktop\l.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:36 UTC	8950	OUT	GET /v7.0/products/lookup?alternateId=PackageFamilyName&value=BytedancePte.Ltd.TikTok_6ycncdn6064se&market=US&languages=en-US%2Cen%2Cneutral&fieldsTemplate=InstallAgent&mold=Public&oemId=Public&scmlId=Public HTTP/1.1 Connection: Keep-Alive Content-Type: application/json User-Agent: Install Service MS-CV: ZSKdUuY0ZkeYnvBl.0.2.4 Host: displaycatalog.mp.microsoft.com
2022-04-08 08:03:36 UTC	8951	IN	HTTP/1.1 200 OK Connection: close Date: Fri, 08 Apr 2022 08:03:35 GMT Content-Type: application/json; charset=utf-8 Server: Kestrel Transfer-Encoding: chunked Vary: Authorization MS-CorrelationId: e826c113-1332-4a41-8db4-898e2d2a9711 MS-RequestId: 8f6662b5-e9b5-497b-84f4-8090a66953cd MS-CV: ZSKdUuY0ZkeYnvBl.0.2.4.422987951.0.1.422987951.2321971560.0 X-Content-Type-Options: nosniff MS-ServerId: 469858-xzfbf Region: neu Node: aks-systempool-37630073-vmss00002l MS-DocumentVersions: 9NH2GPH4JZS4J572
2022-04-08 08:03:36 UTC	8951	IN	Data Raw: 61 66 30 37 0d 0a 7b 22 42 69 67 49 64 73 22 3a 5b 22 39 4e 48 32 47 50 48 34 4a 5a 53 34 22 5d 2c 22 48 61 73 4d 6f 72 65 50 61 67 65 73 22 3a 66 61 6c 73 65 2c 22 50 72 6f 64 75 63 74 73 22 3a 5b 7b 22 4c 61 73 74 4d 6f 64 69 66 69 65 64 44 61 74 65 22 3a 22 32 30 32 32 2d 30 33 2d 30 38 54 32 30 3a 31 31 3a 35 31 2e 33 38 33 38 35 37 30 5a 22 2c 22 4c 6f 63 61 6c 69 7a 65 64 50 72 6f 70 65 72 74 69 65 73 22 3a 5b 7b 22 46 72 61 6e 63 68 69 73 65 73 22 3a 5b 5d 2c 22 49 6d 61 67 65 73 22 3a 5b 7b 22 46 69 6c 65 49 64 22 3a 22 33 30 36 35 30 33 39 34 32 36 39 36 31 31 33 32 33 30 36 22 2c 22 45 49 53 4c 69 73 74 69 6e 67 49 64 65 6e 74 69 66 69 65 72 22 3a 6e 75 6c 6c 2c 22 42 61 63 6b 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 74 72 61 6e 73 70 61 72 65 Data Ascii: af07{"BigIds":["9NH2GPH4JZS4"],"HasMorePages":false,"Products":[{"LastModifiedDate":"2022-03-08T20:11:51.3838570Z","LocalizedProperties":[{"Franchises":[],"Images":[{"FileId":"3065039426961132306","EISListingIdentifier":"","null","BackgroundColor":"transpare
2022-04-08 08:03:36 UTC	8955	IN	Data Raw: 37 2e 31 33 36 33 34 30 35 32 35 39 35 36 31 30 35 31 31 2e 38 39 61 39 30 34 30 30 2d 62 34 39 62 2d 34 63 33 35 2d 61 37 37 37 2d 36 30 63 39 32 65 61 31 65 33 39 38 2e 30 35 36 34 65 35 61 65 2d 65 66 36 30 2d 34 39 61 32 2d 61 33 31 36 2d 61 32 66 66 31 36 30 33 32 61 39 63 22 2c 22 57 69 64 74 68 22 3a 36 36 7d 2c 7b 22 46 69 6c 65 49 64 22 3a 22 33 30 34 39 39 34 35 38 38 31 34 34 35 37 37 32 38 34 22 2c 22 45 49 53 4c 69 73 74 69 6e 67 49 64 65 6e 74 69 66 69 65 72 22 3a 6e 75 6c 6c 2c 22 42 61 63 6b 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 74 72 61 6e 73 70 61 72 65 6e 74 22 2c 22 43 61 70 74 69 6f 6e 22 3a 22 22 2c 22 46 69 6c 65 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 33 35 38 38 2c 22 46 6f 72 65 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 22 Data Ascii: 7.13634052595610511.89a90400-b49b-4c35-a777-60c92ea1e398.0564e5ae-ef60-49a2-a316-a2ff16032a9c","Width":66},{"FileId":"3049945888144577284","EISListingIdentifier":null,"BackgroundColor":"transparent","Caption":"","FileSizeInBytes":3588,"ForegroundColor":""
2022-04-08 08:03:36 UTC	8959	IN	Data Raw: 38 32 35 38 39 39 37 22 2c 22 45 49 53 4c 69 73 74 69 6e 67 49 64 65 6e 74 69 66 69 65 72 22 3a 6e 75 6c 6c 2c 22 42 61 63 6b 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 74 72 61 6e 73 70 61 72 65 6e 74 22 2c 22 43 61 70 74 69 6f 6e 22 3a 22 22 2c 22 46 69 6c 65 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 31 33 35 32 31 2c 22 46 6f 72 65 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 22 2c 22 48 65 69 67 68 74 22 3a 33 30 30 2c 22 49 6d 61 67 65 50 6f 73 69 74 69 6f 6e 49 6e 66 6f 22 3a 22 22 2c 22 49 6d 61 67 65 50 75 72 70 6f 73 65 22 3a 22 54 69 6c 65 22 2c 22 55 6e 73 63 61 6c 65 64 49 6d 61 67 65 53 48 41 32 35 36 48 61 73 68 22 3a 22 56 6b 6b 75 57 65 38 45 4f 64 75 46 42 69 75 67 45 45 64 51 6c 61 75 74 36 77 53 52 64 62 34 71 44 47 70 76 74 51 4e 39 71 76 30 Data Ascii: 8258997","EISListingIdentifier":null,"BackgroundColor":"transparent","Caption":"","FileSizeInBytes":13521,"ForegroundColor":"","Height":300,"ImagePositionInfo":"","ImagePurpose":"Tile","UnscaledImageSHA256Hash":"VkkuWe8EOduFBIugEEdQlaut6wSRdb4qDGpvtQN9qv0
2022-04-08 08:03:36 UTC	8963	IN	Data Raw: 61 20 67 6c 6f 62 61 6c 20 63 6f 6d 6d 75 6e 69 74 79 20 6f 66 20 63 72 65 61 74 6f 72 73 20 61 72 65 20 6f 6e 20 54 69 6b 54 6f 6b 20 73 68 6f 77 63 61 73 69 6e 67 20 74 68 65 69 72 20 69 6e 63 72 65 64 69 62 6c 65 20 73 6b 69 6c 6c 73 20 61 6e 64 20 65 76 65 72 79 64 61 79 20 6c 69 66 65 2e 20 4c 65 74 20 79 6f 75 72 73 65 6c 66 20 62 65 20 69 6e 73 70 69 72 65 64 2e 5c 72 5c 6e 5c 72 5c 6e e2 96 a0 20 41 64 64 20 79 6f 75 72 20 66 61 76 6f 72 69 74 65 20 6d 75 73 69 63 20 6f 72 20 73 6f 75 6e 64 20 74 6f 20 79 6f 75 72 20 76 69 64 65 6f 73 20 66 6f 72 20 66 72 65 65 5c 72 5c 6e 45 61 73 69 6c 79 20 65 64 69 74 20 79 6f 75 72 20 76 69 64 65 6f 73 20 77 69 74 68 20 6d 69 6c 6c 69 6f Data Ascii: a global community of creators\r\nMillions of creators are on TikTok showcasing their incredible skills and everyday life. Let yourself be inspired.\r\n\r\nAdd your favorite music or sound to your videos for free\r\nEasily edit your videos with millio

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:36 UTC	8967	IN	Data Raw: 72 5c 6e 5c 72 5c 6e e2 96 a0 20 57 61 74 63 68 20 65 6e 64 6c 65 73 73 20 61 6d 6f 75 6e 74 20 6f 66 20 76 69 64 65 6f 73 20 63 75 73 74 6f 6d 69 7a 65 64 20 73 70 65 63 69 66 69 63 61 6c 6c 79 20 66 6f 72 20 79 6f 75 5c 72 5c 6e 41 20 70 65 72 73 6f 6e 61 6c 69 7a 65 64 20 76 69 64 65 6f 20 66 65 65 64 20 62 61 73 65 64 20 6f 6e 20 77 68 61 74 20 79 6f 75 20 77 61 74 63 68 2c 20 6c 69 6b 65 2c 20 61 6e 64 20 73 68 61 72 65 2e 20 54 69 6b 54 6f 6b 20 6f 66 66 65 72 73 20 79 6f 75 20 72 65 61 6c 2c 20 69 6e 74 65 72 65 73 74 69 6e 67 2c 20 61 6e 64 20 66 75 6e 20 76 69 64 65 6f 73 20 74 68 61 74 20 77 69 6c 6c 20 6d 61 6b 65 20 79 6f 75 72 20 64 61 79 2e 5c 72 5c 6e 20 5c 72 5c 6e e2 96 a0 2 0 45 78 70 6c 6f 72 65 20 76 69 64 65 6f 73 2c 20 6a 75 73 74 20 Data Ascii: \n\n\n Watch endless amount of videos customized specifically for you\n\nA personalized video feed based on what you watch, like, and share. TikTok offers you real, interesting, and fun videos that will make your day.\n\n \n\n Explore videos, just
2022-04-08 08:03:36 UTC	8971	IN	Data Raw: 7b 5c 22 63 61 74 65 67 6f 72 79 2e 66 69 72 73 74 5c 22 3a 5c 22 61 70 70 5c 22 2c 5c 22 63 61 74 65 67 6f 72 79 2e 73 65 63 6f 6e 64 5c 22 3a 5c 22 45 6e 74 65 72 74 61 69 6e 6d 65 6e 74 5c 22 2c 5c 22 6f 70 74 4f 75 74 2e 62 61 63 6b 75 70 52 65 73 74 6f 72 65 5c 22 3a 66 61 6c 73 65 2c 5c 22 6f 70 74 4f 75 74 2e 72 65 6d 6f 76 65 61 62 6c 65 4d 65 64 69 61 5c 22 3a 66 61 6c 73 65 7d 2c 5c 22 70 6f 6c 69 63 79 32 5c 22 3a 7b 5c 22 61 67 65 52 61 74 69 6e 67 5c 22 3a 33 2c 5c 22 6f 70 74 4f 75 74 2e 44 56 52 5c 22 3a 66 61 6c 73 65 2c 5c 22 74 68 69 72 64 50 61 72 74 79 41 70 70 52 61 74 69 6e 67 73 5c 22 3a 5b 7b 5c 22 6c 65 76 65 6c 5c 22 3a 39 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 33 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 38 31 2c 5c 22 73 79 73 Data Ascii: {"category.first":"appl","category.second":"Entertainment","optOut.backupRestore":false,"optOut.re moveableMedia":false},"policy2":{"ageRating":3,"optOut.DVR":false,"thirdPartyAppRatings":{"level":"9,"system Id":3},"level":81,"sys
2022-04-08 08:03:36 UTC	8975	IN	Data Raw: 32 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 32 39 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 39 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 37 30 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 35 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 36 37 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 33 7d 5d 7d 7d 22 2c 22 50 61 63 6b 61 67 65 44 6f 77 6e 6c 6f 61 64 55 72 69 73 22 3a 6e 7 5 6c 6c 2c 22 46 75 6c 66 69 6c 6c 6d 65 6e 74 44 61 74 61 22 3a 7b 25 72 6f 64 75 63 74 49 64 22 3a 30 2c 22 39 4e 48 32 47 50 48 34 4a 5a 53 34 22 2c 22 57 75 42 75 6e 64 6c 65 49 64 22 3a 22 39 63 34 33 66 35 31 38 2d 65 62 64 31 2d 34 62 62 61 2d 61 35 62 38 2d 35 33 30 63 34 38 34 30 61 65 66 66 22 2c Data Ascii: 2},{level":29,"systemId":9},{level":78,"systemId":16},{level":70,"systemId":15},{level":67,"systemI d":13}}},"PackageDownloadUris":null,"FulfillmentData":{"ProductId":"9NH2GPH4JZS4","WuBundled":"9c43f518-ebd1-4bba-a5b8-530c4840aef",
2022-04-08 08:03:36 UTC	8979	IN	Data Raw: 50 6c 61 74 66 6f 72 6d 4e 61 6d 65 22 3a 22 57 69 6e 64 6f 77 73 2e 54 65 61 6d 22 7d 2c 7b 22 4d 61 78 56 65 72 73 69 6f 6e 22 3a 32 31 34 37 34 38 33 36 34 37 2c 22 4d 69 6e 56 65 72 73 69 6f 6e 22 3a 30 2c 22 50 6c 61 74 66 6f 72 6d 4e 61 6d 65 22 3a 22 57 69 6e 64 6f 77 73 2e 48 6f 6c 6f 67 72 61 70 68 69 63 22 7d 2c 7b 22 4d 61 78 56 65 72 73 69 6f 6e 22 3a 32 31 34 37 34 38 33 36 34 37 2c 22 4d 69 6e 56 65 72 73 69 6f 6e 22 3a 30 2c 22 50 6c 61 74 66 6f 72 6d 4e 61 6d 65 22 3a 22 57 69 6e 64 6f 77 73 2e 43 6f 72 65 22 7d 2c 7b 22 4d 61 78 56 65 72 73 69 6f 6e 22 3a 32 31 34 37 34 38 33 36 34 37 2c 22 4d 69 6e 56 65 72 73 69 6f 6e 22 3a 30 2c 22 50 6c 61 74 66 6f 72 6d 4e 61 6d 65 22 3 a 22 57 69 6e 64 6f 77 73 2e 38 38 32 38 30 38 30 22 7d 5d 7d 2c Data Ascii: PlatformName":"Windows.Team"},"MaxVersion":2147483647,"MinVersion":0,"PlatformName":"Windows.Holo graphic"},"MaxVersion":2147483647,"MinVersion":0,"PlatformName":"Windows.Core"},"MaxVersion":2147483647,"Min Version":0,"PlatformName":"Windows.8828080"}],
2022-04-08 08:03:36 UTC	8983	IN	Data Raw: 65 76 65 72 79 20 67 65 6e 72 65 2c 20 69 6e 63 6c 75 64 69 6e 67 20 48 69 70 20 48 6f 70 2c 20 45 64 6d 2c 20 50 6f 70 2c 20 52 6f 63 6b 2c 20 52 61 70 2c 20 61 6e 64 20 43 6f 75 6e 74 72 79 2c 20 61 6e 64 20 74 68 65 20 6d 6f 73 74 20 76 69 72 61 6c 20 6f 72 69 67 69 6e 61 6c 20 73 6f 75 6e 64 73 2e 5c 72 5c 6e 5c 72 5c 6e e2 96 a0 20 45 78 70 72 65 73 73 20 79 6f 75 72 73 65 6c 66 20 77 69 74 68 20 63 72 65 61 74 69 76 65 20 65 66 66 65 63 74 73 5c 72 5c 6e 55 6e 6c 6f 63 6b 20 74 6f 6e 73 20 6f 66 20 66 69 6c 74 65 72 73 2c 20 65 66 66 65 63 74 73 2c 20 61 6e 64 20 41 52 20 6f 62 6a 65 63 74 73 20 74 6f 20 74 61 6b 65 20 79 6f 75 72 20 76 69 64 65 6f 73 20 74 6f 20 74 68 65 20 6e 65 78 74 20 6c 65 76 65 6c 2e 5c 72 5c 6e 5c 72 5c 6e e2 96 a0 20 45 64 Data Ascii: every genre, including Hip Hop, Edm, Pop, Rock, Rap, and Country, and the most viral original sounds.\n\n\n Express yourself with creative effects\n\nUnlock tons of filters, effects, and AR objects to take your videos to the next level. \n\n\n Ed
2022-04-08 08:03:36 UTC	8987	IN	Data Raw: 42 79 74 65 64 61 6e 63 65 50 74 65 2e 4c 74 64 2e 54 69 6b 54 6f 6b 5f 36 79 63 63 6e 64 6e 36 30 36 34 73 65 22 2c 22 4d 61 69 6e 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 46 6f 72 44 6c 63 22 3a 6e 75 6c 6c 2c 22 50 61 63 6b 61 67 65 46 75 6c 6c 4e 61 6d 65 22 3a 22 42 79 74 65 64 61 6e 63 65 50 74 65 2e 4c 74 64 2e 54 69 6b 54 6f 6b 5f 31 2e 30 2e 33 2e 37 30 5f 6e 65 75 74 72 61 6c 5f 7e 5f 36 79 63 63 6e 64 6e 36 30 36 34 73 65 22 2c 22 50 61 63 6b 61 67 65 49 64 22 3a 22 36 32 61 66 39 30 66 35 2d 38 63 66 61 2d 36 63 38 30 2d 63 31 35 38 2d 30 61 64 66 62 37 36 63 33 38 34 39 2d 4e 65 75 74 72 61 6c 22 2c 22 50 61 63 6b 61 67 65 52 61 6e 6b 22 3a 33 30 30 31 30 2c 22 50 6c 61 74 66 6f 72 6d 44 65 70 65 6e 64 65 6e 63 69 65 73 22 3a 5b 7b Data Ascii: BytedancePte.Ltd.TikTok_6yccndn6064se","MainPackageFamilyNameForDlc":null,"PackageFullName":"Byted ancePte.Ltd.TikTok_1.0.3.70_neutral_-_6yccndn6064se","PackageId":"62a90f5-8cfa-6c80-c158-0adfb76c3849-Neutral ","PackageRank":30010,"PlatformDependencies":[{"
2022-04-08 08:03:36 UTC	8991	IN	Data Raw: 22 50 6c 61 74 66 6f 72 6d 44 65 70 65 6e 64 65 6e 63 69 65 73 22 3a 5b 7b 22 4d 61 78 54 65 73 74 65 64 22 3a 32 38 31 34 37 35 30 39 37 30 34 37 38 35 39 32 2c 22 4d 69 6e 56 65 72 73 69 6f 6e 22 3a 32 38 31 34 37 35 30 38 33 35 32 37 37 38 32 34 2c 22 50 6c 61 74 66 6f 72 6d 4e 61 6d 65 22 3a 22 57 69 6e 64 6f 77 73 2e 44 65 73 6b 74 6f 70 22 7d 5d 2c 22 50 6c 61 74 66 6f 72 6d 44 65 70 65 6e 64 65 6e 63 79 58 6d 6c 42 6c 6f 62 22 3a 22 7b 5c 22 62 6c 6f 62 2e 76 65 72 73 69 6f 6e 5c 22 3a 31 36 38 38 38 36 37 30 34 30 35 32 36 33 33 36 2c 5c 22 63 6f 6e 74 65 6e 74 2e 6 2 75 6e 64 6c 65 64 50 61 63 6b 61 67 65 73 5c 22 3a 5b 5c 22 42 79 74 65 64 61 6e 63 65 50 74 65 2e 4c 74 64 2e 54 69 6b 54 6f 6b 5f 31 2e 30 2e 34 2e 30 5f 78 38 36 5f 5f 36 79 63 63 Data Ascii: "PlatformDependencies":{"MaxTested":2814750970478592,"MinVersion":2814750835277824,"PlatformName" :~"Windows.Desktop"},"PlatformDependencyXmIBlob":{"blob.version":1688867040526336,"content.bundledPackages": [{"BytedancePte.Ltd.TikTok_1.0.4.0_x86__6ycc
2022-04-08 08:03:36 UTC	8995	IN	Data Raw: 5d 2c 22 4f 72 64 65 72 4d 61 6e 61 67 65 6d 65 6e 74 44 61 74 61 22 3a 7b 22 47 72 61 6e 74 65 64 45 6e 74 69 74 6c 65 6d 65 6e 74 4b 65 79 73 22 3a 5b 5d 2c 22 50 72 69 63 65 22 3a 7b 22 43 75 72 72 65 6e 63 79 43 6f 64 65 22 3a 22 55 53 44 22 2c 22 49 73 50 49 52 65 71 75 69 72 65 64 22 3a 66 61 6c 73 65 2c 22 4c 69 73 74 50 72 69 63 65 22 3a 30 2e 30 2c 22 4d 53 52 50 22 3a 30 2e 30 2c 22 54 61 78 54 79 70 65 22 3a 22 2c 22 57 68 6f 6c 65 73 61 6c 65 43 75 72 72 65 6e 63 79 43 6f 64 65 22 3a 22 2d 7d 7d 2c 22 50 72 6f 70 65 72 74 69 65 73 22 3a 7b 7d 2c 22 53 6b 75 49 64 22 3a 22 30 30 31 31 22 2c 22 44 69 73 70 6c 61 79 52 61 6e 6b 22 3a 32 2c 22 52 65 6d 65 64 69 61 74 69 6f 6e 52 65 71 75 69 72 65 64 22 3a 66 61 6c 73 65 7d 5d 7d 5d 7d 5d 2c 22 Data Ascii:],"OrderManagementData":{"GrantedEntitlementKeys":[],"Price":{"CurrencyCode":"USD","IsPIRequired": false,"ListPrice":0.0,"MSRP":0.0,"TaxType":"","WholesaleCurrencyCode":""},"Properties":{"Skuld":"0011","DisplayRank": 2,"RemediationRequired":false}}}]},
2022-04-08 08:03:36 UTC	8995	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
66	192.168.2.3	50045	52.152.110.14	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:37 UTC	8995	OUT	GET /SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%7D/x64/10.0.17134.1/0?CH=17&L=en-US&P=&PT=0x30&WUA=10.0.17134.1&MK=4MtpozR6MODPIGb&MD=EefvrDUR HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Windows-Update-Agent/10.0.10011.16384 Client-Protocol/1.81 Host: sls.update.microsoft.com
2022-04-08 08:03:37 UTC	8995	IN	HTTP/1.1 200 OK Cache-Control: no-cache Pragma: no-cache Content-Type: application/octet-stream Expires: -1 Last-Modified: Mon, 01 Jan 0001 00:00:00 GMT ETag: "wy8fVV3cy06QlZhZUaOlBEoVMBnt4x8NjH3c50VWOxM=_1440" MS-CorrelationId: 2f29306b-1ab3-4da9-8087-f01a026244d0 MS-RequestId: 0c161728-6f6e-4fc2-9d4c-a468ef107fa1 MS-CV: HobnU17tkUip/rJn.0 X-Microsoft-SLSCClientCache: 1440 Content-Disposition: attachment; filename=environment.cab X-Content-Type-Options: nosniff Date: Fri, 08 Apr 2022 08:03:36 GMT Connection: close Content-Length: 30958
2022-04-08 08:03:37 UTC	8996	IN	Data Raw: 4d 53 43 46 00 00 00 00 be 37 00 00 00 00 00 00 44 00 00 00 00 00 00 03 01 01 00 01 00 04 00 20 e0 00 00 14 00 00 00 00 00 10 00 be 37 00 00 30 41 00 00 00 00 00 00 00 00 00 64 00 00 00 01 00 01 00 f3 5b 00 00 00 00 00 00 00 00 00 00 00 80 00 65 6e 76 69 72 6f 6e 6d 65 6e 74 2e 63 61 62 00 27 c3 6c fd 52 37 f3 5b 43 4b ed 7a 05 58 55 dd d6 ee de 9b ee 96 6e 11 e9 b5 e9 52 69 a5 a4 bb 5b a4 bb 6b d3 ad a2 74 77 08 08 08 d2 21 25 dd a0 80 80 48 4a 4a 83 c4 dd e8 17 9e ef d4 7f fe 7b cf 73 fe 7b ef b7 9f 67 ef bd e6 5c 73 ce 35 63 8c f1 8e 77 8c 25 af 22 2e 05 82 7f da c9 40 df 3f 12 3f fe 40 08 60 30 08 0c 42 04 bd f8 08 02 11 7e af c1 fd de 06 10 05 fd f6 31 85 7f af 5b 85 72 83 7e fa f8 83 cc 6c 5d 2d 1d ed 6c 6d cc 6c 9d 9d dd 6d ac 41 f8 7a 2e Data Ascii: MSCF7D 70Ad[environment.cab]R7[CKzXUnRi[ktw!%HJJ{s(g's5cw%".@@?@`0B~1[r~l]~lmlmAz.
2022-04-08 08:03:37 UTC	9011	IN	Data Raw: b3 49 a2 0d ff f6 07 56 2e e0 cd 9b 1f 2c 88 a2 01 ec 5e 7b 96 ac 79 f1 dc 76 c5 85 50 e5 c7 c8 45 07 64 59 b3 b7 80 da 46 59 e2 3c b1 95 cb ed 18 a0 46 1e 05 b6 ad 0f aa c7 d6 26 8a 7a 17 6e 85 5c 5c 6e b7 9b 98 29 fc 15 9c b1 63 23 9c 27 9a ba 82 04 21 f1 ec 76 cf 7a 3c 9a dc 26 02 a4 4b 13 b7 f5 66 dc 71 d6 12 42 66 da ba 5c 82 4f 0a 63 8b 27 ed ac 5b 4a 30 41 b8 22 8b 2f b7 4c 07 eb 6d 35 30 dd 9f 04 c2 94 77 e9 20 77 b3 ca 0d 58 a9 21 17 bb 64 c6 3c 80 fd e9 00 b3 78 2d 96 fe 20 b6 4c c6 4a 0b e6 fc 7a 35 83 21 a9 5b fb 9f ec fd f1 bd a9 3a 79 0e 3d a3 0c 9a 4f 59 1e be de 85 65 6f ea 2b b7 1c 1f d9 51 fd 01 a2 7c 91 b5 30 82 07 05 30 82 04 ed a0 03 02 01 02 02 13 33 00 00 00 08 59 e3 94 e0 54 c7 17 5d 00 00 00 00 00 08 30 0d 06 09 2a 86 48 86 f7 0d Data Ascii: IV.,^{yPEdYFY<F&znl\n)c#^!vz<&KfqBfOc[J0A"/Lm50w wXld<x- Ljz5l[y=OYeo+Q[003YT]0*H

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
67	192.168.2.3	50046	52.242.101.226	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:37 UTC	9026	OUT	GET /SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%7D/x64/10.0.17134.1/0?CH=17&L=en-US&P=&PT=0x30&WUA=10.0.17134.1&MK=4MtpozR6MODPIGb&MD=EefvrDUR HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Windows-Update-Agent/10.0.10011.16384 Client-Protocol/1.81 Host: sls.update.microsoft.com
2022-04-08 08:03:37 UTC	9026	IN	HTTP/1.1 200 OK Cache-Control: no-cache Pragma: no-cache Content-Type: application/octet-stream Expires: -1 Last-Modified: Mon, 01 Jan 0001 00:00:00 GMT ETag: "wy8fVV3cy06QlZhZUaOlBEoVMBnt4x8NjH3c50VWOxM=_1440" MS-CorrelationId: c0b85a32-7e2a-4318-a93f-feb7bee0b006 MS-RequestId: f9c1cd8f-b1b3-4f3f-b522-36e7b11ec468 MS-CV: vckRcQT5DUCutb6p.0 X-Microsoft-SLSCClientCache: 1440 Content-Disposition: attachment; filename=environment.cab X-Content-Type-Options: nosniff Date: Fri, 08 Apr 2022 08:03:37 GMT Connection: close Content-Length: 30958

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:37 UTC	9027	IN	Data Raw: 4d 53 43 46 00 00 00 00 be 37 00 00 00 00 00 00 44 00 00 00 00 00 00 03 01 01 00 01 00 04 00 20 e0 00 00 14 00 00 00 00 00 10 00 be 37 00 00 30 41 00 00 00 00 00 00 00 00 00 64 00 00 00 01 00 01 00 f3 5b 00 00 00 00 00 00 00 00 00 00 80 00 65 6e 76 69 72 6f 6e 6d 65 6e 74 2e 63 61 62 00 27 c3 6c fd 52 37 f3 5b 43 4b ed 7a 05 58 55 dd d6 ee de 9b ee 96 6e 11 e9 b5 e9 52 69 a5 a4 bb 5b a4 bb 6b d3 ad a2 74 77 08 08 08 d2 21 25 dd a0 80 80 48 4a 4a 83 c4 dd e8 17 9e ef d4 7f fe 7b cf 73 fe 7b ef b7 9f 67 ef bd e6 5c 73 ce 35 63 8c f1 8e 77 8c 25 af 22 2e 05 82 7f da c9 40 df 3f 12 3f fe 40 08 60 30 08 0c 42 04 bd f8 08 02 11 7e af c1 fd de 06 10 05 fd f6 31 85 7f af 5b 85 72 83 7e fa f8 83 cc 6c 5d 2d 1d ed 6c 6d cc 6c 9d d9 dd 6d ac 41 f8 7a 2e Data Ascii: MSCF7D 70Ad[environment.cab]IR7[CKzXUnRi[ktw!%HJJ[s{g!s5cw%".@??@ '0B~1[r-]!lmIaZ.
2022-04-08 08:03:37 UTC	9042	IN	Data Raw: b3 49 a2 0d ff f6 07 56 2e e0 cd 9b 1f 2c 88 a2 01 ec 5e 7b 96 ac 79 f1 dc 76 c5 85 50 e5 c7 c8 45 07 64 59 b3 b7 80 da 46 59 e2 3c b1 95 cb ed 18 a0 46 1e 05 b6 ad 0f aa c7 d6 26 8a 7a 17 6e 85 5c 5c 6e b7 9b 98 29 fc 15 9c b1 63 23 9c 27 9a ba 82 04 21 f1 ec 76 cf 7a 3c 9a dc 26 02 a4 4b 13 b7 f5 66 dc 71 d6 12 42 66 da ba 5c 82 4f 0a 63 8b 27 ed ac 5b 4a 30 41 b8 22 8b 2f b7 4c 07 eb 6d 35 30 dd 9f 04 c2 94 77 e9 20 77 b3 ca 0d 58 a9 21 17 bb 64 c6 3c 80 fd e9 00 b3 78 2d 96 fe 20 b6 4c c6 4a 0b e6 fc 7a 35 83 21 a9 5b fb 9f ec fd f1 bd a9 3a 79 0e 3d a3 0c 9a 4f 59 1e be de 85 65 6f ea 2b b7 1c 1f d9 51 fd 01 a2 7c 91 b5 30 82 07 05 30 82 04 ed a0 03 02 01 02 02 13 33 00 00 00 08 59 e3 94 e0 54 c7 17 5d 00 00 00 00 00 08 30 0d 06 09 2a 86 48 86 f7 0d Data Ascii: IV.,^{yPEdYFY<F&zn\\n)c#!vz<&KfqBfOc'[J0A"/Lm50w wXld<x- LJz5[:y=OYeo+Q]003YT]0"H

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
68	192.168.2.3	50047	20.54.110.249	443	C:\Users\user\l\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:38 UTC	9057	OUT	GET /v7.0/products/lookup?alternateId=PackageFamilyName&value=AdobeSystemsIncorporated.AdobePhotoshopExpress_ynb6jyjte8ga&market=US&languages=en-US%2Cen%2Cneutral&fieldsTemplate=InstallAgent&mold=Public&oemId=Public&scmlId=Public HTTP/1.1 Connection: Keep-Alive Content-Type: application/json User-Agent: Install Service MS-CV: n1sA5W1j10WVDp3K.0.2.4 Host: displaycatalog.mp.microsoft.com
2022-04-08 08:03:38 UTC	9057	IN	HTTP/1.1 200 OK Connection: close Date: Fri, 08 Apr 2022 08:03:38 GMT Content-Type: application/json; charset=utf-8 Server: Kestrel Transfer-Encoding: chunked Vary: Authorization MS-CorrelationId: 942f430a-3b28-4f89-8f6d-88f49ba14651 MS-RequestId: c5a2dca1-a734-4255-8f74-5e60d742588a MS-CV: n1sA5W1j10WVDp3K.0.2.4.422988222.0.1.422988222.0.0 X-Content-Type-Options: nosniff MS-ServerId: 469858-979zz Region: neu Node: aks-systempool-37630073-vmss00002m MS-DocumentVersions: 9WZDNCRFJ27N]4206
2022-04-08 08:03:38 UTC	9058	IN	Data Raw: 31 31 62 61 66 0d 0a 7b 22 42 69 67 49 64 73 22 3a 5b 22 39 57 5a 44 4e 43 52 46 4a 32 37 4e 22 5d 2c 22 48 61 73 4d 6f 72 65 50 61 67 65 73 22 3a 66 61 6c 73 65 2c 22 50 72 6f 64 75 63 74 73 22 3a 5b 7b 22 4c 61 73 74 4d 6f 64 69 66 69 65 64 44 61 74 65 22 3a 22 32 30 32 32 2d 30 33 2d 33 30 54 30 35 3a 34 38 3a 30 36 2e 36 32 36 31 30 39 33 5a 22 2c 22 4c 6f 63 61 6c 69 7a 65 64 50 72 6f 70 65 72 74 69 65 73 22 3a 5b 7b 22 46 72 61 6e 63 68 69 73 65 73 2 2 3a 5b 5d 2c 22 49 6d 61 67 65 73 22 3a 5b 7b 22 46 69 6c 65 49 64 22 3a 22 33 30 30 35 35 35 35 30 33 36 35 31 36 38 33 36 32 37 35 22 2c 22 45 49 53 4c 69 73 74 69 6e 67 49 64 65 6e 74 69 66 69 65 72 22 3a 6e 75 6c 6c 2c 22 42 61 63 6b 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 74 72 61 6e 73 70 61 72 65 6e 74 22 2c 22 43 61 70 74 69 6f 6e 22 3a 22 2c 22 46 69 6c 65 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 31 39 31 35 2c 22 46 6f 72 65 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 74 72 61 6e 73 70 61 72 Data Ascii: 11baff["BigIds":["9WZDNCRFJ27N"],"HasMorePages":false,"Products":[{"LastModifiedDate":"2022-03-30T05:48:06.6261093Z","LocalizedProperties":{"Franchises":[],"Images":{"FileId":"3005555036516836275","EISListingIdentifier":null,"BackgroundColor":"transpar
2022-04-08 08:03:38 UTC	9061	IN	Data Raw: 34 34 39 2e 39 30 37 30 39 63 65 33 2d 30 35 30 63 2d 34 63 65 66 2d 38 64 34 61 2d 39 65 66 32 31 33 62 38 39 65 66 32 2e 33 35 37 64 38 64 34 39 2d 66 63 61 62 2d 34 64 35 30 2d 39 66 34 39 2d 32 65 37 32 30 35 33 64 39 61 65 33 22 2c 22 57 69 64 74 68 22 3a 36 36 7d 2c 7b 22 46 69 6c 65 49 64 22 3a 22 33 30 32 32 30 30 33 36 33 33 35 38 33 31 32 36 36 37 32 22 2c 22 45 49 53 4c 69 73 74 69 6e 67 49 64 65 6e 74 69 66 69 65 72 22 3a 6e 75 6c 6c 2c 22 42 61 63 6b 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 74 72 61 6e 73 70 61 72 65 6e 74 22 2c 22 43 61 70 74 69 6f 6e 22 3a 22 2c 22 46 69 6c 65 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 31 39 31 35 2c 22 46 6f 72 65 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 22 2c 22 48 65 69 67 68 74 22 3a 38 38 2c 22 49 6d Data Ascii: 449.90709ce3-050c-4cef-8d4a-9ef213b89ef2.357d8d49-fcab-4d50-9f49-2e72053d9ae3","Width":66},{"FileId":"3022003633583126672","EISListingIdentifier":null,"BackgroundColor":"transparent","Caption":"","FileSizeInBytes":1915,"ForegroundColor":"","Height":88,"Im
2022-04-08 08:03:38 UTC	9065	IN	Data Raw: 66 69 65 72 22 3a 6e 75 6c 6c 2c 22 42 61 63 6b 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 74 72 61 6e 73 70 61 72 65 6e 74 22 2c 22 43 61 70 74 69 6f 6e 22 3a 22 2c 22 46 69 6c 65 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 33 37 37 31 2c 22 46 6f 72 65 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 2c 22 48 65 69 67 68 74 22 3a 33 30 30 2c 22 49 6d 61 67 65 50 6f 73 69 74 69 6f 6e 49 6e 66 6f 22 3a 22 2c 22 49 6d 61 67 65 50 75 72 70 6f 73 65 22 3a 22 54 69 6c 65 22 2c 22 55 6e 73 63 61 6c 65 64 49 6d 61 67 65 53 48 41 32 35 36 48 61 73 68 22 3a 22 52 52 45 38 38 6e 61 62 59 58 36 6b 76 74 64 72 4d 6b 63 42 32 6b 50 48 69 6d 39 67 55 2f 70 45 61 56 6e 65 65 42 4a 59 6b 75 55 3d 22 2c 22 55 72 69 22 3a 22 2f 2f 73 74 6f 72 65 2d 69 6d 61 67 65 73 2e 73 2d Data Ascii: fier":null,"BackgroundColor":"transparent","Caption":"","FileSizeInBytes":3771,"ForegroundColor":"","Height":300,"ImagePositionInfo":"","ImagePurpose":"Tile","UnscaledImageSHA256Hash":"RRE88nabYX6kvtdrMkcB2kPHim9gU/pEaVneeBJYkuU=","Uri":"","store-images.s-

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:38 UTC	9069	IN	Data Raw: 34 34 39 2e 66 66 35 39 32 37 39 30 2d 35 34 39 36 2d 34 36 32 65 2d 62 38 36 62 2d 34 63 38 61 32 65 33 63 63 32 62 32 2e 65 32 34 39 62 37 64 62 2d 38 35 34 35 2d 34 33 61 30 2d 61 37 34 64 2d 63 33 64 31 65 64 32 30 34 34 64 61 22 2c 22 57 69 64 74 68 22 3a 34 31 34 7d 2c 7b 22 46 69 6c 65 49 64 22 3a 22 31 31 35 32 39 32 31 35 30 34 36 30 37 31 31 38 33 37 36 22 2c 22 45 49 53 4c 69 73 74 69 6e 67 49 64 65 6e 74 69 66 69 65 72 22 3a 6e 75 6c 6c 2c 22 42 61 63 6b 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 74 72 61 6e 73 70 61 72 65 6e 74 22 2c 22 43 61 70 74 69 6f 6e 22 3a 22 22 2c 22 46 69 6c 65 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 37 31 38 30 37 38 2c 22 46 6f 72 65 67 72 6f 75 6e 64 43 6f 6c 6f 72 22 3a 22 22 2c 22 48 65 69 67 68 74 22 3a 31 32 38 Data Ascii: 449.ffa52790-5496-462e-b86b-4c8a2e3cc2b2.e249b7db-8545-43a0-a74d-c3d1ed2044da",{"Width":414},{\"File Id\":\"1152921504607118376\",\"EISListingIdentifier\":null,\"BackgroundColor\":\"transparent\", \"Caption\":\"\", \"FileSizeInBytes\":718 078,\"ForegroundColor\":\"\", \"Height\":128
2022-04-08 08:03:38 UTC	9073	IN	Data Raw: 35 64 2d 39 66 63 62 2d 30 38 36 65 33 66 38 34 62 64 32 38 22 2c 22 57 69 64 74 68 22 3a 32 34 30 30 7d 2c 7b 22 46 69 6c 65 49 64 22 3a 22 31 31 35 32 39 32 31 35 30 34 37 34 33 31 38 31 39 38 31 22 2c 22 45 49 53 4c 69 73 74 69 6e 67 49 64 65 6e 74 69 66 69 65 72 22 3a 6e 75 6c 6c 2c 22 42 61 63 6b 67 72 6f 75 6e 64 43 6f 6c 6f 72 61 6e 73 70 61 72 65 6e 74 22 2c 22 43 61 70 74 69 6f 6e 22 3a 22 42 6f 72 64 65 72 73 20 2d 20 43 6f 6d 70 6 c 65 74 65 20 74 68 65 20 6c 6f 6f 6b 20 62 79 20 61 64 64 69 6e 67 20 63 6f 6f 6c 20 62 6f 72 64 65 72 73 22 2c 22 46 6 9 6c 65 53 69 7a 65 49 6e 42 79 74 65 73 22 3a 31 37 39 37 30 38 31 2c 22 46 6f 72 65 67 72 6f 75 6e 64 43 6f 6c 6f 72 2 3a 22 22 2c 22 48 65 69 67 68 74 22 3a 31 30 38 30 2c 22 49 6d Data Ascii: 5d-9fcb-086e3f84bd28\", \"Width\":2400},{\"FileId\":\"1152921504743181981\", \"EISListingIdentifier\":null, \"B ackgroundColor\":\"transparent\", \"Caption\":\"Borders - Complete the look by adding cool borders\", \"FileSizeInBytes\" :1797081,\"ForegroundColor\":\"\", \"Height\":1080,\"Im
2022-04-08 08:03:38 UTC	9077	IN	Data Raw: 75 72 65 20 61 6e 64 20 54 69 6e 74 5c 72 5c 6e 55 73 65 20 54 65 6d 70 65 72 61 74 75 72 65 20 61 6e 64 20 54 69 6e 74 20 63 6f 6e 74 72 6f 6c 73 20 74 6f 20 69 6e 74 72 6f 64 75 63 65 20 77 61 72 6d 74 68 20 6f 72 20 63 6f 6c 64 6e 65 73 73 20 74 6f 20 79 6f 75 72 20 70 68 6f 74 6f 2e 20 59 6f 75 20 63 61 6e 20 61 6c 73 6f 20 63 6f 6e 74 72 6f 6c 20 74 68 65 20 61 6d 6f 75 6e 74 20 6f 66 20 67 72 65 65 6e 20 61 6e 64 20 72 65 64 20 74 6f 6e 65 73 20 69 6e 20 79 6f 75 72 20 70 68 6f 74 6f 2e 5c 72 5c 6e 55 73 65 20 74 68 65 20 54 65 6d 70 65 72 61 74 75 72 65 20 73 6c 69 64 65 72 20 63 6f 6e 74 72 6f 6c 73 20 74 6f 20 69 6e 63 72 65 61 73 65 20 6f 72 20 64 65 63 72 65 61 73 65 20 74 68 65 20 61 6d 6f 75 6e 74 20 6f 66 20 6f 72 61 6e 67 65 20 6f 72 20 62 Data Ascii: ure and Tint\\r\\nUse Temperature and Tint controls to introduce warmth or coldness to your photo. You can also control the amount of green and red tones in your photo.\\r\\nUse the Temperature slider controls to increase or decrease the amount of orange or b
2022-04-08 08:03:38 UTC	9081	IN	Data Raw: 22 47 48 22 2c 22 47 49 22 2c 22 47 4c 22 2c 22 47 44 22 2c 22 47 50 22 2c 22 47 55 22 2c 22 47 47 22 2c 22 47 4e 22 2c 22 47 57 22 2c 22 47 59 22 2c 22 48 54 22 2c 22 48 4d 22 2c 22 48 4e 22 2c 22 41 5a 22 2c 22 42 53 22 2c 22 42 42 22 2c 22 42 59 22 2c 22 42 5a 22 2c 22 42 4a 22 2c 22 42 4d 22 2c 22 42 54 22 2c 22 4b 4d 22 2c 22 43 47 22 2c 22 43 44 22 2c 22 43 4b 22 2c 22 43 58 22 2c 22 43 43 22 2c 22 43 43 22 2c 22 4a 4d 22 2c 22 4a 4d 22 2c 22 53 4a 2 2 2c 22 4a 45 22 2c 22 4b 49 22 2c 22 4b 47 22 2c 22 4c 41 22 2c 22 4c 53 22 2c 22 4c 52 22 2c 22 4d 4f 22 2c 22 4d 4b 22 2c 22 4d 47 22 2c 22 4d 57 22 2c 22 49 4d 22 2c 22 4d 48 22 2c 22 4d 51 22 2c 22 4d 55 22 2c 22 59 54 22 2c 22 46 4d 22 2c 22 4d 44 22 2c 22 4d 4e 22 2c 22 4d 53 22 2c 22 4d 5a 22 2c Data Ascii: \"GH\", \"GI\", \"GL\", \"GD\", \"GP\", \"GU\", \"GG\", \"GN\", \"GW\", \"GY\", \"HT\", \"HM\", \"HN\", \"AZ\", \"BS\", \"BB\", \"BY\", \"BZ\", \"BJ\", \"BM \", \"BT\", \"KM\", \"CG\", \"CD\", \"CK\", \"CX\", \"CC\", \"CI\", \"CW\", \"JM\", \"SJ\", \"JE\", \"KI\", \"KG\", \"LA\", \"LS\", \"LR\", \"MO\", \"MK\", \"MG\", \"MW\", \"IM \", \"MH\", \"MQ\", \"MU\", \"YT\", \"FM\", \"MD\", \"MN\", \"MS\", \"MZ\",
2022-04-08 08:03:38 UTC	9085	IN	Data Raw: 68 69 67 68 6c 69 67 68 74 73 2c 20 6d 69 64 74 6f 6e 65 73 2c 20 61 6e 64 20 73 68 61 64 6f 77 73 2c 20 77 69 74 68 6f 75 74 20 63 6f 6d 70 72 6f 6d 69 73 69 6e 67 20 6f 6e 20 6f 74 68 65 72 61 72 65 61 73 20 6f 66 20 74 6f 6e 61 6c 69 74 79 2e 5c 72 5c 6e 55 73 65 20 42 6c 61 63 6b 73 20 61 6e 64 20 57 68 69 74 65 73 20 74 6f 20 73 65 74 20 62 6c 61 63 6b 20 70 6f 69 6e 74 20 61 6e 64 20 77 68 69 74 65 20 70 6f 69 6e 74 20 6f 66 20 74 68 65 20 70 68 6f 74 6f 2e 20 54 68 69 73 20 6d 61 6b 65 73 20 63 6f 6c 6f 72 73 20 61 70 70 65 61 72 20 63 6f 6d 70 6c 65 74 65 6c 79 20 62 6c 61 63 6b 20 6f 72 20 77 68 69 74 65 2e 5c 72 5c 6e 5c 72 5c 6e 2a 20 54 65 6d 70 65 72 61 74 75 72 65 20 61 6e 64 20 54 69 6e 74 5c 72 5c 6e 55 73 65 20 54 65 6d 70 65 72 61 74 Data Ascii: highlights, midtones, and shadows, without compromising on other areas of tonality.\\r\\nUse Blacks and Whites to set black point and white point of the photo. This makes colors appear completely black or white.\\r\\n\\r\\n* Temperature and Tint\\r\\nUse Temperat
2022-04-08 08:03:38 UTC	9089	IN	Data Raw: 55 22 2c 22 4e 46 22 2c 22 50 57 22 2c 22 50 53 22 2c 22 50 41 22 2c 22 50 47 22 2c 22 50 59 22 2c 22 52 45 22 2c 22 52 57 22 2c 22 42 4c 22 2c 22 4d 46 22 2c 22 57 53 22 2c 22 53 54 22 2c 22 53 4e 22 2c 22 4d 50 22 2c 22 50 4e 22 2c 22 53 58 22 2c 22 53 42 22 2c 22 53 4f 22 2c 22 53 43 22 2c 22 53 4c 22 2c 22 47 53 22 2c 22 53 48 22 2c 22 4b 4e 22 2c 22 4c 43 22 2c 22 50 4d 22 2c 22 56 43 22 2c 22 54 4a 22 2c 22 54 5a 22 2c 22 54 47 22 2c 22 54 4d 22 2c 22 54 4f 22 2c 22 54 4d 22 2c 22 54 43 22 2c 22 54 56 22 2c 22 55 4d 22 2c 22 55 47 22 2c 22 56 49 22 2c 22 56 47 22 2c 22 57 46 22 2c 22 45 48 22 2c 22 5a 4d 22 2c 22 5a 57 22 2c 22 55 5a 22 2c 22 56 55 22 2c 22 53 52 22 2c 22 53 5a 22 2c 22 41 44 22 2c 22 4d 43 22 2c 22 53 4d 22 2c 22 4d 45 22 2c 22 56 Data Ascii: U\", \"NF\", \"PW\", \"PS\", \"PA\", \"PG\", \"PY\", \"RE\", \"RW\", \"BL\", \"MF\", \"WS\", \"ST\", \"SN\", \"MP\", \"PN\", \"SX\", \"SB\", \"SO\", \"SC\", \"SL\", \"GS\", \"SH\", \"KN\", \"LC\", \"PM\", \"VC\", \"TJ\", \"TZ\", \"TG\", \"TK\", \"TO\", \"TM\", \"TC\", \"TV\", \"UM\", \"UG\", \"VI\", \"VG\", \"WF\", \"EH\", \"ZM\", \"ZW\", \"UZ\", \"VU\", \"SR\", \"SZ\", \"AD\", \"MC\", \"SM\", \"ME\", \"V
2022-04-08 08:03:38 UTC	9093	IN	Data Raw: 68 6f 74 6f 20 26 20 76 69 64 65 6f 5c 22 2c 5c 22 6f 70 74 4f 75 74 2e 62 61 63 6b 75 70 52 65 73 74 6f 72 65 5c 22 3a 66 61 6c 73 65 2c 5c 22 6f 70 74 4f 75 74 2e 72 65 6d 6f 76 65 61 62 6c 65 4d 65 64 69 61 5c 22 3a 66 61 6c 73 65 7d 2c 5c 22 70 6f 6c 69 63 79 32 5c 22 3a 7b 5c 22 61 67 65 52 61 74 69 6e 67 5c 22 3a 31 2c 5c 22 6f 70 74 4f 75 74 2e 44 56 52 5c 22 3a 66 61 6c 73 65 2c 5c 22 74 68 69 72 64 50 61 72 74 79 41 70 70 52 61 74 69 6e 67 73 5c 22 3a 5b 7b 5c 22 6c 65 76 65 6c 5c 22 3a 37 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 35 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 32 7d 2c 7b 5c 22 6c 65 76 65 6c 5c Data Ascii: hoto & video\",\\\"optOut.backupRestore\\\":false,\\\"optOut.removeableMedia\\\":false},\\\"policy2\\\":{\\\"ageRating\\\":1 ,\\\"optOut.DVR\\\":false,\\\"thirdPartyAppRatings\\\":{\\\"level\\\":7,\\\"systemId\\\":3},\\\"level\\\":12,\\\"systemId\\\":5},\\\"level\\\":48,\\\"systemI d\\\":12},\\\"level\\
2022-04-08 08:03:38 UTC	9097	IN	Data Raw: 62 38 37 35 2d 63 66 36 32 63 33 62 61 63 64 66 36 22 2c 22 57 75 43 61 74 65 67 6f 72 79 49 64 22 3a 22 63 30 38 61 30 64 37 32 2d 32 38 61 31 2d 34 36 35 61 2d 39 65 37 30 2d 36 61 35 62 38 30 62 34 34 64 36 30 22 2c 22 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 22 3a 22 41 64 6f 62 65 53 79 73 74 65 6d 73 49 6e 63 6f 72 70 6f 72 61 74 65 64 2e 41 64 6f 62 65 50 68 6f 74 6f 73 68 6f 70 45 78 70 72 65 73 73 5f 79 6e 62 36 6a 79 6a 7a 74 65 38 67 61 22 2c 22 53 6b 75 49 64 22 3a 22 30 30 31 30 22 2c 22 43 6f 6e 74 65 6e 74 22 3a 6e 75 6c 6c 2c 22 50 61 63 6b 61 67 65 46 65 61 74 75 72 65 73 22 3a 6e 75 6c 6c 7d 7d 2c 7b 22 41 70 70 6c 69 63 61 74 69 6f 6e 73 22 3a 5b 7b 22 41 70 70 6 c 69 63 61 74 69 6f 6e 49 64 22 3a 22 41 70 70 22 7d 5d 2c 22 41 Data Ascii: b875-cf62c3bacdf6\", \"WuCategoryId\":\"c08a0d72-28a1-465a-9e70-6a5b80b44d60\", \"PackageFamilyN ame\":\"AdobeSystemsIncorporated.AdobePhotoshopExpress_ynb6ijyzte8ga\", \"Skuld\":\"0010\", \"Content\":null, \"PackageFeat ures\":null}}, {\"Applications\": [{\"ApplicationId\":\"App\"}], \"A

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:38 UTC	9101	IN	Data Raw: 70 45 78 70 72 65 73 73 5f 79 6e 62 36 6a 79 6a 7a 74 65 38 67 61 22 2c 22 4d 61 69 6e 50 61 63 6b 61 67 65 46 61 6d 69 6c 79 4e 61 6d 65 46 6f 72 44 6c 63 22 3a 6e 75 6c 6c 2c 22 50 61 63 6b 61 67 65 46 75 6c 6c 4e 61 6d 65 22 3a 22 41 64 6f 62 65 53 79 73 74 65 6d 73 49 6e 63 6f 72 70 6f 72 61 74 65 64 2e 41 64 6f 62 65 50 68 6f 74 6f 73 68 6f 70 45 78 70 72 65 73 73 5f 32 30 31 37 2e 39 32 31 2e 31 34 33 34 2e 30 5f 6e 65 75 74 72 61 6c 5f 7e 5f 79 6e 62 36 6a 79 6a 7a 74 65 38 67 61 22 2c 22 50 61 63 6b 61 67 65 49 64 22 3a 22 63 65 36 62 34 38 39 66 2d 33 30 66 33 2d 34 36 63 36 2d 62 32 65 34 2d 35 65 37 66 30 32 31 31 63 33 35 66 2d 58 38 36 2d 58 36 34 2d 41 72 6d 22 2c 22 50 61 63 6b 61 67 65 52 61 6e 6b 22 3a 32 30 30 31 33 2c 22 50 6c 61 74 66 Data Ascii: pExpress_ynb6jyjte8ga","MainPackageFamilyNameForDlc":null,"PackageFullName":"AdobeSystemsIncorporated.AdobePhotoshopExpress_2017.921.1434.0_neutral_~_ynb6jyjte8ga","PackageId":"ce6b489f-30f3-46c6-b2e4-5e7f0211c35f-X86-X64-Arm","PackageRank":20013,"Platf
2022-04-08 08:03:38 UTC	9105	IN	Data Raw: 61 67 65 6d 65 6e 74 44 61 74 61 22 3a 7b 22 47 72 61 6e 74 65 64 45 6e 74 69 74 6c 65 6d 65 6e 74 4b 65 79 73 22 3a 5b 5d 2c 22 50 72 69 63 65 22 3a 7b 22 43 75 72 72 65 6e 63 79 43 6f 64 65 22 3a 22 55 53 44 22 2c 22 49 73 50 49 52 65 71 75 69 72 65 64 22 3a 66 61 6c 73 65 2c 22 4c 69 73 74 50 72 69 63 65 22 3a 30 2e 30 2c 22 4d 53 52 50 22 3a 30 2e 30 2c 22 54 61 78 54 79 70 65 22 3a 22 22 2c 22 57 68 6f 6c 65 73 61 6c 65 43 75 72 72 65 6e 63 79 43 6f 64 65 22 3a 22 22 7d 7d 2c 22 50 72 6f 70 65 72 74 69 65 73 22 3a 7b 7d 2c 22 53 6b 75 49 64 22 3a 22 30 30 31 30 22 2c 22 44 69 73 70 6c 61 79 52 61 6e 6b 22 3a 31 2c 22 52 65 6d 65 64 69 61 74 69 6f 6e 52 65 71 75 69 72 65 64 22 3a 66 61 6c 73 65 7d 2c 7b 22 41 63 74 69 6f 6e 73 22 3a 5b 22 4c 69 63 65 Data Ascii: agementData":{"GrantedEntitlementKeys":[],"Price":{"CurrencyCode":"USD"},"IsPIRRequired":false,"ListPrice":0.0,"MSRP":0.0,"TaxType":"","WholesaleCurrencyCode":""},"Properties":{"Skuld":"0010","DisplayRank":1,"RemediationRequired":false},"Actions":["Lice
2022-04-08 08:03:38 UTC	9109	IN	Data Raw: 68 69 73 20 6d 61 6b 65 73 20 63 6f 6c 6f 72 73 20 61 70 65 61 72 20 63 6f 6d 70 6c 65 74 65 6c 79 20 62 6c 61 63 6b 20 6f 72 20 77 68 69 74 65 2e 5c 72 5c 6e 5c 72 5c 6e 2a 20 54 65 6d 70 65 72 61 74 75 72 65 20 61 6e 64 20 54 69 6e 74 5c 72 5c 6e 55 73 65 20 54 65 6d 70 65 72 61 74 75 72 65 20 61 6e 64 20 54 69 6e 74 20 63 6f 6e 74 72 6f 6c 73 20 74 6f 20 69 6e 74 72 6f 64 75 63 65 20 77 61 72 6d 74 68 20 6f 72 20 63 6f 6c 64 6e 65 73 73 20 74 6f 20 79 6f 75 72 20 70 68 6f 74 6f 2e 20 59 6f 75 20 63 61 6e 20 61 6c 73 6f 20 63 6f 6e 74 72 6f 6c 20 74 68 65 20 61 6d 6f 75 6e 74 20 6f 66 20 67 72 65 65 6e 20 61 6e 64 20 72 65 64 20 74 6f 6e 65 73 20 69 6e 20 79 6f 75 72 20 70 68 6f 74 6f 2e 5c 72 5c 6e 55 73 65 20 74 68 65 20 54 65 6d 70 65 72 61 74 75 Data Ascii: his makes colors appear completely black or white.\n\n* Temperature and Tint\n\nUse Temperature and Tint controls to introduce warmth or coldness to your photo. You can also control the amount of green and red tones in your photo.\n\nUse the Temperatu
2022-04-08 08:03:38 UTC	9113	IN	Data Raw: 54 4d 22 2c 22 54 43 22 2c 22 54 56 22 2c 22 55 4d 22 2c 22 55 47 22 2c 22 56 49 22 2c 22 56 47 22 2c 22 57 46 22 2c 22 45 48 22 2c 22 5a 4d 22 2c 22 5a 57 22 2c 22 55 5a 22 2c 22 56 55 22 2c 22 53 52 22 2c 22 53 5a 22 2c 22 41 44 22 2c 22 4d 43 22 2c 22 53 4d 22 2c 22 4d 45 22 2c 22 56 41 22 2c 22 4e 45 55 54 52 41 4c 22 5d 7d 5d 2c 22 50 72 6f 64 75 63 74 49 64 22 3a 22 39 57 5a 44 4e 43 52 46 4a 32 37 2c 22 60 70 65 72 74 69 65 73 22 3a 7b 22 46 75 6c 66 69 6c 6c 6d 65 6e 74 44 61 74 61 22 3a 7b 22 50 72 6f 64 75 63 74 49 64 22 3a 22 39 57 5a 44 4e 43 52 46 4a 32 37 4e 22 2c 22 57 75 43 61 74 65 67 6f 72 79 49 64 22 3a 22 63 30 38 61 30 64 37 32 2d 32 38 61 31 2d 34 36 35 61 2d 39 65 37 30 2d 36 61 35 62 38 30 62 34 34 64 36 30 22 2c 22 50 Data Ascii: TM","TC","TV","UM","UG","VI","VG","WF","EH","ZM","ZW","UZ","VU","SR","SZ","AD","MC","SM","ME","VA","NEUTRAL"]},"ProductId":"9WZDNCRFJ27N","Properties":{"FulfillmentData":{"ProductId":"9WZDNCRFJ27N","WuCategoryId":"c08a0d72-28a1-465a-9e70-6a5b80b44d60"},"P
2022-04-08 08:03:38 UTC	9117	IN	Data Raw: 6c 65 76 65 6c 5c 22 3a 37 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 33 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 34 38 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 32 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 32 37 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 39 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 37 36 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 36 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 36 38 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 35 7d 2c 7b 5c 22 6c 65 76 65 6c 5c 22 3a 35 34 2c 5c 22 73 79 73 74 65 6d 49 64 5c 22 3a 31 33 7d 5d 7d 7d 22 2c 22 50 61 63 6b 61 67 65 44 6f 77 6e 6c 6f 61 64 55 72 69 73 22 3a 6e 75 6c 6c 2c 22 46 75 6c 66 69 6c 6c 6d 65 6e 74 44 61 Data Ascii: level":7,"systemId":3},{level":12,"systemId":5},{level":48,"systemId":12},{level":27,"systemId":9},{level":76,"systemId":16},{level":68,"systemId":15},{level":54,"systemId":13}}},"PackageDownloadUri":null,"FulfillmentDa
2022-04-08 08:03:38 UTC	9121	IN	Data Raw: 75 49 64 22 3a 22 30 30 31 31 22 2c 22 43 6f 6e 74 65 6e 74 22 3a 6e 75 6c 6c 2c 22 50 61 63 6b 61 67 65 46 65 61 74 75 72 65 73 22 3a 6e 75 6c 6c 7d 7d 2c 7b 22 41 70 70 6c 69 63 61 74 69 6f 6e 73 22 3a 5b 7b 22 41 70 70 6c 69 63 61 74 69 6f 6e 49 64 22 3a 22 41 70 70 22 7d 5d 2c 22 41 72 63 68 69 74 65 63 74 75 72 65 73 22 3a 5b 22 78 36 34 22 5d 2c 22 43 61 70 61 62 69 6c 69 74 69 65 73 22 3a 5b 22 69 6e 74 65 72 6e 65 74 43 6c 69 65 6e 74 53 65 72 76 65 72 22 2c 22 70 69 63 74 75 72 65 73 4c 69 62 72 61 72 79 22 2c 22 4d 69 63 72 6f 73 6f 6e 74 2e 73 74 6f 72 65 46 69 6c 74 65 72 2e 63 6f 72 65 2e 6e 6f 74 53 75 70 70 6f 72 74 65 64 5f 38 77 65 6b 79 62 33 64 38 62 62 77 65 22 5d 2c 22 45 78 70 65 72 Data Ascii: uld":"0011","Content":null,"PackageFeatures":null},"Applications":[{"ApplicationId":"App"},"Architectures":["x64"],"Capabilities":["internetClient","internetClientServer","picturesLibrary","Microsoft.storeFilter.core.notSupported_8wekyb3d8bbwe"],"Exper
2022-04-08 08:03:38 UTC	9125	IN	Data Raw: 74 65 38 67 61 22 2c 22 50 61 63 6b 61 67 65 49 64 22 3a 22 63 65 6d 32 34 38 39 66 2d 33 30 66 33 2d 34 36 63 36 2d 62 32 65 34 2d 35 65 37 66 30 32 31 31 63 33 35 66 2d 58 38 36 2d 58 36 34 2d 41 72 6d 22 2c 22 50 61 63 6b 61 67 65 52 61 6e 6b 22 3a 32 30 30 31 33 2c 22 50 6c 61 74 66 6f 72 6d 44 65 70 65 6e 64 65 6e 63 69 65 73 22 3a 5b 7b 22 4d 61 78 54 65 73 74 65 64 22 3a 31 36 38 38 38 36 32 37 34 35 31 36 35 38 32 34 2c 22 4d 69 6e 56 65 72 73 69 6f 6e 22 3a 31 36 38 38 38 36 32 37 34 35 31 36 35 38 32 34 2c 22 50 6c 61 74 66 6f 72 6d 4e 61 6d 65 22 3a 22 57 69 6e 64 6f 77 73 2e 57 69 6e 64 6f 77 73 38 78 22 7d 5d 2c 22 50 6c 61 74 66 6f 72 6d 44 65 70 65 6e 64 65 6e 63 79 58 6d 6c 42 6c 6f 62 22 3a 22 7b 5c 22 62 6c 6f 62 2e 76 65 72 73 69 6f 6e Data Ascii: te8ga","PackageId":"ce6b489f-30f3-46c6-b2e4-5e7f0211c35f-X86-X64-Arm","PackageRank":20013,"PlatformDependencies":[{"MaxTested":1688862745165824,"MinVersion":1688862745165824,"PlatformName":"Windows.Windows8x"}],"PlatformDependencyXmlBlob":{"blob.version
2022-04-08 08:03:38 UTC	9129	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
69	192.168.2.3	50048	40.125.122.176	443	C:\Users\user\Desktop\l.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:39 UTC	9129	OUT	GET /SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%D/x64/10.0.17134.1/0?CH=17&L=en-US&P=&PT=0x30&WUA=10.0.17134.1&MK=4MtpozR6MODPIGb&MD=EefvrDUR HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Windows-Update-Agent/10.0.10011.16384 Client-Protocol/1.81 Host: sls.update.microsoft.com
2022-04-08 08:03:39 UTC	9129	IN	HTTP/1.1 200 OK Cache-Control: no-cache Pragma: no-cache Content-Type: application/octet-stream Expires: -1 Last-Modified: Mon, 01 Jan 0001 00:00:00 GMT ETag: "wy8fVV3cy06QlZhUaOlBEoVMBnt4x8NJH3c50VWOxM= _1440" MS-CorrelationId: 919d3ed8-c98e-4c4a-a066-fabf56ff9af9 MS-RequestId: 3b152273-94bb-4a0c-ad48-35ba86306244 MS-CV: e7OvT1fLEE+57nMI.0 X-Microsoft-SLSClietCache: 1440 Content-Disposition: attachment; filename=environment.cab X-Content-Type-Options: nosniff Date: Fri, 08 Apr 2022 08:03:38 GMT Connection: close Content-Length: 30958
2022-04-08 08:03:39 UTC	9130	IN	Data Raw: 4d 53 43 46 00 00 00 00 be 37 00 00 00 00 00 00 44 00 00 00 00 00 00 03 01 01 00 01 00 04 00 20 e0 00 00 14 00 00 00 00 00 10 00 be 37 00 00 30 41 00 00 00 00 00 00 00 00 64 00 00 00 01 00 01 00 f3 5b 00 00 00 00 00 00 00 00 00 00 80 00 65 6e 76 69 72 6f 6e 6d 65 6e 74 2e 63 61 62 00 27 c3 6c fd 52 37 f3 5b 43 4b ed 7a 05 58 55 dd d6 ee de 9b ee 96 6e 11 e9 b5 e9 52 69 a5 a4 bb 5b a4 bb 6b d3 ad a2 74 77 08 08 08 d2 21 25 dd a0 80 80 48 4a 4a 83 c4 dd e8 17 9e ef d4 7f fe 7b cf 73 fe 7b ef b7 9f 67 ef bd e6 5c 73 ce 35 63 8c f1 8e 77 8c 25 af 22 2e 05 82 7f da c9 40 df 3f 12 3f fe 40 08 60 30 08 0c 42 04 bd f8 08 02 11 7e af c1 fd de 06 10 05 fd f6 31 85 7f af 5b 85 72 83 7e fa f8 83 cc 6c 5d 2d 1d ed 6c 6d cc 6c 9d d9 dd 6d ac 41 f8 7a 2e Data Ascii: MSCF7D 70Ad[environment.cab'IR7[CKzXUnRi[ktw!%HJJ[s{gls5cw%".@??@ '0B~1[r-]lmlAz.
2022-04-08 08:03:39 UTC	9145	IN	Data Raw: b3 49 a2 0d ff f6 07 56 2e e0 cd 9b 1f 2c 88 a2 01 ec 5e 7b 96 ac 79 f1 dc 76 c5 85 50 e5 c7 c8 45 07 64 59 b3 b7 80 da 46 59 e2 3c b1 95 cb ed 18 a0 46 1e 05 b6 ad 0f aa c7 d6 26 8a 7a 17 6e 85 5c 5c 6e b7 9b 98 29 fc 15 9c b1 63 23 9c 27 9a ba 82 04 21 f1 ec 76 cf 7a 3c 9a dc 26 02 a4 4b 13 b7 f5 66 dc 71 d6 12 42 66 da ba 5c 82 4f 0a 63 8b 27 ed ac 5b 4a 30 41 b8 22 8b 2f b7 4c 07 eb 6d 35 30 dd 9f 04 c2 94 77 e9 20 77 b3 ca 0d 58 a9 21 17 bb 64 c6 3c 80 fd e9 00 b3 78 2d 96 fe 20 b6 4c c6 4a 0b e6 fc 7a 35 83 21 a9 5b fb 9f ec fd f1 bd a9 3a 79 0e 3d a3 0c 9a 4f 59 1e be de 85 65 6f ea 2b b7 1c 1f d9 51 fd 01 a2 7c 91 b5 30 82 07 05 30 82 04 ed a0 03 02 01 02 02 13 33 00 00 00 08 59 e3 94 e0 54 c7 17 5d 00 00 00 00 00 08 30 0d 06 09 2a 86 48 86 f7 0d Data Ascii: IV,^[{yvPEdYFY<F&zn\\n)c#\\vz<&KfqBfOc'[J0A"/Lm50w wX!d<x- LJz5![:y=OYeo+Q[003YT]0*H

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49986	20.82.210.154	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:27 UTC	32	OUT	GET /v3/Delivery/Placement?pubid=da63df93-3dbc-42ae-a505-b34988683ac7&pid=338387&adm=2&w=1&h=1&wpx=1&hpx=1&fmt=json&cltp=app&dim=le&rafb=0&nct=1&pm=1&cfmt=text,image,poly&sft=jpeg,png,gif&topt=1&poptin=0&localid=w:472DC600-FAEB-E7F8-720D-1E33F00FD1E7&ctry=US&time=20220408T170226Z&lc=en-US&pl=en-US&idtp=mid&uid=4388269c-b420-4134-ac19-bc7ca8a19ac1&aid=00000000-0000-0000-0000-000000000000&ua=Windows ShellClient%2F9.0.40929.0%20%28Windows%29&asid=619c052a6e5140c4b5cee07576f42985&ctmode=MultiSession&arch=x64&cdm=1&cdmver=10.0.17134.1&devfam=Windows.Desktop&devform=Unknown&devosver=10.0.17134.1&disp horzres=1280&dispsize=17.1&dispvertres=1024&isu=0&lo=1463022&metered=false&nettype=ethernet&npid=sc-338387&oemName=hsehht%2C%20Inc.&oemid=hsehht%2C%20Inc.&ossku=Professional&rver=2&sc-mode=0&smBiosDm=hsehht%2C1&tl=2&tsu=1463022&waasBldFlt=1&waasCfgExp=1&waasCfgSet=1&waasRetail=1&waasRing= HTTP/1.1 Accept-Encoding: gzip, deflate X-SDK-CACHE: chs=0&imp=0&chf=0&ds=50583&fs=32319&sc=6 X-SDK-HW-TOKEN: t=EwDYAppeBAAUIAKXDAofTQM+n+MaRVFKzH/ehWgAAdVW0iu23GlxjRyUBGA+V5LMoU//MaTj obBnQosoTe6w30OZEf3HulBKeYXog3CqxSfjOHeF/J4iLS/gKyhq/ZV/xtrYHZ35PhcBmS2qzlwNBiXp0+4lefq5ns DEEEsQ06VT9dPxHYgWIFLG65LRysydA1IM9dDPzftFvDLM/ickJDFevqkA3hg2mKV46lqHL4CT7eP4Hk0/MorRp8JB 5tew/jl7o25TIEcXl9Ohbx1KlwUuqQcpj0nFDAUZEjkQqVS2z/wQaH+/fdlFO/AoxQl3Cbc0TeaCp3XlesBJX0bxVN zc22qQqCPfGWQ/Sb52rGvkgBRvdW8DFg8ToMjfQpYDZgAAACE3mODPOPAwVqAFPV53gZzc0aOkGu+jJWn w46hEU9aCkIpEDkH6SywZSj+Z6lyumM/ZCz1/Exb6MZih9PGVRFV0dS4rZOftTsxExw5x6gJoWeqkJZJqul+/LQNZp daM/TGNQWhUnnbhyzuL3J52vfTsZzAtC6HDHUtfcP567luQfNjw1zOBQG/Pho8+d+FIHWtCPKMXaDH+rX7PpflRpHT m7bd+H+rsPvLvdstjafDCGAADV0pkaM4oU0n35rzdzoAWTcazcHXkrs0Gr34gDLpKE96nUwLpeDIXN3LOntP44gHn gfTJA4vz4io7zKxVkmOUwHoTarQk7POiXKiwa8x1QRMWrr0xK5k34elR6SWW4uOhaTkCvnxjxlUvc2iz/sxwQS6ZoJu zJ60lcBcq6ptimZGdy/yulx2kCNycUG/nBNXBdKiF3Kz0nMb3Ry9n0Qlmc/nP9d68+s4WiRlc+RuW5MPI3aHMGgT2s nchu87pA34+QQKDXqPjZVZnC+RaoA8mYS8BGPqZ//PidcqGGmzw2vccoT1N6pSAD7mXPyM9QONX68BD3 4uYAk1VCPHrpsKh41QE=&p= Cache-Control: no-cache MS-CV: BYqskdYKuUKf7ZeJ.0 User-Agent: WindowsShellClient/9.0.40929.0 (Windows) X-SDK-HWF: tch0,m301,m751,mA01,mT01 Host: arc.msn.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:27 UTC	41	IN	HTTP/1.1 200 OK Cache-Control: no-store, no-cache Pragma: no-cache Content-Length: 24532 Content-Type: application/json; charset=utf-8 Expires: Mon, 01 Jan 0001 00:00:00 GMT Server: Microsoft-IIS/10.0 ARC-RSP-DBG: [{"RADIDS":"","3,P425056668-T700379701-C128000000003026329+B+P90+S1,P425462535-T700374422-C128000000003097149+B+P80+S2,P40090958-T700355890-C128000000002241509+B+P20+S3"}, {"BATCH_REDIRECT_STORE":"","BWW_128000000003026329_EN-US+P0+S0"}, {"BATCH_REDIRECT_STORE":"","BWW_128000000003097149_EN-US+P0+S0"}, {"BATCH_REDIRECT_STORE":"","BWW_128000000002241509_EN-US+P0+S0"}, {"OPTOUTSTATE":"","256"}] X-ARC-SIG: Zk9JuFMVqrJW3UUjX9sliH4RLpxbkrSyRowC9C07tVMvE29gio6hjWUzpvZJ0v+uInplUQEn13WXLTIYLXiEMFXfGGdVsXZ2SAZDDiGUgh+fGS1YqtJQ9NXzh182LJ4aAdFQrTyg2aAD/HdF5baQJZ3qdJyEruijo7464WS0AhRsz1djbBC5sIYCbd5otrP6+ixsdYQqEhvUPeMm5rUBuyZXTv/5dB17jpRYNA/Dsyniu/g5Ie1KKoM92zzY+0AOQaWrkaV8FTE2xLDh2gM2Er1ZXc0ZH7j58/OwektyNAkgmwbik4532li7BHsWx3YaRBtY1mCu5mYR/jyv7tj7qw== Accept-CH: UA, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform, UA-Platform-Version X-AspNet-Version: 4.0.30319 X-Powered-By: ASP.NET Strict-Transport-Security: max-age=31536000; includeSubDomains Date: Fri, 08 Apr 2022 08:02:27 GMT Connection: close
2022-04-08 08:02:27 UTC	43	IN	Data Raw: 7b 22 62 61 74 63 68 72 73 70 22 3a 7b 22 76 65 72 22 3a 22 31 2e 30 22 2c 22 69 74 65 6d 73 22 3a 5b 7b 22 69 74 65 6d 22 3a 22 7b 5c 22 66 5c 22 3a 5c 22 72 61 66 5c 22 2c 5c 22 76 5c 22 3a 5c 22 31 2e 30 5c 22 2c 5c 22 72 64 72 5c 22 3a 5b 7b 5c 22 63 5c 22 3a 5c 22 43 44 4d 5c 22 2c 5c 22 75 5c 22 3a 5c 22 53 75 62 73 63 72 69 62 65 6 4 43 6f 6e 74 65 6e 74 5c 22 7d 5d 2c 5c 22 61 64 5c 22 3a 7b 5c 22 63 6c 61 73 73 5c 22 3a 5c 22 63 6f 6e 74 65 6e 74 5c 22 2c 5c 22 63 6f 6c 6c 65 63 74 69 6f 6e 73 5c 22 3a 5b 5d 2c 5c 22 6e 61 6d 65 5c 22 3a 5c 22 4c 6f 63 6b 53 63 72 65 65 6e 5c 22 2c 5c 22 70 72 6f 70 65 72 74 79 4d 61 6e 69 66 65 73 74 5c 22 3a 7b 5c 22 6c 61 6e 64 73 63 61 70 65 49 6d 61 67 65 5c 22 3a 7b 5c 22 74 79 70 65 5c 22 3a 5c 22 69 6d 61 Data Ascii: {"batchrsp":{"ver":"","1.0","items":[{"item":{"f":"","rafl","v":"","1.0"},"rdrl":{"c":"","CDMI"},"ul":"","SubscribedContent"},""],"ad":{"class":"","content","collections":"","","name":"","LockScreen","propertyManifest":{"landscapelmage":{"type":"","ima
2022-04-08 08:02:27 UTC	57	IN	Data Raw: 3a 34 37 32 44 43 36 30 30 2d 46 45 41 42 2d 45 37 46 38 2d 37 32 30 44 2d 31 45 33 33 46 30 30 46 44 31 45 37 26 44 53 5f 45 56 54 49 44 3d 39 33 33 35 35 30 66 32 62 61 65 61 34 33 37 61 61 30 37 62 32 36 62 64 38 33 63 36 35 31 33 33 26 42 43 4e 54 3d 31 26 50 47 3d 50 43 30 30 30 50 30 46 52 35 2e 30 30 30 30 30 30 49 52 53 26 55 4e 49 44 3d 33 33 38 33 38 37 26 4d 41 50 5f 54 49 44 3d 32 44 34 46 42 36 33 44 2d 35 45 39 30 2d 34 39 33 41 2d 41 39 41 39 2d 38 39 31 30 30 44 30 44 44 35 36 42 26 4e 43 54 3d 31 26 50 4e 3d 44 41 36 33 44 46 39 33 2d 33 44 42 43 2d 34 32 41 45 2d 41 35 30 35 2d 42 33 34 39 38 38 36 38 33 41 43 37 26 41 53 49 44 3d 36 31 39 43 30 35 32 41 36 45 35 31 34 30 43 34 42 35 43 45 45 30 37 35 37 36 46 34 32 39 38 35 26 52 45 Data Ascii: :472DC600-FEAB-E7F8-720D-1E33F00FD1E7&DS_EVTID=933550f2baea437aa07b26bd83c65133&BCNT=1&PG=PC000P0FR5.00000000IRS&UNID=338387&MAP_TID=2D4FB63D-5E90-493A-A9A9-89100D0DD56B&NCT=1&PN=DA63DF93-3DBC-42AE-A505-B34988683AC7&ASID=619C052A6E5140C4B5CEE07576F42985&RE

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
70	192.168.2.3	50049	40.125.122.176	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:39 UTC	9160	OUT	GET /SLS/%7B9482F4B4-E343-43B6-B170-9A65BC822C77%7D/x64/10.0.17134.1/0?CH=17&L=en-US&P=&PT=0x30&WUA=10.0.17134.1&MK=4MtpozR6MODPIGb&MD=EefvrDUR HTTP/1.1 Connection: Keep-Alive Accept: /* User-Agent: Windows-Update-Agent/10.0.10011.16384 Client-Protocol/1.81 Host: sls.update.microsoft.com
2022-04-08 08:03:40 UTC	9162	IN	HTTP/1.1 200 OK Cache-Control: no-cache Pragma: no-cache Content-Type: application/octet-stream Expires: -1 Last-Modified: Mon, 01 Jan 0001 00:00:00 GMT ETag: "wy8fVV3cy06QlZhZUaOlBEoVMBnt4x8NJH3c50VWOxM= _1440" MS-CorrelationId: 1520d0b6-a979-4f3b-8943-44a80080d27a MS-RequestId: ba7d0dc4-f931-4f80-908c-863e96edde55 MS-CV: vvBsoygK10KK2Vjp.0 X-Microsoft-SLSCClientCache: 1440 Content-Disposition: attachment; filename=environment.cab X-Content-Type-Options: nosniff Date: Fri, 08 Apr 2022 08:03:39 GMT Connection: close Content-Length: 30958
2022-04-08 08:03:40 UTC	9163	IN	Data Raw: 4d 53 43 46 00 00 00 00 be 37 00 00 00 00 00 44 00 00 00 00 00 00 03 01 01 00 01 00 04 00 20 e0 00 00 14 00 00 00 00 10 00 be 37 00 00 30 41 00 00 00 00 00 00 00 00 64 00 00 00 01 00 01 00 f3 5b 00 00 00 00 00 00 00 00 00 00 80 00 65 6e 76 69 72 6f 6e 6d 65 6e 74 2e 63 61 62 00 27 c3 6c fd 52 37 f3 5b 43 4b ed 7a 05 58 55 dd d6 ee de 9b ee 96 6e 11 e9 b5 e9 52 69 a5 a4 bb 5b a4 bb 6b d3 ad a2 74 77 08 08 d2 21 25 dd a0 80 80 48 4a 4a 83 c4 dd e8 17 9e ef d4 7f fe 7b cf 73 fe 7b ef b7 9f 67 ef bd e6 5c 73 ce 35 63 8c f1 8e 77 8c 25 af 22 2e 05 82 7f da c9 40 df 3f 12 3f fe 40 08 60 30 08 0c 42 04 bd f8 08 02 11 7e af c1 fd de 06 10 05 fd f6 31 85 7f af 5b 85 72 83 7e fa f8 83 cc 6c 5d 2d 1d ed 6c 6d cc 6c 9d d9 dd 6d ac 41 f8 7a 2e Data Ascii: MSCF7D 70Ad[environment.cab]IR7[CKzXUnRi[ktw!%HJJ[s[gs5cw%".@??@~0B~1[r~l~lmlmAz.

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:40 UTC	9178	IN	Data Raw: b3 49 a2 0d ff f6 07 56 2e e0 cd 9b 1f 2c 88 a2 01 ec 5e 7b 96 ac 79 f1 dc 76 c5 85 50 e5 c7 c8 45 07 64 59 b3 b7 80 da 46 59 e2 3c b1 95 cb ed 18 a0 46 1e 05 b6 ad 0f aa c7 d6 26 8a 7a 17 6e 85 5c 5c 6e b7 9b 98 29 fc 15 9c b1 63 23 9c 27 9a ba 82 04 21 f1 ec 76 cf 7a 3c 9a dc 26 02 a4 4b 13 b7 f5 66 dc 71 d6 12 42 66 da ba 5c 82 4f 0a 63 8b 27 ed ac 5b 4a 30 41 b8 22 8b 2f b7 4c 07 eb 6d 35 30 dd 9f 04 c2 94 77 e9 20 77 b3 ca 0d 58 a9 21 17 bb 64 c6 3c 80 fd e9 00 b3 78 2d 96 fe 20 b6 4c c6 4a 0b e6 fc 7a 35 83 21 a9 5b fb 9f ec fd f1 bd a9 3a 79 0e 3d a3 0c 9a 4f 59 1e be de 85 65 6f ea 2b b7 1c 1f d9 51 fd 01 a2 7c 91 b5 30 82 07 05 30 82 04 ed a0 03 02 01 02 02 13 33 00 00 00 08 59 e3 94 e0 54 c7 17 5d 00 00 00 00 08 30 0d 06 09 2a 86 48 86 f7 0d Data Ascii: IV.,^{\yvPEdYFY<F&zn\ln)c#~!vz<&KfqBfOc"[J0A"/Lm50w wX!d<x- LJz5![:y=OYeo+Q 003YT]0*H

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
71	192.168.2.3	50050	20.82.210.154	443	C:\Users\user\l\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:40 UTC	9160	OUT	POST /v3/Delivery/Events/Impression HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Content-Length: 1516 Content-Type: text/plain; charset=UTF-8 Host: arc.msn.com Connection: Keep-Alive Cache-Control: no-cache
2022-04-08 08:03:40 UTC	9161	OUT	Data Raw: 50 49 44 3d 34 30 30 30 39 31 36 38 38 26 54 49 44 3d 37 30 30 31 32 39 37 30 32 26 43 49 44 3d 31 32 38 30 30 30 30 30 30 30 34 30 32 39 32 36 26 42 49 44 3d 31 36 36 37 32 34 34 36 34 34 26 50 47 3d 50 43 30 30 30 50 30 46 52 35 2e 30 30 30 30 30 30 49 52 54 26 54 50 49 44 3d 34 30 30 30 39 31 36 38 38 26 52 45 51 41 53 49 44 3d 35 46 34 42 36 43 38 39 42 32 43 38 34 36 36 30 39 46 33 45 31 46 35 35 33 42 42 34 38 41 33 37 26 41 53 49 44 3d 35 64 37 37 36 66 61 61 34 30 36 66 34 65 30 65 62 61 65 63 66 34 62 36 61 33 37 63 33 64 36 32 26 54 49 4d 45 3d 32 30 32 32 30 34 30 38 54 31 37 30 33 30 35 5a 26 53 4c 4f 54 3d 31 26 52 45 51 54 3d 32 30 32 32 30 34 30 38 54 30 38 30 32 32 37 26 4d 41 5f 53 63 6f 72 65 3d 32 26 50 45 52 53 49 44 3d 44 42 Data Ascii: PID=400091688&TID=700129702&CID=128000000000402926&BID=1667244644&PG=PC000P0FR 5.0000000IRT&TPID=400091688&REQASID=5F4B6C89B2C846609F3E1F553BB48A37&ASID=5d776faa406f4e0e baecf4b6a37c3d62&TIME=20220408T170305Z&SLOT=1&REQT=20220408T080227&MA_Score=2&PERSID=DB
2022-04-08 08:03:40 UTC	9162	IN	HTTP/1.1 200 OK Cache-Control: no-store, no-cache Pragma: no-cache Content-Type: application/xml; charset=utf-8 Expires: Mon, 01 Jan 0001 00:00:00 GMT Server: Microsoft-IIS/10.0 ARC-RSP-DBG: [] X-AspNet-Version: 4.0.30319 X-Powered-By: ASP.NET Strict-Transport-Security: max-age=31536000; includeSubDomains Date: Fri, 08 Apr 2022 08:03:39 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
72	192.168.2.3	50051	20.54.110.249	443	C:\Users\user\l\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:40 UTC	9193	OUT	GET /v7.0/products/lookup?alternateId=PackageFamilyName&value=AmazonVideo.PrimeVideo_pwbj9vvecjh7j&m arket=US&languages=en-US%2Cen%2Cneutral&fieldsTemplate=InstallAgent&mold=Public&oemId=Public&scmId=Public HTTP/1.1 Connection: Keep-Alive Content-Type: application/json User-Agent: Install Service MS-CV: +jUkz8/7C0maDbv2.0.2.4 Host: displaycatalog.mp.microsoft.com
2022-04-08 08:03:40 UTC	9194	IN	HTTP/1.1 200 OK Connection: close Date: Fri, 08 Apr 2022 08:03:40 GMT Content-Type: application/json; charset=utf-8 Server: Kestrel Transfer-Encoding: chunked Vary: Authorization MS-CorrelationId: 51d6eeb3-869b-42b5-9bb6-980dc59f3cf0 MS-RequestId: 887aff01-7fb9-4f74-a841-eda09d36d8c7 MS-CV: +jUkz8/7C0maDbv2.0.2.4.422988576.0.1.422988577.0.0 X-Content-Type-Options: nosniff MS-ServerId: 85 Region: neu Node: aks-systempool-37630073-vmss00002I MS-DocumentVersions: 9P6RC76MSMMJ1423

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
73	192.168.2.3	50052	40.112.88.60	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:42 UTC	9225	OUT	GET /v1/a/impression?CID=12800000000402926®ion=US&lang=EN-US&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.17134.1&mo=&cap=&EID=&&PID=400091688&UIT=P-&TargetID=700129702&AN=1667244644&PG=PC000P0FR5.0000000I&RT&REQASID=5F4B6C89B2C846609F3E1F553BB48A37&UNID=338388&ASID=5d776faa406f4e0ebaecf4b6a37c3d62&PERSID=DBDE13DC697F71846A990CDFDC016FBD&GLOBALDEVICEID=6755432004667435&LOCALID=w:472DC600-FEAB-E7F8-720D-1E33F00FD1E7&DS_EVTID=8450aad1a30f443d9720b7c7f2f80cff&DEVOSVER=10.0.17134.1&REQT=20220408T080227&TIME=20220408T170303Z&ARCRAS=&CLR=CDM HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Host: ris.api.iris.microsoft.com Connection: Keep-Alive
2022-04-08 08:03:42 UTC	9225	IN	HTTP/1.1 204 No Content Content-Length: 0 Server: Microsoft-HTTPAPI/2.0 request-id: e1be6095-270d-44eb-86cf-472ebc6c8070 Date: Fri, 08 Apr 2022 08:03:41 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
74	192.168.2.3	50053	40.112.88.60	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:42 UTC	9226	OUT	GET /v1/a/impression?CID=12800000000402926®ion=US&lang=EN-US&oem=&devFam=WINDOWS.DESKTOP&ossku=PROFESSIONAL&cmdVer=10.0.17134.1&mo=&cap=&EID=&&PID=400091688&UIT=P-&TargetID=700129702&AN=1667244644&PG=PC000P0FR5.0000000I&RT&REQASID=5F4B6C89B2C846609F3E1F553BB48A37&UNID=338388&ASID=5d776faa406f4e0ebaecf4b6a37c3d62&PERSID=DBDE13DC697F71846A990CDFDC016FBD&GLOBALDEVICEID=6755432004667435&LOCALID=w:472DC600-FEAB-E7F8-720D-1E33F00FD1E7&DS_EVTID=8450aad1a30f443d9720b7c7f2f80cff&DEVOSVER=10.0.17134.1&REQT=20220408T080227&TIME=20220408T170303Z&ARCRAS=&CLR=CDM HTTP/1.1 Accept-Encoding: gzip, deflate User-Agent: WindowsShellClient/9.0.40929.0 (Windows) Host: ris.api.iris.microsoft.com Connection: Keep-Alive
2022-04-08 08:03:42 UTC	9226	IN	HTTP/1.1 204 No Content Content-Length: 0 Server: Microsoft-HTTPAPI/2.0 request-id: 9803d7ab-0499-4a37-ad20-680d627da505 Date: Fri, 08 Apr 2022 08:03:41 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
75	192.168.2.3	50054	204.79.197.200	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:46 UTC	9227	OUT	POST /threshold/xls.aspx HTTP/1.1 Origin: https://www.bing.com Referer: https://www.bing.com/AS/API/WindowsCortanaPane/V2/Init Content-type: text/xml X-MSEdge-ExternalExpType: JointCoord X-MSEdge-ExternalExp: d-thshld39,d-thshld42,d-thshld77,d-thshld78,d-thshldspcl40 X-PositionerType: Desktop X-Search-CortanaAvailableCapabilities: CortanaExperience,SpeechLanguage X-Search-SafeSearch: Moderate X-Device-MachineId: {A2AB526A-D38D-4FC9-8BA0-E34B8D6354E8} X-UserAgeClass: Unknown X-BM-Market: US X-BM-DateFormat: M/d/yyyy X-CortanaAccessAboveLock: false X-Device-OSSKU: 48 X-BM-DTZ: -480 X-BM-FirstEnabledTime: 132061295966656129 X-DeviceID: 0100748C09004E33 X-BM-DeviceScale: 100 X-Search-TimeZone: Bias=480; StandardBias=0; TimeZoneKeyName=Pacific Standard Time X-BM-Theme: 000000;0078d7 X-BM-DeviceDimensionsLogical: 1232x1024 X-BM-DeviceDimensions: 1232x1024 X-Search-RPSToken: t%3DEwDYAkR8BAAUcvamItSE/vUHpyZRp3BeyOJJPQDsAAVSBzJQ7SndUQxOscvEa3/5SXdkPufL/GUOE9StMSHM%2BBv9BrCWOBuPACB/HvUBkHG7KqfXcp/OICf0lNBepJeoZa/GhlnRKT2FV03lZcos5CD4i7bvSYXXyOXXV1aW2K6HZoPv6/fuJEL9ByKw8yy5thHZadWohgCAyM8AddCJzw7SYR3ef8oUGrfcldQPbBgSsdjq1CgKG9qBcdhnJtbRLxzzqdWfsOiachqgglOI30fXHosrPc6JWkyg/0sefV2HxnxO48CiVNvyxZCKbAdRckucw9OWft228cz9xjjqx16ae9VAbs34gwpj%2BmRdyRWE%2B4NoTo3%2BSYTKZHwqp5xwYDZgAACDyXdYmos%2BHwqAEGhsAMzqUuSzN8aKnKgfszMilfZc9tCWVFSWusnQfpFI7m9uFOD2scDPcid%2BT3%2BORhjJSS0hBMof9q%2Bn9njmJoRz08pOZNg7nqHZHk2h9FKr600KqWUY65b2ylFh0itZo8VUANAPfFe25fdCAGKopLHGWyi49hwhaoptCWef37t8l3U9m1A1WqiUYLjlsrq1fEMaM1vIW2w744bAFfECcDqstLM6n%2BljSJRwamgBTds654u/UHQ7U7Gm3ZPa680vBOI%2BFPVCDhte1NbaKSeDqJOHuxnLf8baSue%2BFj/RQJAXvgrym9Q9Ui9tUVy%2B/rEUubo6sZu4Y Cv55BMRTdFINRsmAl0z7%2BuBcTZHvgOM61YMIprvdkgeuMviej3UUXkGkhjO8YDaaZQvWpokXPXRyzyQDMoySC9XL3PP0FKRw528uwLo6KKQ65awOvWkNtEgi8SbEjjn5D29jFNwGDTz9DHIRtlmrrCq72pZP/Kz4gWxgiTqsJX0dlQkJdGhrX%2BjmYBa62uHPuh5aaCjX/mS7umGCAB4Yv9KMn/9EoRr8xhPT7oaMFJ5E1AE%3D%26p%3D X-Agent-Deviceld: 0100748C09004E33 X-BM-CBT: 1646757043 X-Device-isOptin: true X-Device-Touch: false X-Device-ClientSession: A8428518F8734E219844F3AB426417E3 X-Search-AppId: Microsoft.Windows.Cortana_cw5n1h2txyewy!CortanaUI X-BM-ClientFeatures: pbitecpdisabled,AmbientWidescreen,rs1musicprod,CortanaSPAXamlHeader Accept: /* Accept-Language: en-US Accept-Encoding: gzip, deflate, br User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Cortana 1.10.7.17134; 10.0.0.0.17134.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134 Host: www.bing.com Content-Length: 76344 Connection: Keep-Alive Cache-Control: no-cache Cookie: MUID=1E17B9B70E9B4C6E957D159ED3646FFF; _SS=CPID=1649437283858&AC=1&CPH=4ef661f2; S RCHUID=V=2&GUID=C051922770D44EDAB6B540D172E9CCE7&dmnchg=1; BM-Identity-Error=3002; SRCHD=A F=NOFORM; SUID=M; SRCHUSR=DOB=20220408; SRCHHPGUSR=SRCHLANGE=en; ANON=A=E6EAEF30D7E9C145923C068AFFFFF; MUIDB=1E17B9B70E9B4C6E957D159ED3646FF
2022-04-08 08:03:46 UTC	9229	OUT	Data Raw: 3c 43 6c 69 65 6e 74 49 6e 73 74 52 65 71 75 65 73 74 3e 3c 43 49 44 3e 31 34 44 35 41 36 39 41 42 45 46 46 36 39 36 32 30 31 34 35 41 44 30 35 42 46 43 37 36 38 35 38 3c 2f 43 49 44 3e 3c 45 76 65 6e 74 73 3e 3c 45 3e 3c 54 3e 45 76 65 6e 74 2e 43 49 51 75 65 75 65 45 72 72 6f 72 3c 2f 54 3e 3c 49 47 3e 38 33 63 61 66 37 65 37 64 30 6 2 34 35 63 65 61 35 64 37 62 32 35 33 31 39 63 34 31 30 63 33 3c 2f 49 47 3e 3c 44 3e 3c 21 5b 43 44 41 54 41 5b 7b 22 43 75 72 55 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 62 69 6e 67 2e 63 6f 6d 2f 41 53 2f 41 50 49 2f 57 69 6e 6 4 6f 77 73 43 6f 72 74 61 6e 61 50 61 6e 65 2f 56 32 2f 49 6e 69 74 22 2c 22 50 69 76 6f 74 22 3a 22 51 46 22 2c 22 43 4 6 22 3a 22 70 62 69 74 63 70 64 69 73 61 62 6c 65 64 2c 41 6d 62 Data Ascii: <ClientInstRequest><CID>14D5A69ABEFF69620145AD05BFC76858</CID><Events><E><T>Event.CIQueu eError</T><IG>83caf7e77d0b45cea5d7b25319c410c3</IG><D><![CDATA[["CurUrl": "https://www.bing.com/AS/AP I/WindowsCortanaPane/V2/Init", "Pivot": "QF", "CF": "pbitecpdisabled,Amb
2022-04-08 08:03:46 UTC	9245	OUT	Data Raw: 4e 61 6d 65 22 3a 22 76 32 2e 38 22 2c 22 53 56 22 3a 22 34 22 2c 22 50 22 3a 7b 22 43 22 3a 37 2c 22 4e 22 3a 32 2c 22 49 22 3a 22 34 72 74 22 2c 22 53 22 3a 22 4d 54 2b 55 22 2c 22 4d 22 3a 22 56 2b 4c 2b 4d 2b 4d 54 2b 45 2b 4e 2b 43 2b 4b 2b 42 44 22 2c 22 54 22 3a 31 31 39 33 39 2c 22 4b 22 3a 22 38 6c 6d 2b 38 6d 65 2b 38 71 69 2b 39 37 68 2b 38 68 68 2b 38 6a 71 2b 38 6d 64 2b 38 6d 6e 2b 38 6f 6f 22 2c 22 46 22 3a 31 7d 2c 22 4c 22 3a 22 40 66 2f 39 2f 44 49 56 23 53 57 2f 2f 30 2f 35 30 2f 39 6b 2f 31 30 2f 61 2f 54 2f 2d 31 2b 40 66 2f 61 2f 44 49 56 23 67 72 31 31 2f 2f 30 2f 34 34 2f 39 6b 2f 77 2f 39 2f 54 2f 2d 31 2b 40 66 2f 62 2f 40 32 2f 2f 30 2f 34 34 2f 39 6b 2f 31 77 2f 37 2f 4d 54 2f 2d 31 2b 40 67 2f 63 2f 49 4d 47 2f 2f 73 2f 33 36 Data Ascii: Name": "v2.8", "SV": "4", "P": { "C": "7", "N": "2", "I": "4rt", "S": "MT+U", "M": "V+L+M+MT+E+N+C+K+BD", "T": "11939, "K ": "8lm+8me+8qi+97h+8hh+8jq+8md+8mn+8oo", "F": "1", "L": "@f/9/DIV#SW/0/50/9k/10/a/T/-1+@f/a/DIV#gr11/0/44/9k/w/9/ T/-1+@f/b/@2/0/44/9k/1w/7/MT/-1+@g/c/IMG/ls/36
2022-04-08 08:03:46 UTC	9261	OUT	Data Raw: 6f 6d 2f 41 53 2f 41 50 49 2f 57 69 6e 64 6f 77 73 43 6f 72 74 61 6e 61 50 61 6e 65 2f 56 32 2f 49 6e 69 74 22 2c 22 50 69 76 6f 74 22 3a 22 51 46 22 2c 22 43 46 22 3a 22 70 62 69 74 63 70 64 69 73 61 62 6c 65 64 2c 41 6d 62 69 65 6e 74 57 69 64 65 73 63 72 65 65 6e 2c 72 73 31 6d 75 73 69 63 70 72 6f 64 2c 43 6f 72 74 61 6e 61 53 50 41 58 61 6d 6c 48 65 61 64 65 72 22 2c 22 65 72 72 6f 72 54 79 70 65 22 3a 22 53 65 6e 64 54 69 6d 65 64 4f 75 74 22 2c 22 66 61 69 6c 43 6f 75 6e 74 22 3a 31 2c 22 54 53 22 3a 31 36 34 36 37 35 37 30 35 33 35 33 35 2c 22 52 54 53 22 3a 31 30 3 6 33 30 2c 22 53 45 51 22 3a 33 2c 22 55 54 53 22 3a 31 36 34 39 34 33 37 34 32 35 39 39 30 7d 5d 5d 3e 3c 2f 44 3e 3c 54 53 3e 31 36 34 36 37 35 37 30 35 33 35 33 35 3c 2f 54 53 3e 3c Data Ascii: om/AS/API/WindowsCortanaPane/V2/Init", "Pivot": "QF", "CF": "pbitecpdisabled,AmbientWidescreen.rs1music prod,CortanaSPAXamlHeader", "errorType": "SendTimedOut", "failCount": "1", "TS": "1646757053535", "RTS": "10630", "SEQ": "3", "UTS": "1649437425990"...</D><TS>1646757053535</TS><

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:46 UTC	9277	OUT	Data Raw: 44 41 54 41 5b 7b 22 43 75 72 55 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 62 69 6e 67 2e 63 6f 6d 2f 41 53 2f 41 50 49 2f 57 69 6e 64 6f 77 73 43 6f 72 74 61 6e 61 50 61 6e 65 2f 56 32 2f 49 6e 69 74 22 2c 22 50 69 76 6f 74 22 3a 22 51 46 22 2c 22 43 46 22 3a 22 70 62 69 74 63 70 64 69 73 61 62 6c 65 64 2c 41 6d 62 69 65 6e 74 57 69 64 65 73 63 72 65 65 6e 2c 72 73 31 6d 75 73 69 63 70 72 6f 64 2c 43 6f 72 74 61 6e 61 53 50 41 58 61 6d 6c 48 65 61 64 65 72 22 2c 22 45 6e 72 69 63 68 65 64 43 6c 69 65 6e 74 49 6e 66 6f 22 3a 7b 22 4d 55 49 44 22 3a 22 31 45 31 37 42 39 42 37 30 45 39 42 34 43 36 45 39 35 37 44 31 35 39 45 44 33 36 34 36 46 46 46 22 2c 22 41 43 56 65 72 22 3a 22 34 65 66 36 36 31 66 32 22 2c 22 46 44 50 61 72 74 6e 65 72 45 6e 74 Data Ascii: DATA[{"CurUrl":"https://www.bing.com/AS/API/WindowsCortanaPane/V2/Init","Pivot":"QF","CF":"pbitecpd isabled,AmbientWidescreen,rs1musicprod,CortanaSPAXamlHeader","EnrichedClientInfo":{"MUID":"1E17B9B70E9B4C6E957D159ED3646FFF","ACVer":"4ef661f2","FDPartnerEnt
2022-04-08 08:03:46 UTC	9293	OUT	Data Raw: 49 64 22 3a 22 53 54 48 5f 38 64 30 36 66 38 33 63 2d 64 61 35 38 2d 34 63 30 32 2d 38 66 65 38 2d 62 61 32 63 30 34 39 64 39 38 30 39 22 7d 7d 2c 7b 22 54 22 3a 22 44 2e 53 54 22 2c 22 41 70 70 4e 53 22 3a 22 53 6d 61 72 74 53 65 61 72 63 68 22 2c 22 53 65 72 76 69 63 65 22 3a 22 41 75 74 6f 53 75 67 67 65 73 74 22 2c 22 53 63 65 6e 61 7 2 69 6f 22 3a 22 53 54 22 2c 22 53 43 22 3a 34 2c 22 44 53 22 3a 5b 7b 22 54 22 3a 22 44 2e 55 72 6c 22 2c 22 4b 22 3a 31 30 30 31 2c 22 51 22 3a 22 43 68 65 63 6b 20 66 6f 72 20 75 70 64 61 74 65 73 22 2c 22 4d 51 22 3a 22 75 70 64 61 74 65 73 22 2c 22 56 61 6c 22 3a 22 53 54 22 2c 22 48 6f 22 3a 32 2c 22 47 72 22 3a 31 2c 22 44 65 76 69 63 65 53 69 67 6e 61 6c 73 22 3a 7b 22 52 61 6e 6b 22 3a 36 30 39 37 2c 22 50 48 69 Data Ascii: Id":"STH_8d06f83c-da58-4c02-8fe8-ba2c049d9809"}},{ "T":"D.ST","AppNS":"SmartSearch","Service":"Auto Suggest","Scenario":"ST","SC":4,"DS":{"T":"D.Url","K":1001,"Q":"Check for updates","MQ":"updates","Val":"ST","Ho":2,"Gr ":1,"DeviceSignals":{"Rank":6097,"Phi
2022-04-08 08:03:46 UTC	9304	IN	HTTP/1.1 204 No Content Access-Control-Allow-Origin: * X-Cache: CONFIG_NOCACHE Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version X-MSEdge-Ref: Ref A: 1DB273A35AE14AF4BDEF758C6C79AABC Ref B: FRA31EDGE0612 Ref C: 2022-04-08T08:03:46Z Date: Fri, 08 Apr 2022 08:03:46 GMT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.2.3	50055	20.199.120.182	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:03:55 UTC	9304	OUT	Data Raw: 43 4e 54 20 31 20 43 4f 4e 20 32 34 36 0d 0a 43 6f 6e 74 65 78 74 3a 20 63 65 30 34 38 62 38 62 33 36 62 35 38 39 62 34 0d 0a 0d 0a Data Ascii: CNT 1 CON 246Context: ce048b8b36b589b4
2022-04-08 08:03:55 UTC	9304	OUT	Data Raw: 3c 63 6f 6e 6e 65 63 74 3e 3c 76 65 72 3e 32 3c 2f 76 65 72 3e 3c 61 67 65 6e 74 3e 3c 6f 73 3e 57 69 6e 64 6f 77 73 3c 2f 6f 73 3e 3c 6f 73 56 65 72 3e 3c 70 72 6f 63 3e 78 36 34 3c 2f 70 72 6f 63 3e 3c 6c 63 69 64 3e 65 6e 2d 55 53 3c 2f 6c 63 69 64 3e 3c 67 65 6f 49 64 3e 32 34 34 3c 2f 67 65 6f 49 64 3e 3c 61 6f 61 63 3e 30 3c 2f 61 6f 61 63 3e 3c 64 65 76 69 63 65 54 79 70 65 3e 31 3c 2f 64 65 76 69 63 65 54 79 70 65 3e 3c 64 65 76 69 63 65 4e 61 6d 65 3e 56 4d 77 61 72 65 37 2c 31 3c 2f 64 65 76 69 63 65 4e 61 6d 65 3e 3c 2f 61 67 65 6e 74 3e 3c 2f 63 6f 6e 6e 65 63 74 3e Data Ascii: <connect><ver>2</ver><agent><os>Windows</os><osVer>10.0.0.0.17134</osVer><proc>x64</proc><lcid>en-US</lcid><geold>244</geold><aoac>0</aoac><deviceType>1</deviceType><deviceName>VMware7,1</deviceName></agent></connect>
2022-04-08 08:03:55 UTC	9305	OUT	Data Raw: 41 54 48 20 32 20 43 4f 4e 5c 44 45 56 49 43 45 20 31 30 31 34 0d 0a 43 6f 6e 74 65 78 74 3a 20 63 65 30 34 38 62 38 62 33 36 62 35 38 39 62 34 0d 0a 0d 0a 3c 64 65 76 69 63 65 3e 3c 63 6f 6d 70 61 63 74 2d 74 69 63 6b 65 74 3e 74 3d 45 77 43 6f 41 75 70 49 42 41 41 55 31 62 44 47 66 64 61 7a 69 44 66 58 70 6a 4e 35 4e 36 63 59 68 54 31 77 62 6d 51 41 41 51 77 65 75 52 78 64 54 45 52 58 49 34 58 73 61 55 64 61 66 67 57 47 68 6d 46 42 32 63 6a 51 30 2b 6c 52 4d 56 52 66 4d 58 33 46 77 79 4e 35 6e 68 5a 42 49 69 50 59 61 52 4e 51 2f 64 77 71 38 33 2f 58 59 37 5a 42 55 72 6d 54 65 77 44 66 6a 2f 57 6d 4f 6e 51 35 6b 4e 32 56 76 44 35 75 46 4d 37 47 6a 4c 78 56 73 37 55 78 36 70 69 69 71 41 6d 6c 4d 6d 4e 7a 57 34 6d 36 7a 78 2f 52 66 32 38 74 48 6b 4a 46 73 Data Ascii: ATH 2 CON\DEVICE 1014Context: ce048b8b36b589b4<device><compact-ticket>t=EwCoAupIBAAU1bDG fdaziDfXpjN5N6cYhT1wbmQAAQweuRxdTERXl4XsaUdafgWGHmFB2cjQ0+HRMVRfMX3FwyN5nhZBIiPYaRNQ/dwq83 /XY7ZBUrmTewDfj/WmOnQ5kN2VvD5uFM7GjLxVs7Ux6piiqAmIMmNzW4m6zx/Rf28thkJFs
2022-04-08 08:03:55 UTC	9306	OUT	Data Raw: 42 4e 44 20 33 20 43 4f 4e 5c 51 4f 53 20 32 39 0d 0a 43 6f 6e 74 65 78 74 3a 20 63 65 30 34 38 62 38 62 33 36 62 35 38 39 62 34 0d 0a 0d 0a Data Ascii: BND 3 CON\QOS 29Context: ce048b8b36b589b4
2022-04-08 08:03:55 UTC	9306	IN	Data Raw: 32 30 32 20 31 20 43 4f 4e 20 35 38 0d 0a Data Ascii: 202 1 CON 58
2022-04-08 08:03:55 UTC	9306	IN	Data Raw: 4d 53 2d 43 56 3a 20 32 64 66 6c 33 38 46 32 45 30 4b 4c 72 41 2f 6f 37 39 71 36 61 77 2e 30 0d 0a 0d 0a 50 61 79 6c 6f 61 64 20 70 61 72 73 69 6e 67 20 66 61 69 6c 65 64 2e Data Ascii: MS-CV: 2df138F2E0KLrA079q6aw.0Payload parsing failed.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49987	20.82.210.154	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:27 UTC	34	OUT	GET /v3/Delivery/Placement?pubid=da63df93-3dbc-42ae-a505-b34988683ac7&pid=338388&adm=2&w=1&h=1&wpx=1&hpx=1&fmt=json&cltp=app&dim=le&rafb=0&nct=1&pm=1&cfmt=text,image,poly&sft=jpeg,png,gif&topt=1&poptin=0&localid=w:472DC600-FEAB-E7F8-720D-1E33F00FD1E7&ctry=US&time=20220408T170226Z&lc=en-US&pl=en-US&idtp=mid&uid=4388269c-b420-4134-ac19-bc7ca8a19ac1&aid=00000000-0000-0000-0000-000000000000&ua=WindowsShellClient%2F9.0.40929.0%20%28Windows%29&asid=5f4b6c89b2c846609f3e1f553bb48a37&ctmode=MultiSession&arch=x64&cdm=1&cdmver=10.0.17134.1&devfam=Windows.Desktop&devform=Unknown&devosver=10.0.17134.1&disp horzres=1280&dispsize=17.1&dispvertres=1024&isu=0&lo=1463022&metered=false&nettype=ethernet&npid=sc-338388&oemName=hsehht%2C%20Inc.&oemid=hsehht%2C%20Inc.&ossku=Professional&rver=2&smBiosDm=hsehht%2C1&tl=2&tsu=1463022&waasBldFlt=1&waasCfgExp=1&waasCfgSet=1&waasRetail=1&waasRing= HTTP/1.1 Accept-Encoding: gzip, deflate X-SDK-CACHE: chs=0&imp=0&chf=0&ds=50583&fs=32319&sc=6 X-SDK-HW-TOKEN: t=EwDYAppeBAAUIAKXDAoFTQM+n+MaRVFKZh/ehWgAAdVW0iu23GlXjRyUBGA+V5LMoU/IMaTj obBnQosoTe6w300ZEF3HulBKeYXog3CqxSfjOHeF/J4iLS/gKyhq/ZV/xtrYHZ35PhcBmS2qzlwNBiXp0+I4efq5ns DEEEESQ06VT9dPxpHYgWIFLG65LRysydA1IM9dDPzftFvDLM/ickJDFevqkA3hG2mKV46lqHL4CT7eP4Hk0/MORp8JB 5tewfjl7o25TIEcXI9Ohbx1KlwUuqQcpj0nfDAUZEjkQqVS2z/wQaH+/fdlFO/AoxQI3Cbc0TeaCp3XlesBJX0bxVN zc22qQqCPfGWQ/Sb52rGvkBRvdW8DFg8ToMjfQpYDZgAAcE3mODPOPAwVqAFPV53gZZc0aOkGu+JjWn w46hEU9aCKlpEDkH6SywZSQt+Z6lyumM/ZCz1/Exb6MZih9PGVRFV0dS4rZOFTTSEXw5x6gJoWeqkIJZJquL/LQNZp daM/TGNQWWhUnnbhyzuL3J52vftSZZAtC6HDDHutfCP567luQfNJw1zOBQg/Pho8+d+FIHWtcPKMXaDH+rX7PpflRpHT m7bd+I+rsPvLvdstjafDcGAADV0pkaM4oU0n35rzdjzoAWTcazcHXkrs0Gr34gDLPkE96nUwLpeDlXN3LOntP44gHn gFTJAav4io7zKxVkmOUwHoTarQK7POiXKiwa8x1QRMWrij0xK5k34eIR6SWW4uOhaTcVnkJxlUvc2iz/sxwS6ZoJu zJ60lCbcq6ptimZGdy/yulx2CKNYcUG/nBNXbdKtF3Kz0nMb3Ry9n0QIm/ncP9d68+s4WiRlc+RuW5MPI3aHMGgt2s nchu87pA34+QQKDXqPJVZnC+RaoA8mYS8BGPqZ//PidcqGGmwz2vccoT1N6pSAD7mXPm9QONX68BD3 4uYAk1VCPPhRpsKh41QE=&p= Cache-Control: no-cache MS-CV: BYqskdYKuUKf7ZeJ.0 User-Agent: WindowsShellClient/9.0.40929.0 (Windows) X-SDK-HWF: tch0,m301,m751,mA01,mT01 Host: arc.msn.com Connection: Keep-Alive
2022-04-08 08:02:27 UTC	36	IN	HTTP/1.1 200 OK Cache-Control: no-store, no-cache Pragma: no-cache Content-Length: 4481 Content-Type: application/json; charset=utf-8 Expires: Mon, 01 Jan 0001 00:00:00 GMT Server: Microsoft-IIS/10.0 ARC-RSP-DBG: [{"RADIDS":"","1,P400091688-T700129702-C128000000000402926+B+P20+S1"},"{"OPTOUTST ATE":"","256"}] X-ARC-SIG: VD4O9BkESblBx60f1cBmGuMM2uj8Kq0b/vUJ27/y6foRFXMT19pK8EOASr689fmykp+9aonifo5/MaVZ kdg9hi7MgstWV8iFe2nXKHD57Oo+TiCi37X0AVmVx7L8vT7Q1tp+URr4DDzubSDW8v+sJJXnciC1GCC5VFPEl1nvm w4Dow3BjhXF8/4SszyGDafm+AjmAU8Pott2vLH819o8T+e8msblSoXLbv0m23cZRyqQCldBFoPdQzrBaNzJtRBpwzl Ve06ZrJPB4QAtcuZoaVs4U3ysSE+nykNlyuMRgfwmqOgFGjdssNFBaLmZ+GtpHmPo98urtvsyn/19A6ijjQ== Accept-CH: UA, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform, UA-Platform-Version X-AspNet-Version: 4.0.30319 X-Powered-By: ASP.NET Strict-Transport-Security: max-age=31536000; includeSubDomains Date: Fri, 08 Apr 2022 08:02:27 GMT Connection: close
2022-04-08 08:02:27 UTC	37	IN	Data Raw: 7b 22 62 61 74 63 68 72 73 70 22 3a 7b 22 76 65 72 22 3a 22 31 2e 30 22 2c 22 69 74 65 6d 73 22 3a 5b 7b 22 69 74 65 6d 22 3a 22 7b 5c 22 66 5c 22 3a 5c 22 72 61 66 5c 22 2c 5c 22 76 5c 22 3a 5c 22 31 2e 30 5c 22 2c 5c 22 72 64 72 5c 22 3a 5b 7b 5c 22 63 5c 22 3a 5c 22 43 44 4d 5c 22 2c 5c 22 75 5c 22 3a 5c 22 53 75 62 73 63 72 69 62 65 6 4 43 6f 6e 74 65 6e 74 5c 22 7d 5d 2c 5c 22 61 64 5c 22 3a 7b 5c 22 63 6c 61 73 73 5c 22 3a 5c 22 63 6f 6e 74 65 6e 74 5c 22 2c 5c 22 63 6f 6c 6c 65 63 74 69 6f 6e 73 5c 22 3a 5b 5d 2c 5c 22 69 74 65 6d 50 72 6f 70 65 72 74 79 4d 61 6e 69 66 65 73 74 5c 22 3a 7b 5c 22 74 65 6d 70 6c 61 74 65 54 79 70 65 5c 22 3a 7b 5c 22 74 79 70 65 5c 22 3a 5c 22 74 65 78 74 5c 22 7d 2c 5c 22 6f 6e 52 65 6e 64 65 72 5c 22 3a 7b 5c 22 74 Data Ascii: {"batchrsp":{"ver":"1.0","items":[{"item":{"f":"rafi","v":"1.0"},"rdrt":{"l":"CDMI","u":"SubscribedCont entl"}}, {"ad":{"class":"content","collections":[""],"itemPropertyManifest":{"templateType":{"type":"text"},"onRender": {"t

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49988	20.82.210.154	443	C:\Users\user\Desktop\ll.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2022-04-08 08:02:28 UTC	67	OUT	GET /v3/Delivery/Placement?pubid=da63df93-3dbc-42ae-a505-b34988683ac7&pid=338389&adm=2&w=1&h=1&wpx=1&hpx=1&fmt=json&cltp=app&dim=le&rafb=0&nct=1&pm=1&cfmt=text,image,poly&sft=jpeg,png,gif&topt=1&poptin=0&localid=w:472DC600-FEAB-E7F8-720D-1E33F00FD1E7&ctry=US&time=20220408T170227Z&lc=en-US&pl=en-US&idtp=mid&uid=4388269c-b420-4134-ac19-bc7ca8a19ac1&aid=00000000-0000-0000-0000-000000000000&ua=WindowsShellClient%2F9.0.40929.0%20%28Windows%29&asid=19c443aabf954506a4b84500aa0b4498&ctmode=MultiSession&arch=x64&cdm=1&cdmver=10.0.17134.1&devfam=Windows.Desktop&devform=Unknown&devosver=10.0.17134.1&disp horzres=1280&dispsize=17.1&dispvertres=1024&isu=0&lo=1463022&metered=false&nettype=ethernet&npid=sc-338389&oemName=hsehht%2C%20Inc.&oemid=hsehht%2C%20Inc.&ossku=Professional&smBiosDm=hsehht7%2C1&tl=2&tsu=1463022&waasBldFlt=1&waasCfgExp=1&waasCfgSet=1&waasRetail=1&waasRing= HTTP/1.1 Accept-Encoding: gzip, deflate X-SDK-CACHE: cid=128000000001627409&chs=0&imp=0&chf=0&ds=50583&fs=32319&sc=6 X-SDK-HW-TOKEN: t=EwDYAppeBAAUIAKXDAoFTQM+n+MaRVFKzH/ehWgAAdVW0iu23GlXjRyUBGA+V5LMOU/IMaTj obBnQosoTe6w30OZEf3HulBKeYXog3CqxSfjOHeF/J4iLS/gKyhq/ZV/xtrYHZ35PhcBmS2qzlwNBiXp0+I4efq5ns DEEEESQ06VT9dPxHYgWIFLG65LRysydA1IM9dDPzftFvDLM/ickJDFevqkA3hG2mKV46lqHL4CT7eP4Hk0/MORp8JB 5tew/fjl7o25TIEcXI9Ohbx1KlwUuqQcpj0nfDAUZEjkQqVS2z/wQaH+/fdlFO/AoxQI3Cbc0TeaCp3XlesBJX0bxVN zc22qQcPfGWQ/Sb52rGvkgBRvdW8DFg8ToMjfQpYDZgAAcE3mODPOPAwVqAFPV53gZZc0aOkGu+jJWn w46hEU9aCKlpEDkH6SywZSQt+Z6lyumM/ZCz1/Exb6MZih9PGVRFV0dS4rZOFTTSEXw5x6gJoWeqkJZJquL/LQNZp daM/TGNQWWhUnnbhyzuL3J52vTsZzAtC6HDHUtfcP567luQfNJw1zOBQG/Pho8+d+FIHwtkPKMXaDH+X7PpflRpHT m7bd+I+rsPvLvdstjafDcGAADV0pkaM4oU0n35rzdjzoAWTcazcHXkrs0Gr34gDLPkE96nUwLpeDlXN3LOntP44gHn gFTJAvz4io7zKxVkmOUwHoTarQK7POiXKiwa8x1QRMWrij0xK5k34eIR6SWW4uOhaTkCvknjxlUvc2iz/sxwQS6ZoJu zJ60lcBcq6ptimZGdy/yulx2CKNYcUG/nBNXbdKtF3Kz0nMb3Ry9n0QlIm/ncP9d68+s4WiRlc+RuW5MPI3aHMGgt2s nchu87pA34+QQKDXqPJVZnZc+RaoA8mYS8BGPqZ//PidcqGgmzw2vccoT1N6pSAD7mXPym9QONX68BD3 4uYAk1VCPPhRpsKh41QE=&p= Cache-Control: no-cache MS-CV: BYqskdYKuUKf7ZeJ.0 User-Agent: WindowsShellClient/9.0.40929.0 (Windows) X-SDK-HWF: tch0,m301,m751,mA01,mT01 Host: arc.msn.com Connection: Keep-Alive
2022-04-08 08:02:28 UTC	69	IN	HTTP/1.1 200 OK Cache-Control: no-store, no-cache Pragma: no-cache Content-Length: 3067 Content-Type: application/json; charset=utf-8 Expires: Mon, 01 Jan 0001 00:00:00 GMT Server: Microsoft-IIS/10.0 ARC-RSP-DBG: [{"RADIDS":"","1,P425116219-T700333446-C128000000001627409+B+P10+S1"},{"OPTOUTST ATE":"","256"}] X-ARC-SIG: ceFbxwQIPsk2VUOjFT/2SElGq4kbjxH8r1U7pK0kug3QxBt8bGcGieps7/hhh/Jre1sQPC7XJ/NtVlvi6+wyRhw jqCcAklyOpKg+sanJp7DsfGyryJPuPoi6v7n1g933MCO+BJ8FlgSbtizkyNWNuppUuOHVaxl2xS7srcc48AV770iR UIIMJ60SSk9q24pf+C9v67qvrfdWmPfbfHe9ugWftctLrcjbovtUfBd43dd45ISmrlQNgkuZRMjKskEmdJbsv+O/rT RMiUaLqC76Toe+knsWs/5Ezq9w34zYvbgbfrVGjaD3QKFfHEI9kmKi6taRcW5ulj1Bc03FEJA== Accept-CH: UA, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform, UA-Platform-Version X-AspNet-Version: 4.0.30319 X-Powered-By: ASP.NET Strict-Transport-Security: max-age=31536000; includeSubDomains Date: Fri, 08 Apr 2022 08:02:27 GMT Connection: close
2022-04-08 08:02:28 UTC	70	IN	Data Raw: 7b 22 62 61 74 63 68 72 73 70 22 3a 7b 22 76 65 72 22 3a 22 31 2e 30 22 2c 22 69 74 65 6d 73 22 3a 5b 7b 22 69 74 65 6d 22 3a 22 7b 5c 22 66 5c 22 3a 5c 22 72 61 66 5c 22 2c 5c 22 76 5c 22 3a 5c 22 31 2e 30 5c 22 2c 5c 22 72 64 72 5c 22 3a 5b 7b 5c 22 63 5c 22 3a 5c 22 43 44 4d 5c 22 2c 5c 22 75 5c 22 3a 5c 22 53 75 62 73 63 72 69 62 65 6 4 43 6f 6e 74 65 6e 74 5c 22 7d 5d 2c 5c 22 61 64 5c 22 3a 7b 5c 22 63 6c 61 73 73 5c 22 3a 5c 22 63 6f 6e 74 65 6e 74 5c 22 2c 5c 22 63 6f 6c 6c 65 63 74 69 6f 6e 73 5c 22 3a 5b 5d 2c 5c 22 69 74 65 6d 50 72 6f 70 65 72 74 79 4d 61 6e 69 66 65 73 74 5c 22 3a 7b 5c 22 6e 6f 4f 70 5c 22 3a 7b 5c 22 74 79 70 65 5c 22 3a 5c 22 61 63 74 69 6f 6e 5c 22 7d 7d 2c 5c 22 69 74 65 6d 73 5c 22 3a 5b 7b 5c 22 70 72 6f 70 65 72 74 69 Data Ascii: {"batchrsp":{"ver":"","1.0","items":[{"item":{"f":"rafi","v":"","1.0"},"rdrt":{"c":"CDMI","u":"","SubscribedCont ent"},"ad":{"class":"","content","collections":"","itemPropertyManifest":{"noOp":{"type":"action"}},"items":{"property

Statistics

 No statistics

System Behavior

Analysis Process: ll.exe PID: 7164, Parent PID: 5608

General

Target ID:	1
Start time:	10:01:35
Start date:	08/04/2022

Path:	C:\Users\user\Desktop\ll.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ll.exe"
Imagebase:	0xf20000
File size:	179712 bytes
MD5 hash:	F746EA39C0C5FF9D0A1F2D250170AD80
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities								
File Created								
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol	
C:\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW	
C:\MSOCache\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW	
C:\PerfLogs\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW	
C:\Program Files\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW	
C:\Program Files (x86)\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW	
C:\ProgramData\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW	
C:\Recovery\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW	
C:\Users\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW	
C:\MSOCache\All Users\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW	
C:\Program Files\Common Files\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW	
C:\Program Files\Google\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW	
C:\Program Files\internet explorer\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW	
C:\Program Files\Microsoft Office\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW	
C:\Program Files\MSBuild\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW	
C:\Program Files\Reference Assemblies\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW	
C:\Program Files\Uninstall Information\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW	
C:\Program Files\UNPI\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW	
C:\Program Files (x86)\adobe\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW	
C:\Program Files (x86)\autoit3\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW	

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\bqakjno dudhbhouxlasvwtefrqplaxongjfrh ccpfknshmhilopyapddposogtd\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\common files\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\google\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\internet explorer\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\java\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\downloader\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\microsoft analysis services\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\microsoft office\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\microsoft sql server\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\microsoft.net\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\mozilla firefox\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\msbuild\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\reference assemblies\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Adobe\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\dbg\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft Help\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft OneDrive\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Oracle\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Package Cache\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\regid.1991-06.com.microsoft\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\SoftwareDistribution\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\USOPrivate\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\USOShared\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Users\Default\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files\internet explorer\SIGNUP\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files\Microsoft Office\Office16\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files\MSBuild\Microsoft\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files\Reference Ass embles\Microsoft\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files\UNP\Log\Logs\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files\UNP\UpdateNotificationMgr\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\adobe\Acrobat Reader DC\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\autoit3\Aut2Exe\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\autoit3\AutotlX\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\autoit3\Examples\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\autoit3\Extras\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\autoit3\icons\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\autoit3\Include\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\autoit3\SciTE\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\common files\Adobe\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\common files\DESIGNER\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\common files\Java\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\common files\microsoft shared\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\common files\Oracle\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\common files\Services\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\common files\system\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\google\CrashReports\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\google\Update\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\internet explorer\en- US\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\internet explorer\images\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\internet explorer\SIGNUP\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\java\jre1.8.0_211\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\downloader\config\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\microsoft analysis services\AS OLEDB\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\microsoft office\CLIPART\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\microsoft office\Document Themes 16\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\microsoft office\Office16\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\microsoft office\Stationery\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\microsoft sql server\110\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\microso ft.net\ADOMD.NET\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\microsoft.net\Primary Interop Assemblies\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\microso ft.net\RedisList\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\mozilla firefox\plugins\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\msbuild\Microsoft\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\Program Files (x86)\reference assemblies\Microsoft\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Adobe\ARM\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Adobe\Setup\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\AppV\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\Crypto\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\Device Stage\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\DeviceSync\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\Diagnosis\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\DRM\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\IdentityCRL\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\MapData\R3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\MF\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\NetFramework\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\Network\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\OFFICE\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\Provisioning\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\Search\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\Settings\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\SmsRouter\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\Spectrum\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\Speech_OneCore\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\Storage Health\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\UEV\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\User Account Pictures\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\Vault\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\WDF\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\WinMSIPC\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft\WwanSvc\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Microsoft OneDrive\setup\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Oracle\Java\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Package Cache\{050d4fc8-5d48-4b8f- 8972-47c82c46020f}\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Package Cache\{12578975-C765-4BDF- 8DDC-3284BC0E855F}\v14.21.27702\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Package Cache\{13A4EE12-23EA-3371- 91EE-EFB36DDFFF3E}\v12.0.21005\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Package Cache\{19F7E289-17B8-44EC- A099-927507B6F739}\v14.21.27702\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Package Cache\{213668DB-2263-4E2D- ABB8-487FD539130E}\v14.21.27702\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Package Cache\{33d1fd90-4274-48a1- 9bc1-97e33d9c2d6f}\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Package Cache\{37B8F9C7-03FB-3253-8781-2517C99D7C00}\v11.0.61030\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Package Cache\{49697869-be8e-427d-81a0-c334d1d14950}\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Package Cache\{929FBD26-9020-399B-9A7A-751D61F0B942}\v12.0.21005\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW
C:\ProgramData\Package Cache\{A749D8E6-B613-3BE3-8F5F-045C84EBA29B}\v12.0.21005\IR3ADM3.txt	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	F35875	CreateFileW

File Moved						
Old File Path	New File Path	Completion	Count	Source Address	Symbol	
C:\bootTel.dat	C:\bootTel.dat.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\Program Files\desktop.ini	C:\Program Files\desktop.ini.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\Program Files (x86)\desktop.ini	C:\Program Files (x86)\desktop.ini.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\Users\desktop.ini	C:\Users\desktop.ini.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\Program Files (x86)\Autolt3\Au3Check.dat	C:\Program Files (x86)\autoit3\Au3Check.dat.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\Program Files (x86)\Autolt3\Autolt v3 Website.url	C:\Program Files (x86)\autoit3\Autolt v3 Website.url.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\Program Files (x86)\Autolt3\Autolt.chm	C:\Program Files (x86)\autoit3\Autolt.chm.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\ProgramData\Microsoft Help\MS.DATABASECOMPARE.16.1033.hxn	C:\ProgramData\Microsoft Help\MS.DATABASECOMPARE.16.1033.hxn.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\ProgramData\Microsoft Help\MS.EXCEL.16.1033.hxn	C:\ProgramData\Microsoft Help\MS.EXCEL.16.1033.hxn.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\ProgramData\Microsoft Help\MS.GRAPH.16.1033.hxn	C:\ProgramData\Microsoft Help\MS.GRAPH.16.1033.hxn.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\ProgramData\Microsoft Help\MS.GROOVE.16.1033.hxn	C:\ProgramData\Microsoft Help\MS.GROOVE.16.1033.hxn.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\ProgramData\Microsoft Help\MS.LYNC.16.1033.hxn	C:\ProgramData\Microsoft Help\MS.LYNC.16.1033.hxn.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\ProgramData\Microsoft Help\MS.LYNC_BASIC.16.1033.hxn	C:\ProgramData\Microsoft Help\MS.LYNC_BASIC.16.1033.hxn.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\ProgramData\Microsoft Help\MS.LYNC_ONLINE.16.1033.hxn	C:\ProgramData\Microsoft Help\MS.LYNC_ONLINE.16.1033.hxn.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\ProgramData\Microsoft Help\MS.MSACCESS.16.1033.hxn	C:\ProgramData\Microsoft Help\MS.MSACCESS.16.1033.hxn.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\ProgramData\Microsoft Help\MS.MSOUC.16.1033.hxn	C:\ProgramData\Microsoft Help\MS.MSOUC.16.1033.hxn.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\ProgramData\Microsoft Help\MS.MSPUB.16.1033.hxn	C:\ProgramData\Microsoft Help\MS.MSPUB.16.1033.hxn.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\ProgramData\Microsoft Help\MS.ONENOTE.16.1033.hxn	C:\ProgramData\Microsoft Help\MS.ONENOTE.16.1033.hxn.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\ProgramData\Microsoft Help\MS.OUTLOOK.16.1033.hxn	C:\ProgramData\Microsoft Help\MS.OUTLOOK.16.1033.hxn.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\ProgramData\Microsoft Help\MS.POWERPNT.16.1033.hxn	C:\ProgramData\Microsoft Help\MS.POWERPNT.16.1033.hxn.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\ProgramData\Microsoft Help\MS.SETLANG.16.1033.hxn	C:\ProgramData\Microsoft Help\MS.SETLANG.16.1033.hxn.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\ProgramData\Microsoft Help\MS.SKYPEFB.16.1033.hxn	C:\ProgramData\Microsoft Help\MS.SKYPEFB.16.1033.hxn.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\ProgramData\Microsoft Help\MS.SKYPEFB_BASIC.16.1033.hxn	C:\ProgramData\Microsoft Help\MS.SKYPEFB_BASIC.16.1033.hxn.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\ProgramData\Microsoft Help\MS.SKYPEFB_ONLINE.16.1033.hxn	C:\ProgramData\Microsoft Help\MS.SKYPEFB_ONLINE.16.1033.hxn.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\ProgramData\Microsoft Help\MS.SKYPEFB_ONLINEG.16.1033.hxn	C:\ProgramData\Microsoft Help\MS.SKYPEFB_ONLINEG.16.1033.hxn.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\ProgramData\Microsoft Help\MS.SPREADSHEETCOMPARE.16.1033.hxn	C:\ProgramData\Microsoft Help\MS.SPREADSHEETCOMPARE.16.1033.hxn.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\ProgramData\Microsoft Help\MS.WINWORD.16.1033.hxn	C:\ProgramData\Microsoft Help\MS.WINWORD.16.1033.hxn.NB65	success or wait	1	F2C6CB	MoveFileW	
C:\ProgramData\Microsoft Help\mslist.hxl	C:\ProgramData\Microsoft Help\mslist.hxl.NB65	success or wait	1	F2C6CB	MoveFileW	

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\regid.1991-06.com.microsoft\regid.1991-06.com.microsoft Microsoft Office Professional Plus 2016.swidtag	C:\ProgramData\regid.1991-06.com.microsoft\regid.1991-06.com.microsoft Microsoft Office Professional Plus 2016.swidtag.NB65	success or wait	1	F2C6CB	MoveFileW
C:\ProgramData\regid.1991-06.com.microsoft\regid.1991-06.com.microsoft_Windows-10-Pro.swidtag	C:\ProgramData\regid.1991-06.com.microsoft_Windows-10-Pro.swidtag.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Users\Default\NTUSER.DAT	C:\Users\Default\NTUSER.DAT.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Users\Default\NTUSER.DAT.LOG1	C:\Users\Default\NTUSER.DAT.LOG1.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Users\Default\NTUSER.DAT{8ebe95f7-3dc6-11e8-a9d9-7cfe90913f50}.TM.blf	C:\Users\Default\NTUSER.DAT{8ebe95f7-3dc6-11e8-a9d9-7cfe90913f50}.TM.blf.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Users\Default\NTUSER.DAT{8ebe95f7-3dc6-11e8-a9d9-7cfe90913f50}.TMContainer000000000000000001.regtrans-ms	C:\Users\Default\NTUSER.DAT{8ebe95f7-3dc6-11e8-a9d9-7cfe90913f50}.TMContainer000000000000000001.regtrans-ms.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Users\Default\NTUSER.DAT{8ebe95f7-3dc6-11e8-a9d9-7cfe90913f50}.TMContainer000000000000000002.regtrans-ms	C:\Users\Default\NTUSER.DAT{8ebe95f7-3dc6-11e8-a9d9-7cfe90913f50}.TMContainer000000000000000002.regtrans-ms.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Users\user\ntuser.ini	C:\Users\user\ntuser.ini.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Users\Public\desktop.ini	C:\Users\Public\desktop.ini.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0011-0000-0000-000000FF1CE}-C\Office64WW.xml	C:\MSOCache\All Users\{90160000-0011-0000-0000-000000FF1CE}-C\Office64WW.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0011-0000-0000-000000FF1CE}-C\pkeyconfig-office.xrm-ms	C:\MSOCache\All Users\{90160000-0011-0000-0000-000000FF1CE}-C\pkeyconfig-office.xrm-ms.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0011-0000-0000-000000FF1CE}-C\ProPlusWW.xml	C:\MSOCache\All Users\{90160000-0011-0000-0000-000000FF1CE}-C\ProPlusWW.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0011-0000-0000-000000FF1CE}-C\Setup.xml	C:\MSOCache\All Users\{90160000-0011-0000-0000-000000FF1CE}-C\Setup.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0016-0409-0000-000000FF1CE}-C\ExcelLR.cab	C:\MSOCache\All Users\{90160000-0016-0409-0000-000000FF1CE}-C\ExcelLR.cab.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0016-0409-0000-000000FF1CE}-C\ExcelMUI.xml	C:\MSOCache\All Users\{90160000-0016-0409-0000-000000FF1CE}-C\ExcelMUI.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0016-0409-0000-000000FF1CE}-C\Setup.xml	C:\MSOCache\All Users\{90160000-0016-0409-0000-000000FF1CE}-C\Setup.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0011-0000-0000-000000FF1CE}-C\OWOW64WW.cab	C:\MSOCache\All Users\{90160000-0011-0000-0000-000000FF1CE}-C\OWOW64WW.cab.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0018-0409-0000-000000FF1CE}-C\PowerPointMUI.xml	C:\MSOCache\All Users\{90160000-0018-0409-0000-000000FF1CE}-C\PowerPointMUI.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0018-0409-0000-000000FF1CE}-C\Setup.xml	C:\MSOCache\All Users\{90160000-0018-0409-0000-000000FF1CE}-C\Setup.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0019-0409-0000-000000FF1CE}-C\PublisherMUI.xml	C:\MSOCache\All Users\{90160000-0019-0409-0000-000000FF1CE}-C\PublisherMUI.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0018-0409-0000-000000FF1CE}-C\PptLR.cab	C:\MSOCache\All Users\{90160000-0018-0409-0000-000000FF1CE}-C\PptLR.cab.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0019-0409-0000-000000FF1CE}-C\Setup.xml	C:\MSOCache\All Users\{90160000-0019-0409-0000-000000FF1CE}-C\Setup.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0019-0409-0000-000000FF1CE}-C\PubLR.cab	C:\MSOCache\All Users\{90160000-0019-0409-0000-000000FF1CE}-C\PubLR.cab.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-001A-0409-0000-000000FF1CE}-C\OutlookMUI.xml	C:\MSOCache\All Users\{90160000-001A-0409-0000-000000FF1CE}-C\OutlookMUI.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-001A-0409-0000-000000FF1CE}-C\OutlkLR.cab	C:\MSOCache\All Users\{90160000-001A-0409-0000-000000FF1CE}-C\OutlkLR.cab.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-001A-0409-0000-000000FF1CE}-C\Setup.xml	C:\MSOCache\All Users\{90160000-001A-0409-0000-000000FF1CE}-C\Setup.xml.NB65	success or wait	1	F2C6CB	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\Setup.xml	C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\Setup.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordMUI.xml	C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordMUI.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordLR.cab	C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordLR.cab.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proofing.xml	C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proofing.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Setup.xml	C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Setup.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.xml	C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfLR.cab	C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfLR.cab.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\Setup.xml	C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\Setup.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.cab	C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.cab.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.xml	C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\Setup.xml	C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\Setup.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.xml	C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\Setup.xml	C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\Setup.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveLR.cab	C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveLR.cab.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveMUI.xml	C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveMUI.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OnoteLR.cab	C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OnoteLR.cab.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\Setup.xml	C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\Setup.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.cab	C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.cab.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.xml	C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\Setup.xml	C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\Setup.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\OSMUXMUI.xml	C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\OSMUXMUI.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\OSMUXMUI.cab	C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\OSMUXMUI.cab.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\Setup.xml	C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\Setup.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\branding.xml	C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\branding.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeMUI.xml	C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeMUI.xml.NB65	success or wait	1	F2C6CB	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeMUISet.xml	C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeMUISet.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeLR.cab	C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeLR.cab.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OffSetLR.cab	C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OffSetLR.cab.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW2.cab	C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW2.cab.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\pss10r.chm	C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\pss10r.chm.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\Setup.chm	C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\Setup.chm.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\Setup.xml	C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\Setup.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\ShellUI.MST	C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\ShellUI.MST.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUI.xml	C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUI.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUISet.xml	C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUISet.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\OWOW64LR.cab	C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\OWOW64LR.cab.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Setup.xml	C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Setup.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\AccessMUISet.xml	C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\AccessMUISet.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Setup.xml	C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Setup.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\LyncMUI.cab	C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\LyncMUI.cab.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\LyncMUI.xml	C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\LyncMUI.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\Setup.xml	C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\Setup.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW.cab	C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW.cab.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files\internet explorer\SIGNUP\install.ins	C:\Program Files\internet explorer\SIGNUP\install.ins.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files\Microsoft Office\Office16\Custom.propdesc	C:\Program Files\Microsoft Office\Office16\Custom.propdesc.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files\Microsoft Office\Office16\Mso Example Setup File A.txt	C:\Program Files\Microsoft Office\Office16\Mso Example Setup File A.txt.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files\Microsoft Office\Office16\VisioCustom.propdesc	C:\Program Files\Microsoft Office\Office16\VisioCustom.propdesc.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files\UNP\Log\UpdateNotificationPipeline.001.etl	C:\Program Files\UNP\Log\UpdateNotificationPipeline.001.etl.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files\UNP\Log\UpdateNotificationPipeline.002.etl	C:\Program Files\UNP\Log\UpdateNotificationPipeline.002.etl.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files\UNP\Log\UpdateNotificationPipeline.003.etl	C:\Program Files\UNP\Log\UpdateNotificationPipeline.003.etl.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Adobe\Acrobat Reader DC\ReadMe.htm	C:\Program Files (x86)\adobe\Acrobat Reader DC\ReadMe.htm.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX.chm	C:\Program Files (x86)\autolt3\AutoltX\AutoltX.chm.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX.psd1	C:\Program Files (x86)\autolt3\AutoltX\AutoltX.psd1.NB65	success or wait	1	F2C6CB	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX3.Assembly.xml	C:\Program Files (x86)\autoit3\AutoltX\AutoltX3.Assembly.xml.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX3_DLL.h	C:\Program Files (x86)\autoit3\AutoltX\AutoltX3_DLL.h.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX3_DLL.lib	C:\Program Files (x86)\autoit3\AutoltX\AutoltX3_DLL.lib.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX3_x64_DLL.lib	C:\Program Files (x86)\autoit3\AutoltX\AutoltX3_x64_DLL.lib.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Examples\calculator.au3	C:\Program Files (x86)\autoit3\Examples\calculator.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Examples\count-do.au3	C:\Program Files (x86)\autoit3\Examples\count-do.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Examples\count-for.au3	C:\Program Files (x86)\autoit3\Examples\count-for.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Examples\count-while.au3	C:\Program Files (x86)\autoit3\Examples\count-while.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Examples\functions.au3	C:\Program Files (x86)\autoit3\Examples\functions.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Examples\inputbox.au3	C:\Program Files (x86)\autoit3\Examples\inputbox.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Examples\msgbox.au3	C:\Program Files (x86)\autoit3\Examples\msgbox.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Examples\notepad1.au3	C:\Program Files (x86)\autoit3\Examples\notepad1.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Examples\notepad2.au3	C:\Program Files (x86)\autoit3\Examples\notepad2.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Examples_ReadMe_.txt	C:\Program Files (x86)\autoit3\Examples_ReadMe_.txt.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Extras_ReadMe_.txt	C:\Program Files (x86)\autoit3\Extras_ReadMe_.txt.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Icons\lau3.ico	C:\Program Files (x86)\autoit3\Icons\lau3.ico.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Icons\lau3script_v10.ico	C:\Program Files (x86)\autoit3\Icons\lau3script_v10.ico.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Icons\lau3script_v11.ico	C:\Program Files (x86)\autoit3\Icons\lau3script_v11.ico.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Icons\lau3script_v9.ico	C:\Program Files (x86)\autoit3\Icons\lau3script_v9.ico.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Icons\filetype-blank.ico	C:\Program Files (x86)\autoit3\Icons\filetype-blank.ico.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Icons\MyAutolt3_Blue.ico	C:\Program Files (x86)\autoit3\Icons\MyAutolt3_Blue.ico.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Icons\MyAutolt3_Green.ico	C:\Program Files (x86)\autoit3\Icons\MyAutolt3_Green.ico.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Icons\MyAutolt3_Red.ico	C:\Program Files (x86)\autoit3\Icons\MyAutolt3_Red.ico.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Icons\MyAutolt3_Yellow.ico	C:\Program Files (x86)\autoit3\Icons\MyAutolt3_Yellow.ico.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\analysis\stimer.au3	C:\Program Files (x86)\autoit3\Include\analysis\stimer.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\APIComConstants.au3	C:\Program Files (x86)\autoit3\Include\APIComConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\APIConstants.au3	C:\Program Files (x86)\autoit3\Include\APIConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\APIDiaGConstants.au3	C:\Program Files (x86)\autoit3\Include\APIDiaGConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\APIDlgConstants.au3	C:\Program Files (x86)\autoit3\Include\APIDlgConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\APIErrorsConstants.au3	C:\Program Files (x86)\autoit3\Include\APIErrorsConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\APIFilesConstants.au3	C:\Program Files (x86)\autoit3\Include\APIFilesConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\APIGdiConstants.au3	C:\Program Files (x86)\autoit3\Include\APIGdiConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\APILocaleConstants.au3	C:\Program Files (x86)\autoit3\Include\APILocaleConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\APIMiscConstants.au3	C:\Program Files (x86)\autoit3\Include\APIMiscConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\APIProcConstants.au3	C:\Program Files (x86)\autoit3\Include\APIProcConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3\Include\APIRegConstants.au3	C:\Program Files (x86)\autoit3\Include\APIRegConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\APIResConstants.au3	C:\Program Files (x86)\autoit3\Include\APIResConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\APIShellExConstants.au3	C:\Program Files (x86)\autoit3\Include\APIShellExConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\APIShPathConstants.au3	C:\Program Files (x86)\autoit3\Include\APIShPathConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\APISysConstants.au3	C:\Program Files (x86)\autoit3\Include\APISysConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\APIThemeConstants.au3	C:\Program Files (x86)\autoit3\Include\APIThemeConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\Array.au3	C:\Program Files (x86)\autoit3\Include\Array.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\ArrayDisplayInternals.au3	C:\Program Files (x86)\autoit3\Include\ArrayDisplayInternals.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\AutoltConstants.au3	C:\Program Files (x86)\autoit3\Include\AutoltConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\AVIConstants.au3	C:\Program Files (x86)\autoit3\Include\AVIConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\BorderConstants.au3	C:\Program Files (x86)\autoit3\Include\BorderConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\ButtonConstants.au3	C:\Program Files (x86)\autoit3\Include\ButtonConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\cleanup.au3	C:\Program Files (x86)\autoit3\Include\cleanup.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\Clipboard.au3	C:\Program Files (x86)\autoit3\Include\Clipboard.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\Color.au3	C:\Program Files (x86)\autoit3\Include\Color.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\ColorConstants.au3	C:\Program Files (x86)\autoit3\Include\ColorConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\ComboConstants.au3	C:\Program Files (x86)\autoit3\Include\ComboConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\Constants.au3	C:\Program Files (x86)\autoit3\Include\Constants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\Crypt.au3	C:\Program Files (x86)\autoit3\Include\Crypt.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\CUIAutomation2.au3	C:\Program Files (x86)\autoit3\Include\CUIAutomation2.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\Date.au3	C:\Program Files (x86)\autoit3\Include\Date.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\DateTimeConstants.au3	C:\Program Files (x86)\autoit3\Include\DateTimeConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\Debug.au3	C:\Program Files (x86)\autoit3\Include\Debug.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\DirConstants.au3	C:\Program Files (x86)\autoit3\Include\DirConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\EditConstants.au3	C:\Program Files (x86)\autoit3\Include\EditConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\EventLog.au3	C:\Program Files (x86)\autoit3\Include\EventLog.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\Excel.au3	C:\Program Files (x86)\autoit3\Include\Excel.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\ExcelConstants.au3	C:\Program Files (x86)\autoit3\Include\ExcelConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\File.au3	C:\Program Files (x86)\autoit3\Include\File.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\FileConstants.au3	C:\Program Files (x86)\autoit3\Include\FileConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\FontConstants.au3	C:\Program Files (x86)\autoit3\Include\FontConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\FrameConstants.au3	C:\Program Files (x86)\autoit3\Include\FrameConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\FTPEx.au3	C:\Program Files (x86)\autoit3\Include\FTPEx.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GDIPlus.au3	C:\Program Files (x86)\autoit3\Include\GDIPlus.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GDIPlusConstants.au3	C:\Program Files (x86)\autoit3\Include\GDIPlusConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3\Include\GuiAVI.au3	C:\Program Files (x86)\autoit3\Include\GuiAVI.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GuiButton.au3	C:\Program Files (x86)\autoit3\Include\GuiButton.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GuiComboBox.au3	C:\Program Files (x86)\autoit3\Include\GuiComboBox.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GuiComboBoxEx.au3	C:\Program Files (x86)\autoit3\Include\GuiComboBoxEx.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GUIConstants.au3	C:\Program Files (x86)\autoit3\Include\GUIConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GUIConstantsEx.au3	C:\Program Files (x86)\autoit3\Include\GUIConstantsEx.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GuiDateTimePicker.au3	C:\Program Files (x86)\autoit3\Include\GuiDateTimePicker.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GuiEdit.au3	C:\Program Files (x86)\autoit3\Include\GuiEdit.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GuiHeader.au3	C:\Program Files (x86)\autoit3\Include\GuiHeader.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GuiImageList.au3	C:\Program Files (x86)\autoit3\Include\GuiImageList.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GuiIPAddress.au3	C:\Program Files (x86)\autoit3\Include\GuiIPAddress.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GuiListBox.au3	C:\Program Files (x86)\autoit3\Include\GuiListBox.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GuiListView.au3	C:\Program Files (x86)\autoit3\Include\GuiListView.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GuiMenu.au3	C:\Program Files (x86)\autoit3\Include\GuiMenu.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GuiMonthCal.au3	C:\Program Files (x86)\autoit3\Include\GuiMonthCal.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GuiReBar.au3	C:\Program Files (x86)\autoit3\Include\GuiReBar.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GuiRichEdit.au3	C:\Program Files (x86)\autoit3\Include\GuiRichEdit.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GuiScrollBars.au3	C:\Program Files (x86)\autoit3\Include\GuiScrollBars.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GuiSlider.au3	C:\Program Files (x86)\autoit3\Include\GuiSlider.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GuiStatusBar.au3	C:\Program Files (x86)\autoit3\Include\GuiStatusBar.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GuiTab.au3	C:\Program Files (x86)\autoit3\Include\GuiTab.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GuiToolBar.au3	C:\Program Files (x86)\autoit3\Include\GuiToolBar.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GuiToolTip.au3	C:\Program Files (x86)\autoit3\Include\GuiToolTip.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\GuiTreeView.au3	C:\Program Files (x86)\autoit3\Include\GuiTreeView.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\HeaderConstants.au3	C:\Program Files (x86)\autoit3\Include\HeaderConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\helper.au3	C:\Program Files (x86)\autoit3\Include\helper.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\htmlfetcher.au3	C:\Program Files (x86)\autoit3\Include\htmlfetcher.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\ie.au3	C:\Program Files (x86)\autoit3\Include\ie.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\ImageListConstants.au3	C:\Program Files (x86)\autoit3\Include\ImageListConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\Inet.au3	C:\Program Files (x86)\autoit3\Include\Inet.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\InetConstants.au3	C:\Program Files (x86)\autoit3\Include\InetConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\IPAddressConstants.au3	C:\Program Files (x86)\autoit3\Include\IPAddressConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\ListBoxConstants.au3	C:\Program Files (x86)\autoit3\Include\ListBoxConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\ListViewConstants.au3	C:\Program Files (x86)\autoit3\Include\ListViewConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\liveprocess.au3	C:\Program Files (x86)\autoit3\Include\liveprocess.au3.NB65	success or wait	1	F2C6CB	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autol3\Include\Math.au3	C:\Program Files (x86)\autoit3\Include\Math.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\MathConstants.au3	C:\Program Files (x86)\autoit3\Include\MathConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\Memory.au3	C:\Program Files (x86)\autoit3\Include\Memory.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\MemoryConstants.au3	C:\Program Files (x86)\autoit3\Include\MemoryConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\MenuConstants.au3	C:\Program Files (x86)\autoit3\Include\MenuConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\Misc.au3	C:\Program Files (x86)\autoit3\Include\Misc.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\MsgBoxConstants.au3	C:\Program Files (x86)\autoit3\Include\MsgBoxConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\NamedPipes.au3	C:\Program Files (x86)\autoit3\Include\NamedPipes.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\NetShare.au3	C:\Program Files (x86)\autoit3\Include\NetShare.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\NTSTATUSConstants.au3	C:\Program Files (x86)\autoit3\Include\NTSTATUSConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\PowerPoint.au3	C:\Program Files (x86)\autoit3\Include\PowerPoint.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\PowerPointConstants.au3	C:\Program Files (x86)\autoit3\Include\PowerPointConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\Process.au3	C:\Program Files (x86)\autoit3\Include\Process.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\ProcessConstants.au3	C:\Program Files (x86)\autoit3\Include\ProcessConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\ProgressConstants.au3	C:\Program Files (x86)\autoit3\Include\ProgressConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\RebarConstants.au3	C:\Program Files (x86)\autoit3\Include\RebarConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\RichEditConstants.au3	C:\Program Files (x86)\autoit3\Include\RichEditConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\ScreenCapture.au3	C:\Program Files (x86)\autoit3\Include\ScreenCapture.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\ScrollBarConstants.au3	C:\Program Files (x86)\autoit3\Include\ScrollBarConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\ScrollBarsConstants.au3	C:\Program Files (x86)\autoit3\Include\ScrollBarsConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\Security.au3	C:\Program Files (x86)\autoit3\Include\Security.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\SecurityConstants.au3	C:\Program Files (x86)\autoit3\Include\SecurityConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\SendMessage.au3	C:\Program Files (x86)\autoit3\Include\SendMessage.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\SliderConstants.au3	C:\Program Files (x86)\autoit3\Include\SliderConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\Sound.au3	C:\Program Files (x86)\autoit3\Include\Sound.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\SQLite.au3	C:\Program Files (x86)\autoit3\Include\SQLite.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\StaticConstants.au3	C:\Program Files (x86)\autoit3\Include\StaticConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\StatusBarConstants.au3	C:\Program Files (x86)\autoit3\Include\StatusBarConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\String.au3	C:\Program Files (x86)\autoit3\Include\String.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\StringConstants.au3	C:\Program Files (x86)\autoit3\Include\StringConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\StructureConstants.au3	C:\Program Files (x86)\autoit3\Include\StructureConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\TabConstants.au3	C:\Program Files (x86)\autoit3\Include\TabConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\Timers.au3	C:\Program Files (x86)\autoit3\Include\Timers.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\ToolBarConstants.au3	C:\Program Files (x86)\autoit3\Include\ToolBarConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autol3\Include\ToolTipConstants.au3	C:\Program Files (x86)\autoit3\Include\ToolTipConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3\Include\TrayConstants.au3	C:\Program Files (x86)\autoit3\Include\TrayConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\TreeViewConstants.au3	C:\Program Files (x86)\autoit3\Include\TreeViewConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\UDFGlobalID.au3	C:\Program Files (x86)\autoit3\Include\UDFGlobalID.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\UIAWrappers.au3	C:\Program Files (x86)\autoit3\Include\UIAWrappers.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\UpDownConstants.au3	C:\Program Files (x86)\autoit3\Include\UpDownConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\Visa.au3	C:\Program Files (x86)\autoit3\Include\Visa.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPI.au3	C:\Program Files (x86)\autoit3\Include\WinAPI.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPICom.au3	C:\Program Files (x86)\autoit3\Include\WinAPICom.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPIConstants.au3	C:\Program Files (x86)\autoit3\Include\WinAPIConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPIConv.au3	C:\Program Files (x86)\autoit3\Include\WinAPIConv.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPIDiag.au3	C:\Program Files (x86)\autoit3\Include\WinAPIDiag.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPIDlg.au3	C:\Program Files (x86)\autoit3\Include\WinAPIDlg.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPIError.au3	C:\Program Files (x86)\autoit3\Include\WinAPIError.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPIEx.au3	C:\Program Files (x86)\autoit3\Include\WinAPIEx.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPIFiles.au3	C:\Program Files (x86)\autoit3\Include\WinAPIFiles.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPIGdi.au3	C:\Program Files (x86)\autoit3\Include\WinAPIGdi.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPIGdiDC.au3	C:\Program Files (x86)\autoit3\Include\WinAPIGdiDC.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPIGdiInternals.au3	C:\Program Files (x86)\autoit3\Include\WinAPIGdiInternals.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPIHObj.au3	C:\Program Files (x86)\autoit3\Include\WinAPIHObj.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPIIcons.au3	C:\Program Files (x86)\autoit3\Include\WinAPIIcons.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPIInternals.au3	C:\Program Files (x86)\autoit3\Include\WinAPIInternals.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPIlangConstants.au3	C:\Program Files (x86)\autoit3\Include\WinAPIlangConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPILocale.au3	C:\Program Files (x86)\autoit3\Include\WinAPILocale.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPIMem.au3	C:\Program Files (x86)\autoit3\Include\WinAPIMem.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPIMisc.au3	C:\Program Files (x86)\autoit3\Include\WinAPIMisc.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPIProc.au3	C:\Program Files (x86)\autoit3\Include\WinAPIProc.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPIReg.au3	C:\Program Files (x86)\autoit3\Include\WinAPIReg.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPIRes.au3	C:\Program Files (x86)\autoit3\Include\WinAPIRes.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPIShellEx.au3	C:\Program Files (x86)\autoit3\Include\WinAPIShellEx.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPIShPath.au3	C:\Program Files (x86)\autoit3\Include\WinAPIShPath.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPISys.au3	C:\Program Files (x86)\autoit3\Include\WinAPISys.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPISysinfoConstants.au3	C:\Program Files (x86)\autoit3\Include\WinAPISysinfoConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPISysInternals.au3	C:\Program Files (x86)\autoit3\Include\WinAPISysInternals.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPISysWin.au3	C:\Program Files (x86)\autoit3\Include\WinAPISysWin.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinAPITheme.au3	C:\Program Files (x86)\autoit3\Include\WinAPITheme.au3.NB65	success or wait	1	F2C6CB	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3\Include\WinAPI\keysConstants.au3	C:\Program Files (x86)\autoit3\Include\WinAPI\keysConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WindowsConstants.au3	C:\Program Files (x86)\autoit3\Include\WindowsConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WinNet.au3	C:\Program Files (x86)\autoit3\Include\WinNet.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\Word.au3	C:\Program Files (x86)\autoit3\Include\Word.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include\WordConstants.au3	C:\Program Files (x86)\autoit3\Include\WordConstants.au3.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\Include_ReadMe_.txt	C:\Program Files (x86)\autoit3\Include_ReadMe_.txt.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Autolt3\SciTE\au3.keywords.properties	C:\Program Files (x86)\autoit3\SciTE\au3.keywords.properties.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Common Files\DESIGNER\MSADDNDR.OLB	C:\Program Files (x86)\common files\DESIGNER\MSADDNDR.OLB.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Google\Update\GoogleUpdate.bk	C:\Program Files (x86)\google\Update\GoogleUpdate.bk.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Internet Explorer\SIGNUP\install.ins	C:\Program Files (x86)\internet explorer\SIGNUP\install.ins.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Java\jre1.8.0_211\COPYRIGHT	C:\Program Files (x86)\java\jre1.8.0_211\COPYRIGHT.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Java\jre1.8.0_211\LICENSE	C:\Program Files (x86)\java\jre1.8.0_211\LICENSE.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Java\jre1.8.0_211\README.txt	C:\Program Files (x86)\java\jre1.8.0_211\README.txt.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Java\jre1.8.0_211\release	C:\Program Files (x86)\java\jre1.8.0_211\release.NB65	success or wait	1	F2C6CB	MoveFileW
C:\Program Files (x86)\Java\jre1.8.0_211\THIRDPARTYLICENSEREADME-JAVAFX.txt	C:\Program Files (x86)\java\jre1.8.0_211\THIRDPARTYLICENSEREADME-JAVAFX.txt.NB65	success or wait	1	F2C6CB	MoveFileW

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 5f 2f 5c 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \\\ _ v _ _ v L // _ _ _ \ . ` _ _ \ _ _ \ \ v v L / \ \ \ _ / \ _ \ \ _ \ _ / _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\IR3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ _ _ _ \ _ _ _ _ _ _ _ \ / / _ _ _ _ _ \ _ _ \ _ _ \ \ _ _ / \ / \ \ _ / \ _ \ _ \ _ \ _ \ _ \ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\bootTel.dat	80	524	58 17 27 28 66 fd 01 1a fd 19 7f 24 5e 79 fd fd fd 34 44 fd fd fd 68 fd 04 53 fd fd 11 fd fd 06 fd fd fd 6e fd 2c fd fd fd 53 fd 1b fd fd 2e 09 fd 61 fd fc e2 49 43 12 36 09 fd 7b 36 46 1b fd fd 0a fd 17 22 fd 7c 67 20 fd fd fd 1f 0e 15 fd fd fd fd 30 fd 22 4d 60 fd 5b fd 60 54 62 3b 7b 75 fd fd 69 fd 47 fd fd 09 58 fd 13 32 fd 03 70 fd 3d 2d 4f 61 39 fd 68 59 3e 18 17 2d fd fd 1f 5c fd 4b 65 7c 60 fd 21 3e 18 fd 4d fd 62 fd 30 1c 1c 1d fd fd 12 43 65 12 fd 30 fd 7b 60 fd fd 24 7f 24 19 fd 16 fd 7a fd fd 74 fd 3e 66 67 fd 76 63 fd 08 fd fd fd 24 fd fd 49 01 fd fd 4b 08 27 72 5b fd fd fd 71 bc fd fd 65 fd fd 1f fd 24 25 fd fd 4f fd 35 fd 9d fd 21 bd fd fd 06 37 1b fd 64 37 fd fd fd fd fd 5e fd fd 0c fd 3a fd fd fd fd 13 36	X'(\$^y4DhSn,S.aIC6{6F" g 0M'["Tb;{uiGX2p=- Oa9hY>-\\Ke`!>Mb0C e0{ '\$\$zt>fgvc\$IKr[qe\$% O5!7d7^:6	success or wait	1	F2CBF8	WriteFile
C:\bootTel.dat	604	10	24 00 50 00 00 00 00 00 00 00	\$P	success or wait	1	F2CC68	WriteFile
C:\bootTel.dat	0	80	fd 1c a3 67 fd fd fd fd fd 11 0d fd fd fd 36 fd fd fd 00 0e fd 1f 32 40 49 53 fd 36 fd 25 fd 53 1b 77 49 45 fd 3b fd fd fd 30 fd b9 09 6c 3c 12 fd fd 02 48 fd 01 fd 3f 72 05 5e fd 13 3c 54 fd 02 fd fd 7a fd 04 fd 3f fd 63 61	g2@!S6%SwIE;0l<H? r^<Tz?ca	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\PerfLogs\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ _ _ _ \\ _ _ v _ _ _ _ \ / / / _ _ _ _ \ . ' _ _ \\ _ _ \ \ \ / / \ / \ _ / \ _ \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\Program Files\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ _ _ _ \\ _ _ v _ _ _ _ \ / / / _ _ _ _ \ . ' _ _ \\ _ _ \ \ \ / / \ / \ _ / \ _ \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ v _ _ v \ / / _ _ _ _ v . ' _ _ \ _ _ \ \ v / \ / \ \ _ / \ _ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\Program Files\desktop.ini	174	524	4f fd 6a 4f 48 fd 04 fd 42 16 fd fd 4c 22 fd 14 79 5a 42 fd 99 fd fd a4 fd fd 2c fd fd 71 fd 20 6f 50 40 7f 45 10 fd 43 fd 43 fd fd 4b fd 60 07 fd f7 fd 18 fd fd 15 fd fd fd 66 13 d4 fd 2c 3d 75 fd 4d fd 66 fd 79 37 fd 98 fd 4c fd fd fd 58 6b 39 6a 4e fd ab fd fd 1f 5c 32 fd 04 02 2d fd fd 6b fd fd fd fd a4 e4 fd 09 fd 71 fd fd 2f fd 5b fd fd 53 6c 4e 56 57 78 39 fd 18 fd 4b 68 fd fd fd fd 17 44 fd 2e 33 fd fd 25 00 2e 2c 44 fd fd fd 07 fd 31 fd 74 7d 56 fd fd 30 fd fd 40 6c fd 73 28 4b fd fd fd 32 fd 10 fd fd fd fd fd 07 fd 42 73 fd 08 fd 5a 65 fd 54 06 00 07 fd fd 10 fd fd 39 4c 64 78 5d fd 67 40 fd fd 31 fd 46 2e 10 7b 23 2b 6d 5a 48 42 fd 04 21 fd fd 63 47 1c fd fd 6a fd 2d 08 78 71 57 fd fd 44 61	OjOHLB"yZB,q oP@ECCk'f,=uMfy7L Xk9jN2- kq/[SINVWx9KhD.3%,Dt } V0@!s(K2BsZeT9Ldx]g @1F.{#+mZHB!cGj- xqWD	success or wait	1	F2CBF8	WriteFile
C:\Program Files\desktop.ini	698	10	24 00 fd 00 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\Program Files\desktop.ini	0	174	65 fd fd fd 5a 70 fd fd 1b fd fd 12 fd 59 dd fd 1f fd 03 18 fd 63 fd fd fd fd fd 70 fd fd 21 6b fd 61 fd 6b 5a 59 70 45 1f 55 fd 57 fd 06 2a fd 64 2f fd 3d 67 fd fd 0b 33 fd fd fd 2c fd 50 73 fd 0b fd 17 fd 16 30 4c 12 62 fd 7c fd 17 fd fd 4c fd 4c fd 40 1a fd 37 56 6b 7a fd 49 fd fd fd fd fd 76 ae fd fd fd 6c fd fd 6b 2f fd fd 51 46 34 0a 4c 44 04 fd fd fd fd fd 38 4e fd 33 fd fd 27 42 fd fd fd fd 4b fd 72 fd 6f fd fd fd fd 29 1b 4e fd 21 fd fd 55 fd 00 f1 fd 75 fd 31 02 fd fd fd 75	eZpYcplkakZYpEUW*d/= g3,Ps0Lb]L L@7Vkzllk/QF4LD8N3'B Kro)N!Uu1u	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ _ _ _ \\ _ _ v _ _ _ _ \ / / _ _ _ _ \ . ` _ _ \ _ _ \ \ \ \ / / \ / \ \ _ / \ _ _ \ _ _ \ _ _ \ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\Program Files (x86)\desktop.ini	174	524	4a fd 0d 58 5a 46 fd fd fd fd 60 7b 74 fd 06 fd 08 16 52 77 23 6b 62 18 45 33 6e 76 fd fd 75 fd 50 5c fd fd 12 4a fd 3a 62 fd fd fd fd fd 45 fd fd fd fd fd fd fd 5c 4e fd 57 fd fd fd 29 fd 44 19 a7 fd 3b fd 5a 59 76 43 0c 42 00 fd fd fd 54 49 48 fd 63 fd 01 fd fd fd 78 fd fd 45 fd 0a fd 02 10 55 6f fd 1a fd 79 fd fd fd fd fd 07 6f 1b fd 7f 31 fd fd 61 39 1b 03 fd fd 2c 45 72 60 28 fd 2a fd 3c 5d 6f fd 65 21 7c 09 fd 7a 68 56 65 47 16 70 7f 63 5b 59 47 fd fd 57 7c fd 71 fd fd fd 1a fd fd fd fd 39 fd ab 7b fd 68 5b fd fd 62 25 fd 07 fd 53 fd fd 31 fd 69 59 1f 7d fd fa fd 3b 18 0c 67 79 65 67 49 fd 00 7b fd 51 fd fd fd fd fd fd 3c fd fd fd 57 05 0e 44 0b 1c 4e fd fd 14 57 f6 5e fd 5a cf	JX`{Rw#kbEnvuPl:bE\N W)D;ZYvBT IHcxEUoy1a9,Er(* <]oe! zhVeGpc[YGW q9{h[b%S1iY};gyeg !{Q<WDNW^Z	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\desktop.ini	698	10	24 00 fd 00 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\Program Files (x86)\desktop.ini	0	174	05 43 fd e9 fd 16 0d 40 fd 7a 35 53 5e 22 17 68 fd 67 fd 35 7f 68 fd 7b 65 4c 20 fd 56 67 6d fd fd 6f 4c fd 02 f5 fd 10 5e fd 23 fd 0a 76 03 fd 7f 72 fd 7b fd 20 7b 42 44 74 fd 02 fd 38 12 7c 7c 61 fd fd fd 24 fd fd 43 fd 06 fd 01 fd 6f fd 1e 3b fd 41 4b fd fd fd 0a 52 57 56 50 7b 6c 4e fd 2e 1f fd 33 4c 57 fd 1b 00 66 43 fd fd 2e 23 3a 70 fd 63 fd 7d 4c 56 7f 31 69 fd fd fd 0a fd 01 fd 07 fd fd fd fd fd 0e fd fd fd 76 13 4c 2a 05 0a 0f 64 fd fd 18 15 fd fd fd fd 31 fd 1c fd fd 4c b7 5f 76 fd fd 04	C@z5S^"hg5h{eL VgmoL^#vr{ {BDt 8 a\$Co;AKRWVP{IN.3L WfC.#;pc}LV1ivL*d1L_v	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Recovery\IR3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ v _ _ _ _ \ / / _ _ _ _ \ . ' _ _ \ _ _ \ \ \ / / \ / \ _ / \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\Users\IR3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ v _ _ _ _ \ / / _ _ _ _ \ . ' _ _ \ _ _ \ \ \ / / \ / \ _ / \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\Common Files\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ v _ _ _ _ / / _ _ _ _ \ . ' _ _ _ _ \ \ / / \ / \ _ / \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\Program Files\Google\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ v _ _ _ _ / / _ _ _ _ \ . ' _ _ _ _ \ \ / / \ / \ _ / \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\MSBuild\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ v _ _ _ _ v / / / _ _ _ _ . ' _ _ \ _ _ \ \ v v / / \ / \ _ / \ _ \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\Program Files\Reference Ass embles\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ v _ _ _ _ v / / / _ _ _ _ . ' _ _ \ _ _ \ \ v v / / \ / \ _ / \ _ \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\Uninstall Information\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ _ _ _ \\ _ _ v _ _ _ _ \ / / / _ _ _ _ \ . ' _ _ \\ _ _ \ \ \ / / \ / \ _ / \ _ \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your environ- ment has been infected with r	success or wait	1	F358DF	WriteFile
C:\Program Files\UNP\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ _ _ _ \\ _ _ v _ _ _ _ \ / / / _ _ _ _ \ . ' _ _ \\ _ _ \ \ \ / / \ / \ _ / \ _ \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your environ- ment has been infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Reader\3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 5f 2f 5c 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \\ _ _ v _ _ _ _ / / _ _ _ _ . ' _ _ \ _ _ \ \ / / \ / \ _ / \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your environ- ment has been infected with r	success or wait	1	F358DF	WriteFile
C:\Program Files (x86)\Autol3\3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 5f 2f 5c 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \\ _ _ v _ _ _ _ / / _ _ _ _ . ' _ _ \ _ _ \ \ / / \ / \ _ / \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your environ- ment has been infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3\Au3Check.dat	0	12931	78 fd 1c fd 7c 74 71 44 fd fd fd fd fd 07 73 fd fd 62 fd fd fd 04 fd fd fd 4e fd fd 46 07 20 fd 7e 74 3e 01 fd fd fd fd 5a fd 75 fd fd 15 fd 3e 6d 7f fd 32 77 fd fd fd 21 fd fd fd 6e 6e 74 fd fd fd fd 50 14 54 39 fd 78 fd fd 62 2c fd 0c 22 fd 69 fd 76 06 fd 32 32 16 39 68 42 3b fd 0f 24 25 fd 4e 57 fd 41 62 fd 0f fd 26 fd 25 fd 06 fd 5b 1f 39 fd 77 04 40 6d 1a 59 fd 10 fd fd fd fd fd fd fd fd 76 fd fd 26 06 70 3f 10 55 6d 7c 2e 69 fd 0c 55 fd fd 56 3c 40 57 09 58 30 fd fd fd fd 2c fd 61 28 3d 00 fd 29 40 fd 79 fd 71 fd fd 31 3e 53 67 1b 12 64 0d 1b 02 fd 2d 41 29 fd fd 2b fd 3d 23 fd 53 fd 23 33 44 fd 5b 66 fd 09 fd 6b fd 14 72 fd fd fd 6a f9 26 fd 2d 3f fd 13 fd fd 39 4f f9 45 41 fd fd fd fd 50 5f fd 57 34 47 fd 59 57 23 04	x tqDsNF ~t>Zu>m2w!nntPT9xb,"v 229hB;\$%NWAb&% [9w@mYv&p?Um].iU V<@WX0,a(=)@yq1>Sg d-A)+=#S#3D[!krj&-? 9OEAP_W4GYW#	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Autolt3\Autoltv3 Website.url	204	524	2a 72 fd fd fd 58 01 fd fd 1f fd 0b 2e 41 90 7a 30 fd 22 fd fd 6b fd fd fd 02 65 fd 5e fd fd fd 5d fd 23 fd 0d fd fd 56 fd 32 02 02 73 4f 41 fd 7d 59 33 fd 25 fd fd 0f 4c fd 04 fd 6b 34 7b 7f fd 18 fd fd 29 55 4d 15 29 db 6c fd 3b fd 25 fd 69 fd 46 fd 16 02 fd 47 fd 23 0b fd 24 3e 51 fd fd 53 fd fd fd 58 60 23 fd fd 7c fd fd 2e fd 4e fd 10 50 08 69 fd fd 7c 61 fd 4b fd fd 0e 56 fd 38 59 fd fd 7c fd fd 12 38 68 47 1e fd 37 08 60 1d 1e 73 1d 3f fd 4d fd 48 14 d4 fd 5f 67 22 16 fd 05 32 51 06 fd 70 fd fd 46 fd 78 fd 55 fd fd 4a 25 3d 21 fd fd 33 fd cd 09 61 fd 25 0f 44 fd fd fd 45 7d fd 6c fd 57 1e fd 76 fd fd dc fd 14 61 12 fd 23 fd 02 24 fd fd 54 39 fd fd 41 76 fd 01 04 40 49 2b 39 fd fd 36 fd 73 fd fd 24 35 04 fd fd fd	*rX.Az0"ke"]#V2sOA}Y3 %Lk4()UM) I;%iFG#\$>QSX`# .NP !aK V8Y[8hG7`s? MH_g"2QpFxFxUJ%=!3a% DE)!Wva#\$\$ T9Av@!i+96s\$5	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3\Autoltv3 Website.url	728	10	24 00 fd 00 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\Program Files (x86)\Autolt3\Autoltv3 Website.url	0	204	fd fd 1d fd fd fd 01 38 75 46 fd 54 86 14 fd 7f 3e fd fd 34 18 fd 6e 78 fd 08 fd 74 64 3b fd fd 48 fd fd 0a fd 05 6a fd fd fd fd 28 28 fd 7e fd fd 07 19 fd fd 45 fd fd fd 23 75 67 fd 9b fd 2d 40 fd 51 2a 4b fd 04 fd 44 fd fd fd fd 74 fd 35 fd fd fd e7 fd fd 26 30 fd 2b 2a 20 04 fd 79 6f fd fd 22 3a 3b 3d fd 6f fd fd 77 15 71 62 fd fd fd fd 31 60 fd fd fd fd 58 41 fd fd 56 1e 37 fd 40 03 fd fd fd 38 fd fd 07 44 fd 76 5b 2d 4b fd 4f 78 fd fd fd 60 fd fd 1b fd 73 59 6c 7d fd fd 7e 4d fd 1c fd fd 49 fd 08 82 90 3c fd fd 47 fd 25 fd 58 fd 9c fd 39 fd fd 0c fd fd fd	8uFT>4nxttd;Hj((~E#ug- @Q*KDt5&0+* yo";owqb1`XAV7@8Dv[- KOx`sY!]-MI<G%X9	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3 \Autolt.chm	700544 9	524	fd fd fd 0c 04 63 38 fd 21 fd 64 fd 41 3e fd 0e fd 78 15 fd fd fd 04 1b fd fd 14 3e fd fd fd 1b 7d 1a 3c 3d 5f 6d fd 27 fd fd fd 07 fd 0d fd a2 39 0b fd fd fd 34 fd 6e 09 27 57 fd fd fd 76 fd 15 11 fd 27 fd fd 41 fd fd fd 4b fd fd 03 56 6b 2e 2f fd 67 0d 4e fd 62 fd fd fd fd fd 06 fd 07 fd fd fd 0f fd fd fd 0f 1e fd 4a 3b fd fd 0e fd fd 40 fd fd fd 6c fd fd 38 23 2d fd 75 fd fd 20 fd fd 5a 7a fd fd 74 fd fd fd fd 79 40 f7 72 fd 3a fd 63 64 fd 0c fd 2b fd 6f fd fd fd 76 34 4f 0a fd 28 5f fd 23 fd fd 46 fd 07 fd 05 5f 68 37 6e 04 fd fd 5c 4e 37 47 57 fd fd 11 fd 3e fd 74 fd fd fd 0b 38 fd f2 72 1e fd 73 fd fd fd 03 fd fd 66 fd fd 62 fd 5f 2f fd 73 5b 3f fd bb 3d fd 60 fd 6f 6c 49 fd fd 47 fd 29 fd 34 fd 02 51 fd	c8!dA>x>} <=_m'94n'Wv'AKVkJ./NbJ @l8#-u Zzty@r:cd+ov4O(_#F_h7 n\N7GW>t8rsfb_/s[? 'ollG)4Q	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3 \Autolt.chm	700597 3	10	25 32 09 fd 6a 00 00 00 00 00	%2j	success or wait	1	F2CC68	WriteFile
C:\Program Files (x86)\Autolt3 \Autolt.chm	0	700540	61 fd 49 fd 26 fd 3a fd 2e fd fd 45 fd fd fd 12 07 fd 50 48 4b 59 18 fd 7f 30 46 6d fd fd fd 14 7f 3f 2e 39 fd fd fd fd 6f 24 67 fd fd fd 5b fd fd 45 fd e1 1e fd 10 fd 45 0d fd 67 fd 69 74 48 4c 71 79 4b 5c fd fd 36 fd fd 1a fd fd 58 fd 33 12 46 4c 1e 14 fd 44 fd 3b fd 73 fd 05 fd 77 fd 70 fd fd fd 57 4f fd 78 0a fd 18 fd fd 7c 59 00 fd 22 72 78 fd 7a fd fd 0c 06 6c fd 0b fd 7b fd 22 fd fd 52 fd fd 79 fd 55 fd fd 4a 1c fd 1c 35 fd fd 10 fd 30 fd 04 fd 02 fd 34 14 71 fd fd fd 6f 77 60 fd 30 fd 8b 10 7f 78 fd fd fd 1e 12 47 fd fd 0e 36 fd 31 fd fd fd 27 fd 02 fd 00 53 fd 7d fd 36 13 4d 0c fd fd fd 03 fd c3 0c fd 1f fd fd 3a fd 18 59 fd 3b 2d fd 64 fd fd fd 4f fd fd 01 fd 51 fd fd 1c 7e fd fd 6e 69 5d 4b 50 fd 1b 20 fd 14 ad	al&:EPHKY0Fm?.9o\$g[E EgitHLqyK\ 6X3FLD;swpWOx Y"rxzl{ "RyUJ504q ow'0xG61'S}6M:Y;- dOQ~nij]	success or wait	5	F2C055	WriteFile
C:\Program Files (x86)\Common Files\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ ____ _ _ _ _ \ _ _ v _ _ _ _ v _ / / _ _ _ _ \ : ' _ _ \ _ _ _ \ \ v \ / / \ / \ \ _ / \ _ _ \ _ _ \ _ _ \ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Google\ R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \\ _ _ v _ _ _ _ v L / / / _ _ _ \ . ' _ _ \ _ _ \ \ v v L / / \ / \ _ / \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\Program Files (x86)\Internet Explorer\ R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \\ _ _ v _ _ _ _ v L / / / _ _ _ \ . ' _ _ \ _ _ \ \ v v L / / \ / \ _ / \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Java\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ _ _ _ \\\n _ _ _ _ _ _ _ _ _ _ \\\n / / _ _ _ _ _ _ _ _ _ _ \\\n _ _ _ _ _ _ _ _ _ _ \\\n _ _ / _ _ _ _ _ _ _ _ _ _ \\\n _ _ _ _ _ _ _ _ _ _ _ _ _ _ /By\now it's probably painfully\napparent that your enviro\nnment hasbeen infected\nwith r	success or wait	1	F358DF	WriteFile
C:\Program Files (x86)\j\Downloader\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ _ _ _ \\\n _ _ _ _ _ _ _ _ _ _ \\\n / / _ _ _ _ _ _ _ _ _ _ \\\n _ _ _ _ _ _ _ _ _ _ \\\n _ _ / _ _ _ _ _ _ _ _ _ _ \\\n _ _ _ _ _ _ _ _ _ _ _ _ _ _ /By\now it's probably painfully\napparent that your enviro\nnment hasbeen infected\nwith r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Microsoft Analysis Services\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ _ _ _ \\ _ _ v _ _ _ _ v / / / _ _ _ _ \ . ' _ _ \\ _ _ \ \ v v / / \ / \ \ _ / \ _ \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\Program Files (x86)\Microsoft Office\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ _ _ _ \\ _ _ v _ _ _ _ v / / / _ _ _ _ \ . ' _ _ \\ _ _ \ \ v v / / \ / \ \ _ / \ _ \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Microsoft SQL Server\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \\ _ _ v _ _ _ _ v _ / / _ _ _ _ v . ' _ _ \ _ _ \ \ v v _ / \ _ / \ _ / \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\Program Files (x86)\Microso ft.NET\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \\ _ _ v _ _ _ _ v _ / / _ _ _ _ v . ' _ _ \ _ _ \ \ v v _ / \ _ / \ _ / \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Mozilla Firefox\IR3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \\ _ _ v _ _ _ _ v L / / / _ _ _ \ . ' _ _ \\ _ _ \ \ v \ L / / \ / \ _ / \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\Program Files (x86)\MSBuild\IR3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \\ _ _ v _ _ _ _ v L / / / _ _ _ \ . ' _ _ \\ _ _ \ \ v \ L / / \ / \ _ / \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Reference Assemblies\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \\ _ _ v _ _ _ _ v L / / / _ _ _ \ . ' _ _ \ _ _ \ \ v v L / / \ / \ _ / \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\ProgramData\Adobe\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \\ _ _ v _ _ _ _ v L / / / _ _ _ \ . ' _ _ \ _ _ \ \ v v L / / \ / \ _ / \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\dbg\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ v _ _ _ _ / / _ _ _ _ . ' _ _ _ _ \ \ / / \ / \ _ / \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\ProgramData\Microsoft\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ v _ _ _ _ / / _ _ _ _ . ' _ _ _ _ \ \ / / \ / \ _ / \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft Help\MS.EXCEL.16.1033.hxn	874	10	24 00 5e 01 00 00 00 00 00 00	\$^	success or wait	1	F2CC68	WriteFile
C:\ProgramData\Microsoft Help\MS.EXCEL.16.1033.hxn	0	350	fd ce 11 47 61 fd 0a fd fd 13 64 18 fd 3e 77 fd 5d fd fd 20 fd fd 4b 6b fd fd fd 16 fd fd fd 50 fd fd fd 1b 65 fd fd 3d fd fd fd 0c 34 2d 49 13 fd 1c 63 6f fd fd 77 fd 21 5f fd fd 76 23 fd 57 51 fd 4f 5c 43 fd e6 48 fd fd 35 28 fd 0c fd 07 2c 66 57 38 11 fd 5d 33 33 fd 5f 79 fd 7a fd 17 1c ce 16 fd fd fd fd 2a fd 4f 61 fd 7c 70 22 6a fd fd 20 56 fb fd fd fd 14 fd 44 6c fd 53 69 19 fd 4a 04 fd fd fd fd fd 43 fd fd 65 1f e3 ef 2d fd fd fd 2d fd 6a 3a 7e 57 fd fd 38 7a 47 7e fd 3a fd fd 28 57 4e 34 fd 74 fd 5b 38 57 28 7f 46 64 7d fd 57 fd fd fd fd fd 6f fd 37 fd 1b fd 6f 37 69 19 49 3e fd 5f 26 01 32 7f fd 82 4c 56 6a 62 fd 3b fd 1e 62 02 fd fd c8 fd 4f 6f fd fd 58 5e 33 20 2c fd 0f fd d8 fd 26 1d fd fd fd 25 44 fd fd 7e	Gad>w] KkPe=4-lcow!_v#WQO\CH5(,fW8]33_yz*Oa p"j VDI\$IJCe--j:~W8zG~:(WN4t[8W(Fd)Wo7o7il>_&2LVjb;bOoX^3 ,&%D~	success or wait	1	F2C055	WriteFile
C:\ProgramData\Microsoft Help\MS.GRAPH.16.1033.hxn	350	524	fd 6b fd 1a 30 fd 38 fd 5f 1b 5c fd fd fd fd 17 33 fd fd fd fd 59 0a fd fd 58 fd fd 8a 54 e0 fd 36 fd fd 07 09 9a fd 03 7f 25 fd 67 fd 59 fd 02 6e fd 0e 70 fd 7b fd 1f fd 4d fd 00 fd fd 23 fd 25 17 58 39 7d 23 47 fd 27 fd fd 41 2f fd fd 4e fd 06 fd fd 2f fd 75 07 fd 1f fd fd 2a 4a 21 fd 51 fd 16 fd 17 e1 71 fd 16 fd fd fd 42 6f fd 33 0b 3b fd 53 34 fd 83 01 fd 2a 1d fd 18 fd fd 60 fd 18 fd fd 7c 7c 68 fd 0d fd 3a 7f 48 fd fd fd 48 fd 1c cb fd fd fd 6b fd 0c fd fd fd 30 5e 37 39 41 39 fd fd fd 68 0c 75 4c 67 fd fd 57 fd 43 15 1c fd 0b 74 4c fd 6e fd fd 0f 03 fd 65 18 fd 33 56 fd fd fd 36 2c 7a 61 7b 2b 26 72 fd 51 fd 29 19 0b 27 fd fd 72 fd fd 36 87 fd 42 fd 4f fd 37 68 fd 1a fd 74 08 fd 12 10 fd 6d	k0_ \3YT6%gYnp{M#%X9 }#G'A/N/u*J !QBo3;S4*` h:HHk079A9 huLgWCtL ne3V6,za{+&rQ)'r6Bhtm	success or wait	1	F2CBF8	WriteFile
C:\ProgramData\Microsoft Help\MS.GRAPH.16.1033.hxn	874	10	24 00 5e 01 00 00 00 00 00 00	\$^	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft Help\MS.GRAPH.16.1033.hxn	0	350	5e 1d 32 3e 78 60 63 fd 8e 54 0d fd fd fd fd 03 2b 12 fd 4c fd fd fd 43 21 fd fd 6a fd fd fd 16 fd 7f 02 fd 1b 16 31 49 64 fd 22 49 4c 65 fd 5d fd fd 6c 0e 33 36 fd 61 65 fd 44 fd 19 59 fd f4 24 fd fd fd fd fd 5d fd 21 fd fd fd fd fd 3f 38 fd fd fd 0b 30 fd 05 fd 49 fd fd fd 26 fd fd fd fd 6a fd fd 53 11 fd 62 fd fd 19 a1 fd 69 fd fd 73 fd 19 36 fd 00 74 6b fd 25 fd fd fd 4c 5d fd 0c fd fd fd fd fd 6c fd 75 fd fd 28 32 20 fd fd 45 17 0a 74 fd 29 7e fd fd 51 17 10 68 1a 44 fd fd 27 7b 6a fd fd 18 6c 09 fd fd 66 10 fd 30 47 fd fd 4c 57 1a fd 06 7e 38 49 fd fd fd 11 fd 22 fd 51 46 44 64 20 3e fd 49 fd 06 47 fd fd 60 fd fd 62 fd 7c fd 35 4b 6d 54 fd fd fd 67 fd fd fd 75 6b 43 fd 30 fd 57 fd 64 4a 4a fd 33 fd 2c fd 2d fd 29 fd	^2>x' cT+LC!j1!"Le]]36ae DY\$!]?8 0l&jSbis6tk%L]lu(2 Et)~QhD'fjl f0GLW~8!"QFDd >IG`b5KmTgukC0WdJJ,-	success or wait	1	F2C055	WriteFile
C:\ProgramData\Microsoft Help\MS.GROOVE.16.1033.hxn	356	524	5b 39 34 fd 08 fd 68 1a 3b fd 3c 2e 24 1d fd fd 6e fd 03 6c 49 fd fd fd 02 fd fd fd 39 66 fd 66 fd 19 3e 3f fd 47 fd fd fd 13 fd 7b fd 24 fd 22 fd 42 fd 29 fd 49 2b 60 fd 13 6b fd 72 fd 53 c0 40 fd 78 fd fd 59 46 10 fd 0f a6 51 fd 07 57 fd fd 56 21 3a fd 21 fd 7d fd 03 51 fd fd 72 fd fd fd 77 18 fd 4e 55 fd fd 46 44 fd fd fd 42 87 5d 77 7b 48 fd 2b 55 fd fd fd 71 68 36 fd 6f fd 77 6e fd 76 fd fd 06 2f fd fd fd fd 55 1e fd fd 09 1b 4e fd 63 60 4b 14 fd 55 4b fd 08 5e fd fd 3f fd fd 12 33 65 5d 4b 1f 7a 30 fd 5e 01 fd fd 5a 6c fd fd 00 48 46 fd 59 fd 1c a6 fd 75 fd fd 76 fd 3e 77 fd 33 fd 2b fd 55 fd 61 fd 06 3f fd 76 4c 61 2b fd 47 66 34 fd fd 15 4c 5f 09 51 57 fd 4d 5f fd 17 43 fd fd 35 fd fd fd fd 51 1b fd 42 4e 62 fd	[94h;<.\$nll9ff>? G{"B)l!+`krS@x YFQWV!;!}rwNUFDB]w{H +Uqh6ownv/UNC'KUK^? 3e]Kz0^ZIHfYuv>w3+Ua ? vLa+Gf4L_QWM_C5QBN b	success or wait	1	F2CBF8	WriteFile
C:\ProgramData\Microsoft Help\MS.GROOVE.16.1033.hxn	880	10	24 00 64 01 00 00 00 00 00 00	\$d	success or wait	1	F2CC68	WriteFile
C:\ProgramData\Microsoft Help\MS.GROOVE.16.1033.hxn	0	356	5f 2a fd 28 44 40 fd fd 10 4a 52 fd 2f fd fd fd fd 6a fd 16 fd fd 0a 0e fd 6b fd 08 47 fd fd 0f fd 7a 01 fd fd fd 63 fd 41 6d fd fd fd 21 fd fd 4d 2f fd fd 67 6a 58 68 fd 70 37 36 0c 27 70 52 4b fd 22 37 fd 58 22 fd f1 fd 4d 17 fd fd fd fd fd 6a fd 74 41 fd fd 34 fd 19 fd 40 fd 31 6e 18 53 fd fd 4f 5a fd 69 fd 13 fd fd fd 3d 5e fd 31 2d fd 5c 10 fd fd 4f fd 31 41 fd 6f fd 7e 2e 33 12 fd 0b fd 0a 42 0f fd fd 06 2d 21 fd 67 fd fd 41 53 39 5d fd fd 24 27 fd 0f fd 14 15 fd 5b fd fd fd fd fd 2f fd 7e fd 3e 73 fd fd fd 44 7d 68 6f 40 50 fd fd fd fd 5d fd 02 41 fd 08 fd fd 0f fd fd fd fd 53 fd fd 60 fd 1e 29 1e 2f 3a 29 fd 94 7e a4 17 fd fd 0a 02 20 fd fd fd 0e 50 0d fd 44 21 74 fd 3e 52 38 fd 1c fd fd d6 fd 78 5a fd fd	_* (D@JR/jkGzcAmM/gjXhp 76'pRK"7 X"MjtA4@1nSOzi=^1- \O1Ao~.3-!gA S9]\${[/~>sD}ho@P]AS`)/:)- PD!t>R8xZ	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft Help\MS.LYNC.16.1033.hxn	344	524	0d 72 fd fd 08 fd fd 42 fd 71 6b fd 2c 84 fd 6f 5b fd 1b 29 fd 19 fd 56 27 03 fd 0e 28 4a 19 fd fd 58 37 fd 75 7e fd fd 4b fd 57 fd fd fd fd 7e 37 fd fd 00 30 fd 68 fd 5a fd fd fd fd 38 fd 39 fd fd fd 17 98 6c fd 21 70 60 fd fd 71 6d 29 16 04 12 fd fd fd 38 ae ea fd 51 5f 65 13 22 fd 5d fd 2f 20 fd 49 0e 18 f6 fd 35 71 58 4d 59 fd fd 62 6d fd fd fd 60 6f 05 fd 6a fd fd fd 39 77 a7 fd 1d 70 79 25 01 30 3e fd fd 35 37 fd 53 08 6e fd 74 18 fd fd 36 fd 23 fd fd fd fd 52 fd fd fd 43 6a fd fd 69 fd fd 79 2d 79 fd fd 77 fd 17 10 fd 20 58 0b fd fd 63 fd fd 1e fd fd 8f 1a 1f fd 29 fd fd fd fd 07 6e fd 69 39 4e 3b fd 6c 44 fd 29 fd 78 0d fd 5b 69 3a fd fd fd fd fd 31 68 26 0f fd fd 2f 76 79 fd fd 4c 49 02 5b 0a fd 5d 37 52 fd	rBqk,o]V'(JX7u~KW~0h Z89!l'p`qm)8Q_e")/ l5qXMYbm`oj9wpy%0>5 7Snt6#RCjly-yw Xc)ni9N;ID)x[i:1h &/vyLI[]7R	success or wait	1	F2CBF8	WriteFile
C:\ProgramData\Microsoft Help\MS.LYNC.16.1033.hxn	868	10	24 00 58 01 00 00 00 00 00 00	\$X	success or wait	1	F2CC68	WriteFile
C:\ProgramData\Microsoft Help\MS.LYNC.16.1033.hxn	0	344	fd 1b fd 2d fd 30 42 73 fd 2a fd fd 7c 11 4f fd 6d 64 fd 1e fd 76 79 fd a4 77 15 fd 10 06 fd 6c 2d 60 4d fd fd 69 fd fd 6c 6b 3e fd 01 fd fd 02 fd 6d fd 99 52 6b 7a fd fd 1a fd 38 6f 69 fd fd fd fd 78 fd fd 12 fd 04 fd fd fd fd fd 74 11 fd fd fd 28 0f fd fd 46 fd fd fd 70 6b fd 1e fd fd fd 15 72 29 fd 1a fd 7a fd fd 19 01 02 fd fd fd 00 fd 47 27 fd fd 79 fd b8 fd fd cc fd 1b f2 4d fd fd 2f 0c fd 16 fd 52 fd fd 22 71 2a 62 fd 7f fd 25 26 fd 3f fd 3f 02 fd fd 04 5f fd 21 fd 5c 51 fd fd fd 72 fd 19 fd 7f 33 fd fd fd 05 7b fd fd fd fd fd 56 fd 71 fd 5b fd 38 fd 4a 2d fd 77 08 0d fd 07 fd fd 6e 6c fd 4a 7e 48 6f fd 45 31 3a 46 6e 16 fd ad 16 fd fd fd fd fd fd 04 7b fd fd 28 fd fd 1b 61 fd 60 fd 1e ea 0c fd 04 fd fd fd 3a 7d	-0Bs* Omdvywl- 'Milk>mRkz8oixt(Fpkr)zG'yM/R"q*b&?? _!Qr3{Vq[8J- wnJ~HoE1:Fn(a`:)}	success or wait	1	F2C055	WriteFile
C:\ProgramData\Package Cache\I3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ v _ _ _ _ v \ / / / _ _ _ _ v : ' _ _ \ _ _ _ \ \ v \ / / \ / \ \ _ / \ _ \ _ \ _ _ \ _ _ \ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft Help\MS.LYNC_ONLINE.16.1033.hxn	0	386	fd fd fd fd fd fd 5e fd fd 7f 26 fd 5f 60 78 fd 7a 70 00 10 fd 45 25 fd 61 58 0d fd fd fd fd fd fd 24 fd fd 02 fd fd 66 25 fd 41 11 6f fd 64 fd fd fd 2d fd 66 fd 0f fd ac fd fd 3b fd 28 18 38 53 fd fd 39 fd 20 fd 68 fd 7a fd 29 fd 23 17 fd 11 71 00 fd fd 0e 5f 46 fd fd 37 fd 75 6b fd 1d fd fd fd fd fd 20 56 fd fd fd 22 06 fd fd 35 7e fd 59 fd fd fd 22 fd 15 fd fd 6c 09 7f fd 62 1e 61 11 bf fd b5 fd 43 2c 69 fd 28 fd 14 31 fd 24 19 fd fd 3d 2f 1a 28 6e fd fd 4f 73 57 fd 26 fd 68 fd 23 0f 58 1e fd 1c fd 7c 4b fd fd 7b fd 32 fd fd 69 7d fd fd 09 fd 63 32 fd 00 2d 2e fd 52 10 fd 12 74 fd fd fd 45 52 fd 0c fd 00 57 43 fd 7e fd 1c 19 fd fd fd fd fd 61 fd fd 0e fd fd fd 71 16 76 0d fd fd 6b 4b 7c fd 5a 42 4d 08 fd fd 7d	^&_`xzpE%aX\$%Aod-f; (8S9 hz)#q_7uk V["5~"lbC,i(1\$=/(nOsW&h # K{2i}c2- .RtERWC~aqvkK ZBM}	success or wait	1	F2C055	WriteFile
C:\ProgramData\Microsoft Help\MS.MSACCESS.16.1033.hxn	368	524	43 fd 4d fd fd fd 5d fd fd fd 65 fd 6a fd 43 19 20 07 5d 52 5c a8 fd 08 16 3b 7a 1d 58 fd fd fd fd fd 35 fd fd fd 46 fd fd fd fd 37 fd fd 5f fd fd b8 25 7f 24 5e 14 fd fd fd 29 72 3c fd fd fd 5b fd 25 7d fd fd fd 53 fd 70 fd 4a fd 15 4f 1f fd fd fd 03 fd 45 69 4c 07 fd fd 18 fd fd fd 7c 44 fd fd 7a 63 17 54 57 23 3f fd 20 79 60 29 fd 12 fd fd 06 78 fd 15 7c 07 32 fd fd 5a fd 26 fd fd fd 0c 11 14 d6 fd 64 50 38 fd 5e fd 06 fd 17 68 1e 78 fd 63 fd 7b 36 fd fd 16 0c 7d 48 fd 5e fd fd 18 13 24 c5 72 fd 16 68 3f 47 fd 6d 45 31 fd fd fd fd fd 6a 0a 42 02 fd 33 16 79 fd 7a fd 5a 5c fd fd 77 14 09 13 fd fd 76 fd fd fd 02 fd 02 fd fd 49 fd 3b 64 7c fd 73 69 21 1b 21 20 31 fd 10 fd 6b fd 24 2d 30 fd 5b 0c fd fd fd fd fd 5b 5f fd	CM]ejC]R\;zX57_%%\$^)^r<[%}SpO EiL DzcTW#? y`)x 2Z&dP8^hxc(6)H^ rh? GmE1jB3yzZ\wvl;d si!! 1k\$-0[[	success or wait	1	F2CBF8	WriteFile
C:\ProgramData\Microsoft Help\MS.MSACCESS.16.1033.hxn	892	10	24 00 70 01 00 00 00 00 00 00	\$p	success or wait	1	F2CC68	WriteFile
C:\ProgramData\Microsoft Help\MS.MSACCESS.16.1033.hxn	0	368	fd fd 6d 76 7f fd fd 39 2e 4e 06 fd 2d 20 fd 49 fd ec 1f fd fd 10 65 64 fd fd 14 7f 77 fd fd 4b fd 29 fd 71 34 7a 4b 73 fd 00 45 19 fd 37 fd c4 69 58 fd fd fd 1a 20 fd 79 3d fd fd fd 41 fd 5e 38 3c 6c 3d fd 48 fd fd fd 5d 1d fd 41 fd 44 35 3d 3f 56 35 fd 37 45 29 3c 47 fd 06 fd fd 62 fd 11 fd 32 fd fd fd 37 77 75 5b 1c fd 46 fd fd 5d fd fd 45 fd 81 fd 58 0b fd fd fd fd 17 0a 5b 7e fd 24 fd 46 fd 11 fd 36 e8 72 fd fd 7a 3c fd 2e 1e 46 2d fd fd fd fd 57 0d 32 51 fd 11 42 54 fd 2b fd fd 74 fd 6b 72 fd 02 7f 33 58 fd 14 4d 2c fd fd 5d 78 3e 05 fd 45 13 1a fd 40 1e 0e fd fd 30 6a fd 5d fd 67 3c fd 48 fd 30 a0 14 fd 76 5e fd 7b fd fd f5 fd 7c 53 17 61 fd 6b 10 fd fd 3c 5f 27 09 fd 67 fd fd 00 fd fd fd fd 64 99 12 08	mv9.N- ledwK)q4zKsE7iX y=A^8< =HJAD5=?V57E) <Gb27wu[F]X[~\$F6rz<.F- W2QBT+tkr3XM,)x>E@0j]g<H0v^[Sk<_'gd	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft Help\MS.MSOUC.16.1033.hxn	350	524	fd fd fd 2a 5a fd 0c 5a fd 67 fd 62 24 fd fd 55 33 fd 70 fd fd 1e 12 fd fb fd 28 22 fd 78 4c 40 53 14 68 fd 19 fd 74 2b 24 0c fd fd 02 79 fd 0e 68 fd 40 6d fd fd fd 47 11 fd 1d fd 14 fd fd 53 fd fd 19 fd fd 7b fd 55 fd 50 fd 0c 2e fd fd fd 7d fd 71 fd fd fd 3f fd 2f 47 fd 35 57 fd fd fd 22 fd fd 37 fd 44 43 fd fd 4b fd 0d fd 37 fd 64 ba 57 5d 59 fd 7f fd 17 08 fd fd 76 36 09 fd 4f 1b fd 59 32 4f 3d 1f 12 01 44 16 4a fd fd fd fd 0a fd fd 77 12 4a 77 fd fd 47 18 fd 27 fd 09 fd fd 25 fd 5e 59 fd fd fd 66 fd 5a fd 38 20 fd fd 4c 2d fd 67 fd fd 96 fd 01 fd 7a 33 9f fd 34 fd 1b fd fd 55 fd fd 0c fd fd 4d 02 fd 49 fd 66 fd fd 44 4d 04 06 03 fd 04 39 03 fd fd fd 69 fd fd fd fd 44 00 49 2a fd 4f 42 fd fd fd 13 49 68 3b 0a 33 fd	*ZZgb\$U3p("xL@Sht+\$y h@mGS{UP.} q?/G5W"7DCK7dW]Yv6 OY2O=JwJwG"%^YfZ8 L- gz34UMIfDM9iDI*OB!h;3	success or wait	1	F2CBF8	WriteFile
C:\ProgramData\Microsoft Help\MS.MSOUC.16.1033.hxn	874	10	24 00 5e 01 00 00 00 00 00 00	\$^	success or wait	1	F2CC68	WriteFile
C:\ProgramData\Microsoft Help\MS.MSOUC.16.1033.hxn	0	350	09 7b fd 51 7e 58 fd fd fd 63 fd 6e fd fd 0a fd 69 fd 71 fd fd fd 45 67 06 39 fd 08 fd fd 64 fd fd 26 52 59 fd fd 39 fd 7c fd 11 67 fd f3 0f 74 31 fd 1e 7b 1f 71 fd 1b fd 6b fd 12 4a 66 22 fd 16 fd 29 fd 30 fd 1f 67 42 fd 54 fd 16 fd fd fd 28 55 62 fd 4e 45 30 68 fd fd 39 fd 1f 21 04 fd 54 fd 43 fd fd 22 1e fd 1a fd fd fd fd 63 04 20 fd fd 2a 11 02 36 fd fd 55 5c fd fd 75 fd 59 36 1e fd fd fd fd fd fd fd 34 57 fd 24 fd 2b 0d fd fd fd fd fd 6d 13 41 fd 57 fd fd fd fd 33 f8 6a fd fd fd 4d 3a 06 fd 1b fd 01 fd 58 25 08 fd 25 fd 64 5d fd fd fd fd 10 fd 50 04 fd fd 42 fd 1c 31 69 13 fd 6f 64 06 3d fd fd fd 7b fd 27 71 fd fd 7d fd 4a 27 fd 09 fd fd 45 78 4f fd fd fd 18 4f 7e fd fd 27 41 cb 04 fd 2c 41 fd 5c 66 fd fd 1a 31 fd fd 2e fd 5e	{Q~XcniqEg9d&RY9]gt1{ qkJf")0gB T(UbNE0h9!TC"c *6U\uY64W\$mAW3 jM:X%%d]PB1iod= {q}J'ExOO~'A,Af1.^	success or wait	1	F2C055	WriteFile
C:\ProgramData\regid.1991-06.com.microsoft\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ _ _ \ \ / / _ _ _ \ . ' _ _ \ _ _ \ \ \ / / \ / \ \ _ / \ _ \ _ \ _ _ \ _ _ \ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft Help\MS.MSPUB.16.1033.hxn	350	524	6d fd 32 5b fd fd 7b fd fd 48 54 fd 3c 49 65 fd fd 4b 12 3e 3e 17 fd 63 fd 36 70 49 7d fd fd fd 2d fd 2c 63 fd fd 4e 3e 09 79 1a fd 18 3a 4e 31 3d 46 0b 52 fd fd 00 fd fd fd fd 18 fd 35 3a 5e 03 fd fd fd 68 fd 04 fd 1d fd fd 5c 4b fd 7d fd 2c fd 50 5a fd 1a 6a 28 fd fd fd 5a fd 21 06 fd 33 fd fd fd 13 fd fd fd fd 2b fd fd 65 19 7e 27 45 3f 11 fd 77 fd 43 fd fd 0e 13 ff f9 7b 0f 22 48 5b fd fd 1a fd 73 24 49 4a 5c 54 1e 33 13 20 fd 71 07 46 11 6a 2a 56 fd fd 13 fd 16 fd 36 fd 2b 7a 6d fd fd 0a 4d 08 fd fd fd 5a 1a 32 cd 77 fd fd fd 65 75 fd 5d fd 21 fd f1 fd 00 fd fd fd 42 44 01 47 38 fd 0e 28 fd 6b 65 e2 66 fd ee 69 fd 2e 3e 08 1a 13 fd fd fd fd 3d fd fd 69 38 3d fd fd fd 4c 5a fd fd fd fd 05	m2[{}HT<leK>>c6pl)- ,cN>y:N1=FR5 :^\K},PZj(ZI3+e~'E? wC{"H[s\$IJ\T qFj*6+zmMZ2weu)!BDG8 (kef.>=i8=LZ	success or wait	1	F2CBF8	WriteFile
C:\ProgramData\Microsoft Help\MS.MSPUB.16.1033.hxn	874	10	24 00 5e 01 00 00 00 00 00 00	\$^	success or wait	1	F2CC68	WriteFile
C:\ProgramData\Microsoft Help\MS.MSPUB.16.1033.hxn	0	350	fd 00 23 16 69 2e 15 47 fd fd fd fd fd fd 5c ba 74 7a 01 fd 2a 79 6e 2b 1a 51 fd 3b 27 fd fd fd 22 20 28 31 03 fd 21 fd 12 3b 49 76 fd fd 0c 54 70 00 ec 11 fd 20 2f fd fd 13 fd 23 28 fd 5c 47 23 44 fd 51 fd fd fd 64 fd 5e 60 3d fd 12 60 2b 1d 3e 0f 02 72 7c fd 0d 02 fd 3e fd fd 19 45 63 fd fd 72 45 2c 1c 04 fd fd 43 70 fd fd 3d fd fd 7b 71 47 fd 30 fd 47 fd fd 28 0f 0e fd 7e fd 88 0f fd 29 4f fd fd fd 1d 4b 7e fd fd fd 47 fd 23 fd 2b fd fd fd 0f 74 12 fd 47 fd 73 fd fd 0d 79 fd fd fd 62 70 fd 2e fd fd 45 fd fd fd 59 0c fd fd fd 4c 44 fd 74 58 6b fd 70 17 41 33 43 fd fd fd fd fd fd fd fd 2d fd fd fd 09 fd fd 53 fd 06 fd 09 69 fd 6c 4b fd fd 06 0f fd 6b 72 40 2e 2a 57 36 fd 3f 51 76 71 fd fd 30 fd 59 24 68 30 fd 7a fd 40 fd	#i.Gltz*yn+Q;"' (1!;lvTp /# (\G #DQd^`=+>r EcrE,Cp= {G0G(-)OK~ G#+tGsybp.EYLDtXkpA3 C-Silkr@.*W6? Qvq0Y\$hoz@	success or wait	1	F2C055	WriteFile
C:\ProgramData\Microsoft Help\MS.ONENOTE.16.1033.hxn	362	524	fd fd 52 6b fd 7f fd fd 4f 56 5a fd fd fd 34 fd fd 7e 64 0e 6f fd 75 fd 01 72 fd 5f fd 30 fd 06 3d 46 fd 04 54 fd 44 fd 54 fd 7f fd 6c 76 fd 25 fd fd fd 36 16 44 fd fd fd 2b 13 6a fd 2d 07 fd fd 40 26 fd 26 61 fd 61 fd 4b fd 0e 62 fd 58 fd 43 fd 12 44 fd 63 fd 3c 5f 29 0c 34 70 11 0d 04 51 fd 2f 7b fd fd 12 07 7c 3a fd fd 11 5f fd 04 4d 41 63 fd 20 fd fd fd 5b 78 2a 41 13 fd fd fd fd 06 35 74 dc 01 25 fd 33 fd fd 51 fd fd fd fd 37 fd 73 79 fd 74 33 fd 7c fd fd fd 39 fd 10 fd 47 fd 4b 07 fd fd 6b fd fd fd fd fd 26 1f fd fd fd fd 0c 07 53 1d 38 fd fd 4a 83 fd fd fd fd fd fd 37 fd 0e fd 4f 1a 55 1f fd 1e 53 10 fd 59 7b fd 32 1e fd 79 fd 16 64 1c 1e fd 55 fd 38 04 30 0a ba 12 2e fd fd 1e fd fd fd fd 54 fd 78 03 fd 7a fd 72 7e	RkOVZ4~dour_0=FTDTIv %6D+j-@&&a aKbXCDC<_4pQ/{ :_Mac [x*A5t%3Q 7syt39GKk&S8J7OUSY{ 2ydU80.Tx zr~	success or wait	1	F2CBF8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft Help\MS.ONENOTE.16.1033.hxn	886	10	24 00 6a 01 00 00 00 00 00 00	\$j	success or wait	1	F2CC68	WriteFile
C:\ProgramData\Microsoft Help\MS.ONENOTE.16.1033.hxn	0	362	72 de fd 72 fd fd 58 fd fd 4e fd fd 37 6d fd 11 fd 6e 26 23 35 5a fd 4f 56 62 33 08 21 fd fd 0d 14 06 49 fd 46 fd 42 4e fd fd 3f fd fd fd fd 15 fd 69 6e 7f 6b fd fd 73 fd fd fd 6e 41 cb 4b fd fd fd 1f fd 3d fd 29 18 0c fd 15 fd 76 61 aa 37 4a fd 3f 1d 6b 00 fd fd 00 0b fd 4e 71 2c 41 fd 47 77 fd 26 fd 51 fd fd fd fd 5b fd fd 48 5e 7a 50 35 05 1e 19 53 fd 69 fd 3d 2d 60 78 fd fd 67 b7 fd fd 6f fd 2d fd fd fd 44 56 13 fd 0d 0e 6a d6 18 fd 52 24 fd fd 34 fd 0a fd 2d fd 57 fd 51 fd 26 fd 51 fd 17 fd fd fd 33 06 fd 52 14 20 2b 6d fd 5c 2e 05 43 fd 78 16 2d 3a 6a fd fd fd fd 2e 63 fd 3a fd 5b fd 3d fd 7d fd 17 66 45 5d 26 29 0a fd fd 50 fd fd 11 fd fd 1b 3b fd 14 1d 5c 2b fd fd 37 fd 17 fd 14 41 fd 06 68 fd 2b 79	rrXN7mnZOVb3!!IFBN?inksnAK=)va7J?kNq,AGw&Q[H^zP5Si=-`xgo-DVjR\$4-Q&Q3+m\Cx-j.c:[=]fE]&)P;,+7Ahy	success or wait	1	F2C055	WriteFile
C:\ProgramData\Microsoft Help\MS.OUTLOOK.16.1033.hxn	362	524	69 fd fd fd fd 6f 50 3b 3e 50 fd fd fd 04 08 fd fd fd 7c fd fd 27 5c fd 27 fd fd 44 fd 4b 7c 17 69 39 5b fd 4c 05 4d 3a fd 25 1c 2e fd fd 33 48 29 24 fd fd 3f 4d 6e 4b fd 09 65 fd 1a 33 50 fd 25 4a 60 0b 34 fd 4f 59 f8 15 09 6f 34 1b aa fd 24 27 fd fd 33 3b 56 7d fd fd fd fd 7c 3c 19 1f fd 7a 4e 4b fd 0c fd 7e fd 38 6b fd 07 79 fd 0c fd 46 fd fd fd fd 54 5d 04 56 78 fd fd 73 fd 18 fd fd fd 37 22 fd 64 fd 44 33 fd fd 66 35 fd 51 2d fd 5d 6d 12 fd 61 63 fd fd 17 fd fd 44 4d 56 fd fd 54 16 03 fd 40 06 08 fd 38 fd fd fd 0e 59 0b 51 21 fd 44 fd 2b fd 3b 50 fd fd 76 03 fd 42 fd 6e 05 7f fd 10 fd 6a fd fd 44 fd 75 0c 58 fd 4d fd 2c 29 fd fd 55 5b fd d4 2b fd fd 37 54 fd fd fd 27 fd fd 68 14 36 74 fd fd 07 fd 5e 58	oP> \`DK i[LM:%.3H)\$?MnKe3P%J`4OYo4\$3;V]l<zNK~8kyFT]x7"dD3f5Q-]macDMVT@8YQ!D+;PvBnjDuXM,)U[+7T'h6t^X	success or wait	1	F2CBF8	WriteFile
C:\ProgramData\Microsoft Help\MS.OUTLOOK.16.1033.hxn	886	10	24 00 6a 01 00 00 00 00 00 00	\$j	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft Help\MS.OUTLOOK.16.1033.hxn	0	362	20 1e 3f 03 18 7e 63 fd 09 44 77 56 26 45 fd fd 23 23 fd 3e fd fd fd 78 1a 55 52 fd 4e 64 5f 23 70 fd fd fd fd 3a fd 50 fd fd 47 fd 1a 2d 68 1a 0e 02 fd 05 fd 12 32 fd 75 1d fd 2e fd 50 72 fd 4d fd fd 29 fd 39 fd fd fd fd 64 79 23 7f 4d fd fd fd 40 fd fd 7c fd 5b 6c fd fd 42 7f fd fd 6b fd 23 fd fd fd fd 02 fd 7d fd 7a 21 37 fd fd fd 21 39 fd fd fd fd 3d 74 fd 02 fd 21 63 fd fd 33 fd 4b fd fd 1c 28 4c fd 0f fd 13 28 63 b8 71 fd fd fd fd fd 77 fd fd 44 2c 68 fd fd fd 27 25 71 fd 64 9e 68 fd fd fd 10 61 fd 34 fd 12 fd fd 1d 09 fd 42 2d 61 fd fd fd 44 fd fd 54 28 fd fd 5f fd 62 fd 70 fd fd 5a 4b 62 fd 63 3e 18 29 fd fd 32 59 05 79 fd 57 fd fd 29 fd fd 0f 39 fd 04 47 37 47 11 fd fd 7c 35 86 25 fd 0f fd 0f 64 fd 2d fd	? ~cDwV&E##>xURNd_#p: PG-h2u.PrM)9dy#M@ Bk#z!7!9=tlc3K(Lqw D,h%qha4B- aDT(_bpZKbc>)2YyW)9 G7G 5%d-	success or wait	1	F2C055	WriteFile
C:\ProgramData\Microsoft Help\MS.POWERPNT.16.1033.hxn	368	524	fd 39 2b fd fd 1b 44 6a 42 fd 62 6f 3b fd 6a fd fd fd fd 55 fd 67 2c 22 fd fd fd 7c fd fd 7a 7e 56 1e fd fd fd 7e fd fd 4a 42 48 fd d8 0d 56 fd 40 fd 21 77 35 21 fd 30 fd 35 65 fd fd 7c fd 15 fd fd fd 58 fd fd 1c 6c fd 4b 42 55 fd fd 2b fd 69 20 fd fd fd 41 4c fd 50 44 4f 20 4a 62 fd 46 29 7a 60 0c fd 27 fd 5b fd 0d fd fd 08 79 42 fd fd fd 0b fd fd 44 7c 20 fd 45 fd 1f fd 0f 01 fd 69 79 fd fd fd fd 61 fd fd fd 6d 0a 3f fd 13 fd 42 fd fd 0c fd 60 fd fd 35 6c 46 fd fd 45 2b fd 7d 53 52 fd fd fd 73 c0 2b 4f 53 51 bd 34 71 62 fd fd fd 28 1d fd 7d fd 6c 55 48 fd fd fd 06 0b 00 69 18 fd 18 fd 5c 48 fd fd fd 18 68 48 fd fd 30 1f fd fd 2c 15 fd 7c fd fd 53 fd fd 3b 40 fd fd fd fd 24 fd fd 29 71 fd 53 72 74 55 63 67 fd 5b 73 fd 49 fd 00	9+DjBbo;jUg," z~V~JBHV @!w5!05e XIKBU+i ALPDO.JbF)z` yBD  Eiy am? B`5IFE+)SRs+OSQ4qb(UH!Hh H0, S:@\$)qSrtUcg sl	success or wait	1	F2CBF8	WriteFile
C:\ProgramData\Microsoft Help\MS.POWERPNT.16.1033.hxn	892	10	24 00 70 01 00 00 00 00 00 00	\$p	success or wait	1	F2CC68	WriteFile
C:\ProgramData\Microsoft Help\MS.POWERPNT.16.1033.hxn	0	368	7c fd fd fd 24 fd 33 4b 5d fd 44 fd 2b 5e fd 3c fd b3 fd 58 fd fd 2e 07 11 15 3c 16 fd 1b 4a fd fd 0c 5e 74 62 1b fd 1f 65 fd 2a 6b fd fd 73 fd 6b 54 fd 67 fd fd 70 28 fd fd 3a 74 fd 20 fd fd 3a 1a 2d 65 06 57 44 fd 4f fd fd 0c fd fd 14 fd fd fd 46 18 64 31 fd fd 34 fd fd fd fd 06 fd 28 fd 0c 58 05 2e 3a 5a fd fd 11 52 2f fd fd 62 0c 77 5b fd 6c fd 25 25 6f 06 6a fd fd fd fd 66 0c 44 fd 3f 5b fd 65 fd 18 3b 27 fd 4c 34 fd fd fd fd 2a 56 2f fd fd fd 06 21 fd fd fd fd 73 60 45 4a fd fd 03 6b fd 4b 7e 61 22 62 1e fd 3b fd 09 fd fd 03 fd 13 0c fd 09 23 65 fd fd 07 47 fd fd 09 fd 3c fd 36 af fd 1f 5c 78 fd 6c fd 5e fd fd 55 41 fd 13 75 1e fd f1 fd 14 fd 46 fd 60 72 fd ff 59 7f 30 0b 63 fd d0 fd 73 67 05 fd 2f fd 00 fd	[\$3K]D+^<X.J^tbe*kskTg p(:t :-e WDOFd14(X.:ZRBw l% o fD?[e;'L4 *V!s`JkK-a"b;#G<6 x ^U AuF`rY0csg/	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\SoftwareDistrib ution\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ _ _ _ \ _ _ _ _ _ _ _ \ / / _ _ _ _ _ \ _ _ \ _ _ \ \ _ _ / \ / \ _ / \ _ \ _ \ _ \ _ \ _ \ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\ProgramData\Microsoft Help\ MS.SETLANG.16.1033.hxn	362	524	fd fd fd 62 fd fd 19 4d 59 fd 4e 08 13 fd fd 16 28 fd 61 fd fd 1a 1a fd fd 5a fd 27 02 1a fd 52 fd 26 fd fd 43 61 4a fd 4b fd 31 1c fd 1a 21 04 6a fd 05 fd 08 4d fd 44 03 fd 4d fd 37 fd 69 1a fd fd 22 fd 52 fd fd 27 fd 3c 72 fd 26 fd fd 16 fd 2e fd 12 fd fd 6a fd 24 fd fd 4d 1e fd 05 14 44 fd fd 0d 14 fd 59 72 40 7c fd fd 21 fd 72 0f 10 40 3e fd 3d fd fd 33 6a 65 2d 58 03 32 fd fd 26 fd fd 3c fd 43 4a 3a fd 63 fd fd 4d 23 79 fd fd 39 00 fd cc 26 5d fd 73 fd 65 14 25 fd 52 10 fd 4f fd fd 31 fd fd 41 fd fd 10 fd 7f 0c c1 7f fd 3e fd fd fd 0a fd fd fd 13 00 fd 65 fd fd fd 50 7b fd 01 fd fd 01 fd 1a fd fd fd 0b fd 4e 49 64 62 56 fd fd 68 fd 07 fd 3d fd 41 5e fd 09 fd 1e 4b 0d 78 49 2c 47 f9 6b 23 fd 69 1b 05 06	bMYN(aZ'R&CaJK1l)MD M7i'R'<r&.j \$MDYr@ !r@>=3je-X2& <CJcM#y9&]s e%RO1A>ePNdbVh=A^K xl,Gk#i	success or wait	1	F2CBF8	WriteFile
C:\ProgramData\Microsoft Help\ MS.SETLANG.16.1033.hxn	886	10	24 00 6a 01 00 00 00 00 00 00	\$j	success or wait	1	F2CC68	WriteFile
C:\ProgramData\Microsoft Help\ MS.SETLANG.16.1033.hxn	0	362	24 fd fd 07 fd 29 fd fd 21 5d 16 fd 63 fd fd 61 fd 40 30 fd fd fd 3b fd 28 fd fd fd 56 41 fd fd fd 1a 4c fd fd fd fd 4c 38 02 5b 5c fd fd 2c fd 22 21 0a fd 51 fd 7b fd 34 fd fd fd 63 14 08 39 fd 48 30 25 fd 3b 58 fd fd fd 05 2a de fd 7d c1 fd 0f 45 fd fd 1e fd fd 59 fd fd fd fd fd 5c 74 fd 21 fd 1c 3d 5f 3f 29 fd fd 11 3d 54 fd 69 0d fd 3f 17 7b fd 30 10 4c fd fd 5f fd fd fd 56 73 f4 6d 6d fd 11 00 7b fd fd fd 09 fd 2a fd 2f fd 00 2b fd 4d fd 36 58 fd 4d fd 51 27 51 fd fd 27 42 fd fd fd 04 fd fd fd fd 29 1e 44 69 fd fd 6b fd fd f4 fd 4b fd e8 0d fd 7e fd 24 fd 4b fd fd fd 2b fd fd 42 fd 46 3f fd 6e fd fd 60 6c 07 fd 4c fd 12 34 fd 55 fd 2e e9 29 fd fd fd 71 7e 1a fd fd fd 47 25 7c fd 19 18 fd fd fd 56 73 fd	\$)l]ca@0; (VALL8\,"!Q{4c9H0%;X* }EY\!!=_?)=Ti? {0L_Vsmm{*+M6XMX Q'Q'B)DikK~\$K+F? n`lL4.)q-G% Vs	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft Help\MS.SKYPEFB.16.1033.hxn	362	524	fd 41 fd 3e fd fd fd 1f 67 fd 65 02 fd 52 d3 fd 36 f7 fd fd 08 fd fd fd 7e fd 51 61 69 0a 1e 39 41 fd fd 26 4d 4f fd fd 45 fd 25 47 fd 42 fd fd fd 71 12 fd 06 48 25 fd 1c 0e fd fd 12 fd 05 fd 67 fd 21 fd 31 fd fd fd 3f 26 59 fd 0c fd 1e 0f fd 1f fd fd 22 67 fd 6d 37 fd 26 fd 47 4b fd fd fd 38 4a 49 0e 17 15 fd 4f 43 52 fd fd 60 1d 1c 07 fd 8e 0d fd 27 fd fd 25 3a fd fd 5b 04 fd fd 3d fd fd fd 3a 27 05 fd 52 19 fd 1d 28 fd 37 32 fd fd 45 fd fd fd 03 fd 4e fd 60 fd 1c fd 7a 31 1d fd 1d 01 fd fd fd 2c fd 94 31 20 fd 44 fd fd 23 5d 5e 25 49 4b fd fd 50 fd 25 fd fd fd 0c 3a 32 fd 7d fd fd fd 12 fd fd fd 65 06 fd 0f fd 1c fd 2d 13 0d fd fd fd 08 fd fd 6c fd 17 be fd fd fd fd 0e 2a fd 45 fd 30 4d 0a 02 fd fd	A>geR6-Qai9A&MOE% GBqH%gl1?&Ygm 7&GK8JIOCR"%: [=:R(72ENZ1,1 D #]^%KP%:2)e-l*EM	success or wait	1	F2CBF8	WriteFile
C:\ProgramData\Microsoft Help\MS.SKYPEFB.16.1033.hxn	886	10	24 00 6a 01 00 00 00 00 00 00	\$j	success or wait	1	F2CC68	WriteFile
C:\ProgramData\Microsoft Help\MS.SKYPEFB.16.1033.hxn	0	362	51 2d fd 77 fd 31 fd 0a 08 4d fd fd 7a 2f fd 50 1b 2c 3b fd fd 2b 39 fd fd 5e fd fd 28 fd 55 c8 0f 34 fd 57 12 11 fd 29 fd 50 fd 24 6b 7b 98 34 5e 23 41 26 fd 2e 4c fd fd fd 59 09 33 09 59 23 fd 24 fd 48 fd fd 11 fd 42 26 1e 5a 6e 63 67 fd 73 39 21 fd fd 70 fd 13 fd 64 cd 64 4d fd 59 27 fd be 60 fd fd 61 1d 1a fd 7f fd 69 4d 2c 29 fd fd b0 35 5d fd fd 67 fd 67 fd 35 fd fd 5b fd fd 5b 69 fd 1d 13 a1 fd 7d fd 40 25 fd fd 73 1b 5c fd bb fd fd 27 66 49 20 40 fd 1a 17 fd 5f 29 66 fd 52 05 43 fd 19 fd fd 4b fd 2c 00 fd 11 3f 77 fd 34 fd fd fd fd fd fd fd 45 0c 3d 5f 09 79 5f fd fd fd 76 7c 37 6d 3e 4b 64 6e fd 4c fd 15 fd fd 0e fd fd 39 10 5b 64 77 fd 71 fd fd 00 7e 2e 37 1e fd 62 fd fd 39 fd 5d fd 7c fd fd 1f	Q- w1Mz/P,;+9^(U4W)P\$k{4 ^#A&.LY 3Y#&HB&ncgs9lpddMY'a iM.)5]gg5[[i]@%s'l @_)fRCK,? w4E=_y_v 7m> KdnL9[dwq~-.79]]	success or wait	1	F2C055	WriteFile
C:\ProgramData\Microsoft Help\MS.SKYPEFB_BASIC.16.1033.hxn	398	524	fd 60 fd 6c 1c 40 63 8a fd fd 30 42 fd 3e 04 fd 36 54 fd fd 44 09 10 7c fd fd 72 7e 61 fd fd fd 55 78 fd 21 10 59 35 fd 49 07 fd fd 02 fd fd 35 fd fd fd 11 53 dc 2e 4c 0f 4c 34 fd 0d 35 fd 26 fd 51 13 48 fd fd fd fd 73 13 fd fd fd 20 fd 44 25 fd 5e 1c 35 16 5f fd 23 fd fd 63 51 3e fd fd fd 19 38 41 4b 7a fd 05 27 6e 7e 74 fd 0e 7d 30 2e fd fd 23 fd 15 fd 51 12 6d fd fd fd fd 28 fd fd 58 4a 78 fd 6c fd 4f 3d fd 5b 64 3c fd 2c fd 6a 6a fd 63 fd fd 5b fd fd fd 6c fd fd 69 70 3a 37 74 06 fd fd 40 fd fd 0e 13 64 33 34 14 fd 0e 42 4c 49 31 28 fd 6d 42 fd 51 fd fd 6f 54 00 41 fd fd fd 5c 39 4f fd 0f fd 19 fd fd 1b fd 28 fd 78 fd 26 fd 5d fd 1f fd 59 fd 15 fd 49 fd 4e 19 2a fd fd 5b 56 fd dc fd 36 fd 4d 30 46 fd fd 18 66 fd 3d 6c fd 5b fd fd fd	`l@c0B>6TD)r~aUx!Y5I5 S.LL45&QHs D%^5_#cQ>8AKz'n-t}0.# Qm(XJxl O=d<.jjc[lip:7t@d34BLI1(mBQoTA!9O(x&]YIN* [V6M0Ff=[	success or wait	1	F2CBF8	WriteFile
C:\ProgramData\Microsoft Help\MS.SKYPEFB_BASIC.16.1033.hxn	922	10	24 00 fd 01 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft Help\MS.SKYPEFB_BASIC.16.1033.hxn	0	398	fd 0b 0d fd 74 fd fd 03 0b fd 07 fd 36 1e 76 fd 5f fd 20 fd 6d fd 52 fd 2e 0a 05 2e 40 fd fd 6a fd 1a fd fd 63 fd 78 fd fd 13 fd fd 44 fd 1f fd 41 fd 56 1e 18 13 51 46 04 fd fd 34 19 fd 04 fd fd 21 fd fd 67 fd 2f 57 fd fd ed 76 25 13 fd fd 25 40 3b 10 56 4d 61 fd 69 fd 50 4d 00 fd 02 fd 5a fd 5e 4c fd 7f 48 fd fd 57 11 71 2f fd 28 16 fd fd fd fd 10 fd fd fd d7 fd 56 20 4d fd 48 6d 44 fd 53 fd 6b fd fd 4b 31 fd fd 22 fd 3c fd 71 fd fd 27 fd 04 11 fd 32 59 55 fd 3b 78 78 fd fd 17 3d fd 2a 14 fd fd fd 27 fd fd fd 1d 11 1f fd fd fd 27 39 fd 51 58 fd 2d fd fd fd 3f fd 6f fd fd 79 14 fd fd fd 5e 25 3d 3b fd fd 45 fd 1b 53 35 fd 69 fd fd 1d 27 fd 61 fd fd fd 78 49 cc fd 22 fd fd 0e 13 e0 fd fd 5a fd 2d 77 fd fd fd 0f 11 fd 6e 29	t6v_ mR..@jcxDAVQF4!g/Wv %%%@;VMiPMZ^LHWq/(V MHmDSkK1"<q'2YU;x x="9QX-? oy^%=;ES5!axl"Z-wn)	success or wait	1	F2C055	WriteFile
C:\ProgramData\Microsoft Help\MS.SKYPEFB_ONLINE.16.1033.hxn	404	524	64 65 43 7b 0c fd 08 fd 5c 27 5f fd fd 0c 7a fd 6c 4e fd 1a 7c fd fd 5d fd 3e fd 8c 00 27 59 5c 79 7e 62 11 3f fd fd 00 6f fd 0e 5c 74 fd 39 6d 1f 20 0e fd fd 69 fd 6e 69 fd 15 5a 28 0b 60 fd fd fd 2b 5c fd 58 5b 0d 24 4a fd 5c fd 7e 73 fd fd d1 18 61 43 fd fd 52 02 39 70 fd fd 76 fd fd fd 07 38 66 3e 0b 63 fd fd 13 fd 3a 66 fd fd 27 fd 2a 4f 40 fd 38 fd 15 e2 fd 63 33 34 2b fd 74 2b 6e fd 49 fd fd 6d 27 43 27 fd fd 23 5f 43 fd 0f fd fd 1d fd 10 4a fd 5f 0b fd fd 5e 5f 00 18 fd 7c 00 fd fd 45 fd 2b 41 2b fd d4 29 18 5d fd fd 22 fd 4a 14 fd a7 fd fd fd fd 60 fd 6d 31 fd fd 66 37 04 fd 3a 72 24 25 7b 6e fd 75 6e fd fd 5c 2c 24 6e 2a 65 5d fd fd 49 31 5b 1e fd fd 1c fd fd 54 3f fd fd 61 7b fd 18 0b 68 0c 3c fd 05 67 fd	deC{[_zIN]]>"Yly~b? o!t9m niZ(`X[\$J]~saCR9pv8f>c:f*"O @8c34+ t+nlm'C'#_J^_]E+A+)]"J` m1f7:r\$% {nun\,\$n*e]l1[T?a{h<g	success or wait	1	F2CBF8	WriteFile
C:\ProgramData\Microsoft Help\MS.SKYPEFB_ONLINE.16.1033.hxn	928	10	24 00 fd 01 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\ProgramData\Microsoft Help\MS.SKYPEFB_ONLINE.16.1033.hxn	0	404	fd fd fd fd 2a 09 4c fd 54 fd fd 66 fd fd fd 7f 6e fd 2b fd f1 3c fd 2e fd 15 fd 65 71 60 00 24 fd fd 6c fd fd 0e fd fd 59 4e fd fd fd 59 49 6f fd fd 1f fd fd fd 02 fd 0d fd 0f fd 3f 20 58 30 1c fd fd fd 32 5b d0 fd fd 46 00 fd fd 02 fd 2d fd 77 5c 39 71 fd 51 fd 39 fd fd fd fd 6d 7b 3b fd 6f fd 02 fd 01 fd fd 4c fd 1c 5d 1f 64 4a 62 fd bb fd 0f 76 26 fd fd 7d 2e fd 04 fd fd 5f 63 5d 3d 5a fd 47 6f fd fd fd 21 29 fd 23 fd 48 fd 39 fd fd 51 fd 2c fd fd fd 43 31 41 fd 33 54 fd 58 fd 39 58 7b 30 09 18 fd 09 5e 4a 00 47 6c 12 0d 2e 38 25 75 fd fd 27 fd 1f 48 fd fd 40 29 fd fd 21 fd 4c 48 4e fd 4b 3f fd 4a fd 76 fd 50 fd fd fd fd 1f fd 76 fd 73 fd fd 1b fd fd fd 7e 69 fd 04 25 6a 65 70 3d fd fd 62 fd fd 13 16 fd 25 fd fd 31	*LTfn+<.eq"\$IYNYIo? X02[F-w!9q Q9m{;oL]dJbv&}. _c]=ZGo !)#H9QC1 A3TX9X{0^JGl.8%u'H@)! LHNK?JvPvsi9jep=b%1	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\USOPrivate\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ _ _ _ \ _ _ v _ _ _ _ \ / / _ _ _ _ \ . ' _ _ \ _ _ \ \ _ _ / / \ _ \ \ _ / \ _ \ _ \ _ _ \ _ _ \ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\ProgramData\Microsoft Help\MS.SKYPEFB_ONLINEG.16.1033.hxn	410	524	fd 7e 39 fd fd 27 fd fd 41 60 fd fd 54 5a 08 35 2a 3e 5a 34 10 29 08 41 3c fd fd 33 fd 57 fd 40 6f fd 53 09 6d fd 60 7a fd 6a 57 0c 39 fd fd fd 5c fd fd fd 5c fd 5b fd fd 1e 07 14 48 59 35 fd fd 64 22 fd fd fd 27 6b 39 4c 76 11 fd 7a 4c fd 34 fd 66 5e 25 fd 16 16 67 38 fd 55 1d fd fd 2e fd 62 fd fd 5f 38 fd 6d fd 00 fd fd fd fd fd 5e 2e fd 30 07 fd 59 6a fd 09 b8 23 57 01 3a fd fd fd fd fd 4e 03 fd 6d fd 09 fd bc fd 5e fd fd 47 fd fd 56 6d 55 fd 64 fd fd fd 5b fd 00 74 4c 3a fd fd fd 73 0e 38 4b fd 76 fd 71 20 fd fd fd 5b 19 61 fd fd fd fd fd 21 20 fd fd fd fd fd 0f 68 5b 26 38 7c fd 58 39 0d 37 7f 1e fd 2e fd fd fd fd fd 3e fd 7c 4e fd fd fd 72 2d fd fd fd fd 0a fd 37 fd c7 49 fd fd 47 fd fd 34 fd fd fd	~'9'A`TZ5*Z4)A<3W@oS           m`W9\ [HY5d ""k9LvzL4f^%g8U.b_8m^. 0Yj#W:Nm ^GVmUd[tL:s8Kvq [a! h[&8]X97> Nr7IG4	success or wait	1	F2CBF8	WriteFile
C:\ProgramData\Microsoft Help\MS.SKYPEFB_ONLINEG.16.1033.hxn	934	10	24 00 fd 01 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft Help\MS.SKYPEFB_ONLINEG.16.1033.hxn	0	410	70 fd 31 3e fd fd 71 54 7c 00 fd 03 fd fd 26 fd fd fd 0f fd 30 45 05 51 2d 40 fd 01 7f 76 69 fd fd 35 fd 64 4b 7c 7b fd 09 fd 06 58 fd fd fd 51 fd 4d 1b fd 1a fd fd fd 77 fd 6f 44 fd fd 3e 12 fd 06 45 77 20 16 47 fd fd 7e 75 fd 02 fd 50 fd fd 20 b3 24 34 fd 1a fd 38 fd 44 56 fd 09 fd fd fd 40 44 fd 14 0b 1d fd fd 4b 6a fd 17 1c 77 fd 6e fd 0f 19 1e 04 1a fd fd fd 15 67 1c fd 70 5e 5f fd d9 fd 5e fd fd fd 3c 6d fd fd fd 11 38 79 54 fd fd fd 38 fd fd f2 68 6b fd fd 00 22 55 07 fd fd fd 7a 48 68 fd fd 37 69 fd fd fd fd fd 21 37 4e fd 2d fd f6 4e 39 54 36 33 31 fd fd fd fd 7e fd 59 4b fd fd fd 0e fd 05 fd 14 fd fd 6b 2b 5d 4f 64 1d 60 6a fd fd fd 71 22 fd fd fd fd fd fd fd 43 fd 27 fd 5f fd fd 6b 26 fd fd 48 fd 1b 4a fd fd 09 24	p1>qTj&0EQ- @i5dK{XQMwoD>Ew G~u \$48DV@DKjwngp^_^<m8 yT8hk"UzHh7i!7N- N9T631~YKk+}Od`jq"C'_ k&HJ\$	success or wait	1	F2C055	WriteFile
C:\ProgramData\Microsoft Help\MS.SPREADSHEETCOMPARE.16.1033.hxn	436	524	fd 2e fd fd 36 fd fd b3 fd fd 7f 69 19 24 2a 3d fd 3e 19 fd 1c 11 5c fd fd 17 fd 69 7d 07 48 75 fd fd fd fd fd fd fd fd 54 44 fd 14 fd 19 72 fd 1c fd 5e 08 fd fd 2b fd 23 62 54 0d 66 2c fd 2b 03 33 fd 7a fd fd fd fd 28 fd fd 2e 21 fd 3d fd 5e 66 01 fd 10 41 5c fd fd fd 76 3c fd 15 fd fd 4e fd fd 12 fd 00 2c 75 11 fd fd 09 fd 3c fd 08 52 ba 7f fd fd 12 2a 1b 4c 2f 0b fd fd fd 36 fd 68 ca fd 28 45 5b fd fd fd 46 fd fd 54 14 4f fd 0b 26 fd 37 5b fd fd 62 74 fd fd 3b fd fd fd fd 4a 1f fd fd 34 fd fd 7a 7a fd 40 4a fd 73 63 fd 2d fd fd 3b fd fd 56 fd fd fd fd 29 fd 67 2e fd da 4b fd 23 fd 42 fd fd fd 29 1d 21 fd 72 6a fd 09 11 3b 0b fd 03 fd 23 fd 2b 6d fd 3c 08 4c fd 49 70 fd fd 5d 6f 4d d6 17 fd 11 53	.6\$*=>i}HuTDr^+bTf,+3z (.!=^f v<N,u<R*L/6h(E[FTO&7[bto;J4zz@sc- ,V)gK#B)!rj#+m<Llp]oMS	success or wait	1	F2CBF8	WriteFile
C:\ProgramData\Microsoft Help\MS.SPREADSHEETCOMPARE.16.1033.hxn	960	10	24 00 fd 01 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\ProgramData\Microsoft Help\MS.SPREADSHEETCOMPARE.16.1033.hxn	0	436	4a fd fd 58 2e fd fd fd 55 fd 31 b5 24 5f 7f fd 5f 57 08 4d fd 52 fd fd fd fd fd fd 52 fd fd fd 2f fd fd fd 38 fd 32 29 fd 22 fd fd fd fd fd 73 fd 74 52 fd fd 52 fd 10 fd fd 13 5e 30 1d 55 fd fd 2f fd 61 61 0f 2d 2a fd fd fd fd fd fd 1f 7c 18 fd 45 24 fd 47 fd fd fd fd fd 7a 14 47 fd fd fd 77 53 4e 05 fd fd fd 3e 02 62 fd fd fd 2f fd 70 7f 68 fd 3f 4b 55 fd fd 67 5c 46 23 95 fd fd 73 fd 31 fd 6a fd fd fd 1d fd fd fd fd 5a fd 03 2e 6c fd 48 32 fd fd 0d 49 23 22 4a fd 4f fd fd 04 fd 1d 47 61 fd fd 22 fd fd 4c 65 74 fd fd 7b fd fd fd fd 58 fd 2c fd 31 42 fd 0b 2c fd 20 5f 5b fd fd 76 46 fd fd 31 fd 6f 5e 45 fd fd 2f fd 73 fd 18 fd fd 2e 52 78 31 03 1a fd 6c 5e 4d fd 15 24 fd fd 76 6f 4b fd 05 e6 fd 03 6a 40 15 18 fd	X.U1\$__WMRR/82)"stRR 0U/aa-*)E\$ GzGwSN>b/ph? KUg\F#1jZ.IH2l#""JO Ga"Let{X,1B, _[vF1o^E/s.Rx1l^M \$voKj@	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft Help\MS.WINWORD.16.1033.hxn	362	524	58 fd fd 18 72 11 53 fd fd 49 26 fd fd fd 2f fd 38 fd 54 3b 74 1a fd fd 4b 4c fd fd 22 fd fd fd 2e 2c 4d fd 35 34 42 3b fd 03 2c fd 25 48 fd fd 7b 46 5a fd 22 65 18 66 22 67 4b fd fd fd 36 7b 77 fd 4a fd fd 2f fd 04 71 3d fd fd 38 3e 1a 20 fd 01 fd fd 73 0c 7c 6f fd 15 67 fd fd 52 fd 42 fd 04 fd fd fd 42 3f fd 53 77 fd fd fd fd fd fd 00 14 1b fd 3c 36 0f 3e fd 3f fd fd 66 2d fd fd fd 38 14 fd fd 39 7f fd 37 fd fd fd fd fd 4c 7a 65 fd 44 2b fd fd 38 fd 2b 10 7e fd 46 20 6a fd fd fd 4b fd 5e fd fd 6e fd fd 50 fd fd fd fd 7c 13 43 1c 67 60 fd 2f fd fd 60 4a 4b fd 1e 7d fd 35 75 48 fd 21 67 16 78 78 fd fd 81 19 fd 03 fd 61 fd 30 fd fd 2e fd fd fd 34 5e fd ef 16 60 fd fd fd 16 fd 58 47 0e 49 fd fd fd 71 6d 30 45 16 57 76 39 fd 7f	XrSI&/8T;tKL".,M54B;,% H{FZ"ef"gK6{wJ/=-8> s ogRBB?Sw<6>?f-897 LzeD+8+~F jK^nPCg`/`JK}5uH!gxa 04^`XGiqm0EWW9	success or wait	1	F2CBF8	WriteFile
C:\ProgramData\Microsoft Help\MS.WINWORD.16.1033.hxn	886	10	24 00 6a 01 00 00 00 00 00 00	\$j	success or wait	1	F2CC68	WriteFile
C:\ProgramData\Microsoft Help\MS.WINWORD.16.1033.hxn	0	362	60 fd fd fd 10 fd fd fd fd f4 35 fd 7d 7b fd 3c 0d 5a 7b 10 fd fd 13 fd fd fd 58 fd 67 fd 1b fd 4d 7e 67 fd 36 fd 2b fd fd 70 67 fd 73 fd 34 05 fd 6b fd 43 4e 7f b4 26 34 61 31 fd 25 fd fd 7b 11 fd 4f fd 2a fd 04 0c 01 41 1b 44 fd 76 fd fd 73 2b fd 60 fd 67 1c 17 65 fd 03 fd 1b fd 1d fd fd 47 fd fd 4a fd fd fd 7f 40 2d fd 30 00 fd 93 53 fd fd 29 fd 58 16 28 61 2b fd fd 34 fd 32 fd 12 13 fd 0e 18 44 2c 6d fd 3d 33 40 fd 95 fd 76 fd 32 fd fd fd 55 31 11 2c fd fd fd fd 42 34 6b fd 54 fd 63 5d 56 75 fd fd fd fd 02 31 30 fd 6e fd 22 fd fd 42 3f fd 64 4a 00 05 2d fd fd fd 56 fd 16 00 01 fd 65 41 16 fd 56 54 fd fd 6d 76 19 fd fd 09 fd 7a fd fd 35 0f 79 fd fd 0a fd 60 fd fd 29 fd 70 42 6e fd fd fd 1e bb 36 44 fd 68 72 0f 21 fd	`} {<Z{XgM~g6+pgs4CN&4 a1%(O*ADv+`geGJ@- 0S)X(a+42D,m=3@v2U1, B4kTc]Vu10n"B?dJ- VeAVTmvz5y`)pBn6Dhr!	success or wait	1	F2C055	WriteFile
C:\ProgramData\Microsoft Help\nslist.hxl	6262	524	fd fd 13 fd 27 fd fd 42 61 fd fd df 11 0f fd fd db 15 64 26 4c 4b 5c fd fd 3c fd 00 45 fd fd 5e fd 2c 0d 40 fd fd fd 69 7e 41 fd fd fd 57 1c 08 3a fd 09 fd 11 0c 2a 37 0e fd 6e 3a 0c fd 37 fd fd fd 55 fd 32 6d 25 03 17 4a fd fd fd 77 4b fd 2d 7b fd fd fd fd 48 1f 45 fd 7f 7f fd 46 fd 42 fd 59 fd eb 6f 3d 68 fd 0a fd 55 7f 4b fd 6b 02 fd 43 3c fd 10 fd 48 fd fd 6d fd 20 5b 45 fd 05 fd fd 63 0c fd 5a 07 fd 3b fd 43 fd fd 63 4e c8 5e 21 fd 70 fd 73 78 fd 6f 3d fd 17 76 fd fd fd 7e 25 20 fd 48 24 fd 6c 7c fd fd 1d fd 54 47 d4 68 fd fd fd 79 fd 56 fd 22 3c fd fd fd 2b 36 fd fd 5b fd fd 49 3b fd fd 0f fd 1b 15 fd fd 3f fd fd 4f fd 2b fd 1e 50 30 38 53 fd 35 fd 66 fd fd fd 04 fd 1c fd 7c 53 6d fd 74 fd	'Bad&LK\ <E,@i-W:*7n:7Um%JwK - HEFBYo=hKkCHm [EcZ;CcN^!psxo=v-% H\$ TGhyV"<+6[!;? O+P08S5f Smt	success or wait	1	F2CBF8	WriteFile
C:\ProgramData\Microsoft Help\nslist.hxl	6786	10	24 00 76 18 00 00 00 00 00 00	\$v	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft Help\nslist.hxl	0	6262	37 fd 2c 48 73 fd 53 fd 53 3e fd fd fd 0b 6e 09 fd fd fd 4e 16 fd 7b fd fd 62 49 5f 08 1d 3b fd 1e 20 0d 6e fd fd 49 30 fd 62 fd 19 77 1c 05 76 fd 20 fd 44 38 70 fd 2b fd 07 2e 71 fd fd 7e 6f 25 fd 49 fd 20 18 fd fd fd 5e fd 45 28 00 42 36 10 fd 3e 03 5f 75 fd 03 fd fd 46 fd fd 4b 0a 26 fd 3c 32 3d 65 fd 02 44 72 fd fd 20 12 fd 4f 0d fd 3a 3c 06 fd 50 0b fd fd fd fd 1d fd 2b 74 fd 1a fd fd fd fd fd 0e 55 fd fd 06 fd 55 a7 5c fd fd fd fd fd fd 7c 46 fd 63 09 fd 3e 6c dc fd fd 5b fd 11 06 fd 74 7a 57 20 46 fd fd 1d 7c 13 fd fd fd 5d 31 43 5c 36 7b 68 13 8a 15 fd fd 1d 0c fd 5b fd fd 30 66 16 fd 6d 30 fd fd 61 41 3e 77 fd fd 48 fd fd 72 fd 10 fd 0e 2d 77 fd fd 17 12 fd 08 26 fd 0d fd 63 27 fd 25 78 fd fd 12 34 01 fd 22 fd fd 45	7,HsSS>nN{bl_; nl0bwv D8p+.q~o%i ^E(B6>_uFK&<2=eDr O: <P+tUU\c> [tzW F])1C\6{h[0fm0aA>wHr- w&c"%x4"E	success or wait	1	F2C055	WriteFile
C:\ProgramData\USOShared\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 5f 2f 5c 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ v _ _ _ _ v L // _ _ L _ \ . ` _ _ \ _ _ \ \ v v L // \ _ \ \ _ / \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\ProgramData\regid.1991-06.com.microsoft\regid.1991-06.com.microsoft Microsoft Office Professional Plus 2016.swidtag	1065	524	68 fd fd fd 5a fd 6b fd fd 72 fd 60 fd 29 fd fd fd 64 7c fd 3e 74 fd fd fd fd fd 79 fd 67 fd 63 fd fd 63 fd fd 3f fd fd 61 24 4a fd 4a fd fd 05 fd 4c 2b fd fd fd 2b fd 06 fd fd 3d fd fd fd 09 7d fd 67 fd fd 79 60 fd 11 fd fd 06 63 64 64 4e fd fd 08 2a fd fd fd 41 16 6e fd 67 fd 81 74 4c fd fd fd 17 1d fd 43 57 fd 2f fd 05 28 08 fd 29 fd 4f 36 55 02 fd 76 83 fd fd 38 22 fd fd 4a fd fd fd fd 6f 76 7a 15 1e fd 39 fd 37 fd 22 60 fd fd 5a 46 21 49 f2 98 20 29 fd e8 6f fd 1c 5a 21 20 fd 0d 09 fd 70 fd 20 fd 52 6b 17 fd 6f 6f fd 72 18 15 fd 7c 02 cf fd 15 fd 1c fd fd fd fd fd 17 5b fd 28 fd fd 67 fd 4b 5b 3b fd 48 72 4c 10 fd 15 8c fd fd 49 fd 60 56 13 5d 0b 64 fd 3e fd 7f 29 fd fd 18 74 3b 27 fd 21 fd fd 2f fd 43 fd 0a 73	hZkr`)d >tygcc? a\$JJ++=gy`cddN* AngtLCW/()O6Uv8"Jovz9 7""ZF!! JoZ! p Rkooor [[gK[:HrLi`V]d>)t;!/Cs	success or wait	1	F2CBF8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\regid.1991-06.com.microsoft\regid.1991-06.com.microsoft Microsoft Office Professional Plus 2016.swidtag	1589	10	24 00 29 04 00 00 00 00 00 00	\$)	success or wait	1	F2CC68	WriteFile
C:\ProgramData\regid.1991-06.com.microsoft\regid.1991-06.com.microsoft Microsoft Office Professional Plus 2016.swidtag	0	1065	fd 64 35 fd fd fd 2a fd 4c 5b fd fd 59 41 59 fd 24 fd 40 62 13 5e 00 4a 5f 4a 18 19 28 53 49 fd 7d fd fd 09 59 7e fd fd 1c 38 1f 53 fd 47 41 47 fd fd 26 fd 6f 22 fd 5e 60 fd 7c fd fd 5e fd fd 4c fd fd 1c fd 2b 1d 02 17 5e fd 51 fd fd fd 79 65 15 3d fd 1f fd 10 7d fd 6b 6e fd fd fd 20 fd 6d fd 04 fd fd fd fd 69 0e fd 00 29 3f 36 fd 65 fd fd fd 1b 26 12 fd 1b fd fd 23 6d fd 0d 2e 0b fd 31 2b fd 6c 39 7a 31 fd fd 43 fd fd 57 0a 16 4d 25 10 fd 3d 0d fd fd fd fd 6a 58 50 17 2b fd fd fd fd 49 69 fd fd fd fd 20 fd 76 fd 6d 31 3c fd 36 1b 11 fd 2d fd fd fd 60 29 fd fd 73 75 fd fd fd 79 fd 4a fd fd 06 79 fd fd fd 33 02 2a fd fd fd 4a 63 fd d4 02 fd 0a fd 1c 0e fd fd 73 fd 32 fd fd 54 69 22 fd a4 fd 46 fd 03 73 fd	d5*L[YAY\$@b^J_J(SI)Y~8SGAG&o"^`^L+^Qye=)kn i)?6e&#m.1+H9z1CWM%=jXP+li v1<6-`)suyJy3*Jcs2Ti"Fs	success or wait	1	F2C055	WriteFile
C:\ProgramData\regid.1991-06.com.microsoft\regid.1991-06.com.microsoft_Windows-10-Pro.swidtag	993	524	42 fd fd 11 28 5d fd 7e 56 21 25 fd fd 4d fd fd 25 fd 0e 42 fd fd fd 1a fd fd 11 26 69 0e fd fd fd 25 3a 5a fd 42 30 fd 13 36 79 70 fd fd 6c 52 fd fd fd fd fd 30 3b fd 23 2b fd fd fd 70 fd fd 31 fd 75 fd fd 3a 6a 1d fd 66 32 76 fd 72 32 22 24 07 67 fd 0b fd fd 51 fd fd fd 79 fd 31 6d fd 6f 21 1a fd fd 17 7e fd 68 28 28 22 35 25 fd 22 2b fd fd 73 fd 02 2f 32 27 fd 7f fd 18 66 50 bc fd 6f 3c 0b fd 68 64 fd fd 43 15 74 35 2a fd fd 71 0b 0b 4d 51 fd 6c fd fd fd 2b fd fd 14 fd 5e 22 57 fd 5a 74 fd fd 56 5a fd fd fd 3a fd 57 fd 59 7d 5c fd 3a fd 56 fd 44 fd 0c fd fd 1d 08 3a 61 fd 33 fd 08 9a fd 39 fd 40 fd fd 36 fd fd fd 05 fd 39 76 3e 29 fd 3d fd fd 4e fd fd fd fd fd 59 6d 77 fd fd 27 fd fd 10 fd 2f fd 21 13 fd	B]~V!%M%B%:ZB06yplR0;#+p1u:jf2vr2"\$gQy1mo!~h(("5%"s/2'fPo<hdCt5*qMQl+^"WZVZ:WY}\:VD:a39@69v>)=NYmw/!	success or wait	1	F2CBF8	WriteFile
C:\ProgramData\regid.1991-06.com.microsoft\regid.1991-06.com.microsoft_Windows-10-Pro.swidtag	1517	10	24 00 fd 03 00 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\regid.1991-06.com.microsoft\regid.1991-06.com.microsoft_Windows-10-Pro.swidtag	0	993	03 2a fd 4e 69 08 7c fd 38 fd fd fd 34 fd fd fd 58 1c ae 48 fd 07 3a fd 3f 38 0d fd 30 fd fd fd 6f fd fd fd 2c 5e 34 fd 4c fd 2d 6b fd fd fd 09 fd 20 fd 07 6f 1b 41 d7 fd fd fd fd 6c fd fd 31 3f fd 2b 36 fd 78 fd fd fd 55 34 7c 4d fd 79 63 fd fd 11 16 64 30 fd fd fd 7a 7d fd 74 fd 45 71 fd 49 4e 65 22 fd fd 3d 1a fd fd fd 24 0a fd 04 fd 17 04 fd 22 fd 49 3e fd 34 25 0e fd 60 fd fd fd 19 51 43 fd 04 06 fd 0b 1f 42 6d fd 3f fd 6e b2 fd fd 25 31 fd 50 1a 63 fd 43 fd 07 fd 66 19 fd fd 0b 06 fd 12 73 fd 76 1d 3b fd fd fd fd 69 fd 40 46 fd 6a fd d3 fd 47 fd fd 73 52 5f 79 fd fd fd 08 59 fd 19 3a fd 0a 30 78 08 fd fd 47 5d fd fd 1f 5e 61 43 fd 7b 35 a9 fd 5e fd fd 04 fd 2a fd fd 78 fd fd a1 fd 31 fd 28 fd 2b	*Nij84XH:~80o,^4L- oAl1?+6xU4 Mycd0ztEq Ne"\$">4%`Q Cm?n%1PcCf sv;i@FjGsR_yY:0xG]^aC {5^*x1(+	success or wait	1	F2C055	WriteFile
C:\Users\Default\IR3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 5f 2f 5c 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ / / _ _ _ _ _ \ . ` _ _ _ _ \ \ / / \ _ _ _ / _ _ _ \ _ _ _ _ _ _ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\Users\user\IR3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 5f 2f 5c 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ / / _ _ _ _ _ \ . ` _ _ _ _ \ \ / / \ _ _ _ / _ _ _ \ _ _ _ _ _ _ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Default\NTUSER.DAT	262144	524	7d fd 18 fd 17 7b 7f 3c fd fd 4b 50 fd 4a 05 fd 3e fd 37 6d 6e 15 28 fd fd fd fd 73 30 fd fd fd fd 49 57 fd fd fd 3a fd 68 fd fd c1 fd 54 7e fd fd fd fd ef fd 1a fd 15 34 fd 4a fd fd fd 0c fd 05 fd 4b 05 75 03 fd 08 fd 51 fd fd 4b 37 7e 44 fd 7c fd fd fd 59 fd fd fd 26 7c 14 43 33 fd 72 fd 08 28 16 62 fd 05 fd fd 63 fd fd 28 08 3b fd 58 fd 67 fd 2f 3b fd 14 25 fd 43 fd 67 56 77 fd fd 13 fd 74 fd fd fd fd fd 5a 2f 58 fd 4b 1b 5b fd 2b fd 02 6d 51 78 ea 2e 47 13 49 fd fd fd 1c af 5c 1d fd fd fd 63 fd fd 60 3b fd fd 45 fd fd fd fd fd fd 3a fd fd fd 17 0a 05 fd 3b fd 1b fd fd 42 fd fd 17 3b fd fd fd 40 32 fd 6b 5d fd fd 6c 72 55 32 fd fd 76 08 fd 15 fd fd 0c c8 fd 3a 05 fd dc 75 fd fd fd 27 fd fd fd 0b 0a 1a	{ {<KPJ>7mn(s0IW:hT~4J KuQK7~D Y & C3r(bc(;Xg/;%CgVwtZ/ XK[+mx.G l\c';E;;B;@2k]lrU2v:u'	success or wait	1	F2CBF8	WriteFile
C:\Users\Default\NTUSER.DAT	262668	10	24 00 00 00 04 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\Users\Default\NTUSER.DAT	0	262144	a4 04 7c 3b 70 4f fd fd 13 56 fd 35 74 06 71 fd fd fd 8f fd 3e 37 44 fd 25 fd 64 fd fd fd 49 fd 4f 3f fd fd fd 28 fd 5e 77 fd 75 19 23 5a 60 fd 59 ac 4b 5d fd fd 78 fd fd 62 1b 60 fd 32 3f 4e 3b 27 7d fd fd 45 3b 63 03 25 fd fd fd fd fd fd fd fd 7b 65 fd 48 72 fd 5b fd fd fd fd 30 fd fd fd 75 04 fd fd 29 fd 6a 69 fd 17 fd 11 fd 00 fd 77 fd fd 06 fd fd fd 5a 59 fd fd 72 fd 0a 4c 12 fd fd 4b 21 1b 30 59 4e 7a fd fd fd 14 59 0b fd 3c fd fd fd 1c fd fd 06 43 fd 43 67 fd fd 53 fd 5f 06 54 73 fd fd fd 7a fd 17 fd 37 3f 5e 71 24 fd 6d fd 1a 7f 61 fd fd 5f fd 27 5f fd 70 16 7a fd fd 0d 3d 47 fd 41 fd 5e fd fd 5a fd 73 fd 17 fd fd 76 51 77 0c fd 72 fd 13 39 fd fd 7c 3e 6b 62 b0 6d 59 07 fd 03 07 fd fd fd fd fd fd 2e fd 08 10 fd 32 2e 34 3d	};pOV5tq>7D%dIO? (*wu#Z`YK]xb`2? N;`)E;c% {eHr[0u]jiwZYrLK!0YNz Y<CCgS_Tsz7? ^q\$ma_'_pz=GA^ZsvQ wr9!>kbmY.2.4=	success or wait	1	F2C055	WriteFile
C:\Users\Default\NTUSER.DAT.LOG1	57344	524	fd 08 fd 47 fd fd 26 1a fd 5e fd 03 fd 33 1f 3f 11 ce 02 fd 7f fd fd fd 53 17 fd fd 50 63 fd 6e 10 fd 26 fd fd 11 fd 0a 52 3b 48 18 7c fd fd 76 fd fd fd fd 0b 77 26 fd 0b fd 1d 00 fd 29 fd fd 20 fd fd 13 fd fd fd 18 5c fd f7 6d 4d fd 81 fd 61 fd fd 3d 51 fd 7e 59 fd 32 fd fd 25 60 fd 46 6e 05 fd 18 0d fd 4b fd 18 fd fd 07 7f 3a fd 69 62 fd fd 6a fd fd 6f fd fd fd 0a fd fd fd 25 39 5a fd fd fd 56 b7 5a fd fd 65 33 fd 91 7d fd 00 fd 49 fd 11 36 6d 33 fd 7c 2d 3b 5c fd 6f fd 2c 16 fd 6b fd 39 fd 60 65 04 50 fd 2f fd 4f 6f 51 00 fd fd fd fd 5f be 4f 2f 29 1f 45 4d fd fd 67 fd 20 70 fd 45 2d fd fd fd 77 61 21 6c 07 9e fd 16 4e 6c 5e 49 fd 73 8b 21 37 35 fd fd 41 fd fd fd fd fd 46 fd 4a fd fd 02 fd fd 40	G&^3?SPcn&;H vw&) \mMa=Q~Y2%'F nK:ibjo%9ZVZe3]l6m3]- ';lo,k9`eP/OoQ_O/)EMg pE-wa!lNI^!s75AFJ@	success or wait	1	F2CBF8	WriteFile
C:\Users\Default\NTUSER.DAT.LOG1	57868	10	24 00 00 fd 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Default\NTUSER.DAT.LOG1	0	57344	22 08 fd fd fd fd 5e fd 28 03 62 fd 11 fd 0f fd af fd fd 96 1d fd 40 68 fd 58 fd fd 04 58 fd fd 64 26 fd 14 fd 78 2a fd fd 29 51 fd fd fd 6f fd fd 4f fd 24 fd 42 11 11 3a fd fd 51 fd fd 10 29 0f fd fd 26 fd 24 fd 20 fd 00 fd fd 41 fd fd 4f 57 5e fd fd 35 33 4f 54 fd fd 43 fd 58 35 5d fd fd 3b 05 0f 2f fd 75 fd fd fd 07 fd 5f fd fd fd 7d 3d fd 1a fd 37 fd 56 6b fd 3f 2a 0e 13 5a fd fd 4d 11 4b 2d 6e fd fd 3f 28 6d 2c 07 fd 5d 4c 00 fd 23 28 7c fd 18 01 09 fd fd fd 60 66 fd fd fd 0c fd 2e 70 2a 66 18 fd fd 4d 5f fd 7b 3c fd fd fd 51 11 40 fd fd 4f fd 40 fd fd fd 45 01 fd fd fd 24 38 fd 6d fd 5e 0e 17 5c 14 62 fd fd 3a fd 4c cb fd 4d 4f 21 46 fd fd 08 fd 2c fd fd 63 4e 09 30 fd fd fd 35 fd 02 fd 76 1e fd fd fd 02 fd fd 5c	""(b@hXXd&x*)QoO\$B: Q)&\$ AOW^53 OTCX5];/u_)=7Vvk?*ZMK- n?(m,]L#(.p*fM_{Q@O@E8m^lb:L MO!F,cN05v\	success or wait	1	F2C055	WriteFile
C:\Users\Public\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 5f 2f 5c 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ v _ _ _ _ v _ / / _ _ _ _ \ . ` _ _ \ _ _ \ _ _ \ v _ / \ _ / \ _ / \ _ _ \ _ / \ _ _ \ _ _ /By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\Users\Default\NTUSER.DAT{8e be95f7-3dcb-11e8-a9d9-7cfe9091 3f50}.TM.blf	65536	524	24 fd 71 4d fd fd fd 55 4d fd 4a fd fd 69 4b fd 71 2b 43 39 43 7d 60 fd 40 1f 11 fd fd 09 fd fd fd 73 fd fd fd fd 3e 0c fd 1a 0c fd fd fd fd fd 5d fd 11 fd fd 7e 25 fd 54 fd 08 08 0c fd 19 51 fd 68 fd 09 45 fd 42 fd 75 66 fd 4d 40 07 72 4b fd fd fd 28 0b fd 56 46 2c 3d 3c 30 fd fd 14 54 58 fd fd be fd 00 fd 04 fd 4a fd fd 27 16 95 42 fd 1d fd fd fd fd fd fd 42 40 7b fd 97 a1 5b be fd 0e 31 6b fd 20 48 fd 2d fd 5b a5 fd 67 fd fd fd 03 fd fd 3b 07 fd fd fd 24 45 4a 7f fd fd fd fd 62 fd fd 24 46 10 fd 4d fd 11 fd fd fd fd fd 24 fd 67 31 45 5e fd fd fd 41 c1 fd fd 54 fd 69 fd fd 7e fd fd 75 11 fd fd fd fd 85 24 64 75 fd fd fd e6 4f 67 fd 56 fd 3c 65 25 4c a5 40 4a fd fd fd 57 fd fd 09 51 04 fd 4b 79 fd	\$qMUMJiKq+C9C)`@s>] ~%TQhEBufM@K(VF,= <0TXJ'BB@{[k H- [g;\$EJb\$F M\$g1E^ATi~u\$duOgV<e %L@JWQKy	success or wait	1	F2CBF8	WriteFile
C:\Users\Default\NTUSER.DAT{8e be95f7-3dcb-11e8-a9d9-7cfe9091 3f50}.TM.blf	66060	10	24 00 00 00 01 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Default\NTUSER.DAT{8e be95f7-3dcb-11e8-a9d9-7cfe9091 3f50}.TM.blf	0	65536	01 70 fd 47 53 fd 38 63 49 fd 2a 37 31 fd 70 37 fd fd fd 78 7f 65 fd 47 24 fd fd 66 68 fd fd 51 fd 15 fd fd 3b 55 fd fd 71 80 7b 64 23 fd 76 3d 10 fd 0b 3e 26 41 5b 21 26 7f fd fd fd 77 48 4a fd fd 00 fd 33 5f 5a fd fd fd fd 4a 0a 46 67 fd bb fd 2a 69 fd 33 f1 fd 76 7a fd b8 0a 73 69 fd 0d 52 41 fd 26 15 fd 31 76 fd 69 36 fd 5c fd fd fd 73 1e fd 5c fd 34 fd fd fd fd 0e 58 1c fd fd fd 7d fd 12 14 33 fd 51 6f 72 0a 1c 0f 78 fd 74 fd 3c fd 39 64 57 1e fd 63 fd 8d 05 fd 79 fd 2d fd fd 43 26 11 fd fd 14 54 fd fd 51 00 fd 71 27 42 51 43 fd 46 fd 62 fd fd fd 26 fd fd 2f fd 34 fd fd 7e 51 30 16 fd fd 1f fd 2d 61 1a 6d 0b 31 fd fd 41 fd 19 16 47 63 7a 5c fd 76 34 fd 65 20 fd fd fd 15 fd fd 0b fd fd 1f fd 37 fd fd	pGS8cl*71p7xeG\$fQ;Uq{ d#v=>&A!w HJ3_ZJFg*i3vsiRA1vi6\sl 4X}3Qorx<9dWcy- C&TQq'BQCFb&/4~Q0- am1AGczlv4e 7	success or wait	1	F2C055	WriteFile
C:\Users\Default\NTUSER.DAT{8e be95f7-3dcb-11e8-a9d9-7cfe9091 3f50}.TM.Container00000000000000 0000001.regtrans-ms	524288	524	28 01 fd fd 24 fd fd fd fd fd 1b fd 18 51 2f 5a fd fd 63 fd 20 fd 09 5e fd f0 fd 15 55 fd 48 3d 0a 55 fd 06 29 fd 24 0c 21 fd 44 fd fd 63 fd fd fd 65 66 fd fd fd fd 02 fd fd 1d fd fd 24 dc fd fd c6 fd 64 70 fd fd 5c fd 67 5f fd 70 fd fd fd fd fd fd 6b fd 5f 67 41 55 14 0f c1 01 fd 38 6d 3c fd 19 fd fd 1c fd 64 fd 31 6a fd 9f 2c fd fd 55 02 42 52 fd 37 38 fd fd 3c 0f fd 58 fd fd fd 4e 49 fd 5d fd fd fd 2b fd fd fd 71 fd fd 2f fd 05 03 08 fd fd fd 22 0a 66 fd fd 56 26 fd 09 1c fd 75 fd fd d4 fd d6 fd 58 fd 22 fd 21 18 25 fd fd fd 04 22 4a fd 5f fd 35 0f 06 20 15 49 fd fd fd 62 19 fd fd fd fd 26 fd 5e 7d 52 fd fd fd fd 5a fd fd 22 77 fd 19 1f fd 4f fd fd fd 38 fd 49 fd 3b fd fd 3a fd fd 19 5b 77 fd 22 55 fd	(\$Q/Zc ^UH=U)\$!Dcef\$dp\gpk_g AU 8m<d1j,UBR78<XNl]+q/"f V&uX"!9%"_J_5 lb&^}RZ"wO8!;:[w"U	success or wait	1	F2CBF8	WriteFile
C:\Users\Default\NTUSER.DAT{8e be95f7-3dcb-11e8-a9d9-7cfe9091 3f50}.TM.Container00000000000000 0000001.regtrans-ms	524812	10	24 00 00 00 08 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\Users\Default\NTUSER.DAT{8e be95f7-3dcb-11e8-a9d9-7cfe9091 3f50}.TM.Container00000000000000 0000001.regtrans-ms	0	524288	fd fd 3b 57 12 fd 00 fd fd 48 4f fd 4f fd fd 1e fd 67 67 2d fd fd fd 35 4b fd fd 11 56 5f 1a 1a 2b 25 40 fd 16 0b fd 7f 68 02 fd 60 9c 55 fd 3d fd fd 31 10 fd 44 fd 45 2d 64 fd 66 fd c6 00 fd fd 36 0d fd 5d a8 fd 29 36 60 0b fd fd 24 fd 15 fd fd fd 20 fd fd 27 fd fd fd 74 fd 12 fd 33 60 41 2b 05 22 fd fd fd 07 fd 52 4b 41 fd fd 6f fd 4e fd 2c fd 42 fd 68 6a 7a 16 fd fd 16 fd fd 1d fd 30 02 07 1d fd 5c fd 3b fd 20 fd 00 fd 82 33 78 fd fd fd fd 43 04 fd 36 0d fd 6e 0e fd 1e fd fd 31 2e 4e fd 04 fd fd fd 13 fd 6e 6d 89 70 74 68 fd 6e fd 62 28 46 fd fd fd b6 0c fd 43 fd 0e 42 5e fd fd 49 fd fd fd fd 36 fd fd 18 3c 31 6b fd 58 fd 38 fd fd 66 f9 21 75 fd fd 4d 7e fd 5f 58 78 53 44 6d 79 43 3b fd 44 24 fd	;WHOOgg- 5KV_+%@h`U=1DE- df6)6`\$ 't3' A+"RKAoN,BhJz0l; 3xC6n1.N nmpthnb(FCB^!6<1kX8f! uM~_XxSDmyC;D\$	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Default\NTUSER.DAT{8e be95f7-3dcb-11e8-a9d9-7cfe9091 3f50}.TMContainer00000000000000 0000002.regtrans-ms	524288	524	05 fd fd 55 fd 5a 79 4e 7d fd fd 7b 51 fd 3a fd 2e 74 2e fd fd 43 10 0d fd 2a 7d fd 16 00 13 fd fd 51 fd fd fd 12 59 fd fd 2f fd fd fd 71 fd fd 21 0c fd fd fd 1d 34 fd 3b fd 67 26 13 fd 25 fd 77 64 45 fd 4a 1d fd 36 14 0a fd 18 fd fd fd 5b fd fd fd 32 fd 7a fd 45 11 fd 34 fd 57 fd fd fd 2e fd 3c 64 18 6d fd 35 fd 13 fd 4b 63 fd 0b 5f fd 26 fd 10 fd 2a 77 00 fd fd fd 49 fd fd 63 6c 7c 61 8e 14 fd fd 09 64 39 4d 56 fd 22 4d 03 fd 56 fd 5e fd fd 2a fd 6e fd 2e 42 27 fd fd 7e fd fd 19 12 fd 55 fd 73 45 55 fd 0c fd 37 fd fd fd fd 74 65 fd 52 7f 17 fd 30 fd 1b fd 2d fd 5c fd fd 7c 16 2b fd fd 10 fd fd 16 fd 1c 09 2f 77 34 6b fd 27 fd fd fd 26 27 fd fd fd 7b 4f fd 75 fd 48 fd fd fd 75 fd 75 7c fd 10 4c fd 34 49 49 fd 22 5d fd 32	UZYn} {Q:.t.C*)QY/q!4;g&%dEJ 6[2zE4W. <dm5Kc_&*wic ad9MV" MV^*n.B'~UsEU7teR0- \\+/w4k'&{'OuHuu L4I "}2	success or wait	1	F2CBF8	WriteFile
C:\Users\Default\NTUSER.DAT{8e be95f7-3dcb-11e8-a9d9-7cfe9091 3f50}.TMContainer00000000000000 0000002.regtrans-ms	524812	10	24 00 00 00 08 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\Users\Default\NTUSER.DAT{8e be95f7-3dcb-11e8-a9d9-7cfe9091 3f50}.TMContainer00000000000000 0000002.regtrans-ms	0	524288	fd fd 03 15 fd fd fd fd fd 21 47 3a fd fd 7e fd 34 48 fd 1c fd 15 05 1d 79 fd 69 36 25 18 30 2b 25 fd fd 3d fd 42 fd 56 fd fd fd fd 5f 3c fd 04 3d 2e 7f fd 75 fd fd fd fd fd 45 1c 66 fd fd 0a fd 58 fd fd fd fd 4f 74 64 35 4a 5f 15 68 07 4c fd 1d 4d fd 12 fd 1f fd fd fd 13 fd fd 7f 8d 3f 38 42 fd 22 fd fd 18 fd fd 0d fd 2e 73 2b fd 7f 54 fd fd 2d 55 aa fd fd 34 0e fd 19 fd 5d 74 fd fd 41 fd 58 57 fd 57 fd fd 7e 32 4b 65 21 1d fd 2a fd 4f fd fd 3a fd 1c fd 4b 7a 33 46 fd 30 65 fd fd 2c fd 70 66 73 fd fd 05 7b 42 0e 19 65 1a 44 fd fd 02 fd 77 fd 70 fd 37 80 30 15 7c 54 fd fd fd 6b 66 fd 0c 7c 5c fd 49 fd 62 30 23 fd fd 1f 4d fd 43 15 fd 55 5f 11 35 57 fd 4a fd 3f fd 77 fd fd fd 63 fd 61 fd 38 71 5f fd fd 06 78 fd 5e fd 25 fd fd	!G:~4Hyi6%0+%=%BV_<=. uEfXOtd5J_hLM?B".s+T- U4)tAXWW~2Ke!*O:Kz3 F0e,pfs(BeDwp70 Tkf \lb 0#MC_5WJ?wca8q_x^	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ v _ _ _ _ / / _ _ _ _ . ' _ _ \ _ _ \ \ _ _ / / \ / \ _ / \ _ _ \ _ _ \ _ _ \ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ v _ _ _ _ / / _ _ _ _ . ' _ _ \ _ _ \ \ _ _ / / \ / \ _ / \ _ _ \ _ _ \ _ _ \ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ _ _ _ \\\n _ _ _ _ _ _ _ _ _ _ \\\n / / _ _ _ _ _ _ _ _ _ _ \\\n _ _ _ _ _ _ _ _ _ _ \\\n _ _ / _ _ _ _ _ _ _ _ _ _ \\\n _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ /By\now it's probably painfully\napparent that your envir\nonment hasbeen infected\nwith r	success or wait	1	F358DF	WriteFile
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ _ _ _ \\\n _ _ _ _ _ _ _ _ _ _ \\\n / / _ _ _ _ _ _ _ _ _ _ \\\n _ _ _ _ _ _ _ _ _ _ \\\n _ _ / _ _ _ _ _ _ _ _ _ _ \\\n _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ /By\now it's probably painfully\napparent that your envir\nonment hasbeen infected\nwith r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\ntuser.ini	20	524	14 fd 32 46 fd fd 28 fd 2e fd fd 77 2d 6c 2c 32 fd fd fd 6b fd 7d fd fd 4f fd 24 fd 49 69 62 7a 55 36 78 fd fd fd 73 32 fd 2e 33 fd 25 42 53 42 2b 3d 7b fd 46 3e fd 29 fd 7c 73 fd fd fd 6b 02 fd 2b 2e 76 fd 30 66 fd 5d fd fd fd fd fd 0b fd 5b 18 a1 fd fd 36 fd 36 fd 0a 6a fd fd fd 06 fd 61 fd fd 57 03 36 51 11 fd 52 1f fd fd fd 25 fd fd 0a fd fd fd 12 fd fd 00 40 08 fd fd 33 41 66 3d 4a fd 0e 7c fd 4c fd fd fd 77 fd 58 fd 47 77 78 39 4e 78 19 fd fd 06 06 53 fd 10 fd fd fd 10 fd fd 4a fd fd f5 2f 11 09 50 fd 78 fd 2f fd fd fd fd 7d 01 1a 40 0a 63 fd fd 78 fd fd 7e 03 0c 07 fd fd fd 62 fd 60 7c 2e fd fd fd 03 fd 0c 3c fd 52 fd 12 fd 29 56 fd fd 49 20 3a 4b 11 4f fd 39 fd fd 21 fd fd fd 5d 54 5c fd 22 41 4c 65 15 16 71	2F(.w- l,2k}O\$libzU6s2.3%BSB+ ={ F->)sk.v0f]m[66jaW6QR% 3Af=J LwX Gwx9NxSJ/Px/}@cx-b`]. <R)VI :KO9!jT\"ALeq	success or wait	1	F2CBF8	WriteFile
C:\Users\user\ntuser.ini	544	10	24 00 14 00 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\Users\user\ntuser.ini	0	20	19 fd 59 4f fd fd 4b 20 fd c8 23 fd fd 16 50 58 0a fd 0d	YOK #PX	success or wait	1	F2C055	WriteFile
C:\Users\Public\desktop.ini	174	524	6c 01 30 fd 17 fd 64 1e ac fd 6d 4e 41 fd fd 1a fd fc fd 2c 4a 03 fd 20 fd fd 1d 10 fd fd 63 14 fd 78 5b 6d 3a fd 4e fd 00 fd ea 0c 19 6f 65 2e fd fd 63 fd fd 5f 02 fd fd 2d fd 7d 02 1b 49 6f fd 68 fd fd fd fd fd 35 fd fd 53 fd 66 11 14 fd fd fd 14 0c 43 24 1c fd fd 26 fd fd fd fd 4b fd fd 14 fd fd fd fd 37 fd 05 6e 2a 4a 57 6c 25 fd fd fd fd 6a fd 62 fd 4d fd 46 fd fd fd 74 fd fd 3f 1a fd 13 fd fd fd 53 fd fd fd fd 1b fd fd 72 15 fd 44 26 2a fd fd fd 29 fd 55 fa 64 fd fd 53 3e 3e 1c fd fd fd fd fd fd 44 fd 77 24 fd fd 5b fd 7b 16 19 6f fd fd 0d 3f fd fd 7b fd fd fd 77 07 fd fd a7 fd 2c 1d 34 fd 4d fd fd fd 31 16 fd fd fd 75 05 4b fd fd 33 fd fd fd 30 27 28 fd 7a fd 1c 75 6a 5e fd 49 15 fd fd 4c 4f 64 fd cb	l0dmNA, cx[m:Noe.c_- }lh5SfC\$&K 7nJW%jbMFt? SrD&*)UdS>>Dw\$[{o?{ w,4M1uK30'(zj^ILOd	success or wait	1	F2CBF8	WriteFile
C:\Users\Public\desktop.ini	698	10	24 00 fd 00 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\Users\Public\desktop.ini	0	174	fd fd 5b fd fd fd 59 fd 54 02 7c fd fd 90 52 fd fd 3d fd 36 fd fd fd 1f fd fd fd 0d 6c fd 76 fd 45 fd fd fd fd 00 7e 57 08 05 fd fd 04 fd 46 fd 26 62 4d 6a fd 8d fd 2f fd 5e 71 01 01 77 49 fd 52 7f 5c fd fd fd 31 fd 1b 17 7d fd 7a 50 fd fd 1e 6a 26 38 30 76 23 fd fd 1e fd fd fd 0c fd fd fd fd fd 4b fd 1f 00 03 5e fd 10 fd ff 75 fd 3d 0d 31 40 fd fd 10 fd 2c fd fd 25 fd 39 fd fd 35 fd fd 1c fd 24 60 0e 5f fd fd 75 4f 1c fd fd fd fd 72 28 f1 fd fd fd 30 70 fd 68 fd 6b fd 17 fd 79 fd 3b	[YT R=6lvE-WF&Mj/^qwl R\1}zPj&8 0v#K^u=1,%95\$`_uO(0ph ky;	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\OWOW64WW.cab	30592188	524	3e 36 2a fd fd fd 13 44 54 fd 03 fd 1b 29 08 3a 56 fd 38 fd fd 69 14 fd 1e 12 fd 64 fd 63 7e 6a 07 05 76 fd 37 fd 02 05 fd fd fd 31 3a 0f 20 fd 61 05 07 fd 34 10 4d fd 64 40 04 fd fd 69 fd 58 1d 71 05 fd 0c fd 07 fd 32 fd 47 fd 30 60 1d 19 fd fd 34 54 fd 2c fd 2e 26 09 0f fd 04 fd fd fd 6f 76 fd fd 03 39 fd 2a fd 62 fd fd 53 fd 6c 05 fd fd fd 76 77 f1 13 69 fd 2f 22 fd fd fd 3f 10 5d fd 1d bd 4e 07 56 fd 54 fd fd 28 63 fd 05 30 fd fd fd fd 65 04 fd 51 fd 7d 63 4a fd 45 04 0f 6d 37 fd 27 7e fd fd 0d fd fd fd 0b 53 fd fd 1a fd fd 55 fd 4f 2c 22 02 37 fd 6d fd 73 fd 70 fd 23 fd 5d 55 69 fd 3c 6d fd 37 fd 5e 7d fd 65 fd 32 15 36 4a 08 40 ab fd fd fd 6e 5b 5e 5f 1c 1c fd 62 fd fd fd 13 fd fd fd 45 fd fd fd 34 fd 32 1b fd 52 30 08 55 5c fd	>6*DT:V8idc~jv71: a4Md@iXq2G0` 4T,.&ov9*Slvwi"?]NVT(c 0eQ)cJE m7'~SUO,"7msp#]Ui<m7 ^)e26J@n[^_bE42R0U\	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Office64WW.xml	0	4992	3b 08 20 54 77 fd 4a fd 45 fd fd 5c fd 6c fd 5c fd fd fd 13 fd 34 fd 5d fd 13 2b fd fd fd fd 05 15 fd 4d fd fd fd fd 49 fd 48 05 fd 70 2d fd 6a 73 f9 0d fd fd 59 fd fd 56 3f 34 53 fd fd fd fd 4e fd 0b fd fd 7f 2b 01 76 fd 51 6e fd 1d 60 23 35 fd fd 27 fd fd 79 50 32 fd fd 16 3d fd 1d 23 92 fd fd fd fd 78 fd 28 38 fd fd 67 fd fd 31 7a fd 2f fd fd fd fd fd 46 24 fd fd fd 1a fd fd ab fd 0a 61 fd fd fd fd 5b 74 fd 03 fd 64 39 fd 4e fd 09 14 2c 12 1d 0f 62 fd 04 fd fd fd fd 66 fd fd 39 1f fd 01 fd fd 44 20 4b fd 65 fd 61 52 fd fd fd 60 76 fd fd fd 14 6d 76 fd 73 fd fd fd 69 fd 56 fd 6a fd fd fd 71 fd 68 0d fd fd fd 70 09 17 37 00 10 59 5c 47 fd 76 6d 65 11 46 68 fd 43 65 11 fd fd 51 45 fd 52 79 3f fd 7c 1f d0 fd	;TJE\4]+MIHp-jsYV? 4SN+vQn`#5'yP2=# (8g1z/F\$a[td9N,bf9D KeaR `vmvsiVjqhp7Y\GvmeFh CeQRy?]	success or wait	1	F2C055	WriteFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\OWOW64WW.cab	30592712	10	25 32 fd fd fd 01 00 00 00 00	%2	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\OWOW64WW.cab	0	3059210	fd 33 fd 8f 12 49 57 fd fd fd fd 76 fd 62 fd fd 54 70 fd 5c 1f 72 fd fd 08 72 fd 6b fd 61 1b 1c fd 41 fd fd 3f 7a fd fd fd fd fd 59 01 fd 22 fd fd 2c 25 6a fd fd 18 11 a2 fd 65 fd fd fd 59 fd 69 67 18 74 fd fd 36 12 fd 51 38 fd a7 03 61 28 54 49 fd 7f 1c 2f fd fd fd 6a 0b fd fd fd fd 11 4f 1c fd 5d 42 39 6b 1e 7a fd 59 66 fd 18 fd fd 28 fd 73 fd 15 2b 1d 12 68 03 28 7f fd fd fd fd 52 47 6f 0b fd 30 fd fd 6d fd 33 30 fd fd 33 fd 1d fd fd 09 4c 05 39 fd 0d 3f fd 4e e5 fd fd fd 15 fd fd 0d 07 fd fd fd fd 4c 70 fd a5 fd 5b fd fd 4c fd fd 27 0e fd 09 55 0d fd fd 28 fd 28 66 04 fd 13 fd fd fd fd 5f 12 fd 62 1d 27 69 1d 79 fd 10 fd fd 47 fd 22 fd fd 3a 60 49 fd 45 fd fd 2b fd fd 41 fd fd 09 7c 43 38 11 18 0d	3IWvbTp\rrkaA? zY,%jigt68a(TI/ O)B9kzYf(s+h(RGo0m30 L9?Np[L'U((f_biyG":'IE+A C8	success or wait	5	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\pkeyconfig-office.xrm-ms	590523	524	fd 30 fd fd fd fd 17 1d fd 73 70 fd fd fd fd fd 5d 12 0a fd 70 39 fd 45 53 fd fd 72 41 33 05 fd fd 35 fd fd fd 78 fd fd 3b fd 21 26 fd fd 18 04 fd 2b 0f 4e fd fd 2f fd fd 27 fd 5b fd fd fd 07 fd 56 7c fd fd fd fd 42 fd 7f 67 fd fd 3f 6a fd 46 fd 03 0c fd fd 0c fd fd fd 48 26 fd fd 31 fd 89 3b fd fd fd fd fd 1d fd fd 10 53 70 fd fd fd 6d fd 44 fd 2f 60 1c fd fd 67 fd 5f fd 6a 5a 0d 01 fd 04 fd 53 fd 4d 2c fd 00 58 fd 2d fd 01 68 6a 5c 55 fd 58 fd fd fd fd fd 25 fd 3e 00 fd 70 fd 7f fd fd 06 fd 46 fd 7e fd fd 14 fd 01 fd fd fd fd fd 25 fd fd 58 27 fd 64 6e 72 70 f9 56 30 fd fd fd fd 5d 7c 65 45 fd fd 4e 0c fd fd 1a 2f 2b fd 1b fd fd fd fd 5b fd fd 75 fd fd fd 95 2b fd 4e 5d 57 4f 19 44 53 fd 6a fd 26 fd fd 45 0b fd fd fd fd	0sp]9ESrA35x!&+N/[V B g? FH&1; SpmD/'g_jZSM,X- hj\UX%>pF~%X'dn rpV0] eEN/+ [u+N]WODS&E	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\pkeyconfig-office.xrm-ms	591047	10	24 00 fd 02 09 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-00000000FF1CE}-C\pkeyconfig-office.xrm-ms	0	590523	7d 09 fd 10 fd fd 14 fd 24 fd 29 fd 3c 23 fd 2a 62 fd 5c fd 5b fd 61 2e 49 fd 58 34 fd 4f fd fd 4e 18 fd fd fd 45 6e 78 73 fd fd fd fd fd 49 71 0d 1c 7e 69 fd 28 68 fd fd 22 fd 69 5b fd 62 fd 57 13 fd fd fd 46 0b 10 fd fd 8d 33 01 24 3a fd 73 3b 75 fd 47 64 31 3f fd 40 21 fd 63 03 35 76 fd 01 1b fd 59 76 fd fd fd 44 fd 3d fd fd 7a 2f fd 5f 5e 1a fd 72 fd fd 32 fd 1f 78 7a fd 6e 54 fd 19 fd fd 3e 55 fd 28 fd fd 31 ed fd 39 fd 50 1a 14 fd 49 7b 6e 02 fd 2d fd 79 3c 33 1d 79 fd fd 05 fd 21 fd 1b 75 fd fd 64 fd 05 7a 76 13 fd 4c 57 79 72 fd fd fd 5e fd fd 7e fd 31 fd ef 59 fd 4d 10 fd 20 0e 06 fd fd 14 1a 0b 31 fd fd 4c 02 03 3e fd 2b fd 5f fd fd fd 48 2f 10 fd 54 fd 07 fd fd fd fd 07 fd fd fd fd 40 fd fd fd 10 fd ff fd 5d	}\$)<##b\ [a.IXONEnxslq~i(h"i bW F3\$:s;uGd1? @!c5vYvD=z/_r2xzT>U (19P {ny<3y!udzvLWyr^~ 1YM 1L>+_H/T@]	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ v _ _ _ \ / / _ _ _ . ' _ \ _ _ \ \ / \ / \ \ _ / \ _ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPlusWW.xml	17108	524	13 fd fd 43 fd 17 fd 20 3a 36 fd 5f fd fd 30 fd fd fd 61 5f 1d 63 68 24 fd fd fd 03 58 4d fd c8 75 fd fd 1b fd fd fd fd 7f 4c 7f fd fd 79 2b 21 fd 7c 20 24 5d fd 5b 16 74 fd fd fd 55 fd 66 fd 50 fd fd 64 0b fd 46 fd fd fd 70 02 fd fd 05 2c fd fd 71 ad 74 fd 62 fd 7c 53 fd 0b fd 66 fd 47 21 fd fd 72 3c fd 6f fd fd fd 36 66 7e 4a 75 fd fd 31 0f 39 fd 69 fc 4a fd 78 54 1d fd fd 52 fd fd fd fd 66 fd 6a fd 0d 15 4f 0f 14 0e fd fd fd 0f fd fd fd fd 19 13 24 6a 5f fd 79 03 fd fd fd ac 40 43 fd 1f fd fd fd 23 1e fd fd 61 fd fd fd fd fd fd 16 fd 11 fd 04 56 fd fd 38 fd 64 fd fd 4e 1c 1b 6f 7b 16 67 fd 79 7a 12 60 fd 1c 39 68 fd 38 fd 63 fd fd fd fd fd 25 fd fd fd 7a 36 fd fd fd fd fd 01 41 4f 08 fd 23 fd 27 63 fd 76 fd 3d	C :6_0a_ch\$XMuLy+! \$] [tUFpDfP, qb[SfG!r<o6f~Ju19iJxTRf jO\$j_y@ C#aV8dNo{gyz'9h8c%z6 AO#'#cv=	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPlusWW.xml	17632	10	24 00 fd 42 00 00 00 00 00 00	\$B	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPlusWW.xml	0	17108	38 fd 35 02 fd 22 b1 3b fd fd fd 03 fd 29 36 22 04 20 fd 48 3b fd 13 16 40 4f fd 4b 23 22 4a fd fd fd c9 66 fd 0a 09 41 2b fd 37 33 1a fd fd 52 12 0c fd 15 fd 2b 27 fd fd 51 77 fd 3e fd fd 4c fd 5f 2b 4c fd fd 2a fd 20 fd 50 cf 14 5f 2d fd 5c 1d 0e 5b fd fd fd fd fd 17 5b 5a 3d 66 fd 68 16 1e 48 fd fd 39 39 fd fd fd fd 79 2a fd fd 22 6e 27 20 1f fd fd fd 3c fd 70 26 64 fd 64 31 fd 49 23 2f 5b 51 19 fd fd 0e 43 fd 1b 27 7e fd fd fd 7e fd 2e fd 2d fd fd fd 5b 78 fd 56 7b fd 75 6a b7 fd fd 7f 22 c2 12 fd 72 47 1b 17 fd 09 2e 26 fd 18 4a 65 76 fd fd fd 4c fd 89 fd 0e 3d 43 c4 fd fd 74 fd fd 15 76 76 fd fd fd fd fd 7c fd 21 fd 36 53 5e fd 1a fd fd 14 30 2e fd 5b ac fd 4c 3a fd 94 22 46 fd fd fd fd fd 22 39 fd fd 74	85")6 H:~OK#"JfA+73R+'Qw> L_+L* P_-\[Z=fhH9y""n' <p&dd1l#[[QC'~-.- [xV{uj"rG.&JevL=Ctwv !6 S0.[L:"F"9t	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW.cab	323578974	524	19 17 24 fd 5f 39 23 35 fd 5f 7e 00 fd fd fd 1b fd 1a 26 7b fd 47 88 66 17 0d fd 61 fd fd 53 5a fd 76 fd 62 54 6c fd 15 fd 37 fd 59 60 fd 03 71 10 fd 4f 0e 61 fd fd fd 14 fd fd fd fd 7d 7b fd fd 01 30 fd 08 fd 2f 59 4c 6f 70 61 79 7d 28 6a 27 fd 50 fd 3a 19 fd 34 29 69 46 fd fd 41 fd 26 6f 13 fd fd 75 fd 2e fd 66 fd 00 fd 02 01 fd fd fd 60 5b 69 f3 74 fd 2a 46 fd 2e fd 15 21 fd 60 7f fd 22 79 36 64 b6 23 2b 77 16 28 48 12 fd fd fd fd fd 1a 25 fd 0b fd 00 19 2c 05 2c 45 fd fd fd c1 fd 23 fd 0b 63 fd fd 53 20 fd fd fd 3c 28 26 fd 0c 69 fd 7b 5c fd fd fd 01 fd 9e fd 2c 5c 08 68 fd 14 31 fd fd fd 77 3b fd fd 36 11 5d 76 fd fd 06 60 7b 26 6d fd fd 32 61 fd 62 69 fd fd fd 40 1f 65 16 fd 75 4d fd fd 58 fd 16 70 fd 0b 19 61 77	\$_9#5_~&{GfSZvbTl7Y`qOa}{0/YLo pay}(j'P:4)iFA&ou.f[jit*F.!""y6d#+w(H%,,E#cS<(&i\,h1w;6jv`{&m2abi@euMXpaw	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW.cab	323579498	10	25 32 5e 6c 49 13 00 00 00 00	%2^ll	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW.cab	0	5242880	4a fd fd 52 fd fd 1a fd fd 16 0f 61 fd 5e fd fd fd fd 55 45 43 fd 0b 36 fd 19 fd 3d 7e fd fd fd fd 56 32 02 fd 7e 76 fd 2b 1e 20 fd 35 3f 69 33 60 4b fd 23 fd fd fd 22 fd fd 2e fd 4e 46 fd fd 0e fd fd 4a 0e fd 6a 3d fd fd 16 7e 76 79 16 fd fd 54 fd 25 68 56 5b fd 35 fd fd 5a 69 4b fd 5b fd 27 fd 2c fd fd 28 05 00 fd fd fd 2f fd fd 62 41 77 fd fd 39 fd fd c4 68 fd fd 16 fd fd 0f 71 4e 74 fd fd fd 52 fd 2a fd fd fd 20 78 33 fd fd fd 7a 02 fd 3a fd 49 00 6f 37 75 78 fd 59 fd fd fd 40 fd 44 fd fd fd fd 22 5d 1d fd fd 90 37 fd 34 44 50 3f 26 1a fd 83 fd fd 09 50 fd 1f 2f fd 8c fd fd fd fd 56 fd 0b 49 b9 fd fd 02 6d 50 fd fd 34 5a fd 0b 0d fd 46 fd fd 7a 39 34 fd fd fd fd 31 fd fd 26 fd 0e 55 37 5a 5b 03 56 fd 56 fd	JRa^UEC6=~V2~v+ 5?i3`K#".NFJ]=~vyT%hV[5ZiK[,(/bAw9hqNR* x3z:lo7uxY@D"]74DP?&P/VImP4ZFz941&U7Z[VV	success or wait	35	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-00116-0409-1000-0000000FF1CE}-C\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \\ _ _ v _ _ _ _ \ / / _ _ _ _ \ . ' _ _ \ _ _ \ \ / / \ \ \ _ / \ _ _ \ _ _ \ _ _ \ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW2.cab	249155 271	524	4c 54 52 fd 0a fd fd 55 fd 38 fd 63 24 2c 29 1c 7c 1d fd fd fd 64 fd fd fd 42 fd fd 39 fd 16 48 fd 72 fd fd 0c 12 fd fd 09 42 fd 4d 26 64 2b 3d 25 77 63 49 fd 10 fd 5d fd fd fd 0e 65 fd fd fd fd 4d 70 64 22 67 fd 6e fd 10 2d 22 fd 21 6b 31 11 66 59 fd fd fd 0c fd fd fd 44 fd fd 3e 75 69 1f 1f fd 6a fd 3a 70 61 fd fd fd 67 46 fd 0a fd 0f fd 50 74 fd 29 06 2b 38 fd 34 fd 7b 4b fd 5f fd e0 40 fd 22 fd fd fd 35 fd 44 fd 25 14 1e fd fd 1c 75 fd ef 19 4b fd 74 01 fd 17 fd fd fd fd fd 60 fd 72 5e fd fd 48 0b 02 fd 7b 3e 5b fd fd fd 75 45 fd 78 1b 0d 60 fd fd fd fd 93 fd fd e2 fd fd 20 fd 49 fd cf 55 fd 3f fd 0d fd 5e fd 4f 79 96 75 24 fd 5e fd 03 fd 04 26 fd 7f fd fd fd b4 fd 2a fd fd fd fd 39 1d 36 1b fd	LTRU8c\$,)dB9HrBM&d+ =%wci]eMpd"gn- "!k1fYD>uij:pagFPt)+84{ K_@"5D%uKt`r^>[uEx` IU?^Oyu\$^&*96	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW2.cab	249155 795	10	25 32 fd fd fd 0e 00 00 00 00	%2	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW2.cab	0	5242880	fd fd fd 79 05 3c fd 37 7d fd 07 fd fd 6a fd 4d fd 6a 64 fd fd fd 34 7a fd 30 ad 23 08 22 fd 6d fd fd fd 4f 5c fd fd fd 1a 49 6d 18 fd fd 17 44 fd fd 4c fd 2f 68 01 45 fd 76 fd fd fd fd 68 fd 39 5c fd 77 fd 3c fd fd fd fd 74 fd 66 25 66 66 63 7f 14 fd fd 38 fd fd e2 6e fd 58 fd fd fd 5f 01 fd fd 58 fd 6a fd 37 fd fd fd 2a 59 fd fd 05 fd fd fd fd 45 19 77 fd 50 4f 4c 6b fd fd 41 fd fd fd fd 05 14 11 3c fd 2f fd 66 56 fd fd fd 56 56 fd fd 13 5e fd 8e 09 48 62 70 36 fd fd 40 1e 3b 0d fd 6c fd fd 30 63 fd fd fd 1c 1f 11 fd d0 18 fd 40 fd fd 3e fd 11 fd 4b fd fd 1a 77 fd 43 24 4d 13 fd fd 2e 5a 73 fd fd fd 10 fd fd a0 fd 4e fd fd fd 7f 5f 39 6a fd 56 66 41 58 fd 12 15 23 64 6c fd fd fd 25 57 71 fd fd fd fd 56 10 e4 18 7d 5e	y<7}jMjd4z0#"mO\ImDL/ hEvh9lw<t f%ffc8nX_Xj7*YEwOLkA </fVVV^Hbp 6@;l0c@>KwC\$M.ZsN_ 9jVfAX#dl%WqVj^	success or wait	25	F2C055	WriteFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Setup.xml	27782	524	6f fd 27 5e fd 35 06 20 1f 5b 4a 14 34 4f fd 77 fd 3e fd 13 fd d2 1d 49 51 21 61 52 58 21 13 fd 7c 7d fd fd fd 16 0e 48 4e 8c fd 18 4a 75 fd fd fd 2d 54 38 13 fd fd 20 7e 2f 52 1a 1c fd fd fd fd 59 fd 68 c5 80 6a fd fd 5f fd fd 19 49 67 40 37 fd 44 78 4d fd fd fd fd fd 27 69 d2 7a 16 11 22 16 26 fd 48 2b fd fd fd 54 24 fd 16 60 0f 58 fd 8f 7f fd 54 44 61 fd 2a 4c 27 fd fd 62 fd 61 fd fd 0c fd fd 52 35 39 57 0e fd fd fd fd 12 fd fd 3f fd fd fd 10 fd 01 56 5a fd fd 65 7a fd 57 fd fd 3c fd 48 19 37 fd 15 7d fd fd 50 54 1b 48 fd 85 53 aa 21 fd 00 6c fd fd fd fd fd 56 32 73 fd 26 17 fd 74 fd fd 04 2f fd 33 73 fd 34 4c fd 1a fd 14 fd fd 5f fd fd fd 4b fd 46 fd 36 01 fd 00 fd fd 45 2f 31 4b 59 7a 54 fd fd fd fd 2f fd fd	o^5 [J4Ow>!QaRX!]}HNJu-T8 ~/R Yhj_lg@7DxM'iz"&H+T\$ XTDa*L'baR59W? VZezW<H7}PTHS!lV2s&t /3s4L_KF6E/1KYzT/	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Setup.xml	28306	10	24 00 fd 6c 00 00 00 00 00 00	\$l	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Setup.xml	0	27782	44 d9 1f fd 7b fd fd 43 fd fd fd 28 fd 73 34 fd fd fd fd 3d fd fd 62 fd fd 7b 49 77 fd fd fd fd 09 46 fd 0e fd fd 5a fd fd fd 78 fd fd fd 76 7e fd 33 fd 57 fd fd 1f 43 fd fd 7d cc fd fd 25 fd fd 68 fd 1b 76 75 fd 53 5c 7a 3e fd 24 fd 70 fd fd fd fd 28 0b 0b 06 fd 14 fd 0f fd fd 0b 01 2b fd fd 1b 22 4f fd 1d e4 fd 46 16 46 63 05 59 fd 5e 0e fd 32 0e fd 7d fd 63 fd fd fd 0e 40 63 fd 24 0a 4c fd 1c fd 71 fd 13 73 fd fd 32 36 35 fd 5e fd fd 72 17 fd 3a 4e fd 43 32 fd 13 fd 7f fd fd fd fd fd fd 04 7f 6f fd fd 29 fd 05 50 fd 2b a2 74 fd 0d fd fd 68 2d fd 3a 2e 07 fd fd fd 1d 5d fd 35 fd 1b 4e a1 5e fd 79 fd fd 77 14 5d fd fd 69 6f 4a fd fd fd 65 fd fd 06 fd fd 61 19 43 50 2d fd fd 4b 76 fd fd 0a 78 fd fd 54 fd fd	D{C(s4=b{lwFZxv~3WC} %hvuSlz>\$p (+"OFFcY^2}c@c\$Lqs26 5^r:NC0)P+th- .:]5N^ywjjoJeaCP-KvxT	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-00117-0409-0000-0000000FF1CE}-C\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ ____ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ / / _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ / / _ _ _ _ / _ _ _ _ _ _ _ _ _ _ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\MSOCache\All Users\{90160000-00117-0409-0000-0000000FF1CE}-C\ExcelLR.cab	5769566	524	fd 38 fd 48 1a fd fd 7d fd 2e 6f fd 7d 41 18 30 05 fd 49 42 fd fd fd 21 fd fd 51 13 1e 63 fd fd 5f 18 43 5f fd 16 fd fd fd fd fd 7a 5c fd 05 0c 36 46 fd 33 35 fd fd fd 4a 36 38 48 fd 0f 41 d7 39 16 05 fd 3e fd 3c fd 79 fd 0c 7f fd 24 fd fd 48 3d fd 77 47 4a fd 09 48 48 0c fd 43 3f fd fd 17 fd fd 37 4e fd 49 fd 47 3d fd fd 5d fd 2d fd fd 69 4f fd 52 02 56 fd 75 fd 3d 58 fd fd 59 fd 52 fd 55 69 7f fd 2c fd 4e fd fd fd fd 75 05 fd 56 08 fd fd 35 fd 09 7b fd 37 1d 39 06 fd 49 4b fd 36 fd 2e 2a fd fd fd 33 fd 65 71 fd fd 3d fd fd 11 2c 6c fd fd fd fd 2a 7e fd 0f 6e fd fd 5f fd fd 4f 31 fd fd 40 7e fd fd 32 fd 44 fd 47 7a fd 7f fd 36 4d fd 1c fd fd fd 3b 57 1f fd fd fd fd 2a 40 fd 6a 5a 7b fd 77 40 fd fd fd fd fd fd 7c fd	8H}.o}A0B!Qc_C_z\635J 68HA9><\$H=wGJHHC? 7NIG=-} iORVu=XYRUi,NuV 5{79IK6*3eq=, *-n_O@~ 2DGzM;W*@[Z{w@	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-00117-0409-0000-0000000FF1CE}-C\ExcelLR.cab	5770090	10	25 32 5e 09 58 00 00 00 00 00	%2*X	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelLR.cab	0	576950	fd fd 05 0d 78 fd fd 6a 68 fd 20 29 65 fd 09 45 51 6c 69 fd fd 46 58 0c 65 fd 43 79 4a fd 5c fd 03 3e fd fd 17 fd fd fd 24 fd fd 78 fd 62 fd 4c fd fd 17 02 5f 7e fd fd fd fd fd fd 0d 6b 20 1b fd fd 52 5c 45 3f fd fd fd 76 18 fd 55 35 fd 3c fd 4b 7b 2e 04 fd fd fd 32 72 fd fd 7d fd 55 fd fd fd 7c fd fd 23 fd fd 1d 2e 00 89 43 6b 39 77 fd fd fd 5f fd fd 2c fd fd 5f fd 2f fd 51 13 00 97 13 6b 1a fd fd a2 fd 15 fd 38 fd 08 fd 1e fd 4c fd fd 58 5e fd 4b fd 5a fd 59 52 fd fd 47 fd 2d 32 fd 2e 75 00 2f 1f 49 fd fd fd 55 fd fd fd 6f 48 7d 23 0f fd fd f4 54 7a fd fd 13 fd 55 00 19 fd fd 15 fd 10 fd fd fd 79 56 03 fd 3b fd fd fd 0d 5c fd 00 fd fd 2b 5f fd fd 56 fd fd 06 30 15 fd fd fd 1d 04 38 1c fd 24 fd fd fd fd fd fd 31 5b fd fd	xjh)eEQliFXeCyJ\>\$xbL_-k R\IE? vU5<K{.2r}U #.Ck9w_._/ Qk8LX^KZYRG- 2.u/IUo)#TzUyV;\+_V08\$ 1[	success or wait	5	F2C055	WriteFile
C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	____ _ _ _ _ \\ _ _ v _ _ _ _ v _ / / _ _ _ \ . ` _ _ \ _ _ \ \ v v _ / / \ _/ \ _ / \ _ _ \ _ _ \ _ _ \ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\Common Files\microsoft shared\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \\ _ _ v _ _ _ _ v _ / / _ _ _ _ v . ' _ _ \ _ _ \ \ v v _ / \ _ / \ _ / \ _ \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\Program Files\Common Files\Services\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \\ _ _ v _ _ _ _ v _ / / _ _ _ _ v . ' _ _ \ _ _ \ \ v v _ / \ _ / \ _ / \ _ \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\Common Files\system\IR3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ ____ _ _ _ _ \\ _ _ v _ _ _ _ \ _ / / _ _ _ _ \ . ` _ _ \ _ _ _ \ \ _ / \ _ / \ _ / \ _ _ \ _ _ \ _ _ \ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelMUI.xml	1780	524	fd fd 59 66 15 fd 5f 19 7f 67 fd 4f fd fd fd fd fd fd fd 7e fd fd fd fd 2b fd fd fd 23 2d de 7c 4d 3d 44 51 fd de fd 33 19 6e 02 05 fd 5c fd fd fd 08 73 3e fd 31 6e fd fd 7c fd 01 1b 3d fd 51 fd 52 fd 0a fd 4a 58 54 fd 4d fd fd 08 65 69 fd 6e fd 05 42 fd fd 11 fd 6c 53 fd 2c fd fd 78 5c fd 03 51 3a fd 59 0d 3a fd fd fd 7f 72 fd fd 7d 0b 34 fd 68 71 7e 04 60 1e 05 fd 00 fd 35 fd 79 fd 41 06 fd 37 fd 61 fd 41 3e fd fd 38 62 fd 57 4e 5f 43 fd 44 42 05 fd 2a fd 58 fd fd fd fd 46 fd fd 6b fd fd 39 70 d2 fd 6f fd fd fd fd 35 fd 63 fd fd 73 52 fd 46 fd fd 51 70 3e fd fd fd 53 fd 57 16 fd 0d 12 fd 19 fd 63 fd 3d fd fd b6 07 fd fd 5d 36 fd 59 fd fd 55 ee fd fd 56 31 fd fd 20 73 fd 48 47 66 fd fd fd 44 4e 54 1b 81	Yf_gO~+#+ [M=DQ3n\ls>1n]=QRJXT Me inBlS,xl:Y:r]4hq`5yA7aA> 8WN_DB *XFk9po5csRFQp>SWc=]6YUV1 sHGfDNT	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelMUI.xml	2304	10	24 00 fd 06 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0016-0409-0000-00000000FF1CE}-C\ExcelMUI.xml	0	1780	39 fd fd 49 2e fd 57 2e 38 fd 21 4e 0d 37 68 1d 0d 6d 39 4c 32 fd 5e fd 5c fd 19 fd 07 60 cf 1c 44 fd 60 fd 34 52 31 18 50 77 4a fd 6e fd 39 fd fd fd 3f fd 46 7b fd 63 fd fd fd 79 32 e9 fd fd 07 6b 46 04 fd 5b fd 32 fd 32 14 69 fd fd fd fd fd fd 5d 1e 74 75 0b 36 fd 16 1b fd 57 fd fd 5a fd 7c fd fd fd 60 fd 0a fd 75 fd fd fd fd 60 04 fd fd 26 fd 77 fd fd 06 fd fd fd 1a 19 58 fd 79 fd 5f 04 2a 1a 74 fd 3f fd fd fd 6b 41 31 3b 47 fd fd dc 23 74 fd fd fd 76 fd fd 17 fd fd 6c 12 fd fd 48 19 fd 3b 43 fd 24 1d fd 57 fd fd fa 74 fd 10 5b 59 fd 54 fd 0b 7a fd fd 50 fd 33 3f fd fd 3e 50 56 fd e8 fd 37 fd fd 6d 1e fd fd fd 12 fd fd fd 7b fd fd 7d fd 6a 21 fd fd fd 48 77 fd 50 fd 68 fd 59 fd 0a fd fd 42 0d 6e 18 fd fd 1a 4f 3d 37 09 fd fd 21	9l.W.8!Nhm9L2^`D`4R1 PwJn9?F[c y2kF[22i]tu6WZ]`u`&wXy _?kA1; G#tvIH;C\$Wt[YTzP3? >PV7m{ji!HwPhYBnO=7!	success or wait	1	F2C055	WriteFile
C:\Program Files\Google\Chrome\IR3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 5f 2f 5c 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ v _ _ _ _ v _ / / _ _ _ v . ` _ _ \ _ _ \ \ v v _ / / \ _ \ \ _ / \ _ _ \ _ _ \ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\MSOCache\All Users\{90160000-0016-0409-0000-00000000FF1CE}-C\Setup.xml	2482	524	fd fd 78 fd 21 4c 75 0c fd 06 fd fd 37 67 46 8a 5a fd fd fd fd 6c fd 48 63 75 29 fd 25 03 f2 fd 4f 4a fd 32 fd fd 16 fd 06 fd 08 19 28 fd fd 6c fd fd 2d 3d fd fd 3d 7d fd fd 03 39 fd fd fd 71 56 fd 04 4e fd 44 fd 54 fd 46 74 7e fd fd 3b fd fd 7e fd fd fd 65 7c fd fd 6d fd 59 28 fd fd 56 6b 3f fd 14 07 fd fd fd fd 36 fd 59 41 fd fd 2e fd fd 25 fd 63 fd 47 fd fd 30 fd 11 38 0f fd 4d fd 43 fd fd fd 76 fd 3d fd fd fd 44 fd fd 4c 36 6a 75 fd 37 fd fd fd 31 21 13 fd fd 6a 4c 14 fd fd 42 fd fd fd fd 6e fd 36 47 61 52 fd fd fd 7b 40 35 75 78 fd fd 57 37 2c fd 4a 02 fd 19 20 62 fd 35 12 fd 23 74 fd 1c 27 15 fd 04 fd 66 29 fd 71 39 65 fd fd 7e fd 0c 28 37 1b fd 70 fd 34 fd 58 43 fd fd 6f 00 0f fd 66 61 36 fd 6d fd fd fd 3a 40	x!Lu7gFZIHcu)%OJ2(- ==}9qVNDTF t-;-e]mY(Vk? 6YA.%c8MCv=DL6ju71 ljLB6GaR{@5uxW7,J b5#t#f)q9e~(7p4XCofa6m:@	success or wait	1	F2CBF8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\Setup.xml	3006	10	24 00 fd 09 00 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\Setup.xml	0	2482	fd 30 1d 0f 22 3e fd fd 3f fd fd 5b fd 3d 0f 50 fd fd 3c 7b fd fd 61 20 fd fd 03 fd 1a fd 36 67 fd 68 0d 07 fd fd 1e fd 2c 08 2f 27 33 2c fd 63 1f 3b 4f fd 2e fd fd 53 4d 34 52 fd 71 fd fd 4a fd 73 fd fd 60 fd fd 2d 0d 5c 41 fd 12 6a 55 3b fd 7d 20 54 fd 10 fd 23 b6 15 fd 04 fd 21 22 74 01 fd 5f 46 fd 0d 7b 7e 4f fd 51 fd fd 43 e5 12 fd 73 ec 2e fd 56 0d 55 fd 55 3c 6d 2a 0f fd 40 fd 0c 4b 46 0c fd fd 39 42 20 59 2c 1d 38 fd 47 fd fd fd 44 5f fd fd 5f 4c fd 68 55 33 ac fd fd fd fd 58 38 20 fd fd 4b fd 1c 3f 20 fd fd 05 fd 1a 03 6d fd fd 16 14 11 fd 7c fd fd 08 fd fd 9c 39 76 32 af 0b 12 5a fd fd fd 14 66 fd fd fd fd 4d 62 27 fd fd fd 37 fd 64 fd fd fd 4e 57 fd fd fd 38 fd 4d fd 35 fd 7e fd 58 fd fd 31 2d fd 10 fd fd fd 11 06	0">? [=P<{a 6gh,/3,c;O.SM4RqJs`- \\AjU;} T#!"t_F{~OQC.s.VUU<m* @KF9B Y,8GD__LhU3X8 K? m 9v2ZfM b'7dNW8M5~X1-	success or wait	1	F2C055	WriteFile
C:\Program Files\internet explorer\en-US\IR3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ v _ _ _ _ v L / / / _ _ _ _ v . ` _ _ \ _ _ \ \ v v L / / \ / \ \ _ / \ _ _ \ _ _ \ _ _ \ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PowerPointMUI.xml	1661	524	65 fd fd 42 fd 2a 2e fd 2b fd 5f 1d 1c 40 fd 68 0d fd fd 1b 3e 2a 75 39 40 fd fd 4a fd 58 78 fd 2c fd 2f 23 fd 10 5a 04 fd 1f fd 03 57 fd fd fd 46 3f 07 fd 60 57 1d fd 2a fd 4f fd 34 26 fd 59 23 0b 60 2f fd 7c 17 41 fd 5d fd 72 5d fd fd 4c 5e 15 fd 39 fd fd 05 fd 5b fd fd 12 18 73 37 27 fd fd fd 20 fd 7b fd fd fd fd 05 de 5e 54 0b 68 31 fd fd 3b 62 53 fd fd fd 5d 2e fd 00 09 2c 2b fd 3b fd 16 14 fd 7e 14 38 fd 3c fd 7f 03 2e fd fd 3d fd fd 59 fd fd 76 3a 36 fd 17 10 1c fd fd 21 fd fd 5d fd fd 10 dd 79 36 46 07 33 fd fd fd f7 18 2a 7b 4f fd 2f fd fd 73 0b 1b fd fd fd fd fd 21 fd 0c 73 67 1a 7d fd 18 fd 40 30 fd fd fd 74 fd 7e 2c fd fd fd fd fd 15 fd 75 4e fd fd 58 3f fd fd fd 71 23 12 fd fd fd 61 fd 04 5b fd 1d 70 0e	eB*._@h>*u9@JXx,/#Z WF?'W*O4&Y #'/A]r]L^9[s7' {^Th1;bS],+;~8 <.=Yv:6!]y6F3* {O!sg}@t~,uNX?q#a[p	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PowerPointMUI.xml	2185	10	24 00 7d 06 00 00 00 00 00 00	\$}	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PowerPointMUI.xml	0	1661	39 fd fd fd 7e 4d fd 0b 21 fd 59 fd 59 8b 45 36 fd fd 63 fd fd fd 52 15 fd fd 1c 03 fd 4e 4e 2f fd 47 fd 0b 76 20 fd fd 71 6d 1c 26 fd 7a fd 4d fd 2d 0e 23 49 fd 43 1d 5f fd fd 2f fd 7d fd fd fd 4d fd 4d 66 fd 0d 74 fd 01 00 3a fd fd fd fd 08 45 01 3c fd 1d 09 fd fd 01 27 fd 57 66 fd 47 72 40 fd dc fd fd fd 33 27 0b fd 34 40 0e fd 5f fd 16 fd fd fd 79 61 71 68 6f 66 6f e6 37 fd 62 5b 26 23 33 18 1c fd 4d 31 78 22 41 fd fd fd 32 fd fd 13 fd fd 5e fd fd fd 50 0b fd 51 fd 22 fd 70 0c fd fd 5d 2c fd fd 59 fd fd 5e fd fd 49 fd fd fd 14 33 fd fd 11 71 fd 33 40 fd 77 fd 05 fd 2d fd fd fd fd 78 7e fd 6d fd 7e fd fd fd 49 5d fd 1d fd fd fd fd 7c 59 20 fd fd 60 fd 27 38 56 fd fd 7b fd fd 3c 4d ec fd 62 fd fd fd 5b 6f 1b 46 03 fd fd	9-M!YYE6cRNN/Gv qm&zM-#(C_)MM ft:E<'WfGr@3'4@_aqhof o7b[M1 x"A2^PQ'p],Y^!3q3@w- x~m!]]Y`8V{<Mb[oF	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PptLR.cab	0	631010	50 0e fd fd 31 2b 1e fd 22 37 48 31 fd 10 7b fd 64 fd fd 3d 45 fd 79 fd 7d fd fd fd 4b fd 28 fd fd 2b 53 4f fd fd fd 7e 22 29 fd 20 67 fd fd fd 19 0f 56 18 fd fd fd fd fd de 58 12 44 fd fd fd fd 23 3d 1b fd fd 33 18 70 fd 70 51 35 fd 0b fd fd 16 62 fd fd fd 7e fd 14 fd fd d8 7e fd fd fd 58 76 fd fd 4f 45 3c fd 12 54 fd 09 fd 09 fd 6e 41 fd fd 4b 37 fd fd 69 1d 3b 28 73 56 fd 12 fd f2 fd fd 26 fd 06 3c 0e fd fd fd 4e 7f 7d 78 1f fd 35 fd 59 fd 21 fd 44 75 06 05 fd fd 1b fd 4f fd fd 05 66 51 11 02 12 29 20 fd 30 fd 5a 0d fd 4b 23 54 fd fd 65 30 c4 fd 0c fd 20 fd 6d 7b fd 6b fd 62 fd fd 74 fd fd fd 47 fd fd 61 fd 72 fd fd fd fd fd fd 30 fd fd fd 76 34 09 fd fd fd 2c fd fd 47 69 fd 15 fd fd 03 fd fd 6d fd 44 fd 20 fd	P1+"7H1{=Ey)K(+SO~") gVXD#=#3pp Q5b--XvOE<TnA7i;(s& <N)x5Y!DuOfQ) 0ZK#Te0 m{kbtGar0v4,GimD	success or wait	5	F2C055	WriteFile
C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\Setup.xml	2072	524	fd 05 1f fd 76 29 fd fd fd 59 fd 7b fd fd fd 7a 13 fd 2a fd 0b 4c 23 fd 41 fd fd fd 7f fd 0c 44 fd 5b fd 5b fd fd 2b 08 fd 38 79 fd fd 79 fd 7d 49 61 fd fd fd 02 4d fd fd fd fd 73 1e fd 25 fd 08 fd fd 70 5b 35 50 fd 0e 2c fd fd 37 38 fd fd 26 08 fd 11 fd 3c fd fd 06 fd 14 0f 02 69 fd 4b fd fd 72 05 fd 4b 21 fd fd 27 fd 26 fd 4b fd fd 5c fd 5f 38 1b 7e 16 fd 6a fd 4f fd 46 fd 52 fd fd 4c 74 55 fd fd 61 fd fd fd 50 05 04 fd fd 69 fd fd 8e 41 fd fd fd 61 61 fd 11 7d 6f 69 64 fd fd fd 27 fd 67 fd 57 fd 7c 5c fd fd 7d 7c 7b fd fd 49 fd fd 3a 29 fd fd 36 fd fd fd 1b fd fd 1f fd 59 36 fd fd fd fd 30 0c fd fd fd 20 fd 09 40 fd 47 fd fd 49 fd fd 52 41 cc 2b fd fd 3d fd fd 33 6b fd fd 5e fd fd fd 60 fd 4b fd 11 fd e8 fd 34 12 fd	v)Y{z*L#AD[[+8yyIaMs%p[5P,78&< irK!'&K_8~jOFRLtUaPiA aa}oid'gW\}\{!-)6Y60 @GIRA+=3k^ K4	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\Setup.xml	2596	10	24 00 18 08 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\Setup.xml	0	2072	63 fd fd 2d fd fd fd 4d 24 fd 1e 73 fd fd 3c fd 71 fd fd fd fd 19 5d fd 0a fd 47 18 fd fd 0a fd fd 54 4e 63 54 44 75 fd fd 22 3d fd fd 3d fd 3e fd 05 7a 56 62 fd fd 70 5e 61 3d 72 68 2a e2 fd 2c fd 76 fd fd 02 fd fd 43 fd 7a fd 0c fd 0c 52 fd fd 5f fd 78 62 4a 4f fd 55 4e 3e 3e fd 26 fd fd fd 2c fd fd 38 0d fd 04 02 0f 5a 6e fd fd fd 10 5f fd 63 03 fd fd fd 39 79 fd 11 50 0c 7f fd 05 fd fd fd fd fd 50 4d fd 23 2d 5c fd 2b fd fd 6e 64 75 fd fd fd 75 fd fd 42 fd 76 12 fd fd fd fd 5f 45 49 45 69 03 31 fd 53 fd 47 fd fd 2d 17 fd 22 34 37 fd fd fd 61 fd 73 4a 26 49 fd 28 fd 2d 3d fd 53 5c fd fd fd fd fd fd fd fd 2f 58 50 46 b9 fd fd 33 7d fd fd 50 01 60 1b 40 fd 2c 05 fd 7b 7a fd 71 16 1f fd 4d fd 37 1b 42 4e 1f	c- M\$sqjGTNcTDu"==>zVb p^a=rh*,v CzR_xbJOUN>>&,8Z_c9 yPPM#-\+ndu uBv_EIEi1SG-"47asJl(- =SVXPF3)P'@.{zqM7BN	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\internet explorer\SIGNUP\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ ____ _ _ _ _ _ _ _ _ _ _ v _ _ _ _ v / / _ _ _ _ v . ' _ _ _ _ _ _ _ _ _ _ _ _ \ _ / \ _ _ \ _ _ _ _ _ _ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\MSOCache\All Users\{90160000-0019-0409-0000-00000000FF1CE}-C\PublisherMUI.xml	1662	524	fd fd fd fd 4b 01 6e fd 2a 8a fd fd fd 35 fd 62 fd fd 37 46 fd 41 6a 24 fd 05 9a 3d 6f fd fd fd 51 fd fd fd 3b 33 fd 41 fd 41 fd 67 77 70 06 fd 58 58 fd 4a 4a fd 35 fd fd 75 42 fd 49 26 fd 6e 75 fd fd 7a fd fd 7b 6b 48 40 62 15 fd 7f fd 67 2b fd fd fd 75 66 55 fd fd 79 fd fd 5c 69 7a fd 4f fd fd 5f fd 47 3c fd fd 02 78 fd cc fd fd fd 47 31 fd 58 7e fd 39 1c fd fd fd 3b 1a 3d fd 56 fd fd fd fd 00 3f 69 49 fd fd 17 fd 17 52 7c 36 fd 0c 00 2d 77 fd 5f fd fd 70 fd f5 fd 42 15 64 fd 01 fd fd 74 fd 41 13 fd fd 3d 7c fd fd fd 6e 49 54 39 fd 19 41 49 04 7c fd 4b fd fd fd 1c fd 5f 2f fd fd fd 63 fd 2d 22 84 27 46 fd 58 fd 49 29 fd fd 42 fd fd 79 fd fd fd 48 06 08 46 02 fd 0a fd fd 74 fd 2f fd fd 1d fd 17 83 03 3e 04 2c 17 fd 00	Kn*5b7FAj\$oQ;3AAgwp XXJJuBI&nu z{kHbg+ufUyIizO_G<xG1 X~9;:=V?iIR 6- w_pBdtA= nIT9AI K_/c- ""FXI)ByHFt/>,<	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-0019-0409-0000-00000000FF1CE}-C\PublisherMUI.xml	2186	10	24 00 7e 06 00 00 00 00 00 00	\$~	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PubLR.cab	3562171	10	26 00 fd 58 36 00 00 00 00 00 00	&X6	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PubLR.cab	0	1048576	fd fd 67 25 15 fd fd 25 fd fd 22 5e fd 05 00 fd 40 50 2a 4d fd 5e 3f fd 65 64 fd 4c fd fd 40 fd fd fd 20 fd 38 5a 4e 12 fd fd fd 0c 1a 0d fd fd 34 11 fd 8a fd fd 0f 2e fd fd fd 20 79 fd 60 fd 44 13 5b fd 78 1a 2e 33 fd fd 44 fd 21 0e 13 54 36 5d 17 05 41 fd 01 02 74 16 25 45 27 fd 26 fd fd c6 fd 51 fd fd 12 fd fd fd 7e 35 34 4c 2d 73 fd fd fd fd fd 2b fd 79 fd fd 33 46 50 fd 2b fd fd fd 00 fd 20 2d fd 47 1f 6d fd 27 fd 40 fd 05 5d 22 fd 31 6c 14 fd 60 49 fd 1c fd 1b 0c fd fd fd 67 06 6d 0a fd 1c 79 fd 4a 7e 02 fd fd fd fd fd fd 3c 40 4e 2c fd 5a fd 7f fd fd 4e fd 04 1c fd 7b 5e fd fd fd 42 08 00 23 62 fd 15 fd 32 6f fd 0a 5b fd fd 0d 08 00 29 fd fd 9d fd 4c fd fd fd fd 7e 24 79 fd fd fd fd fd 73	g%'^@P*M^?edL@8ZN4 y`D[x.3D!T6]At%E'&Q~54L-+y3FP+-Gm'@]"!lgmyJ~<@NZN{^B#bo])L-\$y	success or wait	1	F2C055	WriteFile
C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\Setup.xml	1795	524	1b fd fd 2f 09 fd 06 fd 7e 51 fd fd 57 14 fd 14 64 78 fd 4d 0d fd fd fd 1c 6e 6d fd 7c 1e 30 10 fd fd 32 fd 5c fd 51 fd 2d fd fd fd 67 fd fd 47 fd 39 2c fd fd fd 25 01 fd fd 0b 1e 75 fd fd fd 3b fd 36 01 80 00 91 fd 67 fd 18 78 26 3e 11 33 2a 05 fd 29 2a 74 fd fd 49 fd fd 00 5e 5b 64 fd 6f fd 05 28 fd 3a fd fd fd 65 58 1f fd fd fd fd fd 70 fd fd 4f fd fd fd 0a fd 17 fd 78 5b 3c fd fd 48 fd 4d 2e 52 fd 12 61 5c fd 2a fd 4e 17 fd fd 72 fd fd 44 fd 38 fd 7a fd fd fd fd 34 fd 32 06 fd 14 fd 1c 44 73 5e 04 11 0c 29 fd 04 fd fd fd 7b fd 1b fd 6c fd 2a 03 fd fd 20 fd fd 12 fd 54 fd 6b 30 76 7b 72 65 fd fd 36 3f 50 fd 59 7c 3f 11 fd 29 15 3d 73 fd fd 3b 64 19 41 07 fd 34 03 fd 6d fd 0b 3f fd 50 2e fd fd 3c 05 fd	/~QdxMnm 0\Q-gG9,%u;6gx&>3*)*tI'[do(:eXpOx[<HM.Ra*rD8z42s^){ Tk0v{re6?PY ?}=s;A4m?P.<	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\Setup.xml	2319	10	24 00 03 07 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\Setup.xml	0	1795	12 0a fd fd fd fd 2d fd fd fd 7d fd 3d fd fd 52 9e fd fd 25 39 fd fd 54 fd fd 7a 58 fd 22 14 05 fd 17 5d 0d fd fd 0f 27 34 64 27 c1 7e 7c fd 03 fd fd 9f fd fd fd 4e df 04 fd fd fd 46 fd fd 40 4f fd fd fd 13 fd 04 4e fd fd 59 fd 74 33 1c 4a fd 02 3b 6e fd fd 5d fd 45 fd 58 68 fd fd 52 7a 62 fd 09 4e 65 fd 1f 0f fd 5a fd fd fd 4e fd 29 fd 5b 66 00 39 0e 68 38 27 7f 01 79 34 fd 24 25 fd fd 7c 1f fd 30 4a 7f fd 5d fd 68 fd fd 13 1a 18 70 1f fd fd fd fd 38 fd fd fd 6c fd fd fd fd 52 7d fd fd fd fd fd fd 1c fd 38 64 35 fd 00 1b 21 68 fd fd 44 55 07 19 fd 58 fd fd 63 f0 0f fd 1b fd 12 fd 73 fd 14 fd fd fd fd 03 47 22 10 fd fd 0d 06 fd fd 48 fd 78 6b fd 7f 19 fd fd fd fd 12 fd 2d 5d fd 2a fd fd fd fd 1b fd 19 41 4b fd fd 76	- }=R%9TzX"J]4d'~[NF@O NYt3J;n]EXhRzbNeZN) [f9h8'y4\$%(0J]hp8IR} 8d5!hDUXcsG"Hxk]*AKv	success or wait	1	F2C055	WriteFile
C:\Program Files\MSBuild\Microsoft\IR3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ v _ _ _ _ v _ / / _ _ _ v . ` _ _ \ _ _ _ \ _ _ v _ / \ _ / \ _ / \ _ _ \ _ / \ _ _ _ \ _ _ / By now it's probably painfully apparent that your environ- ment has been infected with r	success or wait	1	F358DF	WriteFile
C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutkLR.cab	4009185	524	46 fd fd fd 72 56 19 19 42 fd dd 97 fd 1e 41 fd fd fd fd fd fd fd 50 fd 70 fd 0d 24 77 fd 02 46 52 fd 3f 3a 18 fd fd fd 26 fd fd 3d 6b 4b 00 21 75 68 04 fd 34 05 51 fd 7f fd 49 fd 68 69 30 52 fd fd 4b 11 fd 2c fd 1a 34 0b fd 78 fd 77 fd 3f fd fd fd 7b fd fd fd 14 fd 7d 2c 55 fd 5e fd 45 74 5b fd 32 fd fd 7c 27 11 11 fd fd 5b 10 1a fd fd 15 4e fd fd fd 2a 14 0b 06 fd 6f 4b fd 10 15 3c fd 76 cc fd ac 25 fd fd fd fd 52 8e 66 7f 3b 40 3c 0f 4f 57 fd 67 fd fd 25 3d 43 fd fd fd fd 12 38 fd fd 14 fd 29 64 70 fd 3d 14 6c 4b fd 02 44 fd fd 3c fd fd 6c 17 fd 75 5b 6a fd fd 03 40 fd 77 1a fd 59 3f fd 52 2c 38 59 7c fd fd 0e 7a 3f 29 fd fd 92 66 78 fd 14 fd fd 5a 6e 5c 18 fd 6e 0c fd 55 4b 77 45 fd fd fd fd fd 71 fd fd 41	FrVBAPp\$wFR?&=kK!uh 4Q!hi0RK,4xw? {},U^Et[2]![N*oK<v%R;@ <OWg% =C8)dp=IKD<lu[j@wY? R,8Y z?)fxZn\!nUKwEqA	success or wait	1	F2CBF8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlkLR.cab	4009709	10	26 00 fd 2c 3d 00 00 00 00 00 00	&,=	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlkLR.cab	0	1048576	2d 20 1d 1e 1a 26 fd fd 72 5c 09 fd fd 4f fd 71 6e 6e fd 3f 0f fd 30 fd 51 fd 47 fd 40 28 8e 4e fd 61 0c fd 15 fd 7b 0c 1b 43 17 fd fd 42 03 76 fd 57 2e 31 18 19 2c fd fd fd fd 1b 4c 6b fd 6a fd 02 fd 57 fd 80 fd 1b 1a 39 fd 65 02 64 fd fd 69 fd 0e 16 26 fd 38 fd fd 4a fd 09 0b fd fd 1b fd 9a fd 1c fd 67 06 fd 47 39 11 40 fd fd 3d 5f 3f 0f fd 3e 33 69 2a 49 70 66 02 fd 1f fd 04 fd 6f fd 19 fd fd 22 fd 06 42 46 fd 7b 5f 54 7b 03 fd fd 21 6a fd 67 fd fd 46 fd 60 fd 35 fd fd fd 3b fd fd 50 fd fd 1e 5c 8b 4d fd fd 5c 42 fd 24 fd fd fd 86 0a 4f fd 12 fd 45 fd 33 5e 31 11 3d 49 12 79 70 63 12 67 6e 6d 2e 7e 15 4a fd 6a fd 08 53 6c 71 5e 52 6d fd 06 fd fd fd 5b 10 54 fd fd 1a 32 fd 07 1e 67 fd 70 1f	- &r\Oqnn0QG@(Na{CvW. 1,LkjW9edi&8JgG9@=_? >3i*lpfo"BF[_T{!jgF '5;P\B\$O3^1lypcnm.~Jj Slq^Rm[T2gp	success or wait	1	F2C055	WriteFile
C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlookMUI.xml	2837	524	fd 5d 5f 63 27 fd fd 2f 47 31 fd 2c fd fd 45 41 3c 78 fd fd 67 53 fd fd fd fd 62 23 fd 13 fd fd fd fd 6a 06 fd 76 fd 51 71 fd fd 31 45 fd 39 fd fd fd 48 fd fd 37 1b 50 7f fd fd 6b fd fd fd fd fd 3f 35 0e fd fd fd 05 fd fd 03 1d 21 fd 04 39 64 26 d8 31 fd fd 01 fd fd fd fd 16 fd 53 fd 0d fd 28 fd 36 d4 fd 55 36 fd fd 09 fd fd 41 32 0c ad fd 34 fd fd 30 fd fd 6e 52 fd 4a fd fd 02 17 53 70 fd 02 51 fd 4d fd 26 fd 0f fd 36 fd fd 04 49 4f 5c fd 16 fd 42 fd 6c fd fd fd fd 37 fd 82 fd 5f fd 5c 58 86 fd fd 0c fd fd fd fd 32 fd fd 65 7e 1f 03 fd 0e 4a fd fd fd 68 32 06 4f 57 fd 1d fd 2c 49 44 fd 44 fd 14 fd 37 48 fd 39 fd fd fd 7d 3f fd 7d fd fd fd 63 4c 51 07 a6 fd fd fd 4e 7c fd 52 fd 69 3f fd fd fd fd 3f fd 79 14 fd fd	[_c'/G1,EA<xs#jvQq1E 9H7k?5!9d &1S(6U6240nRJSpQM& 6IO\BI7_\X2e ~Jh2OW,IDD7H9)?}cLQN Ri??y	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlookMUI.xml	3361	10	24 00 15 0b 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlookMUI.xml	0	2837	02 fd 22 49 fd fd 2c 3e 70 53 3c 6a fd fd fd 47 fd 0d fd c3 3d 5c 31 57 fd fd 26 fd 57 fd 73 7b fd fd fd 6d fd 3d 5d 42 43 fd 0b fd 55 05 61 fd 5c fd 4f fd fd fd 5b 30 20 56 fd 3e 4a fd 11 fd fd fd 22 fd fd 54 fd 11 fd 67 16 fd 0d fd fd fd 0e 0e 02 09 fd 01 fd 7e 62 fd fd 1c fd 4e 7a fd fd fd fd 77 20 fd fd 13 5d 07 fd 2f fd 25 fd fd 64 02 fd fd 56 52 fd 29 6c 72 fd 7c 2c 1c fd 02 5a fd fd fd 09 40 49 59 fd 29 fd 10 fd fd 1a 06 fd fd 6f 58 2a 2b fd fd fd 15 58 74 22 fd 23 4b fd 5c fd fd fd fd 4e 50 fd fd 00 16 0b fd fd 7f 7d 2d fd 20 fd 63 91 01 3b fd 7f 41 fd 4c fd fd fd fd 4c fd 1f 7c 3a 9d 14 fd 22 fd 3d fd 71 01 4d 34 fd fd fd 07 26 08 fd fd fd 0c fd 38 fd 7f 74 fd 34 fd 00 7f 3d 73 2e fd fd 0d 41 18 4b 08 fd 39 01	"I,>pS<jG=\\1W&Ws{m=] BCUa\O[0 V>J"\"Tg~bNzw]/%dVVR) r ,Z@IYoX*+ Xt\"#K\NP}- c;ALL :=qM&8t4=s.AK9	success or wait	1	F2C055	WriteFile
C:\Program Files\Reference Assemblies\Microsoft\RSADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 5f 2f 5c 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ v _ _ _ _ v _ / / _ _ _ v . ' _ _ \ _ _ _ \ \ _ / \ _ / \ _ / \ _ _ \ _ _ \ _ _ \ _ _ / By now it's probably painfully apparent that your environ- ment has been infected with r	success or wait	1	F358DF	WriteFile
C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\Setup.xml	3870	524	2e 76 fd fd fd 78 70 fd 24 06 fd fd 1b fd fd 76 fd 2d 39 fd fd fd fd fd 06 fd fd 11 93 4b fd fd fd 7f 45 2e 33 fd 78 fd 36 fd 64 61 fd 29 bf 30 6a 3f 64 fd 25 fd fd fd fd 0c fd 00 fd 35 fd 62 fd fd fd 41 3e 61 fd 5f fd 71 fd 6e 6d 6d fd 60 fd fd 2a fd 10 49 fd fd fd fd fd 3e 5d fd 7f fd fd 71 1d 1b 22 03 fd fd 47 41 49 70 fd 3b 39 fd 3c 34 fd fd fd 17 15 4c fd 2e 07 fd 4c fd fd 50 fd 66 fd fd fd 0e fd fd 63 65 40 ca fd 02 fd 45 37 35 25 60 56 6b 08 fd 0b 2d 6e fd fd fd 08 21 fd 4c fd fd 3b fd 3d fd fd fd fd 6b 17 40 28 fd 0b fd 62 46 fd 06 52 16 fd fd fd 7e a8 48 19 fd fd fd 61 fd 42 55 52 fd fd fd 50 3a 53 66 4c 14 33 7d fd 1a fd 0b 59 12 20 fd 76 fd fd ed 79 0a 34 62 33 65 38 0d fd fd 7f 4a 6b fd 60 fd 0f 5f fd	.vxp\$-9KE.3x6da)0j? d%5bA>a_qnm m`*!>]q"GAlp;9<4L.LPfce @E75%"Vk- n!;=k@(bFR~HaBURP:Sf L3}Y vy4b3e8Jk"_	success or wait	1	F2CBF8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\Setup.xml	2772	524	68 fd fd 55 39 2f fd 7c 20 fd 4d 1f 77 1c fd fd fd 77 fd fd 45 2a 34 63 07 fd 7a 2d 7c fd 51 fd 2e fd 70 13 fd fd 10 6b 2d 6c fd 0b 2d 7c 28 fd 60 fd fd fd 65 fd 70 fd 65 fd fd 57 28 fd 5a 59 fd 34 12 fd 7f fd fd fd fd 6e 6d 3b fd 37 47 fd 6d fd 18 24 48 1f fd 78 fd fd fd 7f 7a 47 4c 41 fd 28 fd 12 4f 1f 5e 44 44 63 fd 39 fd fd 76 7c fd fd 71 fd 10 21 87 5c 7b fd 44 fd fd fd fd 58 fd fd 4b 60 fd 78 fd 07 5b 7f 2b 77 fd 45 00 7d 7d 59 2e fd fd fd 75 1e 49 29 21 51 fd fd 05 2a 2a fd 66 fd fd fd 43 75 fd fd 4a 52 08 fd 48 28 04 01 7a 4b fd 26 fd 7f fd 61 62 59 fd 66 fd 32 78 04 48 fd fd 13 fd 55 fd fd 5d fd 58 77 70 fd 56 56 fd fd fd fd fd fd 7e fd 20 5f fd fd fd fd 1a 6b 46 4a 79 fd 2b 40 fd 06 1b fd fd fd 69 72 fd	hU9/ Mww*4- Q.pk-l- (`epeW(ZY 4nm7Gm\$HxzGLA(O^Dc 9v q! {DXK`x [+wE]Y.ul)!Q*fCuJRH(zK &abYf2xHU]XpVV~ _kFJy+@ir	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\Setup.xml	3296	10	24 00 fd 0a 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\Setup.xml	0	2772	fd 72 fd fd fd fd fd 2d 12 5e fd 7d 08 52 2f 0b 50 fd 21 fd 03 23 4e fd fd fd fd fd 4f 35 29 51 fd 11 fd 57 fd fd 00 6b fd fd 7d fd 34 3a fd 29 fd fd 48 60 11 fd fd 70 fd fd 72 fd 17 18 fd 43 fd 59 5a 0b 3d 62 fd fd 7f 5c 10 fd fd 1f 73 7e fd fd 61 53 fd 16 fd 70 fd fd fd 14 20 76 12 6f 01 fd fd 1c fd 6f 73 0f 41 fd fd 0c 5a fd fd 61 fd 4d 04 a9 29 fd 44 25 2e 56 73 01 53 2b 7c 2e 00 43 15 fd 4b fd fd fd fd 77 4a 09 40 fd fd fd 01 fd 52 fd 7a 01 fd fd 24 07 fd fd 0c 1b fd 35 fd fd fd 36 24 32 fd 64 96 14 fd fd fd 27 fd 0f 5f 01 16 fd 16 4a fd 71 51 fd fd fd fd 7a 72 21 fd 2e 0e 27 5a 32 7d 0e 24 fd 64 13 22 fd fd fd 70 fd 1e fd fd 52 53 14 04 fd fd 0e 19 fd fd 0e c3 fd fd 86 fd 28 fd fd 5e fd 48 fd 28 fd 10 66 76 fd fd	r-)R/P!#NO5)QWk}4:)H`pr CZY=b!~aSp vosAZaM)D%.VsS+ .CK wJ@Rz5 6\$2d'_JqQzr!.Z2}\$d"pRS (^H(fv	success or wait	1	F2C055	WriteFile
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordLR.cab	10079733	524	5c fd fd 70 3c fd 78 44 fd 16 47 53 18 fd 5e 6a fd 1c 4b fd fd fd fd 7c fd fd cb 16 57 72 fd fd fd fd fd 25 fd 63 31 21 36 fd fd 5d fd fd fd 25 00 fd 35 77 fd 03 1f 39 fd fd 35 35 6c fd 61 2d fd fd fd 0f 67 3e fd 7e fd 16 7c 09 59 63 36 0e 39 fd 25 fd fd 6a fd 21 fd 74 fd fd 63 1a 68 5f 08 76 fd 11 fd 1b 6a fd 5a 48 1d 0f 1f 54 00 7c fd 1e 47 77 70 fd 38 0f fd fd 14 22 5d fd 65 4e fd 2b 3f fd 57 30 fd fd 3c 23 08 6f 25 fd 22 05 fd fd fd 5a 42 7d 77 fd fd fd 1b 11 fd fd 3d 72 fd fd fd fd fd 49 fd 55 fd 33 fd 33 fd fd fd 13 0e 05 e6 27 17 53 fd 78 44 76 75 fd 19 fd fd fd 07 26 27 2b 6d 11 fd 5c fd 29 fd 04 fd 52 08 1c fd 16 76 34 fd fd fd fd 76 10 1c 4a fd fd 52 6d fd 0e 16 39 2f fd fd 05 fd 53 fd fd 2e 31 fd 52	\p<xDGS^jK W%c 6]5w 955la-g>~ Yc69%j tch_vjZHT Gwp8 "jeN+?W0< #o%"ZBw=rIU33'SxDvu& +m\)Rv4vJRM9/S.1R	success or wait	1	F2CBF8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordLR.cab	10080257	10	25 32 fd 59 00 00 00 00 00	%2	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordLR.cab	0	1007970	49 16 fd 21 fd 46 fd 6b fd fd 39 0d 3b dd fd fd fd fd fd 7d 22 fd fd fd fd fd 56 69 fd 2d 66 3a 52 fd 86 5a 4f b6 fd fd 7a 3f 61 fd 29 20 0a fd 2d 10 2f fd 6c 1c fd fd 43 1b 6b fd 36 6a fd fd 1d 43 fd 09 41 fd 34 fd fd 26 fd 43 07 fd fd 7e fd 51 1a 35 88 fd fd 2b fd 0b 4e fd 44 fd 1e 16 2f fc fd fd fd 40 fd 07 6e 5b cc fd fd 60 fd 3b fd 00 fd fd fd 21 fd 5a fd 73 fd fd 22 1c fd fd fd fd fd 43 fd 67 44 fd 29 23 fd 7f 41 4d 57 42 fd fd 1d fd fd 2b fd fd 3b fd 6d 54 fd fd 1f 10 76 03 fd 65 7c 23 5f 4a 46 fd 6e fd c4 27 fd 4f fd fd e0 0d fd fd 2b fd 1f 20 35 cd fd fd fd fd 06 fd 34 4a fd 5a 23 fd 29 72 fd 53 0a fd 15 fd 75 7c fd 60 27 fd fd fd fd 73 fd fd 29 40 09 fd fd 31 fd fd 35 fd 02 50 3c 5b 39 56 fd	!!Fk9;}"V-f:RZOz?a) - /lCk6jCA4 &C-Q5+ND@n[";!Zs"Cg D)#AMWB+;mT ve /_JFn'O+ 54JZ#)rSul's)@15P<[9V	success or wait	5	F2C055	WriteFile
C:\Program Files\UNP\UpdateNotificationMgr\IR3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 5f 5f 5f 5f 20 5f 5f 5f 5f 5f 5f 5f 5f 5f 5f 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ v _ _ _ _ v / / / _ _ _ v . ` _ _ \ _ _ \ \ v v / / \ / \ _ / \ _ \ _ ^ _ ^ _ ^ _ / By now it's probably painfully apparent that your environment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordMUI.xml	2108	524	3d fd 79 fd 6b fd fd fd 1c fd fd 5f 07 00 fd 60 e5 fd 58 fd fd fd 70 fd 59 46 78 fd fc fd fd fd fd 3d 29 23 fd 4a 32 30 fd 3c fd 2d fd 4e 66 49 fd 48 15 fd 23 fd fd fd fd 69 38 fd fd 1d fd fd 40 e3 fd fd 59 fd 26 60 08 64 1a fd 6d 22 fd 58 fd fd fd 40 fd 2a fd 1e fd fd 5b 4d 3b 26 fd 71 50 5b 76 fd fd fd fd 53 61 fd fd fd 37 fd 63 fd 07 4c 3d 3d 3c 01 fd 27 fd 21 fd 75 fd 64 13 3e fd 53 14 e0 23 67 fd 7d fd 5a fd f6 28 fd 2f 1e fd 45 fd 51 10 16 fd fd 29 01 fd 14 29 fd 6c fd 69 0c fd 75 86 fd 67 20 fd 4a fd fd fd fd 2d 8b 46 fd fd fd fd 14 fd fd 46 34 fd fd 77 fd fd fd 0a 57 fd fd fd 1e 0b 02 2d fd 71 40 1c 2f fd 32 62 36 10 4a 4b fd fd 1e 1e 67 fd fd fd fd fd 5a fd 5d 18 fd fd fd 54 6e 44 fd 28 3c fd fd 1a fd 0d 63 fd 19	=yk_`XpYFx=)#J20<- NfIH#i8@Y&`dm"X@* [M;&qP[vSa7cL== <'!ud>S#g}Z/(EQ))liug J- FF4wW-q@/2b6JKZ] TnD(<c	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordMUI.xml	2632	10	24 00 3c 08 00 00 00 00 00 00	\$<	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordMUI.xml	0	2108	00 32 fd fd 61 fd 5e fd 2a fd fd 35 fd fd fd fd 29 1a fd 57 45 fd fd 3a 02 fd 1b fd 0f 0a 3a fd fd 56 7a 50 fd 42 fd fd 51 fd 13 fd fd 18 fd 25 fd 7f fd 0f 6f 42 fd 3d 49 2a fd 08 fd fd fd 74 fd 09 fd 20 7f 5e 1c 47 fd fd 06 fd 6b fd fd fd fd 5f fd fd fd fd 64 0e fd fd 7c 32 fd 69 fd 7e 3a fd fd fd fd 01 27 fd 75 fd fd 0a fd 3d fd 40 5b fd 3b 44 1e fd 65 06 5c 53 fd 7a fd fd 6d 70 fd 37 3a 61 4b fd fd 71 2f fd fd 00 45 77 d8 5a fd fd fd fd fd fd 7c fd fd fd 06 61 0f 54 fd fd fd fd 56 25 fd 15 68 2a 30 52 67 40 fd fd 70 5a fd 71 6b 64 16 fd 73 fd fd fd 27 1d fd 55 fd fd fd fd 6c fd fd 5a fd 73 1c 3c fd 42 26 65 fd 48 13 fd 5d fd 66 47 37 fd 0a fd 5e fd fd 53 28 3f 46 fd 2e fd fd fd 30 fd 31 fd fd fd 0d 64 27 2b fd 51 57 fd fd	2a^*5)WE:VzPBQ%B=!*t ^Gk_d 2i~ :u=@[:De\Szmp7:aKq/E wZ[aTV%*0 Rg@pZqkds'UIZs<B&eHf G7^S(?F.01d'+QW	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3 \Aut2Exe\I3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ ____ _ _ _ _ \\ _ _ V _ _ _ _ \ / / _ _ _ _ \ . ' _ _ \ _ _ _ \ \ _ _ / / \ _ \ \ _ / \ _ _ \ _ _ \ _ _ \ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\MSOCache\All Users\{90160000- 002C-0409-0000-0000000FF1CE}- C\Proofing.xml	1548	10	24 00 00 04 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000- 002C-0409-0000-0000000FF1CE}- C\Proofing.xml	0	1024	fd 59 fd fd fd fd 17 75 38 fd 4f fd fd 3b 17 6c 2b 74 fd 48 fd fd fd 40 6b 7a fd 00 4d fd fd 54 fd 44 fd 7d 6f fd fd fd 59 fd 36 fd fd 2b fd fd fd fd 2c 51 fd 3f fd fd fd 01 ca 5a 6f fd fd fd fd 36 01 3a fd 7f fd 79 fd 58 fd 1c fd 1e 0d 14 fd 12 2d 26 fd 0a fd 1e fd fd 32 7e 56 37 3a fd fd 27 fd 19 fd 07 43 fd 00 4e fd fd 64 fd fd 42 14 67 2b fd fd 10 32 70 fd 79 06 2e 7e 37 19 fd 1f 1d fd 12 fd fd fd 35 fd fd 1b fd fd 04 51 fd 44 68 07 7b 00 76 7d 12 3c 04 15 5d fd 5c 59 fd fd fd 35 61 35 23 7f 0c fd fd fd fd 26 c9 19 74 47 44 fd 43 fd 2a 38 5b 5b 7c fd 64 3e 20 7d fd 10 44 fd a2 fd 6c 63 15 fd fd 30 fd fd 04 fd 2c fd 49 fd 40 fd fd 73 45 fd 22 6a 06 fd 1a 2d fd 0b 70 fd fd 5b fd 68 fd df 71 78 55 77 0d fd fd fd fd 1f fd fd fd fd	Yu8O;+tH@zMTD}oY6+, Q?Zo6:yX-& 2~V7:'CNdBg+2py.~75Q Dh{v}<)\Y5 a#&tGDC*8[[> >Dlc0,l@sE"j-p[hqxUw	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Setup.xml	6067	524	3a fd fd fd 02 fd bb fd 04 fd 71 21 fd 19 61 03 28 fd 18 05 fd de 1a fd 3f fd 13 fd fd 34 5f 7e fd 43 fd fd 71 fd 58 61 fd fd 7f fd 4a fd fd ca 16 fd 16 16 fd 53 7a fd 79 4f 24 fd fd 6b fd fd 04 fd 3c fd 15 fd 42 fd fd 50 03 fd fd fd fd 1b 18 fd 50 57 fd fd 4f 58 fd 24 fd 3c 20 27 65 76 fd fd 66 fd fd fd 11 fd 12 fd fd 72 fd fd 77 02 21 fd 3a 12 fd fd fd 50 fd 0c 68 67 01 fd 44 fd 59 43 00 3c 8c fd 38 66 3b fd fd fd 21 78 29 48 fd 52 fd fd fd fd 78 fd 63 49 3d fd fd fd fd 17 fd fd fd 2f 5a 70 fd 1a 1a fd 45 fd 1d d0 39 50 fd 71 fd 42 45 03 36 d7 1d fd fd 44 09 4e fd 28 5f fd 1b 0e fd fd 06 07 1e 3d fd fd 3d fd 0c fd 5e fd d8 fd 5a 50 74 11 fd fd 33 fd 44 fd fd 06 31 36 fd 77 fd 79 2b 38 29	:qla(? 4_~CqXaJSzyO\$k<BPP WOX\$< 'evfrwt!:PhgDYC<8f;!x)HR xcl=/Zp E9PBE6DN(_==^ZP1316 wy+8	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Setup.xml	6591	10	24 00 fd 17 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Setup.xml	0	6067	fd 71 fd 79 6d 7a fd 11 fd fd fd 56 7a 6d 32 fd fd fd 45 fd 54 fd fd 14 17 fd fd fd e0 4e 42 fd fd fd fd fd 58 9d fd 6f 20 fd 4f fd fd 16 57 05 fd 54 fd fd 25 0f fd fd fd 5e fd af 67 53 fd 60 7a fd fd fd 7e 67 fd 3c fd fd 0b fd fd fd 52 28 74 fd 18 fd 51 0e fd fd fd 00 fd 51 ad fd 57 7a 4c 32 fd fd 5e 2e fd fd fd fd 30 fd 6c fd 04 6e fd bb 03 fd fd fd 49 fd 6b 28 36 fd 2d fd 12 fd fd fd d6 0d 40 4e 76 fd fd 1f fd 68 fd 60 fd fd fd 56 0a fd fd 5c 0b fd fd 13 50 52 0b 51 fd 78 fd fd fd fd fd 6b fd 7e 08 1f fd 62 06 34 fd fd fd 27 fd fd fd 73 68 15 fd 28 66 fd 74 fd 36 55 13 72 fd 3c fd fd 79 24 4c fd 46 fd 2d 7c fd fd fd 3b 5c fd fd fd 5c fd fd fd 49 23 fd 08 28 77 fd 22 55 20 56 fd 4c fd fd 4c 2b 00 52 1a	qymzVzm2ETNBXo OWT%^gS'z~g<R(t QQWzL2^o0lnlk(6- @Nvh`V\PRQxk~ b4'sh(ft6Ur<y\$LF- ;\\#("U VLL+R	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Autolt3 \AutoltX\IR3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ ____ _ ____ \ ____ V ____ ____ \ _/_/_ ____ ____\ : ` ____\ ____ \ \ ____ /_/_ _/_/_ _/_/_/_/_/_/_/_/_/By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0044-0409-0000-00000000FF1CE}-C\InflR.cab	3911650	524	38 55 40 fd 32 fd fd fd 67 31 59 56 7d 1b fd fd 00 31 fd fd fd fd fd fd 4e fd fd 5f fd 23 fd 7a 02 fd fd fd 52 fd 45 5b 14 f4 14 fd fd 50 33 64 fd fd 50 4b fd 57 34 2f 72 fd fd 53 fd 1c 60 fd 5b fd 46 fd 0b fd fd fe fd 4d fd fd fd fd 09 fd fd 2f 53 2e 28 78 43 6c 1a 3d fd fd 37 fd 9b fd 10 59 2c 33 7e 1d fd 1f fd 61 fd 12 d2 fd fd 5e 24 fd 6f 44 1e fd 5a fd fd 65 fd fd 23 56 5e 0c fd fd fd 02 4b fd fd 5c 31 7f fd fd fd 79 fd fd 62 0e 10 10 13 fd fd 23 2e 0b 61 fd 66 fd 69 fd fd fd fd 76 0f fd 1c fd fd 00 fd fd fd 13 30 12 77 6e fd 63 fd 11 40 65 78 2d 0b 50 6c fd fd 1b fd fd 5c fd 24 fd 7a 41 fd fd 6d fd 79 fd 65 5c fd 73 62 08 44 01 46 fd 66 fd 03 4d fd 62 76 fd 70 fd 40 6e ec fd fd 1c fd 06 fd fd fd fd 28	8U@2g1YV}N_#zRE[P3d PKW4/r`[FM/S. (xCl=7Y,3~a^\$oDZe#V^K \1yb#.afivOwnc@ex- l\$zAmye\sbDFfMbvp@ n(	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-0044-0409-0000-00000000FF1CE}-C\InflR.cab	3912174	10	26 00 fd 3b 00 00 00 00 00	&;	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-0044-0409-0000-00000000FF1CE}-C\InflR.cab	0	1048576	65 22 fd fd 22 7f 54 fd 47 fd fd fd 50 fd fd 2d 20 30 55 fd fd 77 fd 70 60 fd 48 5e 7b fd 13 27 fd 26 68 fd 1d fd 51 fd 64 5c 6c 00 fd 7d f1 fd fd fd fd fd 60 32 40 77 fd fd fd fd 47 ff 1a fd 44 2e fd fd 16 fd 29 fd 10 2e 55 fd 24 fd fd 19 fd 2b fd 19 65 fd 01 fd 70 fd 28 34 fd 06 54 fd 38 23 01 fd fd 1d fd fd 02 1f 3a fd 31 fd fd 5d 33 fd 68 fd fd fd fd fd fd 4c 2f fd fd fd 3a 18 14 6b 7e 09 10 3e 00 fd 42 15 7b 7e 5f 13 5f 4c 66 fd fd 1e 0d 57 36 fd fd 0a 29 30 fd 27 06 15 0e 17 fd 55 23 1b 6c 50 fd 79 fd 30 fd fd 40 74 fd 23 05 25 0a fd 56 0d fd fd 72 fd fd 15 fd fd 32 fd 5f 39 fd fd 42 fd 53 24 fd 70 fd fd fd 0d fd 44 2a 66 3a 01 fd 70 11 fd fd 13 14 fd fd fd 4f e8 fd 06 6d fd 68 fd fd fd 74 4d 37 37 4a 02 51 11 fd fd fd fd 5f fd	e""TGP- 0Up`H^{'&hQdlj}`2@wGD.).\$+ep(4T8#:1]3hL/:k~>B {~_lFW6)0`U#lPy0@t#%Vr2_9BS \$pD*f:pOmhtM77JQ_	success or wait	1	F2C055	WriteFile
C:\MSOCache\All Users\{90160000-0044-0409-0000-00000000FF1CE}-C\InfoPathMUI.xml	1230	524	fd 5a 12 fd fd 70 fd 77 fd 5a fd 1f 3c fd 4e 78 28 02 17 57 30 fd 6a 5c 0e fd 0c fd 72 1d 55 4c 27 79 fd 40 fd fd 35 77 21 5b fd 53 fd fd fd 2b c5 42 fd 68 46 4f fd fd 0f 37 69 15 fd 61 7e 33 fd fd fd fd 3d fd fd 67 0f fd fd fd fd 4d fd 37 fd 75 31 fd 30 4d fd 73 7d fd fd 35 fd 26 fd fd 70 fd fd fd fd 3a 07 7c 27 41 18 5f fd ff fd 6f 50 11 34 fd fd 57 fd 0f 19 49 65 fd fd 6e 1a 33 fd 34 fd 6d 0c fd fd 47 6b fd 12 4e 13 6b 70 fd 4f 74 65 fd 7b 68 67 fd fd fd 01 fd 70 fd 46 3e fd 17 74 fd 6b 34 7c 59 fd 41 fd 41 6b fd 25 fd 5d fd fd 46 fd 49 fd fd 47 fd 49 5d 7e 59 fd fd 1f fd 46 4a fd 6c fd fd fd 78 4d 64 0f 23 fd fd fd fd fd 06 29 54 fd 71 58 fd fd fd fd fd b6 32 fd fd 16 2d 7e 00 05 2f fd fd fd 5c 87 31	ZpwZNx(W0j)rL'y@5w! [S+BhFO7ia~ 3=gM7u10Ms)5&p;!`A_o4 Wle34mGkN kpOte{hgpF>tk4 YAAk%] FIGI]~YFJlxMd)qX2~^/1	success or wait	1	F2CBF8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0044-0409-0000-00000000FF1CE}-C\Setup.xml	1795	524	fd 7b 6d fd fd fd 7e 77 58 fd 76 fd fd 49 fd fd fd fd 17 fd 42 fd fd 39 3f 1a fd fd 22 74 fd 0a 63 fd fd fd 3e 21 35 33 fd fd 0f fd fd 03 2a fd 64 fd fd 33 5e fd 40 fd 70 26 06 0c fd 7c 31 61 fd fd 27 34 fd 71 2a fd 5e 59 19 45 fd 19 55 fd 1e 45 fd 0e fd 54 fd fd fd 1c fd be 50 59 fd fd 5f fd 44 0d fd 58 fd fd 63 2c 93 da 3c fd fd fd 39 fd 12 fd fd 66 6c 14 38 08 fd fd 5b fd 61 fd 69 46 38 59 1c 2e 54 fd fd 33 08 3b 0c 6f 23 fd fd a6 26 fd 0c fd 12 fd 3e 69 2b fd fd 0d 5f 57 25 fd 45 5b 58 07 3a fd 7e 79 4f 0e 60 fd fd 74 fd fd 5f 75 14 7e 61 73 fd 09 fd 23 22 fd fd 6d 51 44 fd 31 30 54 3a fd fd fd fd 64 5e 23 0e fd fd 78 fd 03 70 fd 42 43 1d 11 fd 41 fd fd fd fd fd fd 65 fd 4c fd fb fd 32 6a fd 6a 07 77 fd 41	{m~wXvB9?"tc53*d3^@p [1a'4q*^YE UETPY_DXc<9fl8[aiF8Y. T3;o#&>i+ _W%E[X:~yO`_t_u~as#"m QD10T:d^#x pBCAeL2jjwA	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-0044-0409-0000-00000000FF1CE}-C\Setup.xml	2319	10	24 00 03 07 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-0044-0409-0000-00000000FF1CE}-C\Setup.xml	0	1795	fd 0f 58 fd 40 fd 76 fd 4a 46 2e 72 fd fd 5f 2f 09 7d fd fd 7a fd fd 7d 1a 07 fd fd 02 fd fd fd fd 5f fd fd 30 fd 4f fd fd 03 fd fd 29 46 fd 1a fd 18 1b fd fd 54 50 30 fd 5c 5e 31 fd 17 fd 2a fd 6d fd fd 6a fd fd 66 5c 67 fd fd fd 63 fd 6a fd 43 fd fd 1b fd 72 fd fd 03 fd fd 58 01 5e 06 25 fd fd fd fd 44 fd 66 78 1c fd fd fd fd 32 1f 07 0b 0f fd 48 fd fd fd fd fd f8 5a 0b 69 5a 78 01 fd fd 57 32 fd 44 fd 00 46 62 fd fd 58 fd 3b fd 25 3d 17 fd 69 16 58 fd fd fd 06 5e 38 43 4e 2e fd fd fd fd fd fd 5b 04 fd fd 7a 4f fd 63 2f 4f 60 29 fd 49 fd fd 71 4d 06 06 2e fd 59 63 2c fd 50 fd 7f fd 2c fd 9c 34 69 fd 4f 11 fd 19 66 fd 61 3e fd 56 0d 70 09 7e 0e fd fd 27 53 7a 60 fd 2a 00 54 63 1a fd 37 3b 58 fd 71 29 fd 4f 12 fd 91 fd 11	X@vJF.r_/z}_00)FTP0V^ 1*!f!gcj CrX^%Dfx2HZiZxW2DFb X;%=iX^8CN. [zOc/O`)!qM.Yc,P,4iOfa> Vp~'Sz*Tc7;Xq)O	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3 \Extras\I3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ v _ _ _ _ \ / / _ _ _ _ . ' _ _ \ _ _ \ \ / / \ \ \ _ / \ _ _ \ _ _ \ _ _ \ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\MSOCache\All Users\{90160000- 0090-0409-0000-00000000FF1CE}- C\DCFMUI.cab	641590	524	fd 34 5c 30 0a d0 2b fd 52 00 d9 fd 57 50 16 fd 1d 61 1b fd fd fd 35 55 6f 55 34 fd fd 7c 2d 6a 23 52 2e 20 fd 77 fd 66 fd fd fd 46 17 fd fd fd fd fd 1f 1a b6 09 18 fd fd 7b 7a fd 13 fd 25 6e fd fd 75 fd 45 08 fd 42 39 fd fd fd 29 4f fd 66 fd fd 0f fd 68 fd 3a 79 31 7b fd 1f fd 4c 79 fd 2f 7b 14 fd fd 2f 6b 27 fd 31 3b 72 2e 5d 17 fd 3f 28 fd 2c 32 fd fd 28 54 fd 1b 0a fd 2e 58 3a fd 08 2c fd 0c fd 3c 25 fd fd 23 fd 2e 20 33 09 fd 0f fd 7a 4f fd 02 15 fd fd 7b 06 fd 08 fd 0e fd 66 fd 3b 16 75 fd 57 3d fd fd 4e fd 0d fd 46 fd fd 13 17 03 fd fd fd 08 b3 fd 39 59 fd 0c 37 fd fd 34 fd fd 48 1c fd fd 1e 11 6d 1e 57 fd fd fd 7c fd fd 1f fd fd fd fd fd 01 fd 37 5e fd 08 20 2a 64 6e 3c fd 98 42 fd 0b fd 4f 32 71 21	4!0+RPa5UoU4 -j#R. wfF{z%nUEB9)Ofh:y1{Ly//k'1;r.}?(,2(T., <%#. 3zO{f;uW=NF9Y74HmW 7^ *d<BO2q!	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000- 0090-0409-0000-00000000FF1CE}- C\DCFMUI.cab	642114	10	24 00 36 fd 09 00 00 00 00 00	\$6	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.cab	0	641590	fd 17 3b 2e 77 ea 0e fd fd 34 fd 3d 39 35 fd 46 fd 45 fd 7b 9a 47 5a 5c 58 fd 44 fd fd 0d 14 75 fd 71 72 10 fd fd c0 01 3a 23 fd fd fd 1b 36 0c 0f 04 fd 36 fd 18 01 57 6e fd 69 52 fd 74 4a fd fd 4b fd fd 63 3f 6e fd fd 5e 4e 25 36 fd 10 fd fd fd 67 14 4d 7c 73 fd fd 59 fd fd 41 fd 19 fd 0c fd fd 13 fd 79 fd fd fd 11 69 4f 51 09 25 fd 6d 4e 13 fd fd fd 32 3f 41 7a 62 fd 6c 56 fd 04 5f fd 28 61 fd fd 58 16 0c 0f 43 4a 99 19 5f fd 16 fd 07 0d fd 13 67 14 5f 75 fd 4d fd 54 44 3c 1a 3c fd 4b 72 fd 10 69 fd fd 28 34 fd 6b 4e fd fd 7b 37 56 2c 70 3e fd 5b 5a 62 6a 36 7b 3b fd fd 55 3d 15 fd fd 04 64 73 0d 76 76 5c fd fd 08 ee 39 09 5c fd fd fd 22 fd 3a 43 fd 4c fd fd fd 67 71 1f 31 fd 1f 5d 4d 2b fd fd 48 fd 03 23	;w4=95FE{GZ\XDuqr:#6 WniRtJKc? ^N6gM sYyiOQ% mN2? AzblV_(aXCJ_g _uMTD<<Kri(4k{7V,p> [Zbj6{;U=ds w\9\":CLgq1]M+H#	success or wait	1	F2C055	WriteFile
C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.xml	1215	524	fd fd fd 70 fd fd fd 06 61 05 fd fd fd 76 68 fd fd fd 24 fd 05 fd 70 fd 0e 25 fd 7e fd fd 5c 30 31 66 67 fd 11 fd fd 50 0a 19 2c 42 fd 18 63 fd fd 3b fd 73 fd 43 fd fd fd fd 13 66 6c fd fa 1a fd 3e fd 6a 63 77 6c 24 fd fd fd 2e 6a 24 0c 4e fd fd fd 0d 7c fd 68 14 1a 29 fd 45 fd fd 2b 2e 15 fd 7d 66 18 64 fd 5e 49 34 fd 33 fd fd fd 2f 54 fd fd 68 13 19 5c 17 57 77 47 5b 0e fd 26 fd fd fd fd fd fd 0f fd 48 1f a2 fd 4f 47 59 fd fd fd 77 43 fd 2d 2e 09 fd fd 1d fd 43 29 fd fd fd 22 2c fd c3 25 fd fd fd fd fd fd 06 6b 45 fd 18 2f 48 fd fd 4a 33 fd 41 fd 3b 7c ec 0f 09 21 61 fd fd fd fd 5a fd 59 fd fd fd 21 fd fd 7f fd fd 4e 05 40 20 fd fd fd fd 26 37 21 27 fd 09 fd 74 67 fd 45 5e 49 2a 6e 36 fd fd 76 25 fd fd	pavh\$P%-l01fgP,Bc;sCfl >jcw/\$.j \$(h)E+.}fd^l43/ThlWwG[H OGYwC-. C)",%k/HJ3A;!aZY!N@ &!tgE^!n6v%	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.xml	1739	10	24 00 fd 04 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.xml	0	1215	37 fd 40 32 fd 34 fd 43 fd 04 fd fd fd 10 fd 53 fd fd 20 99 fd fd e8 fd fd 57 7a 23 0f fd 4e fd 15 75 6a fd 11 fd 10 4f 12 fd 7e fd 17 2f fd fd fd 24 fd fd 09 56 4b fd 70 fd fd 65 fd 14 fd 79 58 fd 62 3f fd fd 60 fd fd 43 fd fd fd 28 fd 83 fd fd fd 0e 69 fd 5a 29 fd 3a 53 2d 44 fd fd 36 6e ab 70 fd fd 70 16 fd fd fd 26 fd fd fd 64 fd b1 54 fd 1c fd 3b 4a 73 02 43 fd fd 11 51 fd 38 54 fd fd fd fd 01 4b 16 09 fd 04 fd 12 33 3f fd fd 09 fd fd 6a fd 36 51 0f 02 fd fd fd 5e fd 06 fd 38 fd fd fd 00 5e fd b7 ac 58 fd 0d 4c fd 0b 37 15 04 08 21 51 fd 27 7e 44 fd 64 fd 56 3e 5a fd 4f fd fd 0b 0c 11 fd fd fd 50 7f fd fd 7b fd 2a 63 0b 43 fd fd 56 03 51 fd fd 5a 5e 5b fd fd 14 18 0d fd fd 1f 3f fd 20 fd 3d 5e 70	7@24CS Wz#NujO~/\$VKpeyXb? `C(iZ)S- D6npp&dT;JsCQ8TK3? j6Q^8^XL7 !Q'~DdV>ZOP{*cCVQZ[? =^p	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3 Icons\IR3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ V _ _ _ _ \ / / _ _ _ _ . ` _ _ \ _ _ \ \ / / \ \ _ / \ _ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\MSOCache\All Users\{90160000- 0090-0409-0000-0000000FF1CE}- C\Setup.xml	1808	524	fd 29 06 fd 19 6f 7a 04 0d fd fd fd 0a fd fd 62 06 e9 fd 60 02 30 fd fd 33 13 1e fd fd 66 fd fd fd 4a fd fd 08 fd 50 fd 3d fd fd fd 03 2b 63 fd 03 fd 02 45 74 fd fd 5b fd fd 40 fd 4b fd fd 06 1f 43 fd 6d 7b 0b fd 23 fd fd fd fd 2b fd fd 71 fd 6c 0b fd fd 72 6d 22 fd 3a fd fd 7e 6c 15 fd 20 fd fd 1c fd fd fd 18 60 45 0b fd 56 04 fd fd 62 fd fd 3f 48 42 fd fd 46 fd fd 40 2e 57 fd 1c 6e 00 3a fd 9a 24 53 2c 76 fd fd 68 0d 51 fd fd 4a 79 fd fd fd 89 fd 06 fd 9f 17 38 62 fd 61 fd 1e fd 15 57 fd 72 07 fd 43 5f 70 fd fd 1c 41 a8 4d 6d fd 64 fd 21 6d fd 4d fd fd 3c 7a fd fd fd 18 4d fd fd 12 11 54 fd 3c 54 fd 15 fd 56 0a fd fd fd 4c fd fd 30 fd 5e 12 29 35 70 3f 79 44 fd 0d 56 29 fd fd fd 2b 52 0e fd 5d 17 2c fd fd 1c	)ozb`03fJP=+cEt[KCm{#+ qlrm":-l `EVb? HBF@.Wn:\$S,vhJy8baW rC_pA Mmd!mM<zMT<TV0^)5p ?yDV)+R],	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000- 0090-0409-0000-0000000FF1CE}- C\Setup.xml	2332	10	24 00 10 07 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000- 0090-0409-0000-0000000FF1CE}- C\Setup.xml	0	1808	2a fd fd 24 fd fd 2f fd 5f fd fd 02 77 27 1c fd fd fd fd 5a 20 13 1d 70 fd fd fd 08 fd 70 2b 62 4e 0b fd 45 11 fd 17 51 fd 3b fd fd fd 2c fd 3c fd fd 66 9e 56 fd 01 6a fd fd 73 0d 01 fd 26 4c fd fd fd 36 5b 77 d3 1d ad fd fd 69 de fd 6d 23 fd 6f 0e fd fd 32 fd 20 fd 7a fd fd 57 fd fd fd 2e fd 6b fd 76 fd fd fd fd 0b fd fd 07 6c 7e 52 fd 2e 3d fd 6f fd 59 fd 0a 43 4d 2e fd fd fd 35 fd fd 04 36 fd 4d fd 19 fd fd 00 fd 20 fd 6b 53 fd fd 12 5c 20 fd 3d 66 42 6a fd 3e 20 71 5f fd 16 5f fd fd 07 4e 67 76 1f fd c4 fd fd 4e 62 7f 0a 37 fd 14 61 fd 5b 71 fd 73 fd 3c fd fd 4c fd 70 02 fd 00 19 fd fd 29 fd fd fd 3d 0c fd 5a fd fd 33 fd fd 71 37 fd fd fd 4f fd fd fd fd 50 5c 71 38 fd 72 fd 59 fd fd fd 55 68 fd 70 fd	*\$/_wZ pp+bNEQ;, <IVjs&L6[wim#2 zW.kvl-R.=oYCM.56M k\ =fBj> q__NgvNb7a[qs<Lp)=Z3q 7OP!qrYUhp	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.xml	1817	524	6a 39 32 4b 68 13 0f fd 0a 3d fd 49 16 fd 3f 10 08 3c fd 4b 24 03 fd 6a 0a 46 67 3d fd 05 10 fd fd 70 fd fd fd 54 fd 46 fd 3b fd fd fd 53 fd fd fd 1c 76 fd fd 51 fd fd 68 fd fd fd 0a 43 1d 3e fd 32 75 fd 6a 79 42 29 fd fd fd fd 39 fd fd 28 fd fd 43 06 fd fd 18 79 fd 6e fd 27 77 fd 93 fd 56 14 00 fd fd 79 5f fd 1e 33 fd 66 fd 44 09 fd fd 4b fd fd 39 fd 4a 1f fd fd fd 1e fd 66 fd fd fd fd 4d 62 50 6c fd fd 77 68 fd fd 42 4f 3f fd fd 2b 21 6e 50 fd 3f fd fd fd 0e 15 0b fd 4e 41 11 fd 0c fd fd 68 fd fd fd 44 4c fd fd fd 76 35 fd fd 36 fd fd b3 fd fd fd 5a 6b fd 01 1a fd 23 19 65 fd fd 14 fd fd fd fd 2a fd 73 45 fd fd 25 00 fd fd 4c 1f fd 20 5e 63 09 3d fd fd fd fd 42 4d 43 fd fd 36 fd f1 d2 31 fd 8e fd fd fd 4f fd fd fd 0d 05	j92Kh=I? <K\$jF=pTF;SvQhC>2ujy B) 9(Cyn'wVy_3fK9JfMbPlw hBO?+!nP? NAhDLv56Zk#esE%L ^c=BMC61O	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.xml	2341	10	24 00 19 07 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.xml	0	1817	fd 59 fd 5d 66 fd 0f 3b fd 23 07 38 08 fd 38 fd 30 7e fd fd 7a fd fd fd 59 00 14 66 4d ec 5e fd 01 55 fd fd fd fd fd 62 fd fd fd 6b fd fd 57 0e 2f fd 23 fd 35 fd fd 37 fd 46 fd 27 fd fd 1f fd 0a fd 32 20 fd 51 41 fd 1f 54 20 fd 6e fd 0e fd fd fd fd 5a 68 3e 34 6e 23 1c fd 4a fd 3e 1e 5f fd fd 0c 62 04 34 fd 67 3d fd fd fd fd 16 fd 53 4f fd fd 76 01 fd 5b fd fd 5e fd 29 fd fd 14 fd 0a 08 fd 66 11 4d fd fd 0d 6b fd 3f fd 0a 73 53 fd fd 38 5f 21 6e fd fd 69 fd 52 6f fd fd 0e fd 28 fd 2c 41 3d fd fd fd 44 fd 76 fd 7e 20 fd fd 7c 56 fd fd 11 22 5e 7a fd 1b fd fd fd 55 fd fd 58 4b fd fd 74 fd fd 26 7b fd 71 fd fd fd 1b fd 5a 1c fd 33 f2 5f 0e 32 fd fd 45 2c fd fd fd 03 fd fd fd 34 fd fd fd fd fd fd 33 fd 6d 17 49 23 fd 6e 3f 1f	Y]f;#880~zYfM^Ubk#57F' 2 QAT nZ h>4n#J>_b4g=SOv(^)fMk ?sS8 _lniRo(,A=Dv~ V"zUXK1&{qZ3_2E,43ml #n?	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3\Include\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 5f 2f 5c 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ _ _ _ \ _ _ _ _ _ _ _ _ _ \ / / _ _ _ _ _ \ . ' _ _ _ \ _ _ _ \ \ / / \ \ _ / \ _ \ _ \ _ _ _ \ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OnoteLR.cab	13354772	524	fd 11 fd fd f5 fd 65 2d fd fd fd fd fd 67 fd 6b 5a 76 fd fd fd 42 fd 70 fd fd 60 fd 7b fd 1f 78 58 38 fd fd 79 fd 1a 1f fd 3b fd 28 e6 fd 59 4d fd 2f fd fd fd 75 0c 5f fd 3e 5f 54 fd fd 18 fd fd fd 33 fd 31 fd fd 51 fd 35 fd fd fd fd 4b fd 41 fd 2c fd 7b 38 fd 27 19 fd 0c fd 52 fd 6a fd 5e fd fd 56 fd 65 38 fd fd fd fd 11 fd 20 19 fd 70 77 fd 5e fd 42 0c fd fd 4b fd fd fd 85 fd fd fd 3f 90 73 77 73 fd 38 fd fd 21 fd 71 fd 28 50 fd fd 0f fd 61 6a fd 2e 61 fd 0b fd 3b 4e 47 40 5d fd fd 6e fd 28 55 03 fd fd fd 11 fd 62 5d 72 fd fd fd fd fd 79 fd fd fd 3a c8 7f fd 6e 6d fd 36 fd fd 54 58 fd 1a fd 46 fd 1c fd 46 fd 16 fd 27 ef fd fd fd 69 60 fd 11 fd 41 fd fd 7d 31 fd 36 29 38 fd 69 1b 28 41 fd fd 02 4a fd 39 58	e-gkZvBp`xX8y; (YM/u>T31Q5K,{8' Rj^Ve8 pw^BK? sws8!q(Paja;NG@]n (Ub]ry:nm6TXFF'i A)16)8i (AJ9X	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OnoteLR.cab	13355296	10	25 32 14 fd fd 00 00 00 00 00	%2	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OnotelR.cab	0	1335470	4a fd 5d 51 4b 6a 49 67 1e 1a 56 39 4e fd 6b 3e fd fd fd fd 7a fd fd fd 3c fd 52 fd 0b 41 12 fd 1a 6f 14 73 fd 18 32 7d fd 6d fd 5c fd 7d fd 66 19 33 fd fd 7b 3b fd 1b fd 0c fd 64 fd 14 fd fd fd 37 59 5d fd 6b 47 fd 29 34 7f fd 00 fd fd fd 0b fd 01 41 1d fd 62 11 fd fd 07 fd 63 fd 29 fd fd 21 4c fd 7e fd fd fd 92 fd 4f 5f fd fd 11 28 01 71 36 fd fd 0e 62 fd 70 0f 30 fd 57 fd fd 20 fd 20 fd fd fd fd fd fd 5d 69 fd fd fd 09 40 10 fd fd fd 38 35 fd fd fd 1c fd fd 0a 10 fd fd fd 1e 7e fd 5e fd fd fd 76 44 0a 28 26 fd fd 67 fd 41 fd 3c 45 fd 7f fd 4d fd 6d 2e 65 5c fd fd fd fd fd 15 74 fd fd 78 65 fd fd 68 44 62 30 fd fd fd fd 1c fd fd 74 fd 4d 07 2f 66 6e 0e 1b 4a fd fd 6b fd 6f fd 64 fd 32 7e fd 36 0b fd 00 00 fd 78 fd fd 5c fd 2e	JQKjlgV9Nk>z<RAos2}m \\f3{;d7Y] kG)4Abc)L~O_(q6bp0W ji@8~^vD(&gA<EMm.e\tehDb0tMfn Jkod2~6xl.	success or wait	5	F2C055	WriteFile
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\Setup.xml	2175	524	3b fd fd 00 51 12 54 59 fd 53 fd fd 27 fd 61 67 74 14 20 fd 2e fd fd 5f 20 fd fd 3f 61 4e 19 fd 5d 58 fd 0a fd 09 24 fd 56 2b 5e 19 2e 6e fd 63 55 fd 3d 06 be fd 59 6b 11 21 fd fd fd 07 fd fd 20 fd 45 08 fd fd 71 79 7e 61 21 fd fd 57 3a fd 2a fd fd 6b fd fd 27 fd 1d fd 50 1e 22 fd 2c fd fd fd 6e fd 09 60 60 fd 72 60 fd 53 52 69 55 31 7d 05 fd 6c 7e 13 fd 18 fd e1 3d fd fd fd fd fd 57 fd 0c 09 fd 60 fd 7a 32 fd 41 70 3b fd 02 78 63 fd 10 fd 27 71 0a 39 fd 11 fd 51 fd fd 77 fd fd 7e fd 61 fd fd fd 6d fd fd fd fd 2b fd 7f 54 fd 78 fd fd 5b 70 38 58 fd fd fd 2b 3b fd fd 1f 45 77 fd 2c fd fd 12 1d fd fd 27 fd fd fd f6 fd 87 fd fd 55 24 14 37 fd 7a fd 1c fd fd fd 67 52 3c 5c 48 fd 53 14 fd fd 3f 09 4b fd 6f fd 3f 5e fd 32	;QTYS'agt._ ? aN]X\$V+^.ncU=Yk! Eqy~a!W:*k"P",n``r`SRIU 1}l~=W' zAp;xc;q9Qw~am+Tx[p8 X+:Ew,'U7zgR<IHS?Ko? ^2	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\Setup.xml	2699	10	24 00 7f 08 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\Setup.xml	0	2175	fd 86 08 0f 44 fd fd 7f 77 fd fd fd 0d 2b fd 5d 44 fd fd 46 52 bf fd 03 fd 58 fd fd 76 fd fd 6f fd fd fd 6e 6b 0d 77 fd fd 18 23 fd 59 7b fd fd fd 53 06 fd fd fd fd fd fd fd fd 34 85 41 0c 1e 0d fd 07 fd 53 02 7b 07 3e fd fd fd 6c fd fd 37 fd 18 1d 31 fd 75 98 69 fd fd 93 62 23 71 1c 25 fd fd 2d fd fd b2 fd fd 2b fd fd 77 7b 3c fd fd fd fd 43 fd fd fd fd 5a 76 fd 7a 69 fd fd fd fd 40 fd fd fd 65 06 fd fd 75 fd 9d fd 15 fd fd fd 46 fd 43 fd 6d 17 71 fd 4a fd 2f 35 fd fd fd fd 11 6d fd fd 1d 1f 57 fd fd 51 fd fd 36 11 fd fd 3c fd 6c fd 0f fd fd 24 fd 04 fd fd 4c fd 2e fd fd 22 fd 73 fd 2a 1c fd 75 fd 42 b0 fd fd 0f f6 97 fd 77 fd 39 10 10 fd 2d fd 71 fd fd 6a fd 51 15 4a 1b 44 5f fd fd fd 3e fd	Dw+)]DFXvonkw# {S4AS{>I71uib#q%- w{<CZvzi@euFCmqJ/m WQ6<L."s"uBw9- qjQJD_>	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\AutolT3\SciTE\3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ v _ _ _ \ / / _ _ _ . ' _ _ \ _ _ \ \ _ / \ / \ \ _ / \ _ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveLR.cab	872962	524	fd 57 2d fd fd 7b fd 6f 13 fd 10 34 15 33 fd 49 fd 5f fd fd 50 31 fd fd fd 57 fd 42 58 5b 70 45 fd fd fd fd 7f 1d fd fd 40 2c 5b 33 fd 71 4a 35 42 fd 05 6b 2d 77 fd fd 1b 32 fd fd 41 fd 0d 78 fd fd 43 fd a5 fd fd fd fd fd 42 47 7c 1f 13 fd fd 70 53 42 2f 59 34 20 fd fd fd fd 6a fd fd fd fd fd 54 78 47 fd fd fd 0b 6c 27 27 fd 3f fd fd 08 50 fd 45 1c 63 fd 61 fd 7f fd fd 6b fd 1a 0d 23 37 55 2d fd fd fd fd 64 56 fd 5d fd fd 76 7d 31 63 30 fd fd fd 1c fd fd fd 26 02 6c fd fd 47 2b 43 fd fd 97 63 fd fd 38 fd 7b fd 60 fd fd fd fd fd fd 27 fd fd 73 04 fd 1d a3 fd fd 38 25 7a 32 7e fd 31 fd 27 fd fd fd 76 fd 23 fd fd 3f 5c fd fd 47 3e fd fd 45 42 64 fd fd fd 6a 09 fd fd bc fd 6e 16 fd fd 68 27 fd 13 37 fd 0d fd 53 1a 68 fd	W-{o43l_1WBX[pE@, [3qJ5Bk-w2AxC BG pSB/Y4 jTxGI"? PEcak#7U-dVv }1c0&IG+Cc8{'`s8%z2~1' v#?'[G>Edjnh'7Sh	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveLR.cab	873486	10	24 00 02 52 0d 00 00 00 00 00	\$R	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveLR.cab	0	872962	50 fd fd 71 fd fd 07 fd 45 fd fd fd 77 25 fd 41 fd fd fd fd 5e 06 fd 73 2a a0 fd fd 6e 7c fd 1c 6b 77 3e fd 31 57 35 1b fd fd 34 fd fd fd 53 36 fd 0a 47 fd fd fd 37 27 fd 5b fd 11 fd 21 65 6f fd 2a 40 24 69 00 fd 7d fd 37 fd fd fd 79 61 65 fd fd 4b fd 49 fd 3c fd 77 fd 0a 5a fd fd fd fd 46 23 fd 07 a5 fd fd fd fd fd fd fd 46 fd 21 34 fd 40 17 40 44 1d 04 1b 14 fd 2e fd fd 24 6a 39 fd fd fd 72 2e 70 3f fd 09 fd 5d fd fd fd fd fd fd fd 4c 66 72 08 6d fd fd 18 fc 45 5c 41 19 33 fd 36 fd 60 36 fd c1 1b fd 7e 1f fd fd 61 09 fd 53 a2 6f 72 fd 41 fd 0c fd 54 fd fd 07 fd 6f 4a fd 62 7f 53 fd 6b 4c 64 fd fd 6b fd fd 00 0a fd 68 56 03 fd 50 fd 20 49 fd 65 1c fd 74 fd fd c8 fd 5d 71 7b 68 fd fd	PqEw%A^s*n kw>1W54S 6G7'![eo*\$i }7yaeKI<wZF#FI4@@@D. \$j9r.p?)Lfr mE\A36`6~aSorAToJbSk LdkhVP let]q[h	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Common Files\Adobe\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ v _ _ _ _ v / / / _ _ _ _ v . ' _ _ \ _ _ \ \ v v / / \ / \ \ _ / \ _ \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveMUI.xml	1126	524	fd 17 16 2e 74 18 fd fd 2b fd 70 fd 2b fd 7d 0f fd fd fd 7b fd 1a 34 67 09 53 61 14 fd 77 fd 72 fd 44 4a 58 3b fd 32 0e fd fd fd 0e fd 1a fd 74 1e da fd fd 72 35 5a da fd 40 fd 11 fd 13 fd 7b 58 2b fd 22 fd 6b 39 fd 0b 28 fd 15 3e fd 11 fd fd fd 7f fd fd fd 6f fd fd fd fd 28 23 4e 35 0c fd 28 fd fd fd fd fd 21 4c fd fd 1a 6a 67 71 01 fd 2b 31 fd fd fd fd fd 3f fd 6b 6b 38 fd fd 39 fd 2f fd fd 02 64 fd 2e fd 7a fd fd fd fd f7 f7 fd 1b fd fd 70 71 0f fd 03 fd fd 09 2e fd fd 0f fd 45 41 fd 4a fd fd fd fd fd 49 19 fd 32 fd 45 fd fd fd fd 5a fd 76 02 31 fd 41 fd 6c fd fd 17 23 fd fd e8 26 67 79 7d fd 4a 1a 08 11 fd 43 07 3e fd fd 5c 18 20 01 fd 14 4f fd fd 63 08 08 7b 31 fd fd 70 78 fd 38 fd 7b 01 fd 5f fd fd 18	.t+p+} {4gSawrDJX;2trZ@{X+"k 9(>o(#N5(!Ljgq+1? kk89/d.zpq.EAJI2 Ev1Al#&gy}JC\ Oc{1px8{_ 	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveMUI.xml	1650	10	24 00 66 04 00 00 00 00 00 00	\$f	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveMUI.xml	0	1126	0e fd 73 fd fd fd 4d fd fd fd fa 14 fd 7d fd 74 3b fd 21 fd 25 fd 50 fd fd fd fd fd 79 29 fd 3f fd fd fd 1f fd 16 26 04 38 38 61 64 29 34 72 fd 75 80 67 6d 4a fd fd fd 22 70 fd 28 55 60 58 fd 72 fd fd 2c fd fd e4 2d 6a 30 fd fd 0b fd 48 71 2a 07 fd 60 fd 7f fd 74 39 15 05 fd 2f 1e fd fd fd 6c fd fd fd fd fd fd 2b 69 fd 09 fd fd fd 41 fd 04 4f fd fd 44 fd fd fd 0c 41 3f 01 fd fd 4c 78 fd fd 57 0f fd 0a 01 fd 72 fd 6d 6a 25 4b 27 3b fd 3d fd fd fd 3b 7d fd 58 5f 4e fd 76 ef 14 2f fd fd 6c 18 fd fd 4f fd 00 72 fd 48 fd 4a 3b fd fd 56 34 fd 31 fd 32 fd fd fd fd fd fd 10 fd fd fd 75 fd fd fd fd 3a 16 fd 19 fd fd fd 00 fd fd 47 fd 51 6b fd 2d 79 fd 62 fd 53 5a fd 44 39 4c 2c 55 fd fd 63 fd 49 37 5e fd 7a fd 7a fd fd fd fd	s)t:;!%Py)? &88ad)4rugmJ"p(U'Xr,- j0Hq*"t9/I+IAODALxWrmj %';=-;}X _Nv/IOrHJ;V412u:GQk- bSZD9L,Ucl7^zz	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Common Files\DESIGNER\I3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ _ _ _ \ _ _ _ _ _ _ _ _ _ \ / / _ _ _ _ _ \ . ' _ _ _ \ _ _ _ \ \ / / \ _ _ \ _ / \ _ \ _ \ _ _ _ _ \ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\Setup.xml	1640	524	fd 22 fd 60 4f fd fd fd 0d bb 15 fd 13 6c 3e 4e 64 fd 3c fd 53 02 25 fd 13 09 78 7c fd 42 fd 4e 3a 4d fd fd fd 02 fd d1 4d fd 73 32 4b 41 56 fd 77 43 1d 6d 02 1c fd 10 25 0c 22 fd 32 04 fd 32 fd 47 fd fd 38 fd 4d fd fd 04 2f 27 21 fd fd fd 62 fd 02 05 2b 16 63 49 fd 4b fd fd 18 24 fd 44 1c fd fd fd fd 6c fd fd fd fd 24 fd 24 fd 0e 5d 35 4a fd 48 fd 46 12 25 fd 58 5c fd fd 00 fd 70 20 49 60 fd 26 0d fd 71 6a fd 2a fd 13 02 fd 6c fd 12 31 fd 3a 4d 7d 29 09 fd fd 11 60 34 fd fd 14 50 4d 00 fd d0 7b 69 6c 17 0f fd 2f fd 70 1e fd 2c fd 36 36 e4 77 fd 30 14 5e 7d 30 fd 3a fd fd fd 57 1e fd fd 17 fd be fd 78 fd 41 fd 5a fd fd fd 87 fd fd 14 60 fd fd 29 53 7f fd fd 07 0e fd 4b fd fe fd fd fd 70 d8 1d fd fd fd 56	""Ol>Nd<S%x BN:Mms2 KAVwCm%"22G 8M/!b+cIK\$D\$\$[5JHF%X \p l'&qj* [l:M])`4PMil/p,66w0^}0:W           xAZ`)SKpV	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\Setup.xml	2164	10	24 00 68 06 00 00 00 00 00 00	\$h	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\Setup.xml	0	1640	1e fd 78 7b 0d fd fd fd fd 14 fd 09 fd 13 fd 48 10 fd fd 08 fd 20 fd 1a fd 3d 24 1c 0d 21 23 03 fd fd 58 20 fd fd fd 56 6b fd fd 5e 0a 4d 0c 06 fd 00 fd fd 62 1f 4a fd 49 6b fd fd 31 fd 47 69 65 68 68 fd 63 18 4c 69 3b fd 13 fd fd 75 6d fd 31 4c fd 5b 45 29 57 62 78 fd fd fd fd fd fd fd 35 6d fd fd fd 9a 74 fd 49 1e fd fd 33 fd fd 04 fd fd 4b 74 fd 2a 6b 69 2c 27 60 72 7a 3b 39 22 74 18 49 5f fd 16 6f fd fd 32 67 27 fd 75 fd fd fd 75 fd fd 43 fd fd fd 2d 69 18 31 0f fd 3e 68 fd fd fd 8f 23 5a fd fd 22 0c fd 62 1a 7b 2c fd 14 23 fd 2b 02 37 fd 12 fd 33 fd 22 71 31 67 3f 00 35 12 64 41 5c 39 4e fd 6d 30 08 24 68 2b fd 4b 44 fd 7e fd fd 39 76 fd 77 fd 54 6c fd fd fd 4c 2e fd 66 2d 30 fd fd fd 6d 0a 68 04 5e 4d 37	x{H =\$!#X Vk^MbJlk1GiehhcLi;um 1[E)Wbx5mtl3Ktki,'rz;"tl_ o2g'uuC- i1h#Z"b{,#+73"q1g? 5dAl9Nm\$ h+KD~9vwTIL.f-mh^M7	success or wait	1	F2C055	WriteFile
C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.cab	16813	524	fd 6f fd fd 57 24 4d fd fd 27 fd 03 fd 16 3f fd fd 1d 48 fd 63 fd 6a fd fd 0f 52 fd 36 fd 0e fd 63 1a 3f 4d 4b 3a fd fd 37 23 70 28 fd fd 34 77 fd 79 07 26 fd fd 5c 21 38 fd fd 0f fd 26 fd 32 72 2b fd fd 32 37 6c 56 fd 1d fd 39 fd fd 77 fd fd 04 fd 13 1a 3a 27 f7 2e 61 32 fd 68 10 fd fd 57 fd 6e 2e 18 fd 23 46 fd 62 1a 34 fd 2c fd 51 01 4d 61 fd 53 15 22 fd 2e 26 1d fd fd fd 57 fd 6b fd 5a 24 fd fd 3b 19 5e fd 76 3d 1c 03 29 fd 6a 74 fd 56 32 74 fd 28 07 1a 4d fd 06 40 fd 05 fd fd 75 fd fd 2e 44 1d 0f 71 fd 31 fd 63 05 fd 7f 43 fd 1e 3a fd dd 51 fd 6b fd 0b 12 1b 7c 11 7e 20 3f 0a fd 2c 65 76 6f 52 40 6e fd 64 fd 31 fd 25 fd 4a 4c fd 6b fd 0e 7d 71 49 fd fd 3c fd 7d 4c fd fd fd fd 01 fd 1a fd 02 fd fd 11 64 48 09	oWM'HcjR6c? MK:7#p(4wy&\8&2r+2 7\vw:'.ahWn.#Fb4,QMaS ".&WkZ\$;^ v=)jtV2t(M@u.Dq1cC:Qk ~ ?,eoR@ nd1%JLk q <})LdH	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.cab	17337	10	24 00 fd 41 00 00 00 00 00 00	\$A	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.cab	0	16813	fd fd fd fd fd c5 4f 11 46 35 77 fd fd 3c 6e fd fd 38 fd 49 fd fd fd 28 40 0a 27 fd 09 fd 15 fd 46 5c 75 36 fd 3b 7c 11 4c fd 17 11 07 fd 42 fd 3b 36 77 20 fd fd 61 1b fd dd fd 46 2b b3 fd fd fd 43 12 11 fd fd 0f fd fd 25 56 06 fd 45 fd 53 51 5e fd fd fd 39 7f fd 78 20 fd 7f 3b fd 11 5b fd 3a 34 fd 64 fd fd 39 04 fd fd fd 30 35 5a 5d fd fd 37 5a 69 19 fd 1b fd 30 fd 18 fd fd 00 fd 16 fd 71 fd fd fd 4e 32 fd 13 fd 66 5f 94 fd fd 2a fd fd fd 31 33 fd fd 53 fd fd 42 fd 58 2b fd 27 76 79 fd fd 69 58 3c 2b fd fd 60 fd fd fd 6a fd 31 fd 11 fd 4b fd 59 55 07 fd fd fd fd 3b fd fd 52 11 30 15 fd 16 43 14 fd 33 fd 32 47 fd 86 35 fd 65 05 17 0d 13 fd 06 39 99 43 3f fd 27 fd 76 38 fd fd	OF5w<8l ('@'Flu6; LB;6w aF+C%VESQ^9x ; [:4d905Z]7Zi0qN2f_*13S BX +'vyiX<+'j1YU;R0C32G5 9C?v8	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Common Files\Java\RM3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ v _ _ _ _ v / / _ _ _ _ . ' _ _ \ _ _ \ \ v / / \ \ \ _ / \ _ \ _ \ _ \ _ \ _ \ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\MSOCache\All Users\{90160000-00E1-0409-0000-00000000FF1CE}-C\OSMMUI.xml	1123	524	4d 3f fd fd 5b fd 78 24 fd 38 53 fd fd 73 32 c6 fd fd fd fd 49 47 62 27 4b 1e 40 fd 45 04 27 3a fd 3e 0e fd 26 fd 6c 3b 38 65 0e fd fd 75 fd fd 3b fd fd 1c fd 5e 79 fd 02 3b 42 76 b6 fd 67 fd fd 5a 00 fd 13 fd 3d 3a fd fd 38 fd fd 37 fd 15 25 0f fd 0a 57 2d 44 fd 4e fd 64 fd fd fd 0e 33 fd 53 7d 4a fd 3c 2b fd 0c 72 7e 30 fd fd 3b 07 1e fd 5a fd fd 3c 14 fd 2e fd fd fd fd 32 24 59 fd fd 44 2a fd fd 66 50 50 8c 2a fd 7b 4c fd fd 13 42 76 fd 7a 21 23 fd 54 fd fd fd fd 1b 58 73 fd 04 1f 4d 2e fd fd fd 1e fd fd fd fd fd 63 fd 3c 6b fd fd 18 fd fd 5e 16 fd fd 2d fd 25 fd 62 fd 1a 46 2d fd 4c fd fd 4b 2e fd 5e fd 0d 64 fd fd 5e 5e 37 15 0b 27 fd fd fd fd fd 63 fd 10 32 fd 37 12 fd 2c fd 2e 08 fd fd 64 17 fd 4f 40 fd fd fd	M? [x\$8SslGb'K@E':>&!;8eu; ^y;BvgZ=:87%W- DNd3S}J<+r~0;Z<.2\$YD* fPP*LBvz!#TXsM.c<k^ %bF-LK.^d^^7c27,.dO@	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-00E1-0409-0000-00000000FF1CE}-C\OSMMUI.xml	1647	10	24 00 63 04 00 00 00 00 00 00	\$c	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.xml	0	1123	fd 0f 07 75 74 fd fd fd 40 fd 7f fd 22 fd 50 08 50 fd 12 77 fd fd 76 fd 32 7c 60 fd fd fd 76 fd 0b 4f fd fd 79 fd fd fd fd 43 78 2d 56 fd fd 69 40 fd 53 fd 20 fd 72 03 7a 56 fd fd 25 fd 9f 57 fd fd 6c fd fd 3b fd fd 1e 4c fd 4a 0a fd 4c fd 09 fd 3e 00 fd 57 10 38 7d 5a 50 6b 4f fd 36 4e 27 16 fd fd 01 fd 4f 70 3b 45 fd fd fd 17 14 6a fd 69 3d 6f 78 60 34 04 28 fd 53 51 fd 24 6f fd fd 27 32 4b 4b fd 33 fd fd 72 fd 06 fd fd 7a 0a 79 41 30 fd 70 fd 5d fd 2d 32 5e fd 3f 1b fd 32 fd fd fd 0c fd fd 64 05 fd fd fd 2b 4d 16 59 fd 46 fd fd fd 6a fd 79 fd fd fd 0f fd fd 75 fd fd 6f fd 00 3e fd 30 45 22 50 02 64 59 2a fd 75 6a fd fd fd fd 10 49 7c fd 5c 0c fd 58 fd fd fd 5e 13 20 69 fd 06 fb 18 fd fd fd 34 fd fd fd fd 17 fd	ut@"Pwv2]"vOyCx-Vi@S rzV%Wl;LJ L>W8}ZPkO6N'Op;Ejj=ox '4(SQ\$o'2KK3rzyA0p]- 2^?2d+MFjyuo0E"PdY* ujl\ X^ i4	success or wait	1	F2C055	WriteFile
C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\Setup.xml	2038	524	39 fd fd 54 fd 38 66 fd fd 02 49 fd fd fd 13 2b 25 fd fd bb 09 03 3b 79 28 b2 fd 5a ae 37 88 20 08 22 fd fd fd 51 fd fd fd 12 55 3b fd 44 79 79 09 c5 21 0a 53 fd 04 70 54 fd fd 0f 65 fd fd 36 fd 6b 44 4e fd 63 0d 1d 45 26 05 fd 73 fd 12 46 14 5a fd fd fd fd 36 6c fd fd fd fd 6b fd 20 71 59 fd 5d fd fd fd 0b fd 0b fd 0e fd 62 74 60 fd fd fd 03 23 fd fd fa 7e 73 fd fd fd fd 35 5c fd fd 2b fd fd 23 3f 26 28 fd 71 fd fd 24 fd 3a 69 6f 4f 48 1d fd fd 77 fd fd 42 20 fd fd 21 47 08 4a 0d fd 25 13 19 fd fd 5e 4c 6d fd fd 6d fd fd 01 fd 2d fd 20 1b fd 5c fd fd 67 0c fd fd fd 21 65 fd fd fd 5f fd 11 0d 4c fd 1c 21 fd 1b 26 5b 6e 39 01 fd 2e fd fd 4d fd 0e 05 fd 48 fd fd fd 10 fd fd fd 71 34 fd fd fd 56 fd 25 fd 6d	98fl+%;y(Z7 "QU;Dyy!SpTe6kDNcE &sFZ6lk q]bt`#~s5\?& (q\$:ioOHwB !GJ%^Lmm- \gle_L!&[n9.MHq4V% m	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\Setup.xml	2562	10	24 00 fd 07 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\Setup.xml	0	2038	2d fd fd 2c 5c 32 29 40 fd 42 fd 73 40 fd fd 6e 6d 72 fd 61 07 fd 79 68 04 fd fd fd fd fd 3e 25 00 fd fd 2e fd 0f fd fd 1a fd fd 79 fd fd fd fd 6b fd fd 0a 0c 3b fd fd 63 fd fd e5 15 72 24 fd fd 38 41 fd fd fd 38 fd 01 75 fd fd 71 fd fd fd 6d 95 fd fd 76 0e fd 2d fd 2e fd 49 2b 4b 40 59 09 04 64 fd 8e 35 41 6b 5c 4c fd fd 74 fd 65 2e fd fd fd fd 2d 7b 45 fd fd fd fd 3f fd 1c 3d 21 79 fd 5e e6 58 fd fd fd 05 48 fd 6f 6e 18 6a fd 00 2f 47 7b 70 fd 36 fd 3f fd fd 29 4a 6e fd 5c fd fd 0b fd fd 8f fd 44 61 fd 58 fd 33 53 34 fd 77 68 fd fd 15 fd 3c fd fd 61 06 19 fd fd 1b fd fd 2f fd fd 57 2a 25 fd e1 59 fd fd 4b 2c 69 42 3f fd fd 10 0e fd 7a fd 3d fd fd 27 fd fd fd fd 56 fd fd fd 10 fd fd 1a 60 75 0a fd fd fd 1b 51	- ,\2)@Bs@nmrayh>%k;cr \$8A8uqmv- .l+K@Yd5Ak\LTE.-{E? =ly^XHonj/ G{p6?}Jn\DaX3Swh<a/W *%YK,iBz='`uQ	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\OSMUXMUI.cab	0	1048576	09 5d 4d 47 3d fd fd fd 6e fd 70 4a fd fd 2c 2a fd fd fd fd 75 48 fd fd 0f 70 03 05 66 33 43 16 fd fd 7b 68 00 fd fd fd 13 65 fd fd fd 77 45 fd 4e 59 3d 12 fd 7e fd 46 fd 3a fd fd 41 fd 15 fd 7e 11 fd 6f 45 75 37 fd fd fd 2c 4b fd fd 28 fd fd 2e 2d fd 6d 34 fd 07 fd 17 12 75 fd 34 fd 79 fd fd 58 fd 32 fd 34 fd 0e fd 0c fd fd 42 19 4d 40 77 11 35 d4 fd 32 20 fd 23 57 7e fd fd 40 fd 70 46 fd fd 08 3e 1f 37 08 3c fd 47 fd fd 53 fd fd 24 fd fd fd 79 fd 7b fd fd 38 fd 29 7e 13 6d fd 19 35 fd 49 43 0d fd 03 fd fd 6d 09 77 b0 fd fd fd 66 fd 77 fd fd 2c fd 7f fd fd 14 fd 7b 63 12 11 6c fd fd fd 05 7d fd 6f 09 9a 26 fd 08 06 fd fd fd fd 27 1b 49 fd fd fd 2b fd 0a 6e 0d fd fd 45 3c 10 63 fd fd fd 01 2c 69 fd fd 12 4f	]MG=pJ,*uHp3C{hewEN Y=-F:A~oEu7,K(- m4u4yX24BM@w52 #W~@pF>7< GS\$y{8~m5lCmwfw, {cl}o&'!+nEc,iO	success or wait	1	F2C055	WriteFile
C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\OSMUXMUI.xml	1458	524	fd 1c 0b 76 fd fd 28 5b 10 0c fd 69 fd fd 24 20 2e fd 6a fd 25 09 0c 7e 43 fd fd 29 62 69 fd fd fd 29 36 06 fd 5f 1a 12 47 fd fd 65 fd 0f fd 64 fd fd 01 cb 58 60 1b 59 fd fd fd fd 1f fd 49 fd fd fd 0e fd fd c2 fd 57 6d 39 fd 49 fd 4d fd fd 73 34 71 3d fd fd 3b fd 31 fd 17 cd fd fd fd fd fd 5e fd 2e 4b 3f 3a 05 7e 35 2f fd 41 3f 1a 39 23 70 3e 61 29 5c fd 03 23 3b 5e fd 08 ae fd 36 70 5b 6a 4c fd fd 29 79 19 fd 03 fd 40 2d fd 2d 6f 66 fd fd fd 56 fd 37 73 03 25 fd 75 fd 51 75 fd 48 58 56 fd 42 14 fd fd fd db 0f d7 fd 1d 2f 50 fd 3a fd 66 fd fd fd fd 71 fd 0a fd 6f 53 e1 fd 75 71 7d fd 6b fd 6f fd 0a fd fd 73 fd fd 16 fd 7b fd fd 53 fd 2d 07 21 fd 30 1e 44 1b 55 fd 49 fd fd fd fd fd 3a fd fd fd fd 19	v([i\$.j%-C)bi)6_GedX`YIWm9 M4q=-,1^,K?:-5/A? 9#p>a);^6p[jL)y@-- ofVs%uQuHXVB/P:fqoS q)kos{S-l0DUI:	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\OSMUXMUI.xml	1982	10	24 00 fd 05 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\OSMUXMUI.xml	0	1458	fd 3e fd 45 01 09 28 3f fd 7e fd fd 57 fd fd 4f 58 fd fd fd 00 4b fd 11 fd 2d fd fd fd fd fd fd 57 13 75 fd fd fd 0c fd 78 fd 37 fd 52 35 fd 4b 7b 71 fd fd fd fd fd 55 fd fd fd fd 10 fd fd 84 45 07 fd 3b 7e 1f 0f 03 fd 70 3f 17 54 fd 55 fd 74 fd 66 5e 79 fd fd fd 14 7a fd 4c fd fd fd 64 54 6c 7c 2d 77 33 fd fd 03 04 47 fd fd 50 14 33 07 32 64 65 fd fd 6d fd fd 67 3c 4c 02 fd fd 42 26 5c fd 89 fd 77 6f fd fd 10 fd 4e fd 7c 6a fd 5d fd fd 1d fd fd fd 19 16 fd fd 0d fd 10 77 4c fd fd fd 56 fd 4d 2a fd 75 fd 36 76 66 34 40 da fd 19 1c fd 2c fd fd 0d 0b fd fd fd fd 07 6c 3f 6c 61 3b fd 05 5d fd fd fd fd 32 fd 2d fd fd 48 27 24 fd fd fd 5e fd 52 fd 4b 2a 51 fd fd 13 03 fd 1c fd 2e fd 23 fd fd 83 01 fd 58 fd 1f fd fd 38 28 4d	>E(?~WOXK- Wux7RK{qUE;~p?TUt*f y zLdTI - wGP32demg<LB&lwoN[j] wLVM*u6f4@,l?!a;2- H'\$^RK*Q.#X8(M	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Common Files\Oracle\OR3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ v _ _ _ \ / / _ _ _ . ' _ _ \ _ _ \ \ _ / \ / \ \ _ / \ _ _ \ _ _ \ _ _ \ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\Setup.xml	2454	524	7f fd 5b fd fd 77 3e fd fd fd fd 30 fd 25 1f 2f fd fd fd fd fd 65 77 fd 3d fd 73 14 63 13 fd 30 0c fd 3f 1c 70 fd 08 34 fd 53 fd fd 64 35 04 fd fd fd fd 19 04 27 0f fd 1f 1b 62 77 fd fd fd 0e 7e fd 26 fd 00 fd fd 71 fd 95 7b 1a 1c 04 fd fd fd fd fd 25 03 fd fd 63 fd 12 fd fd fd fd fd 39 fd fd 24 fd fd 4b 41 fd fd fd 78 fd fd 25 fd 43 fd 7b 6b fd fd f3 61 66 59 7c fd 5a 6d fd 50 fd fd 3d fd 53 fd 06 fd 55 fd 14 fd 35 19 5d fd 3c 34 fd 65 5e fd 0d 3a 52 74 0b fd fd fd 03 41 7f 16 fd 64 fd 6e fd fd 26 fd fd 09 fd 1f fd 55 69 73 fd 05 fd fd 70 2d fd fd 30 fd fd 5d fd fd fd 52 60 57 00 fd 5f 65 62 1d 1d 16 fd 21 fd 7b 09 4c 06 fd fd 77 fd 24 fd fd fd 68 fd 4c 60 60 fd c0 57 fd 50 fd fd 28 fd fd fd 3b 22 fd 3b 70 7f fd 2b	[w>0%/ew=sc0? p4Sd5'bw~&q{%c9\$K Ax%C{kafY ZmP=S5] <4e^:RtAn&Uisp- 0]R`_eb![Lw\$h`WP(;";p+	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\Setup.xml	2978	10	24 00 fd 09 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\Setup.xml	0	2454	fd 0a 45 fd fd fd 76 1e 50 fd 73 fd 39 fd fd 74 73 fd fd fd 1d 20 44 fd 20 fd fd 41 6a 45 33 fd fd 76 00 fd fd 2d 78 2f fd 1a fd fd 00 70 2c fd 67 fd fd fd fd 48 12 4f 5c 70 fd 51 48 fd 49 fd fd fd fd 72 72 5b fd 2c fd 65 11 fd 07 fd 39 48 fd fd fd 70 fd fd fd 75 fd 56 fd 80 7c 5c 1c fd 4b fd 0d 20 41 73 fd fd fd 38 fd 22 fd 10 20 08 fd 3a fd 31 7b fd fd fd fd fd 40 fd fd 2d 41 fd 3f fd fd 29 2f fd 2a 71 fd 61 fd fd 7c fd 52 20 59 5c fd 7c fd 22 5b 3c fd fd fd 5e fd 57 35 32 fd 62 fd 4d fd fd 40 fd 1b fd 70 fd 57 52 fd fd 3d fd 7e 3c 6c fd 7b 73 55 07 28 97 29 35 57 73 fd fd 53 fd fd 0f fd fd 44 65 4c 1c fd 1a fd fd be fd 1b fd 69 fd cd 78 fd fd 1b 7c 6b fd fd 4e 77 68 71 64 fd fd fd 24 fd 51 61 41 fd fd fd fd	EvPs9ts DAjE3v- x/p,gHO\pQHirr[,e9HpuV\ K As8" :1{@- A?)/"qa R Y\ " [<^W52bM@pWR=~ <l{sU()5WsS DeLix Nwhqd\$QaA	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\branding.xml	336313	524	47 30 17 fd 6b 00 fd 22 6c 46 fd 34 13 29 fd 0b fd fd fd fd 41 58 fd fd fd 4b 77 fd 01 fd fd 3d 69 fd 25 04 fd 35 fd 37 5c fd fd 68 6d fd 64 fd fd 6b 68 fd fd 47 fd fd 62 03 3f fd 33 08 fd 7a 39 33 31 92 02 63 19 09 fd fd 7c fd fd fd 53 fd 4e 79 fd fd fd fd 22 fd 49 64 31 2c 44 6c fd fd 51 fd 0b 7a 18 04 fd fd 09 5b 42 26 fd fd 7e fd 21 fd fd 54 20 fd c1 fd fd 72 fd fd fd fd fd 6d 32 fd 03 3d 6e fd fd fd fd 01 fd fd 02 d3 0e 7d fd fd 3c 2c 50 fd fd fd 0a 50 fd 09 6e 2f fd 1d 27 fd fd 5f 43 3c 68 fd fd fd 06 fd fd 6a fd fd fd 70 fd 0b fd 33 fd 22 50 fd fd 12 fd 2e 25 fd 31 fd fd 4a 11 fd fd 3d 44 3b 7b 49 5e fd 4a fd fd fd 1d 33 4d fd 08 2d fd c3 fd fd fd fd fd 73 0a fd fd 3c fd 5b 7d fd fd fd 2f fd 50 fd 7f 47 fd	G0k"lF4)AXKw=i%57lhm dkhG?3z931 c SNy"ld1,DIQz[B&-lT rm2=n}<,P Pn/_C<hjp3"P.%1J=D; {^J3M-s<}/PG	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\branding.xml	336837	10	24 00 fd 21 05 00 00 00 00 00	\$!	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\branding.xml	0	336313	fd 1a fd 41 fd 50 74 99 6c 0f 26 fd fd fd 07 12 fd fd 3c fd 2e 26 4d 09 fd fd fd 75 fd fd 7f fd fd c9 fd fd 1b fd fd 75 fd 2e 35 75 63 0b fd fd 4d fd fd 27 fd 19 23 64 fd 53 63 fd fd 2e 23 1a fd fd fd fd fd 62 fd 21 45 fd fd fd fd fd 47 12 fd fd fd 36 78 12 fd 07 05 fd fd 19 76 fd fd 71 fd fd 37 fd 5d fd 2b 0b fd 05 fd 2b 7e 0a fd 66 00 38 68 fd fd 76 fd 49 fd 52 fd fd fd 3f 0f fd fd 3c fd fd 17 fd 11 fd 55 6a fd 5b fd fd fd 5a 56 fd 3e 03 56 fd fd 19 28 3a fd 62 67 58 fd fd fd fd 49 fd fd fd 33 16 fd 12 18 fd fd 07 fd fd fd 2d 3e 1d fd fd fd 7d fd fd 73 3f 59 fd fd 13 40 fd fd fd fd 0e 70 50 fd f9 19 09 fd 31 fd fd 68 01 07 7e fd fd 4c fd 3a fd fd fd 46 fd 03 19 fd fd 65 6b fd 49 3f fd 59 f4 fd 29 fd 58 56 2b fd fd	APtl& <.&Muu.5ucM"#dSc.#b!E G6xv q7]+++f8hvIR<Uj[ZV>V(: bXl3->)s?Y@pP1hL:Fel? YXV+	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Common Files\Services\IR3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ v _ _ _ _ v \ / / / _ _ _ _ v . ' _ _ \ _ _ _ \ \ v \ / / \ / \ \ _ / \ _ \ _ \ _ _ \ _ _ \ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0115-0409-0000-00000000FF1CE}-C\OfficeLR.cab	11706866	524	fd 63 fd 6e fd 6a fd 4f fd fd 36 59 73 4e 45 fd 56 74 08 7c 78 fd fd 55 73 68 27 fd 60 4b fd fd 5a 85 fd 3e 77 2b fd 7b 5c fd 51 13 45 fd 66 fd fd 09 09 fd fd 1b 6a fd 2d fd 3f 1f 9c 14 fd 51 fd fd fd 23 54 63 fd 0a 64 30 fd fd fd 23 69 1c fd 0e 55 6f fd fd fd 24 77 fd fd 3d fd 16 04 fd cb 10 fd fd 65 75 34 4b 77 fd 5c fd fd fd 52 fd fd fd fd fd 61 fd fd 32 fd fd 1a fd 68 fd fd fd 15 64 fd fd 76 fd 25 fd fd fd 33 fd 32 fd fd fd fd 01 fd fd f5 44 fd fd 75 19 6e 6b 67 4a fd 48 fd 1a 4b fd fd 13 4d fd 53 fd 33 76 72 fd fd 4e fd 73 3d fd 0e fd 7a fd 77 23 65 2f fd 67 7e 77 fd fd 29 4f fd 3b fd 78 3d 04 fd 69 fd 07 fd 28 fd fd 2f 7c fd 58 fd 2d 31 4c fd fd fd fd fd 41 72 fd 3e 63 fd 4c fd fd 0b fd fd fd 0f fd 3c 61 fd	cnjO6YsNEVt xUh^KZ>w +{\QEfj-? Q#Td0#iUo\$w=euKw\Ra2 hdv%32Dukg JHKMS3vrNs=zw#e/g~w) O;x=i(/ X-1LAr>cL<a	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-00000000FF1CE}-C\OfficeLR.cab	11707390	10	25 32 fd 00 00 00 00 00	%2	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-00000000FF1CE}-C\OfficeLR.cab	0	1170680	3a fd 0e 49 fd fd 6d fd fd 1a 66 fd fd fd fd 17 44 65 fd fd 1e 59 23 0c fd 08 fd fd 5a fd 11 28 06 3f 18 fd fd 1a fd fd 57 02 5f a8 fd 04 fd fd 6c 12 02 fd fd fd fd 63 fd fd 4c fd fd 7d 3c 5e fd 4a fd fd 1b fd 7b 69 fd fd 35 fd fd fd 07 46 02 47 fd fd 54 fd fd 60 30 3a 72 fd 58 5a 79 3f fd 24 2e 69 fd fd fd fd a2 31 3a 2c 12 54 fd fd 41 68 13 fd 52 fd 28 fd 6b 5c 6c 0c 37 2c fd 68 fd fd ba 53 fd 68 02 30 48 51 fd fd 32 09 78 fd fd 2c fd 22 64 52 72 fd 2e fd 14 2e 6b fd c7 fd 73 24 79 fd 2b 07 fd 1a 5a fd fd 0c fd 19 fd fd fd 45 fd 76 fd 3a fd 6b fd 0d 0a 35 fd 32 3a 7b 41 fd fd fd fd 15 09 fd fd fd fd fd 63 58 fd 4d fd 54 fd 1a fd 46 fd 22 68 01 77 4a fd fd 50 21 fd fd 58 fd fd 37 16 48 58 5b 48 34 fd fd fd 23 fd fd	:lmfDeY#Z(?W_lcl} <^J{i5GT"0:rXZ? \$.i1.;TAhR(klI7hSh0HQ2 x,"dRr..ks\$yZv:k52: {AcXMTF"hwJP!X7HX [H4#	success or wait	5	F2C055	WriteFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-00000000FF1CE}-C\OfficeMUI.xml	5275	524	08 02 fd 41 fd 58 fd fd 21 fd fd fd 76 fd fd 18 77 7c 03 02 6c 53 62 13 19 fd b1 32 fd fd fd 20 13 fd 4a fd 2c 65 47 fd 75 35 fd fd 08 2f fd fd 5e fd 4f fd 46 fd 58 4c 72 0d 76 fd 01 7e fd fd 3e fd 64 fd fd fd fd 34 05 fd 02 27 fd 04 fd 4d fd 7e 6f 16 2d 2f fd 6e fd 4b b0 57 6e 7e 17 fd 55 27 38 fd fd 46 65 05 7a 27 34 0e fd 1d 0e fd 61 73 4e 21 b2 fd 1b fd 54 00 fd 38 fd 28 fd 20 fd fd 66 fd 53 31 51 fd 11 09 7d 2c fd 26 04 32 fd fd 7b fd a3 fd fd 3e b1 14 25 2a 43 fd 6c fd fd fd fd fd 47 08 fd fd fd 0f fd 0a fd 02 50 fd 27 fd 14 fd 6f fd 4e 63 fd fd 54 1b fd 1a 12 56 1f fd 1b 31 fd fd fd fd fd fd fd 19 4b fd fd fd fd fd 22 18 48 22 7e 12 6c fd fd 41 17 fd 29 fd 6b fd 6c 45 fd 35 68 28 7f 77 32 fd d6 58	AX!vwj Sb2 J,eGu5/^OFXLrv~>d4' M~o- /nKWn-U'8Fez'4asN!T8(fS1Q ,&2{>%"ClGP'oNcTV1K" H"-lA)klEsh(wx	success or wait	1	F2CBF8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeMUISet.xml	1556	10	24 00 08 04 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeMUISet.xml	0	1032	fd 6a 2e 28 77 39 fd 02 fd fd 09 0a 60 72 fd fd fd 76 fd 50 fd 24 24 03 1d fd 49 fd fd 4f 9b fd fd 53 fd fd 53 30 fd 64 13 2f fd 5d 12 02 fd fd 7e 69 47 1f fd c4 2c fd 2e 3e fd 02 fd fd fd 3d 6c 14 0b fd fd 19 0a fd fd 2b fd fd 55 4c 4a fd 0a fd fd 23 60 fd fd 3b fd fd 9c 12 59 41 fd 1f 4c fd 1f 51 fd 45 65 72 fd 4f fd 13 fd 64 39 04 fd 35 fd fd 5a 62 fd 07 53 07 fd fd 71 71 46 fd 29 fd fd fd 2e fd fd 36 fd 6f 37 fd 3f 78 7c 12 fd 51 04 fd fd fd 37 46 67 fd fd fd fd fd 46 fd fd 5a fd fd 00 24 61 73 fd fd fd 6f fd 2c fd 3f 6f fd fd 5d 5d 3f 2d fd 5c fd fd 39 1d 61 3e 0f 52 3a fd fd 87 39 26 fd fd 33 fd 64 4f 26 fd 5b 2d 16 0e fd fd fd 79 6a fd fd fd fd 00 fd 6e 1e fd fd fd fd 35 fd 54 7a 07 72 41 fd fd 0c 4c fd fd fd 63	j. (w9`rvP\$\$IOSS0d/-iG.> =I+ULJ #m;YALQEerOd95ZbSqq F).6o7x Q7FgFZ\$aso,? o]]-\9a>R:9&3dO&[-yjn 5TzrALc	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Google\CrashReports\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ v _ _ _ _ \ _ / / _ _ _ _ . ` _ _ \ _ _ \ \ \ _ _ / ^ _ \ _ ^ _ ^ _ ^ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OffSetLR.cab	15708	524	5e 6e 13 fd fd 77 45 3d fd 7b fd 0e 3d 25 4d fd fd fd 2e fd fd 29 fd 5b fd fd fd 45 26 fd fd 82 56 fd 50 fd 21 7c 74 fd fd fd fd 01 70 fd 4d 74 fd fd fd 63 fd 13 fd 26 fd 5e fd fd fd 1f 17 7b fd 6d fd fd 68 14 61 fd fd 76 fd fd 0e 79 fd 41 fd fd 19 fd 2f 69 60 43 4b 72 45 fd fd fd fd fd 18 04 59 fd fd 68 03 fd fd 1a 47 fd 79 fd 3a 1a 34 fd fd 5c 49 fd fd 08 79 fd fd 0f 4b 45 58 fd 70 fd fd fd fd fd fd fd fd 6d 10 fd 4a fd fd 20 fd 08 fd fd 26 fd 4c 2a fd fd fd 08 be 75 53 06 fd 5f fd 00 fd 6d 67 4a fd fd fd fd 31 fd fd fd 0f fd fd fd fd 42 5f 75 fd fd 75 fd fd 14 fd 51 79 68 0d fd 33 04 fd 48 29 fd 40 25 0c 24 fd fd fd fd 47 22 fd 6b fd fd fd 4a 23 fd 58 7c fd fd fd fd fd fd 7f 7d 2c fd	^nwE==%M.) [E&VP! tpMtc&^\{mhayA /i`CKrEYhy:4\lyKEXmJ &L*uS_gJ1 B_uQyh3H@\$G"J#X}},	success or wait	1	F2CBF8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OffsetLR.cab	16232	10	24 00 5c 3d 00 00 00 00 00 00	\$\=	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OffsetLR.cab	0	15708	5e 6d fd 02 4a de fd fd fd 30 2d 49 be 4b 59 fd 5a fd 25 fd fd fd fd 00 2e fd fd fd fd fd cc fd 14 54 fd 17 fd 7e fd fd 70 44 fd 4c fd 6d fd 39 16 fd 30 7d 17 41 76 41 74 fd 14 4b 5d 27 fd fd 7b fd 3a fd fd fd fd fd fd 64 fd 13 05 71 fd 6e fd 24 fd fd fd 2d fd fd 7c 60 fd 67 33 11 49 0a fd 35 fd 74 71 fd 0c fd 44 fd 5c fd fd 04 72 24 0b fd 4b 4e fd 21 52 1d 53 fd fd 77 fd 79 fd fd fd 01 66 54 7a 1d fd fd 6b 75 fd 79 49 fd 69 18 1f fd 54 fd fd fd fd 4e 0d fd 2d 47 55 3f fd 69 6e fd fd fd 52 0a 4b fd fd c5 fd 14 08 50 fd 78 39 fd 51 58 42 01 78 33 fd 1d fd fd 03 33 fd fd fd fd fd fd 3c fd 59 04 1b fd fd fd 7f 5b 0f 57 fd 6a 18 58 6c 4d 57 41 7b fd 66 7a 66 fd 36 fd fd fd 47 26 fd 3e fd 03 fd 06 4b 4c 60 55 fd fd 7a fd fd 39 fd fd	^mJ0- IKYZ%.T~pDLm90}AvAt K]':dqn\$-]`g3!5tqD!r\$KN!RSwyfTzk uyliTN-GU? inRKPx9QXBx33<Y[WjXl MWA{fzf6G&>KL`Uz9	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Google\Update\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ v _ _ _ _ v L / / _ _ _ _ v . ` ' _ _ \ _ _ _ \ \ v v L / / \ / \ \ _ / \ _ _ \ _ _ \ _ _ \ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\pss10r.chm	14598	524	fd 4e 70 fd fd 0a 5d 00 fd fd 2c fd 62 21 31 24 fd fd 0a 09 fd 39 fd fd 10 75 fd fd 6f fd 05 3d fd 5f fd 7f fd 74 fd 27 3e 42 fd 75 22 03 75 fd fd 18 43 fd fd fd 64 43 75 37 0b 01 fd 5d fd 44 26 fd 3a 6d 46 1f 60 6c fd 28 06 54 57 42 fd 25 fd 6c 1d 0a 74 fd 37 fd 62 fd 22 19 26 79 4f 23 fd 0a 7e fd 7e fd fd 94 0c fd fd 11 10 2d 2f fd 49 08 fd fd fd fd 0f 46 6f 18 fd fd 07 fd fd 1b fd fd 56 7e fd c9 fd 66 54 fd 27 e4 fd fd 14 78 15 16 fd fd fd 76 17 fd 67 49 46 fd fd 48 21 64 fd fd 31 10 73 fd 5c fd 14 5d 65 58 fd 5d fd 36 17 19 fd 55 39 23 fd 33 fd fd fd 6f fd bb fd fd 60 fd fd 40 fd 57 fd 68 fd fd 1d 7e 10 39 52 fd 3c 05 fd fd 65 fd 25 22 fd 1e fd fd fd 6b 32 fd 12 65 fd fd 4d 1a 76 38 54 fd 26 03 5a fd 3b 4d fd 2a 1c	Np],b1\$9uo=_t'>Bu"uCd Cu7]D&.m F'!(TWB%lt7b"&yO#~-- /IFoV~fT"x vgIFH!d1s]eX]6U9#3`@ Wh~9R<e%"k eMvT&Z;M*	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\pss10r.chm	15122	10	24 00 06 39 00 00 00 00 00 00	\$9	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\pss10r.chm	0	14598	fd 10 77 2f fd 2a e1 fd fd 4f 06 fd 14 33 fd 5f 1f 44 fd fd 0e fd 3a fd 4e 47 fd fd fd fd fd 2b 4d fd fd fd 33 6c 0d 0d 26 5e 0b 09 6d 1d fd 00 27 fd eb fd fd 54 5c 4c fd 25 fd 0a 06 fd 5a 5d fd fd 2a 44 41 7e fd fd fd 53 6d 61 fd 13 0d fd 45 fd 04 fd fd fd 2d fd 33 7f fd 45 fd 6f 54 fd 61 fd 15 fd 46 fd fd fd 70 0f fd 33 36 08 13 fd 23 3c 7c 1c 3a 43 fd fd fd fd 09 fd 5c fd b6 07 35 69 3b 1e aa fd 23 fd fd 34 fd fd 31 fd 72 15 1b 41 66 fd 72 fd 2a 2b 71 0d 40 28 47 fd 6d fd 6f fd 31 fd 6b fd fd 0c fd fd fd fd 21 fd fd fd 60 fd 56 77 6c fd 33 5b fd fd 3d 7b 53 fd fd fd fd 61 3e fd 0b 67 33 fd 6f 44 fd fd 0a 7a 3b 5f 0e 55 fd 0b 6d 50 29 fd 14 6a 65 fd 3d 7c 32 74 49 fd fd fd 50 30 fd fd fd 0b fd 1e 27 fd fd 64	/*O3_DNG+M3l&^m^m\TLZ]*DA~SmE-3EoTaFp36# <:C\5i;#41rAfr*+q@(Gm o1k!`Vwl3[= {Sa>g3oD;_UmP)je= t IP0'd	success or wait	1	F2C055	WriteFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\setup.chm	82790	524	fd 7d 68 fd 47 77 7a 75 fd 0b 36 16 3e 2f 4e 79 fd fd fd 15 72 fd fd 4d fd fd fd fd fd 77 7c 40 00 64 fd fd 2e fd fd 06 fd fd 46 fd 5a 54 fd 38 7c 46 fd 06 fd 26 19 61 19 fd 7f 2d fd 24 fd fd 7f fd fd 27 4f 00 fd fd fd ed fd fd 5d 41 12 fd fd 1a 32 35 66 fd fd 69 fd 70 fd fd 77 79 37 fd 2a fd 5f fd fd 1d 26 7c 72 5b fd fd fd fd 6e fd fd 46 54 fd 23 00 fd 73 fd fd 63 36 41 fd 00 01 fd 0d fd fd fd 63 0b 00 fd fd fd 7b 3b fd fd 1e fd fd fd fd 27 7e fd fd 52 fd 5b cc fd fd 48 fd 52 fd fd fd fd 33 fd 5d 79 16 fd fd 61 fd 55 fd 10 fd 32 fd 11 5b fd fd 5b fd 2a fd 0f 4b 6e fd 6e 4d 23 fd fd 51 09 63 fd 15 fd fd 76 fd fd 09 44 fd fd 78 fd fd fd 6e 27 1a fd 14 15 fd 6e 18 fd 26 42 66 09 fd fd fd 78 fd 10 fd fd fd fd 1f 60 fd fd 24 6c	}hGwzu6>/NyrMw @d.FZ T8]F&a-\$O] A25fipwy7*_{r[nFT#sc6 Ac{;~R{H R3]a2[["KnnM#cvDxn'n& Bfx`\$l	success or wait	1	F2CBF8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\setup.chm	83314	10	24 00 66 43 01 00 00 00 00 00	\$fC	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\setup.chm	0	82790	fd 6e 4c fd 2f 3f fd 39 03 fd fd fd 69 fd fd 61 22 46 fd 15 fd fd fd 59 3d fd 25 44 23 28 fd 10 fd 2e fd 53 64 fd fd fd 7e fd 7a fd 04 fd fd 16 fd fd 2c 24 5b 4d fd 30 fd fd fd 08 fd 17 fd fd 08 53 fd fd 3d fd 1e 65 fd fd 09 68 fd 1d 7c 78 35 61 1e fd 27 1b 23 10 1f fd fd 55 02 55 4e 7f fd 0f 35 fd 3f fd 2d fd 19 08 fd 32 3b fd 2c fd fd 55 fd 51 76 fd fd f4 2a 5a 14 fd fd 0a 27 fd fd 3e fd 5a 5c fd fd 80 fd fd fd fd 2e fd 52 fd fd 4f fd 55 48 fd fd fd 22 2c 26 50 fd fd 13 fd fd 6e fd fd 1c fd 60 fd 71 0b 4a fd fd 66 58 2e fd fd fd fd fd fd fd 3d 12 33 2f fd 47 08 2f fd fd 6c 86 4d fd fd fd 3b fd fd 5c 0e fd fd fd 57 fd fd fd 6b 24 20 fd 40 fd 3d fd 37 42 22 fd 46 6d 3e 19 fd fd 78 68 44 48 fd 57 28 fd fd 34 03 75	L/?9ia"FY=%D# (.Sd~z,\$[M0S=eh x 5a#UUN5?- 2:,UQ*Z'>Z.ROUH",&Pn `qfX.=3/G/IM;Wk\$ @=7B"Fm>xDHW(4u	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Internet Explorer\en-US\I3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ v _ _ _ _ _ / / _ _ _ _ . ` _ _ \ _ _ \ \ \ _ / \ _ / \ _ / \ _ \ _ ^ _ ^ _ ^ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\Setup.xml	8483	524	68 3f fd 02 0f fd 58 75 11 44 fd 6a fd fd 72 fd fd 5a fd fd 4a 7f 1f fd 4e 0c 4e fd 5f 7e 39 5c fd fd 14 fd fd fd fd 10 6e 20 fd 50 4c 00 fd 3c 51 fd 4a fd 14 39 fd fd fd 48 0c fd fd 15 fd 1e fd 43 4c fd 65 fd 04 fd 57 61 75 19 60 fd 3c 0e fd fd 03 5b fd 58 fd 66 fd fd fd 30 fd fd fd fd fd 67 20 fd 4d 33 0e 20 fd 15 15 fd 43 26 fd fd fd 2f 74 fd fd 16 70 69 fd fd 37 6d 46 7b 41 78 6b fd fd 5d fd fd 51 28 17 21 73 fd 1b fd fd 06 4d fd fd 2e fd fd fd 51 fd 1c 7b 7e fd 64 fd 53 fd fd fd fd fd 70 96 36 fd 6a fd 73 fd 3a fd fd 41 fd 3e 42 42 33 fd fd fd fd 76 4d 2f fd fd 0f 6b fd 30 fd 46 15 fd fd fd fd fd 1b 2d 76 fd fd 6f 08 6b fd 7f 06 fd 44 7d 49 01 5f fd 20 45 4c 19 fd 09 fd 5b 4b 6a fd fd fd 11 0e fd 25 05 58 1a 05 fd fd 5f 1f	h?XuDjrZJNN_~9\ln PL<QJ9HCLeWau`<[Xf0g M3 &/tpi7F{Axk}Q(!sM.Q {-dSp6js:A>BB3vM/k0F-vokD)}_ EL[Kj}%X_	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\Setup.xml	9007	10	24 00 23 21 00 00 00 00 00 00	\$#!	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\Setup.xml	0	8483	fd 06 37 fd c9 37 fd fd 35 fd fd fd fd fd 07 00 fd 38 fd fd fd fd fd fd 3b 79 3c 3a 01 fd fd fd fd 7c 0c 2a 7b fd 03 fd 6a fd 32 4e 17 fd ac fd 66 fd 6a 72 fd 77 91 7c fd 22 fd 76 56 fd 27 20 7c fd fd 14 fd 37 6b fd 78 42 02 fd 70 fd fd fd fd 1e 19 5a 29 36 fd fd 0d 63 fd fd 62 fd 62 fd 41 fd fd 62 c6 6e fd a5 fd 5c 45 6b 07 4c 15 6d fd 48 73 73 fd fd 6f fd 6a 44 2c 70 fd fd fd fd fd 11 38 fd fd 13 64 6d fd fd 0c 5f fd fd 52 43 14 50 fd fd fd 99 62 fd fd fd 64 fd 18 19 fd fd 69 fd fd fd 54 fd 52 3e fd 23 5d fd fd fd fd 67 5c fd 46 fd 5a 66 fd fd fd fd 6c 3b 0e 42 19 2a 4c 26 fd fd fd fd 12 7a fd fd fd fd 39 50 3f fd fd 38 fd 76 fd fd 51 4b fd 54 fd fd fd fd 65 58 64 1a fd fd 10 54 fd fd 68 fd fd	758;y<:]* [j2NfjrwjvV']7kxBpZ)6 cbbAbn\kLmHssojD,p8dm_RCPbdiTR >#j]g\FZfI;B*L&z9P? 8vQKTeXdTh	success or wait	1	F2C055	WriteFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\ShellUI.MST	10752	524	fd 09 42 41 32 fd fd 64 79 fd fd 2f 61 fd 19 20 fd 1d 2a fd fd 6e 16 1b 1e fd fd 59 fd fd 64 08 fd 7c 3d 0e 2f fd 11 fd fd 50 63 2b 17 fd 4a 2b 39 5f fd 78 1c fd fd fd 53 c5 79 5c fd fd 6a 4d fd fd 19 44 1f fd 20 69 06 30 4f fd 1c 1d 32 37 65 fd fd 37 fd fd fd 06 fd fd fd fd 5a 28 76 23 fd 40 fd fd 7c 02 fd fd 04 00 59 fd 70 07 43 5b 03 1f 40 2c fd fd 14 fd 45 02 fd 7e fd fd 2d 3c 49 28 76 06 40 fd 06 fd 47 7f fd 09 4a fd fd 2c fd 25 49 01 fd 51 fd 10 fd 3f fd fd 0c 5b 12 44 f9 0a 2b fd 3c fd 7e 07 fd fd 78 fd 6b 37 fd 54 57 fd 30 7d 7f 2f 50 fd fd 6f fd 5c fd 1c fd 69 fd 5c 6d 68 fd 62 2a fd 65 01 77 fd 68 28 fd 34 fd fd 1d fd 15 34 fd 61 9d fd fd 58 4d 14 fd 6f 03 fd 00 fd 8b fd 58 26 fd a2 7e fd fd 22 0a fd 39 fd fd 64	BA2dy/a *nYd =/Pc+J+9_xSy ojM D i0O27e7(v#@ YC[(@,E~-<l(v@G,%lQ?[D+ <~xk7TW0j/Pol\mhnb*ew h(44aXMo&~"9d	success or wait	1	F2CBF8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\ShellUI.MST	11276	10	24 00 00 2a 00 00 00 00 00 00	\$*	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\ShellUI.MST	0	10752	3c 06 fd 35 fd 15 fd 5c fd 47 fd fd 42 fd 71 39 55 5d 03 38 57 02 fd 36 fd fd fd 0a fd 4f fd fd 66 fd 15 fd 65 0b 37 fd fd 18 3d 6e 39 76 59 fd fd 17 16 fd 75 36 41 48 fd 63 7c 17 0a fd fd 07 2c 42 63 6e 54 46 66 38 fd fd fd 7a 32 25 5b fd fd 1f fd 5d 68 02 fd fd 75 66 56 7e fd 64 fd fd fd 79 71 71 fd 0a 64 fd 6e fd 1c 13 fd 0b fd fd 75 fd 59 56 fd 32 7f 79 fd 77 fd 77 fd 27 fd fd fd fd fd 64 6a fd fd 08 7d 39 fd fd 2e 7c fd 13 30 d9 fd 46 02 fd 6a 79 66 4f 01 5a 62 fd 50 fd 22 fd 1f fd 72 77 fd 01 fd 6e fd 2b 11 fd 0e 7c 1b fd 70 fd 5d fd 72 fd 47 fd 72 fd 6f fd fd fd 0c fd fd 19 6c 06 67 01 fd 32 70 fd fd fd 15 30 32 3b fd 0d fd fd 1b 22 6a 4f fd 74 fd 24 74 25 fd fd fd fd 62 fd fd 49 fd 6c 29 22 53 53	<5\GB9U]8W6Of7=n9vYu6AHc[,BcnTFf8z2[]hufV~dyqqdnuYV2yww'dj}9. 0FjfOZbPrwn+[p]rGrolg2p02;"jOt\$%bll)"SS	success or wait	1	F2C055	WriteFile
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUI.xml	1910	524	fd fd fd 02 fd 15 42 fd 63 64 fd fd fd 6b fd fd 3c 52 1b 29 45 63 0b 22 77 10 1a fd 26 fd fd 3c 6d fd fd fd fd fd fd 3d 3d fd 2a fd fd fd fd 13 01 79 19 54 34 fd fd fd fd fd fd 0c fd 6f fd 25 fd 4f fd 2b 47 50 7c 3e fd 04 fd fd 6e fd fd 7b 3d 64 fd fd fd 7c 4c fd 62 fd 79 fd 40 fd 6d fd 2a fd fd fd fd 31 36 11 fd 63 4a 2a fd fd 0f 6e fd fd 1c 1d 77 6d fd fd fd 6d fd fd fd 61 52 fd 79 1a 48 fd fd 28 fd fd 1b 17 fd 16 fd 15 53 07 60 22 fd ae db fd 0d 23 fd 19 fd fd 71 fd 10 fd 54 fd 73 32 fd 41 fd 14 fd 1a fd fd fd 64 fd 14 14 fd fd 6f fd 10 fd 37 00 fd fd 1b 0e fd fd 1c fd 32 fd fd 33 26 06 77 11 12 0b fd fd 63 1b fd 7a 4c fd fd fd fd 65 7f ff fd 05 45 39 fd 76 70 4f fd 87 64 44 7d 3f 6a fd fd 08 54 fd fd 11 7b	Bcdk<R)Ec"w&<m==*yT4o%O+GP >n{=d Lby@m*16cJ*nwmmaRyH(S""#qs2Ado723&wczLeE9vpOdD}?)T{	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUI.xml	2434	10	24 00 76 07 00 00 00 00 00 00	\$v	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUI.xml	0	1910	6e 27 7c 66 fd 21 fd 64 0b 37 75 fd 73 49 2c fd fd 45 fd 6f 79 fd 42 fd fd 74 fd fd fd 0e 53 6a 7b 06 2a fd fd 66 fd 7e 26 fd fd fd 58 fd fd 66 fd 02 0e 44 fd fd 09 fd 3f fd fd 79 4e 34 7b c4 fd fd fd fd 03 fd fd fd fd fd 1a 41 35 fd 58 fd fd 43 fd 4c fd 36 7a fd fd 29 fd fd fd 15 19 fd 08 73 fd 26 7b fd 81 21 7f fd 6b fd fd 14 2d 62 0c 61 40 50 7b 08 41 29 19 7e 7c 40 38 fd fd fd 2d fd 19 44 fd 68 fd 21 fd 24 fd fd 44 66 fd 37 fd 2b 31 21 fd fd 3c fd fd fd fd 41 52 fd 08 fd fd 5a 2c fd 36 fd fd fd 05 fd 25 fd 2f 49 fd fd 79 fd fd 5f 06 fd eb 37 46 68 5e 45 2d 36 fd 68 0f 6d 5a fd 2c fd 1d fd 05 fd 14 61 fd 7d fd 05 53 fd 2f 7d 06 fd 45 fd 00 fd 11 77 fd fd fd fd fd 25 51 5e 60 fd fd 03 fd 2b 3f fd 23 fd 0d 22 77 74 1c	' fd7usl,EoyBtSj{"f-&XfD ?yN4{A5XCL6z)s&{lk- ba@P{A}- @8Dh!\$D f7+1!<ARZ,6%/l_7Fh^E- 6hmZ,a)S/)Ew%Q^^+? #"wt	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Internet Explorer\images\IR3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 5f 2f 5c 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ v _ _ _ _ v L // _ _ L _ \ . ' _ _ \ _ _ \ \ v v L // \ _ \ \ _ / \ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUISet.xml	1036	524	fd 0e 6d 54 fd 2c 36 0d b8 fd 44 fd fd 4d 6e fd fd 12 3f fd d9 fd 52 06 fd fd fd fd 5e fd 50 56 35 fd fd 05 60 19 42 53 04 fd 20 04 fd 39 68 fd 19 fd 7b fd 6c fd fd fd fd 25 fd 39 16 fd 39 08 fd 6f 56 fd fd 21 fd 6d 7e fd fd 67 fd 43 fd 27 00 76 47 fd 0e fd 17 fd fd 78 6d 07 4c fd 5e 41 fd 45 65 63 fd 37 64 fd fd fd fd 22 fd 02 33 17 77 05 1b d6 fd 5d fd fd 11 fd 6a fd fd 26 fd 47 fd 65 48 34 50 fd 40 fd fd 51 72 fd 1b 15 fd 75 fd fd 34 7c 00 fd fd fd 42 fd fd 08 10 fd 53 20 fd 4b fd ed fd fd 56 fd fd 63 45 60 fd 42 39 0c fd 3c 01 fd 8b 79 90 6e fd 02 24 21 4e 64 fd 1c 69 5e 08 24 fd 62 5a 5d 1e fd 67 fd 74 2d 53 fd 18 fd fd 47 67 fd 5c 7a 12 44 fd 18 31 fd 01 40 18 fd 1f 61 3f 41 fd fd 68 fd 71 fd fd 33 fd 64 4c fd 70 62 2e fd 5e	mT,6DMn?R^PV5`BS 9h{!%99oV!m~g C^vGxmL^AEec7d"3w]j& GeH4P@Qru4 BS KVcE`B9<yn\$!Ndi^\$bZ]gt -SGglzD1@a? Ahq3dLpb.^	success or wait	1	F2CBF8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUISet.xml	1560	10	24 00 0c 04 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUISet.xml	0	1036	fd 6f fd 10 75 2e 11 74 fd fd 2c 0f 1c 75 20 12 fd 06 7b 0b 2b fd 65 fd 5a fd 5b 5a fd fd 2d fd fd 6b fd 32 0f 1c fd 3d fd fd 11 fd fd 09 fd fd fd 50 fd 23 41 fd 69 56 57 fd 5c 11 fd fd 15 fd fd 07 26 10 fd 1f 24 fd 5e 59 fd 6a fd fd fd 76 48 4d 2a fd fd 77 fd fd fd fd 4e 12 fd fd 3e fd fd fd 64 fd 64 fd fd 7d 2f fd 04 fd 58 fd fd 1a 65 20 24 14 29 21 fd 3b 4e 26 fd fd fd 45 36 fd 3f 63 16 fd 24 fd 40 fd 59 09 3e fd 12 6b fd fd 6d fd 35 fd 3f fd 17 6a fd fd fd fd fd 2e 67 68 fd 01 fd 53 fd 42 4b fd 6d fd fd fd fd fd fd 05 06 28 fd 01 fd 0a 78 fd 49 4d fd fd 7a 66 fd 01 39 fd fd 34 fd 4e 22 fd fd 36 61 52 fd fd 32 fd fd fd 7d 55 a6 fd 79 70 50 fd fd 22 fd 5f 53 77 fd 7c 09 fd fd 16 fd fd 77 1c fd fd fd 79 fd 41 fd 15 fd 64 10 fd	ou.t,u {+eZ[Z- k=#AivW&\$^YjvHM *wN>ddj)/Xe \$!;N&E6? c\$@Y>km5?j. ghSBKm(xlMzf94N"6aR2 }UypP" _Sw wyAd	success or wait	1	F2C055	WriteFile
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\OWOW64LR.cab	2060457	524	fd fd fd fd 16 fd 40 fd 36 fd 1b 65 00 fd fd 52 43 fd fd 6e 5d fd 5b 30 7d fd 1c 5a 2a fd 4c fd fd 49 fd 35 fd 17 5d 2c 71 51 fd fd 33 67 fd fd 4d 75 10 37 fd fd 43 45 fd 25 fd 4f 5e fd 43 fd fd 55 3a fd 6a 4a 58 fd fd 7c fd fd 23 6c 31 21 65 53 fd 6b fd fd 65 fd 09 17 fd fd fd fd fd 13 fd fd fd 30 fd 40 6e fd fd fd 68 4d 5c 73 44 59 07 fd 00 5c fd 2f 88 fd fd 0d 4a fd 6d fd 61 1b fd fd 37 6c 6d fd ec fd 3f 55 fd fd 17 fd 1f fd 42 fd fd fd 59 fd fd fd bd 10 fd 3a 20 fd 7c 57 fd 7c 21 fd 4b fd 38 40 29 fd fd fd 77 0e 7a 1d 31 fd 42 fd fd 2d fd 82 fd 20 78 fd 7e fd 37 fd 25 fd fd fd 5a fd 77 fd 6d fd fd 4c 15 63 fd 0b fd 2b fd 64 42 fd fd 3d fd 61 fd 2b fd fd fd fd fd fd 02 1f 3b 74 59 fd fd fd fd 5a fd fd 45 14 fd 01 56	@6eRCn] [0]Z*L!5],qQ3gMu7CE% O^C U;jjX #11eSke0@nhM\s DYVJmalm?UBY: Wj!K8@)wz1B- x~7%ZwmLc+dB =a+;tYZEV	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\OWOW64LR.cab	2060981	10	26 00 fd 70 1f 00 00 00 00 00 00	&p	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\OWOW64LR.cab	0	1048576	fd 2f 6d 5d 14 28 62 7a 19 fd fd fd fd 26 0c fd fd 39 fd 2b 71 03 39 0f fd 33 33 75 15 1b 4b fd fd fd fd 09 fd 17 76 fd 67 fd fd 5f fd 36 fd 2f fd fd 69 fd fd fd fd fd fd 29 79 21 fd 57 73 31 fd 57 fd 16 fd 49 fd fd fd 3a fd 55 fd 45 57 12 fd 50 5f 12 33 fd fd fd fd fd 0c 30 65 fd fd fd 26 4c 10 fd 2c fd 43 fd fd 0e 13 60 fd fd fd 01 79 26 fd 35 fd 1c fd 30 63 fd 6d 28 41 2e 04 fd fd 10 21 fd 45 0f fd 4f 0f 55 0d fd 7e fd 2a 17 fd 62 47 fd 10 fd 47 fd fd 2b fd 74 3b fd fd fd 3e 70 fd fd 48 fd fd fd fd 52 22 5e fd fd fd 5e 5a 59 fd fd 20 fd fd 24 fd 07 fd fd 4c 39 fd 5a fd fd 12 1f fd fd 18 fd 4c fd 36 17 fd 79 0d 36 fd 67 fd 77 fd 20 3f fd 5a fd 50 54 56 fd 19 fd fd 61 14 fd 09 22 fd fd 2d 57 4e fd fd 6b fd fd 4e 0a 01 fd fd 53 58 57 69	/m(bz&9+q933uKvg_6/i)jy !Ws1Wl:U EWP_30e&L,C'y&50cm(A.!EOU~*bGG +t;>pHR"^ZY \$L9ZL6y6w ?ZPTVa"-WNkNSXWi	success or wait	1	F2C055	WriteFile
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Setup.xml	3122	524	1d 32 22 21 fd fd 5e dc 21 fd fd 77 4c fd fd fd 25 5d fd 37 6e 25 5b 7e 54 fd fd 46 fd 1c 82 29 69 fd fd 42 fd d6 fd fd fd fd 52 fd fd fd fd 4c 5c 5d fd 2d 5b 1f 2c fd 72 fd de 2c 69 3e fd 0d fd 5b 24 fd 73 6d 73 fd 48 78 fd 71 fd fd 3f 04 46 fd fd 31 6e 21 0b fd fd fd fd 57 0f 63 40 53 45 55 fd fd 74 6c 09 fd 22 fd fd 70 fd 01 fd 55 fd 67 62 02 3d fd 4d fd fd fd fd 58 fd 1e 53 21 fd fd 40 fd fd fd 3b 04 62 fd 66 fd fd 6a fd 6c fd 2c 4d 51 63 0b fd fd 70 4b 48 35 fd 66 1e fd 1b 69 83 64 51 3d 0a fd 00 fd 03 7d fd fd fd fd fd fd fd 12 fd fd fd 1c fd 63 4a fd fd fd fd fd 37 45 65 fd 5e 5a fd 4f fd fd fd fd fd fd 73 56 36 fd 0b fd 0e 32 fd 5f 3f fd fd 59 72 fd 09 22 fd fd 23 79 0a fd 4b fd fd fd 10 fd 34 74 59	2"!^!wL%)7n% [-TF)iBRL\]-[,r,i> [\$smsHxq? F1n!Wc@SEUtl"pUgb=M XS !@bfj!MQcpKH5fdQ=}cJ 7Ee^ZOsv2_?Yr"#yK4tY	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Setup.xml	3646	10	24 00 32 0c 00 00 00 00 00 00	\$2	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Setup.xml	0	3122	2b 45 3d fd fd 52 fd 24 fd fd 75 74 29 fd 42 0e 2b fd 44 fd 68 fd 0c 03 3a 5c 5d fd 56 fd 6d 48 fd 79 1f fd fd fd 17 45 fd 0c 1e 71 02 53 fd 4d fd 2d 65 fd 1b fd 0a 21 63 5c fd fd fd 29 29 fd fd 16 19 41 5e fd fd 21 38 0f 44 02 fd 33 fd fd 0d fd fd 37 fd 35 fd 64 fd 33 44 18 fd fd fd 3c 16 45 fd 14 fd 31 25 61 2d 74 25 fd 7c fd 1f 18 ce fd 49 fd fd fd 41 4e 2e 16 fd 44 09 58 04 3b 46 7e 57 25 1a fd fd 3f 14 4f fd fd 5f d9 d3 fd 60 2b 4d fd 7b 0c 28 7f 4c fd 23 fd 23 fd fd fd 33 3a fd fd fd 6e fd fd 72 12 fd 2e 78 fd fd 6e 05 fd fd 1d 64 fd fd 0f 61 0b 5f 38 fd fd 20 fd 5a 30 fd 40 5a fd 3e fd 48 41 23 fd fd fd 29 fd 50 12 52 fd 06 4d 43 fd 51 01 55 fd 56 fd 1a 78 07 fd fd 02 33 49 1a 78 fd 77 16 72 fd fd 6b fd 19 fd 1a 6b fd fd fd	+E=R\$ut)B+D:\jVmHyEq SM-elc))A ^!8D375d3D<E1%a- t% AN.DX;F~W%? O_`+M{((L##3:nr.xnda_8 Z0@Z>HA #)PRMCQUVxlxwrkk	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Internet Explorer\SIGNUP\IR3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \\\ _ _ V _ _ _ _ \ _ / / _ _ _ _ \ . ` _ _ \ _ _ _ \ \ _ _ / \ _ / \ _ / \ _ _ \ _ _ \ _ _ \ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\MSOCache\All Users\{90160000-0117-0409-0000-00000000FF1CE}-C\AccessMUISet.xml	1032	524	25 7d fd fd fd 2c fd 54 fd 2a fd 0c 61 04 26 fd ab 31 fd 4a 6b 7c 0d fd fd 0c fd fd 38 fd 77 fd 62 6f fd 4e 34 06 50 fd 23 fd 0d fd 51 6c fd fd 5d 38 fd fd fd 09 fd fd 24 fd 2e 2c fd 1c fd 63 fd 2b 45 fd fd fd 7b 42 0c fd fd 37 49 fd fd 39 2a 06 5d fd 74 4d b1 03 61 fd 30 18 61 5c 74 55 61 4b fd fd fd 3f fd fd 67 68 6f 45 fd fd 49 2a fd 36 b8 11 fd 59 4a 31 fd 71 13 53 3d fd 42 19 5c 47 ca fd 11 0b 28 fd 3b fd fd fd 80 fd 48 fd fd 2c fd fd fd fd 73 55 08 fd 1c fd 29 fd fd 4a 42 13 fd fd 1a fd 61 fd 83 7f 70 3b 00 60 fd 12 7e df 45 59 fd 76 72 6d fd 48 fd fd 2b fd fd 1a 39 79 fd 23 fd fd 58 0a 05 fd 0c 12 fd 4a fd 3e fd 68 3f 51 53 fd fd fd 05 fd 4b 2a 32 fd 39 6b 23 6d fd 2c fd 08 fd 03 fd 69 fd fd 2e fd 36 fd fd 16 5d	%,Ta&1Jk 8wboN4P#Q] 8\$.c+EB7I 9*)tMa0a!tUaK? ghoEI*6YJ1qS=B\G (;H,sU)JBap;`~EYvmH+ 9y#XJ>h?Q SK*29k#m,i.6j	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-0117-0409-0000-00000000FF1CE}-C\AccessMUISet.xml	1556	10	24 00 08 04 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-0117-0409-0000-00000000FF1CE}-C\AccessMUISet.xml	0	1032	fd 49 fd 22 6e 4a fd 57 39 fd fd 71 02 fd fd 1d fd 58 67 fd 2b 34 25 fd fd fd 4b fd 74 62 fd fd 0f fd 66 7b 01 70 79 70 fd 4a 68 50 29 3f 64 fd 2e fd 4c fd fd 25 70 fd 38 fd fd fd e4 4e fd fd 15 58 fd 74 3d 40 60 fd 48 fd 17 fd 15 11 5d fd 3c fd 63 07 fd fd 35 5c fd fd fd 30 14 fd fd 1b 57 fd 28 33 46 3c 06 46 25 27 fd fd 4f 57 73 53 fd 5f 53 73 fd 19 32 46 0a fd 1c fd fd 4c fd 37 66 fd 68 fd 5a 33 62 27 2d fd fd 22 fd 1f 6b 5a 30 1d 37 1b fd fd fd fd 2f 4b fd 51 fd fd fd 3b fd fd fd 69 fd 7c fd fd 5f fd fd 57 fd 2d 70 fd fd 68 fd fd 72 1d fd 14 fd fd fd 5f fd fd fd 38 fd fd cc fd 7d fd 3b 76 fd fd 15 4c 3c 4e 1a 7d fd fd 18 11 fd fd 25 35 fd 68 fd 1f 0b c2 00 1e fd 74 fd fd 24 fd fd 44 3e 02 51 fd fd fd fd 7b 41	InJW9qXg+4%Ktbf{pyph P)?d.L%p8NXt=@`H] <c5\0W3F<F%WS_Ss2F L7fhZb'~"kZ07/KQ:ij_W- phr_};vL<N}%5ht\$D>Q{A	success or wait	1	F2C055	WriteFile
C:\MSOCache\All Users\{90160000-0117-0409-0000-00000000FF1CE}-C\Setup.xml	2584	524	2e 3b fd 6a 6b fd 5b 61 fd 7a 2e 7a fd fd fd fd 1c 2f fd 3b 0f 06 65 fd 4f 42 fd fd fd fd 7c fd 73 7b fd 6d fd fd fd fd 49 fd 42 ac fd fd fd 13 fd 23 fd fd 32 12 fd 78 fd 4c fd 64 56 fd fd fd fd fd fd 1e 28 fd fd 39 fd fd fd fd 3c fd 74 38 46 fd fd fd fd 21 64 10 40 2f fd 3f 28 fd fd 5c 69 5d 09 fd fd 0f fd 38 5f 0f 47 72 fd 2c fd 55 fd 16 18 fd 22 fd 16 5e fd 6d 4b 06 fd 24 fd 7e fd bd fd 2a 73 71 2d fd fd 10 14 fd 6d 5a fd 12 2b fd 5b 7a 2b 0d 7c 22 fd fd fd 6b fd 32 4d 48 fd 67 4a fd 25 13 6d 30 fd fd fd cf 25 fd 0d 1e fd 66 fd 5a fd 5f 52 76 fd 22 6a 22 57 fd fd fd 59 fd 4f fd 50 6f 5c fd fd fd 39 fd 5c fd 4d 54 fd 36 fd fd 22 fd 7d 7e fd 08 fd 10 52 fd fd 35 fd fd fd 31 fd fd fd 08 41 fd 3b fd 68 48 28 fd fd 45 fd 34 29 fd fd 3c	.;jk[az.z;eOB]s{mlB#2LdV m(9<18FId@/? (ij8_Gr,U"^mK\$~*sq-m+ [z + '"k2MHgJ%mo0%fZ_Rv"] "WYOPo\9IM T6")~R51A;hH(E4)<	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-0117-0409-0000-00000000FF1CE}-C\Setup.xml	3108	10	24 00 18 0a 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-0117-0409-0000-00000000FF1CE}-C\Setup.xml	0	2584	fd 56 73 40 7b 41 fd fd fd fd 35 6f 39 fd fd 21 27 1c fd 3b fd 2e fd 1d 3d fd fd fd fd fd fd 57 3f fd 28 fd fd 5d fd fd 53 fd fd 74 fd 3d 5c fd fd 51 33 65 64 13 5f fd 39 55 fd 3a fd fd 51 fd fd 87 27 53 fd fd fd fd 75 76 46 37 1f 02 fd fd fd 6b 47 fd 6b fd fd 1c 28 3f 60 3d fd 4d fd fd fd 4d fd 59 fd fd fd 67 fd 46 fd 43 3d fd fd 26 fd 3d 30 02 0c fd fd 2f fd 55 fd fd 29 fd 55 fd 4a fd fd fd 6d 3f 47 fd fd 3b fd fd fd fd fd fd 3b 6e 31 fd 8d 0c fd 5d 25 3c 33 24 fd 5f fd 32 78 15 fd fd 1f 54 fd 57 75 fd fd fd fd 47 75 75 fd 6b 50 25 66 64 fd 6d 08 58 cd 6b fd 37 fd 54 76 03 fd fd fd fd 56 37 2e fd 1b 65 03 fd fd fd 7b fd 4d 3f 72 15 fd 2a 50 33 6e fd 7d 28 1b fd 15 48 79 4f fd fd fd fd 76 17 fd 2e fd fd 24 fd fd 70 fd 5a 26 7e fd	Vs@{A5o9!';=-W? (jSt=\Q3ed_9U:Q 'SuvF7kGk(? `=MMYgFC=&=0/U)UJm ?G;;n1]%% <3\$_2xTWuGuukP%fdm Xk7TvV7.e{M?r*P3n} (HyOv.\$pZ&~	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\LyncMUI.cab	2608606	524	23 1a 50 4f fd fd 01 32 fd 79 fd 2d fd fd fd 43 15 7c fd 39 28 34 fd 20 fd 4a fd 5c fd 2d 67 fd fd fd fd 71 1c fd 5c fd fd fd 2c 44 fd fd 2e fd fd 7f fd fd 7f 7b fd 07 fd 78 6c fd 07 fd 27 fd 68 fd 23 fd 67 65 13 38 4a fd fd 36 fd 8e 53 7e 3c fd 10 4a fd 21 6a fd 67 ee fd 7a fd 15 75 fd fd 3e fd 28 13 fd 4d 0f fd fd fd 3f 61 fd 57 7d 4d fd fd 32 46 63 fd 1c 79 0c fd 2d 65 29 08 3c fd fd 27 4e 71 fd fd fd 64 fd fd fd fd 07 fd 66 fd 5e fd 2d 5d 0a 39 fd 7d 36 72 fd 35 76 fd 00 5d fd fd fd 2c 7f fd 21 14 72 fd fd 06 71 fd fd 5b 21 8b fd fd 38 5d 38 fd fd fd 10 05 fd fd fd 09 fd 7b fd 63 fd 2b fd fd 2c 1d fd fd fd 0d fd 0c 2b fd fd 3d fd fd 07 5d 58 33 0f 45 5c 0b fd fd 1a 42 fd 60 fd 25 2c 23 fd 4e 7f 48 fd 6c 5a	#PO2y-C[94 J\-gq\,D. {xl'h#ge8J6~<Jljgzu(M? aW}MFcy-e)<'Nqdf-] 9}6r5vj].!rq[!8]8{c+,+=]X3 E\B`%,#NHIZ	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\LyncMUI.cab	2609130	10	26 00 fd fd 27 00 00 00 00 00	&'	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\LyncMUI.cab	0	1048576	fd 76 6c fd 51 21 67 57 24 fd 6e 13 fd fd fd 3a fd 6c b5 fd 1e 45 fd 56 44 fd 15 0b 69 fd 76 66 19 fd fd 30 7e 47 3c fd fd 7c 1f fd 28 fd 5f 4f 3c 0f fd fd 3a fd 08 6e fd 45 fd 77 76 74 04 fd fd fd 0e 47 41 57 25 73 43 6a fd fd 6f 49 fd 3d fd 20 fd 14 fd 4b 7c fd 76 fd fd fd 55 31 30 fd 39 fd fd fd fd 49 fd fd 4c 6e 4d fd 48 fd 53 fd 56 fd 79 3a 52 fd 04 fd fd 61 fd 1b 6e fd 2c fd fd 6e fd 4b fd 0c 64 fd 78 15 fd 7a 41 77 57 3c fd fd fd 56 fd fd 44 58 1f fd 40 c9 43 4b fd fd 07 37 fd 16 67 fd 60 43 79 fd 01 fd fd fd 37 7f fd 59 fd 1d fd fd fd 78 03 fd fd 4f 16 fd fd fd 7e fd fd fd fd fd fd 35 51 fd fd fd fd 84 fd fd 40 73 11 e3 5e fd fd fd 1e fd 53 39 78 fd 79 fd 5a 50 32 7a 38 27 fd fd 40 fd fd 27 fd 51 fd fd fd fd 5a	viQ!gW\$n:IEVDivf0~G<[(_O:nEwvtGAW%\$sCjol= K vU109ILnMHSVY:Ra, nKdzwW<VDX@CK7g`C y7YxO~5Q@s^S9 xyZP2z8'@QZ	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Java\jre1.8.0_211\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ _ _ _ \\ _ _ _ _ _ _ _ _ _ _ \\ / / / _ _ _ _ _ \ . ' _ _ _ _ _ \\ _ _ _ _ _ \ \ \ \ \ / / \ / \ \ _ / \ _ _ \ _ _ _ _ \ _ _ _ _ / By now it's probably painfully apparent that your environ- ment has been infected with r	success or wait	1	F358DF	WriteFile
C:\MSOCache\All Users\{90160000-012B-0409-0000-00000000FF1CE}-C\LyncMUI.xml	1227	524	4b fd 4d fd 7e fd 0e 6a fd fd 3d 6c fd 47 57 0f fd 6a 29 66 fd 6a 02 fd 1f 64 21 45 fd 31 fd 04 1d fd fd 3c fd 4c 39 05 fd fd 02 17 2b 51 52 3d fd fd 4e 16 fd fd 07 27 fd fd fd fd 10 7b 79 3e 10 fd fd fd fd fd fd 0b 3a fd 03 fd 43 12 0b 32 6d 7d fd 14 fd fd fd 6b fd 54 41 fd 50 fd 0d fd 67 4c fd fd 12 fd fd fd 6d fd 09 62 3d 58 32 79 fd fd 4a fd 4b fd fd 54 5c 25 73 2a fd fd fd 34 fd fd fd 2b 71 50 6a 13 fd 66 fd 65 3c 07 fd 00 fd fd fd 7f fd 59 fd fd 42 08 fd fd 69 1f 41 fd fd fd 69 4e fd 1b fd 2e 13 32 73 08 50 fd 6d fd fd fd fd fd 7f fd fd fd fd 79 fd 56 17 2e 2f 16 1c 7d fd 54 40 08 74 fd 6d 5f fd 58 fd 3e 6e fd 5f 59 67 6d fd fd 76 fd fd 7c fd fd fd fd fd fd 58 3a 7e fd fd fd 6b 35 0d 12 fd fd 7b fd 5d fd fd fd 29 fd 58	KMj=IGWj)fjd!E1<L9+QR =N'{y>:C2 m}kTAPgLmb=X2yJKTl% s*4+qPjfe<Y BiAiN.2sPmyV.}T@tm_X >n_Ygmv[X:~5{}}X	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-012B-0409-0000-00000000FF1CE}-C\LyncMUI.xml	1751	10	24 00 fd 04 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\LyncMUI.xml	0	1227	eb fd fd fd 31 55 78 fd 14 fd fd 1e 3d 78 fd 5b 41 fd 06 fd 7c 51 24 fd fd fd 57 fd 78 fd 35 fd 36 fd 6b fd 6b 04 fd 08 fd 66 53 63 fd 3c 04 fd 33 71 3d fd 73 fd 02 72 fd 4a 2b fd 2c 62 45 20 fd 44 6f fd fd 54 36 34 da 64 4a fd fd fd fd 6d fd 57 fd fd 5f fd 05 11 43 fd fd fd 0c 3b 2f 16 11 fd fd 53 5c 07 37 10 05 50 0c 47 fd 52 fd 5a 42 16 51 fd fd 41 2d 09 3e fd 2b 74 28 fd 2a fd 17 65 fd fd 62 73 1a fd 48 35 fd 08 7c 14 6b fd fd 56 77 43 fd 53 fd 4f 5c fd 6d fd 4d 3a fd 00 fd 2c 26 00 fd fd fd 6b fd 48 5c 0e fd 64 55 5c fd fd 58 fd fc fd fd fd 46 fd fd 29 6e 2c 4b 4a 78 2c fd fd 66 fd 21 fd fd 22 33 fd 56 2f 63 6e 7e fd fd fd 0b 4c fd fd fd 51 fd 06 04 5d fd 0d 31 2f 55 7c fd fd fd fd 28 35 62 1e	1Ux=x[A]Q\$Wx56kktSc< 3q=srJ.bE DoT64dJmW_C;/S\7PRZ BQA->+t(*eb sH5 kVwCSO\mM:,&kH\dd U\XF)n,KJx ,mfl!\"V/cn~LQ]1U (5b	success or wait	1	F2C055	WriteFile
C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\Setup.xml	1690	524	73 11 fd fd fd 46 fd fd fd 22 fd 22 fd 7a fd 21 78 3c 0c fd fd 79 68 06 12 25 23 fd 55 fd 33 fd 3f 71 fd 7e fd fd fd 26 fd fd 77 fd 48 fd 1d 0f 57 0f fd fd 28 fd 3f fd fd 64 16 fd 69 20 2b 02 fd 25 fd fd fd 7f fd fd fd 4e fd 17 42 fd fd fd fd 48 58 fd 5e 9b fd 73 60 43 54 70 78 3f 66 0f fd 15 fd fd 2f fd 77 58 43 fd fd fd 1e 63 fd fd 26 6e fd 56 62 56 fd 1c 78 fd fd 54 32 fd 3b 7b 10 58 fd fd fd 79 02 23 fd 32 fd fd fd 37 fd fd 0a fd 22 fd fd 35 fd 33 fd 3e fd fd 10 fd 2e fd 50 fd fd 7b fd 4d fd 40 fd 29 fd 65 fd fd 20 53 66 fd fd 65 70 fd 79 fd 3d fd fd 6b 34 fd fd fd 13 fd 0e 27 13 fd 65 fd fd fd 2c fd 02 4b 74 fd 09 fd 38 fd 6b fd 5f 6d fd fd 64 75 fd 01 fd 69 fd 10 fd 46 fd fd 6f fd fd fd fd 0f 1b fd fd 0f 6d fd 14 42 fd 21 33 fd 7f fd	s"!xyh%#U3? q~&wHW(?di +%NBHX^ s`CTpx? f/wXCc&nVbVxT2; {Xy#7"53>.P{M@)e fepy=k4'e,Kt8k_mdulFo mB!3	success or wait	1	F2CBF8	WriteFile
C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\Setup.xml	2214	10	24 00 fd 06 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\Setup.xml	0	1690	fd 22 79 fd 40 64 44 26 02 45 1b fd fd fd fd fd c7 fd fd 34 0e fd 19 39 4f 78 48 fd 2a 3b 5d fd fd 63 fd 37 58 fd fd e4 fd fd 30 42 3f 00 fd 15 77 0b 6d fd 00 fd fd fd fd 76 fd cc 4a fd 5e fd fd fd 33 fd fd 3c fd 3f fd fd 01 5d fd 14 fd 6e fd fd aa fd 5c 1b fd 5a 16 09 16 29 70 fd 58 27 5f fd fd fd 2a 72 76 fd fd 15 fd fd 27 6c 4b fd 56 fd 12 fd fd 23 64 fd 3a 4c 36 35 fd 69 fd fd 16 5b fd 79 7c 6d fd fd fd 69 19 10 6c 09 fd 03 57 fd 54 04 52 41 2a fd 22 fd 7a fd fd fd 0f fd fd 4f 57 fd 54 fd fd 4c 5e fd 58 fd fd fd 7a 43 fd 11 fd 07 6c fd fd 69 52 fd fd 0a 46 15 fd fd fd 38 fd fd 6d fd 5d 69 fd 37 fd 13 43 4c 7f 03 7f 47 fd 4e fd fd 36 29 fd 72 5a fd fd fd fd fd 57 fd 0e 65 fd fd 0b fd 1d fe fd fd fd 02 6d fd 38	"y@dD&E49OxH*:]c7X0? wmvJ^3<?)n {Z}pX'_*rIKV#d:L65[y mil WTRA* "zOWTL^XzCllRF8m]i7C LGN6)rZWem8	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\j\Downlo ader\config\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ v _ _ _ _ v _ / / _ _ _ _ v . ' _ _ \ _ _ _ \ \ v v _ / \ _ / \ _ / \ _ _ \ _ _ \ _ _ \ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\Program Files\internet expl orer\SIGNUP\install.ins	452	524	fd fd 0b 22 fd 4d 26 17 67 10 fd 08 06 fd fd 6a fd db 37 7d 6d 4e fd 49 fd 3f fd fd fd fd 3c fd fd fd 1a 50 fd fd fd fd 21 4f fd 55 fd 6d fd fd 18 fd fd 1c fd 29 fd 69 fd 04 52 fd 43 fd fd fd 8d 66 03 fd 78 fd 08 16 45 9c 0b fd fd fd 3f 61 37 fd fd fd 53 fd 54 13 45 fd 4e fd fd 58 79 62 79 fd 76 fd fd 05 fd 08 fd 7c 5c 31 3a 31 19 fd 14 7f 5b 70 2f fd 09 29 fd fd fd fd 56 7b fd fd fd 46 84 fd fd 5a 1d fd fd 4b fd fd 5f fd 6b fd fd 29 61 4e fd 57 fd fd fd f9 5c 29 fd 67 30 fd 21 fd 3a fd 79 fd fd 52 fd 69 fd fd aa 4a 3e ca 6e fd 49 fd 1f 78 fd 06 63 fd 64 47 fd fd 13 fd fd 7b 64 fd 16 7b 5b fd fd 35 fd 36 11 2c 3f fd 31 48 21 fd 1a 69 4f fd 35 fd 46 19 57 29 fd 7b 34 59 23 fd 67 fd fd 09 fd 6d fd fd fd 0c fd 39 4f 10	"M&gj)mNI? <PIOUm)iRCfxE? a7STEN Xybyv\ 1:1{p/)V{FZK_k)a NW})g0! :yRiJ>lcdG{d{[56,? 1H!!O5FW){4Y#gm9O	success or wait	1	F2CBF8	WriteFile
C:\Program Files\internet expl orer\SIGNUP\install.ins	976	10	24 00 fd 01 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\Program Files\internet expl orer\SIGNUP\install.ins	0	452	fd 42 01 4b fd fd fd 6b 38 45 fd 47 70 27 fd fd 6c 69 fd 14 fd fd 57 02 fd dd fd 6e d6 20 08 fd fd 05 0e fd fd fd 18 fd 72 3b fd 2b 61 e7 fd 6a fd 25 23 00 2b 3d 10 fd 6a 1d 23 fd fd 2d fd fd 57 fd 7f 03 fd fd fd 56 fd 2d 07 39 fd 5b 32 fd 2b 27 fd 0b 3b fd 09 fd 4c 78 fd fd 31 6e 3f 32 5a fd fd 7c fd fd 05 fd 7d 65 fd fd 61 35 fd 70 fd 26 2e 73 fd 15 5a fd fd 7b fd 1c 18 fd fd 2b fd fd 65 67 fd 60 fd 50 2d fd 45 fd fd fd 06 fd 5a 57 fd 07 fd 31 fd fd 30 fd fd f7 fd 27 fd 20 fd fd 39 29 1a fd fd 67 fd 54 46 38 7f fd 71 fd fd fd 33 fd 7c 72 fd 43 fd 0c 25 47 5c 24 fd 47 13 fd fd 65 3a fd fd fd fd 23 34 fd fd 21 fd 48 64 fd 61 fd fd fd 11 7e 17 70 6c 6d 07 fd 7e fd 50 fd 3e 30 fd 2b 22 fd 64 2b fd fd fd 06 fd 37 fd 73 7f	BKk8EGp"liWn r;+aj%#=#j#-WV-9[2 +';Lx1n? 2Z})ea5p&.sZ{+eg`P- EZW10' 9)gTF8q3 rC%G\\$\$Ge:#4! Hda-plm-P>0+"d+7s	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\Microsoft Office\Office16\Custom.propdesc	1343	524	fd 41 0b fd fd fd 7e 27 01 05 fd 6c fd fd 38 66 67 15 fd 49 fd d4 43 30 fd 72 25 fd 53 12 fd 49 fd 29 54 46 40 2e 2d 1e 78 fd 03 29 fd fd 5f 29 fd 1a 43 49 fd fd fd 43 65 15 6d fd 4a fd 5d fd fd fd 65 12 69 fd fd 38 11 fd 5a 3f 32 10 10 fd 7d fd fd fd 3c fd 30 fd 4c 68 53 72 fd 7c 0d fd 3c fd 28 5e 57 30 fd 0a 0e fd fd fd fd fd 03 fd fd 5e 0c 14 0d fd fd fd fd fd fd 37 fd 25 6c 27 36 fd fd 38 fd 34 fd 3c 2c 6b fd 6f fd 0e 61 fd 75 20 fd fd 0b fd 2e fd 25 12 fd fd fd 74 fd fd 2c fd 7d 5b 7a fd 7e fd 71 fd fd fd fd 03 fd fd fd 46 fd 0d fd 36 fd 49 96 58 fd fd fd 35 fd 3d 4d 2f fd 0c 47 fd fd 6f 7d fd fd fd 7c fd fd 17 fd fd fd fd 09 3b 53 28 00 fd fd 08 fd 76 76 fd 0f 52 5d fd 38 fd 7f fd 06 7d 61 fd 05 fd 54 fd fd 7b fd fd fd 36	A~!8fglC0rSI)TF@.- x)_CICemJei8Z?2} <0LhSr <(^W0^7%l'684<,koau . %t,}[z-qF6lX5=M/Go}}; (vvR}8)aT{6	success or wait	1	F2CBF8	WriteFile
C:\Program Files\Microsoft Office\Office16\Custom.propdesc	1867	10	24 00 3f 05 00 00 00 00 00 00	\$?	success or wait	1	F2CC68	WriteFile
C:\Program Files\Microsoft Office\Office16\Custom.propdesc	0	1343	fd fd 74 12 33 47 38 fd fd 09 fd 11 76 fd 34 fd fd f2 fd 43 2f fd 5c fd fd 16 fd 1c fd fd 43 fd 25 fd fd 7b 47 fd fd fd 67 fd 69 fd fd fd fd fd 07 00 19 fd 77 1a fd 44 24 52 fd fd 21 fd fd fd 0e 4d fd 0c 12 fd 3c fd 59 36 fd 11 70 4a 12 fd fd 29 29 fd fd fd fd fd 31 ad 1b fd 11 27 fd 12 1c 79 fd fd fd fd 75 60 5c 2c fd 6e 46 23 fd 7f 1a fd 6f 17 4d 57 fd 05 fd 7e fd 5c 7c 7a fd 6d d7 fd 26 24 05 75 57 fd fd 6a 79 09 fd fd 13 fd fd fd fd 9c 10 60 fd fd 2b 4b fd fd ad 5f fd fd 4d 46 68 fd fd 51 fd 0e fd 75 fd 7b fd 7f fd 2a 28 7c 6b fd fc 11 6e fd 37 45 fd 34 1c 27 0d 5e fd 49 07 67 fd fd 3b fd 7d fd 2c fd fd 6d fd 44 65 0f fd 3b 33 d6 a9 fd 2b 03 01 18 fd 23 37 4f 3b fd fd 11 6d 29 fd fd 38 3a 4d fd 35 fd fd	t3G84C\lC% {GgiwD\$R!M<Y6pJ))1yu `\,nF#oMW~\ zm&\$uWjy` +K_MFhQu{ * kn7E4^g},mDe;3+#7O; m)8:M5	success or wait	1	F2C055	WriteFile
C:\Program Files\Microsoft Office\Office16\Mso Example Setup File A.txt	78	524	5e 22 fd fd 15 60 fd 52 fd 6c 7e 4d 10 fd fd fd 5f 00 5e fd fd 2c 5c 14 fd 7c fd 15 1b fd fd fd 4a fd fd fd 4e fd 78 fd 60 34 fd 2b 51 fd fd 25 6f fd 02 fd fd 3e 4d fd 57 fd 4b fd fd fd 5d 2b fd fd 53 36 fd 57 fd 14 42 fd 37 fd fd 4a fd 65 0c 7d fd 0d 07 74 fd 51 fd fd 19 fd 62 6f 6e fd fd 23 59 05 fd 64 fd 77 fd 18 fd 05 04 c5 74 14 fd fd 2e 2d fd 6f d7 fd 43 72 22 09 57 48 fd 8f 21 10 32 01 76 fd fd fd fd 02 fd 4a 0b fd fd 0f 7f 3e 29 58 fd 5a 29 fd fd 62 fd 2d fd 2c fd 01 fd 64 38 fd 07 fd fd 65 fd 73 fd 17 1c fd 54 fd fd 6d 35 4d 01 1b fd fd fd 28 fd 64 37 6b 13 fd fd fd fd 44 fd fd 2a fd 5c fd fd 0b 60 1d fd 1a fd fd 29 63 24 25 fd 73 fd 61 33 fd fd 23 fd fd 05 fd 4c 5c 5a 0e 65 2e fd 3a fd 2c 19 fd 7d fd 29	^^"Rl-M_^,\ JNx`4+Q%> MWKj]+S6W B7Je)tQbon#Ydwt.- oCr"WH!2vJ>)>XZ)b- ,d8esTm5M(d7k\`c\$%sa 3#L\Ze.:.}	success or wait	1	F2CBF8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\Microsoft Office\Office16\VisioCustom.propdesc	0	1156	fd fd fd 25 fd 43 43 fd 0b 54 40 fd fd fd 14 fd 0e 39 fd 0b fd 7b fd 27 51 fd 68 36 3f 24 fd fd fd fd 6c 62 fd fd fd fd 0b 77 57 67 fd fd 3f fd fd fd fd 4f fd 73 08 71 6f 6e fd 29 fd 29 fd fd fd 58 fd 76 7b fd fd fd 45 fd fd fd 1b 5a 41 fd fd fd 4e fd 6c 63 fd 44 fd fd 40 42 2b fd 12 fd fd fd fd fd fd fd 62 fd 4c fd fd 08 fd 48 fd fd 73 62 52 7a 65 fd fd fd 0e 23 56 fd 7d 29 fd 02 fd 17 35 1a 55 fd fd 67 13 fd 04 fd fd 7c 0a 5f 6d b1 fd 54 06 fd fd ba 1c fd 53 fd 43 70 fd fd fd fd fd 0b fd 4b 0d 4c 58 4d fd 1d fd 0c fd 05 3c fd 08 19 11 fd fd 37 7f 3d 6e 67 19 fd fd 0e fd fd fd fd 50 fd fd 55 0b fd 11 fd 10 37 57 4d fd 75 30 fd 7c fd 27 fd fd 1e fd fd 73 fd 09 1a fd 65 52 47 46 6c 49 fd fd 65 26 fd 22 7a fd 06 fd 39 52 fd 7d	%CCT@9{'Qh6? \$!bwWg?Osqon))Xv{EZANicD@B+bLHsbRze#V})5Ugl_mTSC pKLXM<7=ngPU7WMu0l'seRGFile&"z9R}	success or wait	1	F2C055	WriteFile
C:\Program Files\UNP\Logs\UpdateNotificationPipeline.001.etl	131072	524	67 fd 15 62 fd fd 06 02 fd fd fd fd ef 3f 40 fd 35 17 fd 5c 7e fd fd 4e 4c 6e fd fd 7b 08 fd 5c 44 9b 69 fd 2d 42 55 fd fd fd 5a 55 63 fd 7d fd 73 fd 60 fd fd 74 78 44 45 fd fd 38 fd 19 2a 6e fd a4 78 02 fd 7f 19 fd 05 6d 2c fd fd 36 5f 70 fd 5f 72 fd fd fd 0e fd 72 46 5c 2f fd 77 fd fd 43 7c 27 3c fd fd 53 fd 26 fd fd 76 fd 1c 08 fd 7e fd 1c 0e 55 fd 7f 10 fd 2b fd a1 fd 62 fd fd fd 10 24 40 06 44 57 fd fd 33 fd 51 fd fd fd 5f fd 35 fd fd 4a fd 6c fd 6d 69 fd 5e fd 46 fd 08 29 1c fd 25 fd fd fd 33 fd 39 fd fd 4f fd 5f 3f fd 50 6e fd 3f fd fd 3b 7c cd 7b 69 fd 02 00 fd fd 6f fd fd 59 52 fd 32 fd 77 fd 2a 0a fd 76 fd 69 29 fd 2b 5b 58 49 fd 3f 5e fd 74 29 fd fd 34 fd fd fd 29 fd 20 fd fd 2e 78 3c fd fd 35 fd 02 3f 32 08 fd	gb?@5\~NLn{\Di-UZUc}s`xDE8*nx m,6_p_rrF\wCj'<S&v~U+b\$@DW3Q_5Jlmi^F)%39O?Pn?; {ioYR2w*vi)+[Xl?^t)4) .x<5?2	success or wait	1	F2CBF8	WriteFile
C:\Program Files\UNP\Logs\UpdateNotificationPipeline.001.etl	131596	10	24 00 00 00 02 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\Program Files\UNP\Logs\UpdateNotificationPipeline.001.etl	0	131072	fd 68 1c 3b fd fd fd 23 fd fd fd 52 4e 1f 18 c7 fd 76 fd fd 37 51 79 1e 0f 28 fd 22 fd 72 16 fd 66 31 7f 7c fd fd 50 fd fd 3a 42 fd 5a 61 74 4e fd 25 27 fd 64 79 fd 1f 0f fd fd fd 8c fd 16 fd fd 76 fd 68 96 f1 fd 0c 21 7d fd fd fd fd fd fd fd 51 fd 44 0a fd 73 fd fd fd 72 fd 62 4c fd 1d fd 32 fd 06 0c 22 fd 7d fd 06 43 68 fd fd 7d 05 fd fd 44 fd fd 39 0d fd 60 fd 5e fd fd 10 0a fd fd fd f2 fd 4d 33 fd 72 21 35 55 fd 13 fd fd fd 5b fd 4e 20 fd fd 72 fd fd 32 47 fd 29 fd 2a fd 37 3e 79 c0 43 40 32 44 3b 01 fd 55 fd 15 76 fd 62 68 2f 43 62 fd fd eb 41 fd 3f fd 10 fd 2a fd 07 fd 4c fd 42 fd 16 fd 03 fd 35 fd fd fd 26 12 24 fd fd 47 3d 6c 7b fd 02 fd 65 51 fd 71 fd fd fd 51 52 4a fd 43 fd 3d fd 0b	h;#RNv7Qy("rf1 P:BZtN%'dyh!}QD srbL2")Ch}D9^M3rl5U[N r2G)*7>yC@D;Uvh/CbA?*LB5&\$G={QqQRJC=	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\UNP\Log\UpdateNotificationPipeline.002.etl	131072	524	7b 4b 52 fd 0f fd 20 17 37 fd 7a fd 24 fd fd 7a fd fd 37 fd 3d fd 6d fd 76 2c fd fd 2c fd fd 25 fd 78 1b fd 5c 69 08 fd 5f 22 68 fd 74 51 fd 6c fd 78 0b 2d fd 5f fd 45 fd 25 fd fd 73 fd 12 2b 1c 42 1e 49 fd 49 14 2c fd fd 62 42 fd 1e 25 fd 10 fd 39 04 fd 0e 50 23 0d 2d 1b 26 fd fd 2a 19 3f 34 fd fd 52 fd ce 1b fd 29 fd fd fd 01 fd 04 fd 7c 23 fd fd 71 fd fd 62 fd 52 fd fd fd fd fd 48 fd fd 63 fd 7e fd 38 fd fd 32 30 0d 45 2a fd fd fd 1c 19 2e 6d fd 6c fd fd 72 7b fd 4e fd 75 fd 63 fd 48 56 fd fd 65 46 34 0e 76 7f af 28 ea fd 2a 0b fd 4a fd 5b fd 2b 56 14 75 2b 1d 00 06 fd fd 62 14 39 55 38 20 5e fd fd fd 59 7b 31 fd fd 08 0a 3a fd 5f 10 10 77 fd fd 48 74 57 20 36 42 51 7b fd 04 70 4e 48 0c 1e fd 26 fd 40 fd fd fd fd fd 0b 74 fd fd	{KR 7z\$z7=mv,,%xli_"htQlx- _E%s+BII,bB%9P#-&*? 4R)]#qbRHc~820E *.mlr{NucHVeF4v(*J]+Vu +b9U8 ^Y{1_wHtW 6BQ[pNH&@t	success or wait	1	F2CBF8	WriteFile
C:\Program Files\UNP\Log\UpdateNotificationPipeline.002.etl	131596	10	24 00 00 00 02 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\Program Files\UNP\Log\UpdateNotificationPipeline.002.etl	0	131072	fd 07 26 fd 59 06 fd 7c fd 6d fd fd 11 73 fd 6d 39 fd 29 fd fd 25 33 55 2c fd fd fd 06 65 fd 0d fd 7c 1e fd 27 c2 fd 6e fd 62 5e fd fd fd 08 d9 fd 4b fd 29 fd fd fd fd 13 fd 6f 75 3a fd 36 fd 47 3c fd fd 7d fd 13 79 2a 24 27 0e fd 1b fd fd fd fd 77 fd 0b fd 5d fd 2b fd 09 fd fd fd fd 4d 62 77 fd 77 fd 53 fd fd fd 64 67 fd fd 34 28 7f 32 6c fd fd fd 7a fd 50 64 47 fd fd fd fd 69 1d fd 67 fd 03 fd fd 69 fd 3c fd 0f 4f fd fd 09 fd fd fd 34 5d 2e fd 5a 27 38 33 fd fd a8 5e fd fd 26 fd 6c fd 4b fd 35 fd 7a 2e fd 48 0e fd 45 fd 0b 22 fd fd 1a fd 32 fd fd 76 fd 3d fd fd fd 0a 74 58 2a fd 4f fd 44 40 fd fd 7f 3e fd 80 53 35 2b fd fd 56 71 fd fd fd 08 7b fd 61 b1 fd 50 fd 01 fd 15 39 fd 33 5b fd fd fd 32 04 06 54 fd fd 1c 7e	&Y msm9)%3U,e 'nb^K)o u:6G<)jy*\$ 'wj]+MbwWsdg4(lzPGigiO 4].Z'83^& IK5z.HE"2v=IX*OD@>S5 +Vq{aP93[2T~	success or wait	1	F2C055	WriteFile
C:\Program Files\UNP\Log\UpdateNotificationPipeline.003.etl	131072	524	54 4f 3f 3b f9 3e 08 57 fd fd fd 27 09 fd fd fd 5f 0e fd fd 9d fd 1a 42 0b 38 4f 08 7c 2a 47 7f 43 29 fd 5c 30 fd fd 36 26 fd fd 6c 2b 08 fd 50 15 94 fd 24 5b fd 1b fd fd 64 fd 0c 77 71 fd 65 fd bd fd 10 fd 17 ba 2c fd fd 08 6e 36 fd 35 fd fd fd 42 3e 29 a2 40 fd fd fd fd 2e fd 07 3c 38 fd fd 72 11 5e 69 fd 42 fd 59 76 72 33 fd 3a fd 41 70 fd 48 16 77 fd 62 fd fd 11 7c fd fd 08 71 fd 01 4e 17 fd 7c 27 fd 50 fd fd fd 7f fd 19 64 fd fd 37 60 09 c5 fd fd 28 fd 76 02 30 fd fd 35 2c 62 fd fd 3e fd fd 6f 72 35 fd 40 0a 75 fd 72 3e fd 6a 5b 48 fd 0d fd 2a fd 2a fd fd 34 fd fd 55 fd 21 fd fd 7b 21 68 fd 32 36 09 fd fd 66 fd fd fd 78 21 15 bc 09 29 fd 03 6d fd fd 00 fd 1a fd fd 40 3b fd fd 45 6f fd fd fd 7f 73 fd fd	TO?;>W" _B8O)*GC)\06&l +P\$(dwqe,n65B>).@. <8r*iBvr3:ApHwb qN 'Pd 7^(v5,b>or5@ur>j[H**4U! {!h26fx!)m@;Eos	success or wait	1	F2CBF8	WriteFile
C:\Program Files\UNP\Log\UpdateNotificationPipeline.003.etl	131596	10	24 00 00 00 02 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\UNP\Log\UpdateNotificationPipeline.003.etl	0	131072	fd 4e fd fd 75 06 fd fd fd fd 2b aa fd 77 fd 1a fd fd 01 fd 51 fd fd 20 fd 0a cb fd 7e 0e 06 fd fd fd 0b 45 49 fd 6b fd 67 5d 11 fd 54 27 fd fd 5d 26 fd 1d 34 fd fd fd 4d 5d fd 03 fd fd fd fd 3a fd 56 fd fd 24 18 fd fd fd 15 fd fd 4d df fd 65 27 27 2a fd 49 fd 67 fd fd fd fd fd 28 63 45 21 11 fd 6a 65 fd 19 70 6b 45 49 56 5d fd fd 06 33 fd 00 40 fd fd fd 10 fd 5a 38 55 fd 4a 14 fd fd fd fd 3d 74 fd 28 fd fd 1c 37 fd 54 75 74 32 fd fd 76 6d fd fd 4d fd 60 05 2b fd 12 f1 1d fd 2f 69 fd 58 fd 78 47 fd 57 3f 12 07 5e fd 68 2f fd fd 30 fd fd 20 0c 46 24 11 41 1b fd 1a fd fd fd 5a 3c fd 79 28 fd 50 fd 43 2a 24 78 fd 01 fd 8c 68 fd fd fd fd fd 71 76 fd 15 fd 11 fd 7b 55 fd 08 fd 27 eb fd 1f 4f 7d 31 57 0d fd 11 09 fd 6b fd fd fd	Nu+wQ ~Elkg]T]&4M]:V\$Me"*IgcE!jepkEIV]3@Z8UJ=t(7 Tut2vmM`+/iXxGW?^h/0 F\$AZ<y(PC*\$xhqv{'O }1Wk	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Microsoft Office\CLIPART\IR3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 5f 2f 5c 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ _ _ _ \\\ I _ _ _ V _ _ _ _ _ _ V L / / _ _ _ _ _ V . ` _ _ _ \\\ _ _ _ \ _ _ _ V V L / / \ _ _ \ _ / \ _ _ _ _ \ _ _ _ _ _ _ _ _ /By now it's probably painfully apparent that your environ- ment has been infected with r	success or wait	1	F358DF	WriteFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\ReadMe.htm	16633	524	fd fd fd 53 fd 69 20 25 fd 1f 54 1a fd fd fd 73 45 fd 02 18 45 52 43 fd 78 fd 11 22 0e 3e fd fd 12 fd 4e fd 45 39 fd 63 3b fd fd fd 54 fd 7a fd 7c 74 5d df 65 43 6d 5e fd 0a fd 66 fd fd 69 21 68 fd fd 20 6b 55 fd fd fd 3f 71 52 3d fd 2d fd fd fd fd 56 00 52 10 1e fd 10 08 12 32 fd fd 40 5b fd fd 2e 6b fd fd fd fd d3 fd 03 fd 00 6c fd 41 1c fd fd fd 15 fd a5 fd fd 08 73 fd 4f 2f fd fd 6b 5e 2f fd fd 2b 4d 61 1c fd 7a fd 2f 77 fd 0a fd fd fd 6f 09 0c fd 2d 27 fd fd fd 65 fd fd 2b 36 07 fd 46 fd fd b9 75 42 fd fd 4b 4a 68 fd fd 03 7b 75 40 5e 28 1f 62 16 24 71 43 14 2a 47 27 0b fd fd 37 fd 16 6c 25 3b fd 72 35 fd 13 fd 25 68 51 fd 11 1d 62 fd fd 73 fd 6c fd fd 32 19 fd fd 3d 05 fd 28 fd fd 3f fd fd 4e 3c 1c fd 14 0b 6d	Si %TsEERCx">NE9c;Tz]t]e Cm^filh kU?qR=- R2@[.klAsO/k^/+Maz/wo- 'e+6FuBJh{u@^(b\$qCG'7I %;r5%hQbsl2=(?N<m	success or wait	1	F2CBF8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Adobe\Acrobat Reader DC\ReadMe.htm	17157	10	24 00 fd 40 00 00 00 00 00 00	\$@	success or wait	1	F2CC68	WriteFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\ReadMe.htm	0	16633	fd 71 fd fd 1b 26 72 50 6c 71 67 56 72 fd 67 fd fd fd fd 42 2f 7b fd 66 56 6e 07 16 54 4e fd 1b b3 fd 0d 4f 29 58 2f fd fd fd fd 84 fd 76 fd 06 3f fd b2 fd fd 3a 38 fd 35 fd fd 54 23 23 fd fd 52 fd fd 4d fd 2b fd 3d fd 39 3a 6c fd 64 10 5d fd fd 54 fd 3d 52 fd 39 fd fd 25 fd 24 65 fd 3b 1c fd fd fd 34 31 6d fd 56 3e 43 67 fd 8c fd 75 52 78 fd 39 fd 2a fd 7d fd fd 52 45 6b 22 fd 1e fd 67 fd 5f 61 fd fd 8c fd fd fd 1f 6f fd 6c 29 30 fd fd fd fd 3e fd fd d5 47 65 35 6a 04 fd fd 30 fd 10 41 fd fd fd 27 1a 65 fd fd 76 3d 6b fd 04 fd fd fd 25 23 1b fd fd 6e fd 56 1b fd fd 7f 42 fd 18 0a 69 41 fd fd fd 73 63 fd 6e a5 31 fd fd 2e fd fd 5f fd 34 6d 56 4e 1c 49 3c fd 3a fd fd fd 0b fd fd fd 0e 09 fd 44 28 27 16 26 fd 7c 0d 19	q&PlqgrgB/{fVnTNO)X/v? :85T##RM +=9:ld]T=R9%\$e;41mV> CguRx9*)RE k"q_aol)0>Ge5j0A'ev=k% #nVBiAsc n1._4mVNI<:D('&	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Autolt3 \AutoltX\AutoltX.chm	200478	524	71 75 4c fd fd 33 09 fd fd fd 66 fd fd fd fd 72 4f 35 66 a3 fd fd 06 12 75 fd fd fd 38 49 2d 55 fd 47 04 5d fd 2f fd 4f fd fd d2 19 fd 20 05 02 72 fd 64 fd 1c 66 4f 05 79 fd 13 69 5e 11 19 41 49 5c fd fd 25 6d fd fd fd 6e fd 72 fd fd 43 15 b6 fd fd fd 2a fd fd 38 18 fd fd 47 03 fd fd 16 fd 53 75 33 fd 49 1f fd 56 16 01 fd fd 53 59 fd fd fd 64 68 fd 69 1f fd 0e 4e fd fd 5e fd 42 0b fd fd fd 08 32 fd 6c fd 61 fd 2e fd 70 c3 20 29 fd 60 fd fd 47 22 68 fd 16 07 4a 14 55 2d 32 4f fd fd 29 0c 28 fd 02 65 fd fd fd fd 38 fd 17 fd fd 10 fd 73 fd 17 fd 57 fd fd 3c 58 53 55 fd 1f 7a 50 fd 0b fd fd 1a fd fd 43 06 fd 2c 57 fd fd fd 7a 3c 66 fd fd fd 47 09 53 fd fd fd fd 31 1a fd 24 45 fd 5c fd 7b fd 25 fd 68 18 fd 4b fd 71 fd	quL3frO5fu8I-UG]/O rdfOyi^AI% mnr*8GSu3ISYdhi^B2la. p)`G" hJU-2O) (e8sW<UzPC,z<fGS1\$E\ {%hKq	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3 \AutoltX\AutoltX.chm	201002	10	24 00 1e 0f 03 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\Program Files (x86)\Autolt3 \AutoltX\AutoltX.chm	0	200478	15 23 42 05 53 fd fd 59 2b 7a fd fd 44 4d fd 16 51 7f 73 3f fd fd fd fd 06 3c fd fd a4 05 fd fd 3d 65 32 44 fd 7d fd fd fd 4b 27 fd fd 30 50 70 5a 1a 33 fd 4d 41 9f fd fd 43 fd 68 fd fd 3e 22 7f fd 48 fd 22 34 fd fd 1d fd fd fd fd fd 4c fd fd 77 fd fd fd fd 2b fd 53 7f 6a fd 36 23 79 7e fd fd fd fd 1a 09 06 fd fd 0d fd fd fd 5c 73 fd 48 5d fd 52 fd 0f 63 46 fd 65 fd 10 49 fd 72 1d 5c fd 1c 16 62 26 73 19 fd fd 73 46 fd fd 4e 5f fd fd fd 71 fd 2f fd fd 1f 78 6a fd fd 0a fd 1a fd fd fd 58 fd 48 74 12 52 fd 76 3f fd fd 69 67 fd 5a 1e 29 4b fd fd fd b0 7f fd 31 fd 7a 03 43 fd 08 fd 26 10 7f 3c fd fd fd 0a 1a fd fd 07 fd 73 fd 16 60 fd fd 72 97 53 78 36 7a 06 0d fd 57 5f 6a fd 50 2f 12 79 75 09 62 fd fd 26 16 33 fd	#BSY+zDMQs? <=e2D}K'0PpZ3MACH>H "4Lw+Sj6#y\ sH]RcFe\lb& ssFN_q\ xj)XhtRv? igZ)K1zC& <s` rSx6zW_jP/yub&	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX.psd1	26418	524	fd fd 70 fd 08 34 7a 3c fd fd 0f 31 40 4c 4f fd 11 36 fd 6e 57 64 fd fd 08 fd 73 fd 59 fd 61 2b 29 fd 7a fd 19 fd 73 29 fd fd 6f 27 6e 5d fd 2e 34 25 fd 17 fd 4d fd fd fd 69 4d fd 7f 00 1d 5b fd fd fd 13 fd 72 fd 56 fd 2b fd fd 12 2e fd fd 6d fd fd 0e 09 fd fd 24 22 fd 0d 26 75 fd 28 69 33 fd fd 1c fd fd fd fd fd 0e 2b 39 fd 3f 3c 00 fd 38 fd 30 fd 2e fd fd 2c fd fd 23 57 fd fd 48 fd 0c 7c fd 0f 3d fd 3a 3c 37 46 2a e2 42 fd 59 24 49 fd fd 05 fd 39 fd fd 42 fd 7e 6d 0a fd 37 fd fd fd fd 5c 54 fd 58 fd 47 fd 07 34 fd fd fd 47 fd fd fd 38 51 5a 61 03 89 42 2f fd fd 05 07 6b 5e 58 5c 30 5f 38 34 fd 07 fd 59 55 1b 37 76 66 0a fd 65 68 79 fd fd fd 39 11 00 fd fd 2f 43 4d fd 46 66 41 fd fd 4c fd 6b bb 6f 38 fd fd 33 fd	p4z<1@LO6nWdsYa+)zs o'n].%MiM[rV+.m\$"&u(i3+9? 80,#WH [:<7F*BY \$I9B~m7\XG4G8QZaB/^ X\0_84YU7vf ehy9/CMFfALKo83	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX.psd1	26942	10	24 00 32 67 00 00 00 00 00 00	\$2g	success or wait	1	F2CC68	WriteFile
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX.psd1	0	26418	fd fd 22 fd fd 73 27 fd 6a 79 fd 44 1a 1c 23 56 fd 63 78 fd fd fd 31 20 5b fd 7a fd fd fd fd fd 1a 7c fd 09 6e fd fd 28 fd 17 12 53 fd 13 fd fd fd 20 20 7c 4f 42 fd 1b 6a fd fd fd 22 fd 73 18 fd 69 03 fd 26 21 47 fd 11 fd 62 2e 39 48 40 44 fd 62 fd fd fd 7e fd fd 2a 79 12 fd 31 fd 08 3b 1a 7b fd 19 fd 69 5e 3b 5a fd fd 60 0a 5c 19 fd 44 fd 47 0c 41 72 14 62 fd 47 fd fd 03 fd 2f 01 01 fd 0f 41 4d fd fd 27 34 5c fd 30 fd fd 1f fd fd 19 42 6e 11 6d 3a fd 53 fd fd 46 4a fd 56 22 24 4c fd 30 58 77 39 fd fd 50 69 13 fd fd 4a fd fd 29 2d fd fd fd fd 3e e2 79 fd fd fd 76 24 75 37 fd fd 16 33 fd fd 52 62 fd fd fd fd 6f 30 fd 17 79 fd fd fd 45 4f 0a 6c 6b fd fd 23 1e 08 74 60 06 fd 68 fd fd 71 cf fd 1d fd 65 fd fd 1e 26 1d 35 00 fd 4a	"s'jyD#Vcx1 [z n(S OBj"si&Gb.9H@Db~*y1; {^:Z`DGArbG/AM'4\ 0Bnm:SFJV"\$L0Xw9PiJ)- >yv\$u73Rb o0yEOlk#t`hqe&5J	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX3.Assembly.xml	49518	524	42 4d 74 17 fd 01 fd 2b fd fd fd fd 17 fd 77 fd fd 52 7a fd 4a fd fd fd fd fd a7 5b fd 29 fd 45 fd 3a 32 fd 74 fd fd 15 fd fd 2b fd fd 1b fd 31 1d 16 37 ad 0b fd fd 21 52 4d 74 fd fd fd fd 54 fd fd fd fd fd 2a fd 7d fd 4d fd fd 55 fd 39 30 fd fd fd fd 0e 3c 5a 57 1f fd fd fd 03 75 30 fd fd 0a fd fd fd 7e fd 48 fd 2a fd fd 5f 66 33 26 fd 08 1d fd 0f fd 5e fd 02 fd fd 67 59 41 1b fd 37 1b 17 08 72 53 64 fd 2a fd 72 7b 3a 02 43 3e fd 08 fd fd fd fd 23 fd 57 32 fd 65 fd 11 60 fd fd fd 47 fd fd 6b 22 fd 19 fd fd fd 5c 3f 8f 5a fd 41 fd 78 14 fd 47 4d 72 7c fd 73 4b 18 4e 27 03 fd fd 0f fd 1d 53 47 2e 13 fd fd 6a 01 57 fd 42 53 fd 6a fd fd fd 53 fd fd fd fd fd bf fd 65 fd 72 fd fd fd fd fd fd 33 28 91 fd 0f fd fd 42 fd	BMt+wRzJ)E:2t+17!RMtT *)M90<ZW0 ~H*_f3&^gYA7rSd*r{C:># W2e'Gk"\'? ZAxGMr sKN'SG.jWBSjS er3(B	success or wait	1	F2CBF8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX3_DLL.h	13517	10	24 00 fd 32 00 00 00 00 00 00	\$2	success or wait	1	F2CC68	WriteFile
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX3_DLL.h	0	12993	2b 14 fd fd fd 58 fd 4b 68 fd 24 fd fd fd 69 24 fd 5b 44 64 3b fd fd fd 05 f7 30 7d 02 fd fd fd fd fd fd 60 fd fd fd fd 73 2e 22 25 00 fd 60 fd 4b 09 fd fd fd 68 fd fd 16 fd 44 3b 44 2e fd 5e 0d 69 fd 5d 5f fd 7a fd fd fd fd 75 fd 78 fd 1d 67 2d 50 3a fd 70 fd fd 51 03 22 4d fd 53 53 29 fd fd 2b 3c 1c 39 fd fd 68 24 fd 46 fd 23 28 fd fd 23 11 fd 4c 06 62 fd 6a 7d df 2a 5e 12 fd 17 77 fd 41 fd fd fd 42 15 fd 44 fd fd fd 6c fd fd fd fd 0f 00 6c fd 21 1a fd 50 5a fd fd 56 30 4b 75 fd 0a 72 23 5f fd fd 5c fd fd 6e fd fd fd 52 fd 22 16 fd 76 7e 41 32 fd fd 20 2f 7d 6b fd 75 1e 8e fd fd 04 fd 61 fd 34 fd fd 1c fd fd 7b 46 fd fd fd 17 12 fd 52 ee 12 6a 06 fd 2f 2d fd 52 fd 3a fd 0c 37 fd 48 fd fd 7a fd 66 7d fd 18 1f fd fd 08 fd fd 6b	+Xh\$[Dd;0}`s."%`KhD;D.^i]_zuxg-P:pQ"MSS)+<9h\$F#(#Lbj)*^wABDIIPZV0Kur#nR"v~-A2/}kua4{FRj/-R:7Hz}k	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX3_DLL.lib	28976	524	04 48 20 31 56 1c fd 44 fd 4d fd fd fd fd 28 4d 39 28 fd 07 3d fd fd fd 7b 52 fd 6e 5b fd fd fd 33 fd fd 25 fd 26 5e 19 fd fd 6a 5a fd 10 fd fd 13 4b 21 fd 6e fd ac 71 fd 08 fd fd 51 70 fd 7e 28 1e fd fd 36 fd fd fd fd 76 fd fd 1d 45 fd 6f fd fd 6c fd fd 4d 36 3f 37 fd 00 64 60 fd 5f fd 43 fd 7a fd fd 5e 7a fd 4c fd fd fd fd fd 50 45 47 0e fd 12 5f fd fd fd 47 4f 38 18 03 02 1c 39 fd 1d 1c fd fd 75 fd 5a 67 fd fd 1a 2c 41 fd fd 34 47 1d fd fd 21 39 6e fd fd fd fd fd fd 13 27 56 bd 49 fd fd 40 09 fd 07 2d fd 6f 9f 29 fd 0f 65 35 fd 3d 16 fd 76 fd 58 54 31 fd 7c 59 fd 45 07 54 6b 23 fd 22 12 fd fd fd 6b fd 3d 7e fd 05 63 fd 2d fd 6a 0a fd 7c fd 07 fd 16 fd 2a 4e 78 0c 6d fd 0c fd fd 0f fd 78 3b fd 5a fd fd fd f3 07 fd fd 30 3a 63	H1VDM(M9(=Rn[3%&^]ZK!nqQp~(6vEolM6?7d'_Cz^zLPEG_GO89uZg,A4G!9n^VI@-o)e5=vXT1 YETk#"k=-c-j]*NxmX;Z0:c	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX3_DLL.lib	29500	10	24 00 30 71 00 00 00 00 00 00	\$0q	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX3_DLL.lib	0	28976	45 1c fd fd 36 fd fd fd 16 15 5f 27 fd 3a 3a fd 19 fd 7e fd 31 5b 6e 3c fd fd 6e fd fd 03 35 32 09 fd ff 70 fd 7c fd 2e 3d 06 25 fd 31 0a 51 0b 66 fd 6f 0b 14 4c fd 14 34 fd 6f 53 fd fd fd 27 05 1d fd 56 fd 66 75 fd fd 56 62 fd 29 77 fd 16 6b 70 fd fd fd 5d fd fd fd 35 fd 64 2d fd 1f 66 fd 19 4d 07 fd 36 fd fd fd 62 fd fd 62 1a 68 0a fd fd 40 11 fd 65 46 29 fd 15 73 1d fd fd fd fd fd 48 fd 32 fd 6e fd fd 75 fd fd fd 13 fd 46 5e fd fd 78 13 fd fd 3e 72 fd 58 0a 26 fd fd 5b fd fd 40 4e 7d fd fd 3f 57 77 fd 30 01 45 33 fd fd 6e fd fd 1f fd 31 6a 5c 4f fd 53 fd fd 17 71 fd 0d 39 03 fd 00 64 50 fd fd 06 61 be fd 2b 4b 5b 71 02 73 fd 7a 61 fd 57 fd fd 61 fd 2d 38 fd 64 32 fd fd 41 fd 5f fd 6a 53 3d fd fd 34 4f fd fd 74	E6_':~1[n<n52p].=%1Qf oL4oS'VfuVb)wkp]5d- fM6bbh@eF)sH2nuF^x> rX&[@N]? W0E3n1j)OSq9Pa+K[qsza Wa-8d2A_s=4Ot	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX3_x64_DLL.lib	27546	524	fd 59 fd 54 fd 5e fd 5e 3d 0a fd fd fd fd 02 fd 2a 0c fd fd 75 13 fd 62 fd fd 73 43 f5 0b fd fd 5e fd 25 4a 06 f8 46 fd 1f fd fd 4f 6c 22 5a 78 1c 45 6b 3f 1b 5c fd fd fd 6a 67 fd fd 00 12 fd fd fd fd 5c 39 04 fd fd 28 07 24 4b fd 44 14 fd 37 0b fd 19 fd fd fd 75 53 1c 1c fd 38 fd fd 64 27 3d fd 36 fd 72 7b 49 fd 18 4d fd fd 39 fd fd 46 2d 19 2d fd 3b 16 0f fd fd 3c fd 47 65 fd 70 fd fd fd 47 59 59 6f fd fd 03 fd 6c fd 3c fd 53 68 04 fd fd fd 2a fd 1f 16 57 7c fd 1d fd fd fd 6e fd fd 3d 67 fd 79 00 fd fd 32 26 7c fd 5c fd fd 58 46 fd fd 5e fd 4c 6b fd fd fd 18 58 43 48 71 61 5f fd 32 51 fd fd fd 65 06 fd 4f 10 fd fd c4 fd fd 37 3d 24 51 fd fd fd 64 48 3b fd 08 55 6e 58 fd 54 82 5d fd f4 fd 75 72 20 1d fd fd 5d fd fd	YT^^~*ubsC^%JFOL"ZxE k\jg\9(\$KD 7uS8d'=6r{!M9F--; <GepGYVol<Sh* W n=gy2& XF^LkCHqa_ QeO7=\$QdH;UnXT]ur]	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX3_x64_DLL.lib	28070	10	24 00 fd 6b 00 00 00 00 00 00	\$k	success or wait	1	F2CC68	WriteFile
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX3_x64_DLL.lib	0	27546	fd fd fd fd fd 2c fd 70 04 fd fd 55 fd 4d fd 5d 11 68 fd 2c 26 5e fd 1e 65 fd 2c 2b 6d 59 48 54 fd fd fd 4e 38 16 70 fd 0c fd 39 34 fd 77 fd 32 fd 70 7c fd fd 50 16 45 fd fd 5f fd 0b 70 ff 5e 4a fd fd 5a fd fd 5c fd 32 6b 3d 1c fd 14 fd 5d 1c 39 1e fd fd fd ea fd fd 39 75 fd 7b fd 0e 3d fd fd 35 01 0c fd fd fd 7e 14 fd 0f 66 fd 41 fd 58 38 fd 5b 54 fd fd 2e 71 fd 10 fd fd 51 3e 5e fd fd fd 0e 28 fd fd 1c fd fd 6d 27 fd 1c 3d fd fd 51 5c 5f 16 fd fd 50 6a 3b fd 50 3a 2f fd 77 fd 1f 47 fd 36 fd 2c fd 5e 9c fd 57 14 2f fd 50 fd 78 74 fd fd fd fd 15 4e fd fd 15 fd 0c 49 fd 71 fd 38 fd fd fd 41 fd 1b fd 58 49 67 fd 5a 5c fd 14 fd fd fd 22 4c 51 59 47 e5 fd 4a fd fd fd fd 54 21 3e 58 30 0a 13 fd 66 fd 49 7c fd fd fd 75 02	,pUM]h&^e,+mYHTN8p9 4w2p]PE_p^J Z\2k=]99u{=5~fAX8[TqQ >^(m'=Q_ Pj;P:/wG6,W/PxtNlq8AXl gZ\^LQYGGJT!>X0fl u	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3 \Examples\calculator.au3	1405	524	fd fd 46 fd 7e 7c fd fd 09 f6 fd fd 1c 36 37 39 fd fd 22 29 4f fd fd 78 fd 09 11 12 fd fd fd 4c 56 fd c2 71 4a 09 50 71 fd 77 f9 fd fd 78 31 fd 5e fd fd 34 61 fd 11 3c 72 09 16 fd f8 76 fd 26 fd 1b 79 24 fd fd fd 1a 59 fd 28 fd 2e 6f 29 fd 0e fd fd 33 62 fd 44 12 75 fd fd 1c fd fd 16 54 fd fd fd fd fd 45 4d fd fd 78 fd fd 33 fd 4a fd fd 7b 4d fd 09 3d fd fd fd fd 2f fd fd fd 07 5e 2f 3b 27 46 fd fd 78 6f fd fd fd fd fd 32 7f 70 fd 25 3d fd 52 fd 32 fd 0c fd 54 5c 37 fd fd 02 fd fd fd 18 7f fd 6e fd fd 56 2b 08 7b fd 28 2c fd fd 45 fd 77 64 fd 48 fd 33 fd 21 79 df 19 fb 4a fd 70 1a fd 20 1c 7b fd 51 fd 4e fd 15 fd 4a 30 fd 2a fd fd 37 78 02 fd 65 fd 4d 0d 66 fd 3f 75 fd 75 fd fd 75 68 2c fd 41 58 31 40 6e	F-[679")OxLVqJPqwx1^4 a<rv&y\$Y(.o)3bDuEMx3J{M=/'/;'Fx op%=R2T\7nV+ {(,EwdH3!y {QNJ0*7xeMf?uuu h,AX1@n	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3 \Examples\calculator.au3	1929	10	24 00 7d 05 00 00 00 00 00 00	\$}	success or wait	1	F2CC68	WriteFile
C:\Program Files (x86)\Autolt3 \Examples\calculator.au3	0	1405	3c 1c 66 40 67 1e fd fd fd 3c 35 fd 2c 62 01 23 75 fd 1c fd 14 fd 3c 09 0b 22 4f fd fd 62 33 16 4c fd 60 64 fd 39 7e 00 18 fd fd 3e fd fd fd 02 60 25 fd 49 1d fd 64 2b 3d 61 30 61 6b fd 40 fd fd fd fd fd 69 fd 48 fd fd 12 6c fd 57 3d 55 fd 4a 3d 14 fd fd fd fd fd 6a fd 52 fd 5b fd 17 0a fd fd 43 1f fd fd 3c 7f fd fd fd 3b 0c fd 73 0d 1b fd fd fd fd 26 21 55 fd 2a fd 32 87 6e 1d 79 72 fd 56 09 fd 35 fd fd 7e fd 2d 1b 2e 42 fd fd 2e 1d fd fd 2a fd 09 6e 3a 77 f9 51 fd 2b fd 2e 79 5e fd 22 53 fd 40 24 fd fd 69 4b fd 54 7e fd fd 66 fd 1b 11 3b fd fd fd 2c fd 29 fd 42 fd 09 38 fd 75 fd fd 23 3e fd 17 fd 10 77 fd fd 1c fd 7c 57 66 45 32 fd fd 0a 63 fd fd fd fd fd 53 fd fd 0d 01 fd 7c 26 3b 08 fd fd 76 30 78 fd 55 fd fd	<f@g<5,b#u<"Ob3`d9~>` %ld+=0ak@ iHIW=UJ=jR[C<;s&!U*2n yrV5--.B. *n:wQ+.y^"S@\$iKTf,)B8 u#>w WfE2cS ;v0xU	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Microsoft Office\Office16\R3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 5f 2f 5c 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \\\ _ _ v _ _ _ _ \ _ / / _ _ _ _ \ . ` _ _ \\\ _ _ _ \ \ \ \ _ / \ \ / \ _ / \ _ _ \ _ \ _ \ _ \ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3 \Examples\count-do.au3	1177	524	fd 21 fd fd 77 5f 57 79 fd 5e 6d fd fd fd fd 3d 42 e5 32 fd 2c 4d 6d 71 fd 3c fd fd 13 fd 4f 00 44 28 5f fd 2b 02 fd 04 2c fd 22 2d fd 06 07 6e fd 28 fd 5a 01 29 fd 06 fd 58 fd 36 17 00 79 7a fd 4c fd 24 fd fd 4b 61 49 fd fd 7d fd fd 61 46 00 fd fd fd fd 52 fd fd 20 fd fd 6e ca fd fd 62 fd fd 41 64 20 6e fd fd 45 fd 51 59 fd 1d fd 7c fd 66 5d fd 01 79 fd 6f fd 13 61 2f 66 fd 48 fd cf fd 07 45 62 fd fd 05 7f 7f 45 19 fd 14 4f 7b fd 21 fd 6d fd fd a6 7f fd 59 60 49 fd fd 2c fd fd 64 fd 7e 49 fd fd 78 1e 1e fd fd 06 fd 18 fd fd fd 43 5d 10 59 fd 6d 2f 5c fd fd 58 fd 2e 4a 41 fd fd fd 74 fd fd 5d fd 3d 59 75 7b 5d 70 fd 2a 3f fd 52 fd fd 19 6f fd 4e fd fd b3 fd 6e fd 1e fd 4a 7b fd 2d 47 30 26 65 56 1e 5f fd fd	lw_Wy^m=B2,Mmq<OD(+,"-n(Z)X6yzL\$Ka)aFR nAd nEQY[f]yoa/fHEbO !mYl,d~!xC]Ym/\XJA!]=Y u{]p*?RoNnJ{-G0&eV_	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3 \Examples\count-do.au3	1701	10	24 00 fd 04 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\Program Files (x86)\Autolt3 \Examples\count-do.au3	0	1177	0f fd fd 46 1d fd 45 00 58 4b 2a 74 fd 27 fd 36 fd 1c fd 7e 4e 04 fd 4a fd 34 fd 65 47 fd 47 4b 43 3f fd fd 69 fd fd 57 69 fd fd 1a 64 fd fd fd 49 45 54 30 fd fd 6f fd 6a 16 60 fd fd fd fd fd fd fd 74 fd fd 11 fd fd fd 36 fd fd fd 11 61 51 fd 46 15 fd 2b fd fd fd 62 fd fd 66 3c fd 6d 66 fd fd fd c4 17 4e 2d fd 08 fd 1f fd fd fd 50 fd fd fd fd 31 56 5a 45 76 fd fd 47 33 fd 3a fd fd 29 6e 8d 61 2d 50 2b fd fd 35 61 fd 3a 75 fd fd 2a fd fd 45 fd fd fd 51 45 17 06 fd 13 63 14 3e fd fd 69 fd 31 fd fd fd 15 fd fd fd fd 13 2d fd 09 fd 5e 33 fd fd 07 19 fd 2e fd fd 56 fd 61 fd fd 20 fd 39 fd 2d 58 fd 58 1c fd 0f fd fd 7a 61 fd 25 3e 53 1e fd 5e fd fd 35 fd 66 fd 51 35 0f fd fd 38 0a fd fd fd 2d 58 0d fd fd fd fd dc 0d 6a fd	FEXK*t6~NJ4eGGKC? iWidlET0oj`t 6aQF+bf<mfN- P1VZEvG3;)naP+5a:u EQEc>1-^3.Va 9- XXza%>S^5f58-j	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Autolt3 \Examples\count-for.au3	964	524	35 3d 4a fd fd e9 fd fd 41 75 fd fd 2c 40 7b fd fd 7c fd 27 fd fd fd 72 fd 00 0f fd 74 fd 77 35 2f f6 fd 3c 2d 39 fd 7d 35 fd 18 fd 22 fd 09 79 fd 7e fd 56 fd 54 58 fd fd 3a fd 4f fd f3 fd 0c 73 fd 01 73 0c 19 4d b2 fd fd 44 4d 0f fd 51 fd 3d 18 46 16 fd 20 53 51 fd 68 11 fd 63 fd 58 34 1b 6b ef fd 24 5a fd 21 1e 56 fd 46 fd 28 07 7d 28 0e 1e 6d fd 58 0a 3f 37 fd 07 18 1f fd 17 fd 17 fd 12 fd 18 fd 58 fd 62 fd 5c 1f 2f 4d 33 08 fd fd 27 43 fd fd 1d fd fd 3a fd 23 0d 01 fd 10 fd fd 0b fd fd 28 fd 57 fd fd 1f fd 34 fd 79 5b 6b fd 4b 1c fd fd 75 53 fd 53 fd fd fd fd 08 0e fd fd 73 4e fd fd 22 fd 7d fd 65 fd 6e fd fd 6d 46 49 55 fd 3d fd 1d 60 fd 30 fd 40 59 fd fd fd fd fd fd fd 2a 0a 08 66 fd fd 34 7e 0d fd	5=JAU,@{!rtw5/<- 9}5*y-VTXOssMDMQ=F SQhcX4k\$Z!VF{)(mX? 7XVM3'C:## (W4[kKuSSsN")enmFIU= '0@Y*f4~	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3 \Examples\count-for.au3	1488	10	24 00 fd 03 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3 \Examples\count-for.au3	0	964	17 fd fd 3b 55 fd 28 fd 1c 17 33 fd 01 31 fd fd fd 23 44 4f fd 48 fd 09 fd 17 4b fd 7e 65 fd 49 41 fd 69 6d 5d 13 55 fd 28 fd fd 07 fd 5e 67 fd fd fd 7d 24 4b 49 23 25 72 4c fd cb fd 34 fd fd fd 1d fd fd fd 30 fd fd fd fd fd 1b fd 17 15 36 1a 4d fd 09 22 fd fd 4f fd fd fd fd fd 31 fd fd 3d fd fd 4e 84 ac 1d fd fd 25 09 fd 1c fd fd fd 62 18 fd 5c fd e3 56 fd 2c 05 20 08 fd 13 20 1d 32 5e 63 fd 49 fd fd fd fd fd fd 68 69 10 fd fd 0b 18 18 1c 57 fd 39 4e 4a 55 fd fd fd 43 2c 27 fd 26 fd 2c fd 21 fd 0a 1b fd fd 6a 3f fd 15 5c fd 6d fd fd 09 69 21 fd 02 fd 53 fd 3d fd 3c fd 4b 5e fd 3d 78 78 5e fd 12 29 fd fd fd 1e 67 fd 73 71 fd 5d 70 fd 25 30 fd 18 fd fd 22 10 fd fd 7a 35 fd 71 fd fd fd 41 fd 15 1d 05 1f fd fd 70	;U(31#DOHK~eIAim]U(^g }\$KI#%rL4 06M"O1=N%b\IV, 2^cIhiW9NJUC,'&,ij? \mi!S= <K^=x^)gsq]p%0"z5qAp	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Autolt3 \Examples\count-while.au3	1169	524	fd 0e fd fd fd fd 5f 41 1a fd 4f 0c 2c fd fd 16 38 fd fd 24 fd 63 fd 58 4c 25 fd 4a 31 fd 0b 0c fd fd 62 49 62 cd fd 41 3e 6f fd 0b 0e fd fd fd fd 7b 36 0f 7c 79 07 44 fd 2a 30 5d 7b fd 70 3c 0e 73 2c fd fd 3c 02 fd 50 fd 2e 69 0d 63 50 3d fd 43 5c fd 46 fd fd fd fd 10 7d fd 4c fd 36 51 6b 22 28 35 fd fd 22 fd 18 00 62 01 6f fd fd 35 68 fd 56 06 fd 59 fd 64 fd fd fd 1a fd 3e 17 78 fd 23 62 fd 5d 71 70 50 fd 46 21 3d fd 79 58 1d fd fd 1c fd fd 23 24 35 fd 01 98 fd 71 46 fd 34 fd 3c 50 fd fd 0c e7 33 fd 6f 4b fd 1b 60 4f fd 48 fd 32 38 56 fd 12 fd 5f fd 7e fd 01 2e 1a 12 75 32 fd fd 3a fd fd fd fd 22 fd 55 14 49 fd fd 12 29 3f fd 5b 42 60 fd 07 fd fd 68 fd fd 68 5c 0d 5f 16 44 44 b1 0f 0f 7c 51 71 fd fd fd 10 f2 fd 27 fd	_AO,8\$cXL%1blbA>o{6jy D0}{p<s,< PicP=ClF}L6Qk" (5"bo5hVYd>x#b]q pPFI=yX#5qF4<P3oK`O H28V_~.u2:"UI)? [B`hh_{DD}Qq'	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3 \Examples\count-while.au3	1693	10	24 00 fd 04 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\Program Files (x86)\Autolt3 \Examples\count-while.au3	0	1169	5b fd fd fd fd fd 48 58 fd fd 47 fd 01 fd fd 57 fd fd 3e fd fd fd 2f 6c fd fd 0a 21 34 28 fd fd fd fd fd fd fd 69 fd 29 6d fd 31 fd fd 38 fd 71 76 fd 3a fd 26 fd fd 52 fd 56 05 37 fd 7f 22 14 7d 3b 30 fd fd fd fd 64 6a fd 79 fd fd fd e1 15 fd 1c fd fd fd fd fd 1c fd 2b fd 2e fd 27 04 5c 3c fd fd 20 1d fd fd 25 fd fd fd 2e 3d b8 fd 1f 72 1b 4b fd fd 45 79 fd fd 44 6d 5d fd 43 fd fd fd 54 fd 4d 33 fd 53 f9 fd fd fd 6a fd 31 13 37 fd 44 fd fd fd 05 38 fd 78 00 7b 32 fd fd 05 4d 26 fd fd 62 78 fd 10 40 3c fd 4b 37 16 36 fd fd 3b 71 fd fd 74 17 fd fd 25 fd fd 6a 72 2d 78 fd 46 fd fd fd fd 21 2d fd 2a fd fd 33 fd 32 fd 7e 06 0d 55 fd 63 31 7e 5e fd 5b 23 77 3f fd fd 53 fd fd 7a fd 4e 57 14 fd fd 30 fd fd fd 08 fd fd	HXGW> l4(i)m18qv:&RV 7");0djy+.\ <%.=rKEyDm]CTM3Sj17 D8x{2M&bx @<K76;qt%jr-xFI- *32~Uc1~^[#w?SzNW0	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3 \Examples\functions.au3	1157	524	2d 59 fd fd 11 23 56 7b fd 32 fd fd fd 0b fd 2a fd 03 fd fd fd 18 fd 64 5f 31 fd 5b 7a 72 1f fd 59 fd 73 fd 4e 33 58 fd fd 4d 40 58 ea fd 01 fd fd fd 6d 2e 36 fd fd 28 66 0f 6d fd 29 fd 1e fd 47 63 6a fd 1d fd fd fd fd 6c fd fd fd 31 fd 29 fd 16 58 77 fd 2b fd fd fd fd fd 07 fd fd fd fd 62 4f 04 cc 74 08 2c fd fd fd 63 78 38 77 fd 38 2d 77 fd 2f 33 fd 44 fd 52 fd 1e 6e fd 39 fd 54 fd fd fd 46 26 7d fd fd fd 00 35 14 fd fd fd fd 70 50 fd fd fd fd fd 3b fd 27 06 fd fd fd fd 65 fd 22 fd fd 45 32 fd fd fd 57 7c fd 0e 5a fd 7a fd fd 2b fd a8 fd 62 67 21 6c 70 50 fd fd 1e 0f 4f fd 4a 73 fd fd 64 fd fd 0e fd 74 fd 2a fd fd 7b fd 6e 5a fd 21 53 07 39 fd 11 fd 04 85 fd 10 64 fd fd 6c 04 a1 fd fd fd fd 13 fd 68 fd 1e 57 fd 2c fd fd 48 fd	- Y#V{2*d_1[zrYsN3XM@ Xm.6(fm)Gc j11)Xw+bOt,cx8w8- w/3DRn9TF&})5p P;'e"E2W Zz+bg!pPOJsd t*{nZ!S9dlhW,H	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3 \Examples\functions.au3	1681	10	24 00 fd 04 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\Program Files (x86)\Autolt3 \Examples\functions.au3	0	1157	fd fd 30 fd fd 31 fd 1a fd 75 fd 7d 36 fd 1c 7a fd 78 fd fd 59 fd 05 fd 32 5b 71 fd fd 3f 58 fd fd 26 fd fd 22 fd 01 3d fd fd 34 5d 04 13 5f fd fd fd 15 57 00 76 fd 60 48 7d fd 15 35 5b fd 41 54 fd 46 fd 43 51 fd 12 fd 76 55 1b 29 70 7e fd fd 50 e1 1d 0c 4d fd fd fd 67 52 01 fd fd 3f 1e 64 fd 5a 72 b0 36 03 fd fd 2a 6e 6f 69 59 59 fd fd fd 71 0c 18 fd 23 06 fd 65 60 4d fd 51 fd fd 65 45 0e 3f fd 7b fd 32 17 54 6d fd fd fd fd 0d 73 fd 1e 4f fd 01 fd 32 73 fd fd 76 fd fd 1b fd 5d 78 47 03 55 fd 08 fd 42 67 20 fd 0c fd fd 4f fd 2e fd 3c fd fd fd 3c fd 68 fd fd fd fd 0f 65 fd fd 5f 35 fd fd 3d 68 7a 7b fd 60 7d fd 61 fd 2a fd fd 13 3e fd fd 0d 51 fd 1d fd fd fd 66 fd 6e 69 fd fd e1 fd fd fd 2b fd 7a fd 4d fd fd 4c 2f 4a	01um}6zxY2[q? X&"=4_vw'H)5[TFCQ vU)p~PMgR? dZr6*noiYq#e`MQeE?{T msOsv)xGUBg O. <<he_5h{' }a*>Qfn i+zML/J	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Microsoft Office\Stationery\IR3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ \ _ _ v _ _ _ _ v \ / / _ _ _ _ . ' _ _ \ _ _ \ \ v v / / \ / \ \ _ / \ _ \ _ \ _ _ \ _ _ \ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3 \Examples\inputbox.au3	1692	524	fd fd 7a fd fd fd 78 0e 00 1c fd fd 42 48 6d 4e fd 05 fd 1d 2b fd 28 51 1f fd 6c fd 43 fd 0d fd 52 fd 09 36 fd 59 50 fd 19 fd 6c 76 fd fd 49 61 fd 26 fd 01 7b 20 fd 60 45 0a 2c 10 11 07 01 12 1d d6 54 3f fd fd 4b 14 fd fd 26 fd fd 0c 44 67 31 57 77 3f 62 32 fd fd fd 69 5f fd 35 6e 4b fd 5c 57 5e fd fd 6b 36 65 fd fd 61 fd fd 59 1f 7e fd 47 6e 3b 0b fd fd 27 fd fd 27 ee 1d fd 6b 47 fd 52 fd fd fd fd 47 fd 31 fd 30 64 fd fd fd 4f 05 77 fd fd fd fd 34 01 2c fd 52 fd fd fd fd 3c 4a fd fd 09 7e 13 08 fd 28 5a 7a fd fd 59 61 6d 13 36 5b 7b 30 5e fd 4a 3f fd 39 fd 2e 40 5f fd 28 07 19 fd fd fd fd 10 fd 1b 00 5c 7a fd 5d fd 05 55 6c 22 32 fd 73 fd 09 16 fd 1f 53 fd fd fd fd 37 fd fd fd 40 fd fd 46 25 fd 34 fd 2c fd fd 28 fd 55 23 fd 1d 2b fd	zxBHmN+(QICR6YPlva& { `E,T?K&Dg1Ww? b2i_5nKW^k6eaY~Gn;"k GRG10dOw4,R<J~ (ZzYam6[{{0^J?9._@_(\z] Ul"2sS7@F%4,(U#+	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3 \Examples\inputbox.au3	2216	10	24 00 fd 06 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\Program Files (x86)\Autolt3 \Examples\inputbox.au3	0	1692	fd fd fd 59 43 fd 2a fd fd 46 7b 54 fd fd fd 42 2d 74 3e 6f 78 fd 05 fd 4f 25 fd ce fd 66 fd 60 08 fd 71 fd 78 4a fd fd fd fd 41 fd 44 fd fd 53 47 fd 3d 46 fd 3b 11 5b 76 35 22 fd fd fd fd 6f fd 5f fd fd 23 fd fd 2b 79 52 1f 23 fd 34 fd 56 45 48 fd 2a 04 60 33 fd 79 1a 64 6a fd 29 55 fd 6e 7e 24 fd f9 fd fd fd fd fd 3e fd 20 f0 fd fd 68 36 fd 7e 17 2a 97 62 fd fd 4d 59 0a 02 01 2a 74 fd 50 69 fd 28 0f fd 0f 69 fd 5b 3b fd fd 7e fd 19 47 fd 22 10 fd 5f fd 22 34 fd fd 77 4c fd 1c 60 29 43 35 2e fd 55 14 fd fd fd 2b fd 42 fd 7c fd 0b 30 fd fd 44 1e fd 4e fd 53 61 15 0f 68 47 fd 6c 4c fd 63 fd 1b fd 2b fd fd 32 fd 06 4a fd 72 40 28 18 fd fd fd 3b 18 fd fd 1b 01 fd 6b 59 0b fd fd fd fd fd fd 25 fd 13 fd fd 75 2c fd 39 fd fd fd 45 fd fd	YC*F{TB- t>oxO%fc qxJADSG=F; [v5" o_#+yR#4VEH*3ydj)Un~ \$> h6~*bM Y*tPi([i;~""4wL`)C5.U+B ODNSah GILc+2Jr@(;kY%u,9E	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Autolt3 \Examples\msgbox.au3	459	524	14 32 fd 00 5c fd fd 4f fd fd 79 2a fd 35 7d 25 14 78 fd 18 60 45 07 fd 7a fd fd 2f fd fd 2e 75 69 fd fd fd fd 30 fd 62 2d 54 2f 04 42 fd fd 34 16 fd 19 fd 39 24 fd fd fd 29 2b fd 10 2e 16 fd fd 38 fd 1a fd 69 6a 23 02 5a 7f fd 40 fd fd fd fd fd fd fd 5d 38 fd 04 05 fd 64 7f fd fd fd 29 fd 64 11 3b 1a 51 fd fd 3c fd 5a fd 7f fd 25 fd fd 63 75 fd 58 fd fd fd fd fd 47 fd fd fd 17 7f 4e 5e 59 fd fd 4a 15 75 68 50 fd 24 fd fd fd 44 fd fd 35 52 47 fd fd 28 fd fd 1c fd fd 17 fd fd fd fd fd fd fd fd fd 60 fd 7c fd fd 2c fd fd 6b 1c fd 7d fd 6b 69 fd fd fd 15 fd fd 78 69 fd 4a fd 19 fd 07 fd 1c 5b 69 41 fd fd fd fd fd fd fd 78 fd fd 41 a0 fd 90 36 66 fd fd fd 32 fd fd fd fd 48 fd 7c fd 26 fd 4e 72 fd 72 fd fd fd 16 fd 33 fd 0c 65 fd fd	2\Oy*5)%x`Ez/.ui0b- T/B49\$)+.8i j#Z@]8d)d;Q<Z%cuXGN ^YJuhP\$D5RG ([,k)kixiJ[iAxA6f2H&Nnr3	success or wait	1	F2CBF8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3 \Examples\msgbox.au3	983	10	24 00 fd 01 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\Program Files (x86)\Autolt3 \Examples\msgbox.au3	0	459	fd fd 48 fd 62 fd 72 7b db 72 10 fd fd 58 fd 34 7a 50 fd 74 60 fd 19 07 fd 64 fd fd 07 50 6e 7e 48 fd 47 12 56 06 0e 6b 66 62 08 34 1d fd fd 61 66 1e 70 fd 26 6d 03 17 fd 4e 49 fd 5e 69 17 fd fd 91 30 57 fd fd 06 fd 18 fd fd 26 62 76 36 4c fd fd fd 06 fd 57 fd 0f fd fd 0f 23 6d fd 52 fd 2a 4e fd fd 6e fd 6a 4c 09 2f 65 fd 5a 49 7f 45 fd 08 fd 5a 3b fd fd 3c fd 4c 0a 7e fd 2e fd c9 41 fd fd fd 26 fd 3d 05 2c fd fd 54 51 15 fd 13 13 37 fd fd fd 5a 15 41 17 6e 7e fd fd 1d fd fd fd 2e 0d 21 fd fd 16 78 fd fd 38 fd 32 fd fd 24 28 31 fd 60 fd 25 fd fd 43 2c fd 21 fd 3a fd 2d fd fd 17 24 fd fd fd 09 fd fd fd fd fd fd 63 65 43 fd fd 69 11 7c fd fd 25 44 2f 39 7c 28 fd fd 78 5b fd fd fd fd 60 30 21 10 fd fd fd fd fd 6b 19 fd 0c 31	Hbr{rX4zPtdPn~HGVkfb4 afp&mNI^i 0W&bv6LW#mR*NnjL/eZ IEZ;A<~.A&, TQ7ZAn~!x82\$(1`%C,!:- \$ceCil %D/9 x[`0!k1	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Autolt3 \Examples\notepad1.au3	1701	524	61 fd 7e 36 fd 3a 3d fd 26 fd 07 45 71 fd fd 4e 03 fd fd 44 fd 16 fd fd fd 73 7f fd fd fd 14 fd fd 5c fd 06 fd fd 19 fd 1a fd 41 fd 77 6a fd 38 6d 29 39 fd 5c 7c 23 3d 43 fd fd fd 7c fd fd 45 53 2a fd 42 54 fd fd 07 6b 09 2c fd fd 2d fd 05 02 72 7c 66 7b 10 fd fd 00 fd 0d 11 fd fd 0e 6d fd 15 2c 2d fd fd 63 5a fd 36 10 fd 32 07 fd fd 20 7d 0f da fd fd 2c 54 fd fd fd 55 fd 4a fd 53 2f fd 7f 71 6d fd c3 fd 00 5b fd fd fd 11 fd 5e 32 18 39 35 fd 1e 6e fd 05 0c 00 32 fd 45 fd 5c 41 55 7c fd fd fd 63 2c fd 55 3e 02 4a fd fd 2b fd 43 fd 3e 29 c1 39 fd fd 00 fd fd fd 31 7d 1f fd 2a 7e fd fd 74 57 7e fd b3 fd 5e fd fd fd fd 4b 3a 52 fd 26 fd fd 07 fd 62 12 57 15 25 fd fd fd fd fd 4d 62 00 4c 5e fd fd fd 2a fd 05 fd 5e 3e 25 fd	~6:=&EqNDs\Awj8m)9\ # =C ES*BTk,-r f{m,-cZ62 ,TUJS/qm[^295n2 EVAU c,U>J+C>)91)*~tW ~^K:R&W%MbL^^^>%	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3 \Examples\notepad1.au3	2225	10	24 00 fd 06 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3 \Examples\notepad1.au3	0	1701	07 fd fd 15 ef 51 23 fd fd fd fd 06 fd 38 fd 62 75 fd 2a 48 14 37 05 fd fd 1b 23 fd 17 34 fd 5a fd fd 36 fd fd 15 fd fd fd fd 6b 4c 24 fd fd 5b 21 3f 1b 4e 38 10 fd fd 10 2c 21 25 26 fd 17 6e 32 51 fd 34 fd 3b 45 fd 04 fd 06 fd fd 03 fd fd fd 06 0d 90 09 fd 43 55 30 fd fd fd fd 2b 65 fd 70 fd 08 fd 51 30 1f fd 4f 04 6d 09 44 fd 54 fd fd 67 fd fd fd 01 79 fd fd fd 2c 75 8d fd 5d 1e 0c fd 50 fd fd 12 fd 6c fd 24 fd 77 5b fd 04 07 12 fd fd 2f fd 4a fd fd 5b fd 68 fd 16 15 fd 76 45 fd 19 0a 5c 12 57 40 6d fd 68 20 fd 1a 3b 36 fd 56 fd 75 35 45 fd 18 05 72 76 fd fd 5b fd 28 64 23 fd 18 fd 2d 31 fd 68 fd fd 12 05 fd fd fd 0c 21 fd 48 59 10 68 af 10 fd fd 5e fd fd fd fd 18 26 fd 47 fd fd 1d 1b fd fd 7e fd fd fd fd 4f 4c	Q#8b*H7#4Z6kL\$[!? N8,!%&n2Q4;EC U0+epQ0OmDTgy,u]P!\$ w[/J[hvE\@mh ;6Vu5Erv[(d#- 1h!HYh^&G~OL	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Autolt3 \Examples\notepad2.au3	1415	524	07 2a fd fd 09 68 fd fd fd fd 6d fd fd fd 41 6d 23 fd 66 fd 10 50 04 05 30 fd 1f 64 41 fd 14 fd fd fd 62 fd 13 fd 7c 3c 0c fd 21 10 4e 64 19 fd fd 2a 1e 7c 6a fd 6a 6a 39 fd 47 fd fd c3 36 6c fd 32 15 fd 44 00 0b 5b 50 36 55 fd fd 04 3e 4e 49 fd fd 78 22 70 fd fd 0b fd 5a fd fd 73 67 fd fd 5d 68 00 fd 44 fd 5a fd 42 fd fd fd fd 7a fd 74 fd fd 6f 41 38 06 fd 18 25 fd 30 fd fd fd 3c 32 fd 57 38 65 08 b5 fd 24 61 fd fd 6a 16 fd fd 33 51 fd fd 29 7b fd fd 0e 4c 76 6a fd 05 fd fd 33 fd fd 10 2f 3b fd fd fd 04 49 fd 47 fd 30 6e 13 fd fd fd fd 5d fd fd 77 fd 2c fd 00 04 fd 25 52 36 4a 56 fd 73 fd 48 1d 1e 3e 30 fd 74 33 fd fd 32 fd fd 34 fd 65 2e fd 2a fd fd 09 29 29 fd 21 0c 54 fd fd 66 41 6f 50 15 09 fd 53 0c 70 1f	*mAm#P0dAb !Nd* jjj9G6 l2D[P6>N lx"pZsg]hDZBztoA8%0<2 W8e\$aj3Q) {Lvj3/;lG0n]w,%R6JVSH> 0t324e.*)!TfAoPp	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3 \Examples\notepad2.au3	1939	10	24 00 fd 05 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\Program Files (x86)\Autolt3 \Examples\notepad2.au3	0	1415	0d fd 4c fd 5c fd fd 5b 83 39 fd 57 fd fd 21 76 fd 0e fd 64 fd fd 2d fd 76 09 fd 52 54 fd 12 05 35 4d fd 68 0c 67 54 fd 55 fd 5c 11 fd 52 25 37 fd fd fd fd 5c fd 68 7a fd fd fd 60 7a 28 fd 11 fd fd fd 38 1f 6a fd 00 fd fd fd 0d fd 4c fd fd 43 59 fd 1e 7b 19 fd 4c fd 2a fd fd 59 30 fd 51 2c fd 32 0c fd 62 fd 3e 01 fd fd 55 fd 38 fd 79 71 fd fd 38 76 11 03 7c fd fd fd fd fd fd 6a 2b 7d 07 42 22 22 36 0c fd 2a 02 78 45 fd a7 fd fd 17 fd fd 46 fd fd fd 55 fd 0e fd 47 75 0e 60 fd 16 fd 39 4b fd 7f fd 47 78 5c fd 60 20 31 03 fd 40 5d fd 44 58 fd fd fd fd 2b 53 fd 4c 59 18 fd 12 fd 67 fd fd fd fd 23 54 fd a1 08 fd 01 74 4d fd fd 71 63 37 fd 79 fd 4e 05 fd 68 7d 66 57 0f 3e 6a fd fd fd 11 64 fd 48 fd fd f9 23 fd fd 00 fd fd 7f	L[9W!vd- vRT5MhgTU\IR%7\hz`z(8j LCY{L*Y0Q,2b>U8yq8vj +}B""6*xEFUGu`9KG\ 1@]DX+SLYg#TtMqcyNh }fW>jdH#	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Microsoft SQL Server\110\3\ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ ____ _ _ _ _ _ _ _ _ _ _ _ _ _ / / _ _ _ _ _ . ' _ _ _ _ _ _ _ _ \ / / _ _ _ _ / _ _ _ _ _ _ _ _ / _ _ _ _ _ / By now it's probably painfully apparent that your envir onment hasbeen infected with r	success or wait	1	F358DF	WriteFile
C:\Program Files (x86)\Autolt3 \Examples_ReadMe_.txt	207	524	20 fd fd fd 4b 0b fd 6a fd fd fd fd 43 7a 23 05 27 fd 18 0f fd 3c 38 1d 64 0f fd 5c 37 2e 7b 22 fd 23 19 52 7c fd 45 62 1d fd 12 73 4f fd 09 e1 fd 0e 1c 46 4e 1d 3c fd 3b 64 05 21 63 fd fd 31 3e fd 08 23 fd fd 61 69 fd fd 3a fd 4e ef fd fd fd fd 6d fd fd fd bf fd fd fd 15 fd fd 31 38 49 58 74 fd fd fd 46 65 6a fd 78 05 79 fd 43 fd 69 28 fd 73 45 fd fd 16 fd 0f fd fd 5f fd 35 19 fd 40 fd 6b 65 7b 3b fd fd 59 2a 0c 23 fd fd fd 4a fd fd fd fd 39 26 fd 7d fd fd 19 fd 6c 76 49 25 7a 0f 57 fd 22 fd 03 07 22 fd 74 fd fd fd fd 02 19 fd fd 40 53 07 fd fd 44 57 fd 11 4e 23 fd fd fd 3f fd fd fd 17 fd 2c 47 5b fd 02 fd 6e 0e fd fd fd fd 12 60 19 fd 60 5c fd 79 fd 6a fd 6d 4e 49 37 4c fd 5c 7f fb fd 2b fd fd fd 3e 3d 13	KjCz#<8\7. {"#R EbOFN<;dlc1># ai:Nm18IXtFejxyCi(sE_5 @ke{;Y*# 9&]lv!%zW""t@SDWN#?, G[n``lyjmNI7L\+=	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3 \Examples_ReadMe_.txt	731	10	24 00 fd 00 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\Program Files (x86)\Autolt3 \Examples_ReadMe_.txt	0	207	fd fd fd fd 64 5f 67 32 fd 1f fd 90 3d fd 1b 23 fd 2d fd 06 fd 38 fd fd 52 7a 7e fd 02 46 97 62 fd 35 53 59 10 1a fd fd fd 6d 05 fd 65 35 fd 52 21 fd 4b fd 1d 51 24 fd 6d 39 fd 24 6c 56 fd fd fd 71 fd fd fd fd fd 79 12 19 03 fd 3b fd 67 fd fd fd fd fd 3c 0e fd 7c 4c fd fd 5d 20 08 11 5b 37 1b 79 fd 4c fd 20 48 58 fd 67 fd 7d fd 06 73 28 fd 54 fd fd 58 fd 47 2d 34 fd 29 68 fd fd fd fd 7a fd 08 45 1d 32 fd 78 fd 0f 02 fd fd fd 49 28 4f 0c 43 4d fd 0e 76 6f 11 fd 72 4d fd fd 6b 66 5f 6b 59 fd 7a fd fd 39 fd fd 26 fd fd fd 64 fd 48 20 fd 74 fd fd 4c 74 57 fd 09 fd fd 48 6d fd 0a fd 4e fd 13	_g2=-#- 8Rz~Fb5SYme5R!KQ\$m 9\$IVqy:g< L] [7yL HXg)s(TXG-4)hzE2xl (OCMorMkf_kYz9&dH tLtHmN	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3\Extras_ReadMe_.txt	177	524	33 fd 4e 7b fd fd 1d 76 fd fd fd fd 7f 65 fd fd fd 50 fd fd 7e 33 42 fd 71 fd fd 00 fd fd fd 6b fd fd 05 fd 48 fd 0e fd 2d aa fd fd fd 4f fd 20 fd 77 fd 77 fd 54 fd 08 fd 57 fd 1f fd fd 0e 2c fd 1c fd 10 fd 31 fd fd 0a 7e fd fd fd 42 11 fd fd fd 00 7a 2f fd 4b 4f fd 44 fd 2f fd 4c 3b fd 47 13 32 64 fd 7b fd 17 07 34 56 fd 03 fd fd 63 fd 26 fd fd 49 fd fd 50 fd 63 fd 59 4c 14 05 61 6b fd 2a fd 96 2f 03 fd fd fd fd 77 4f 5b fd 1e fd 10 23 24 fd 34 7d 78 fd 0d fd fd fd 62 1a 2a 3d fd fd fd 12 64 fd 76 1f 7f 5e 62 fd 04 25 03 fd fd 14 40 5a 52 16 37 fd 33 34 fd 2a fd fd fd 1c 13 fd fd 28 33 41 00 1e 3b 40 fd 0c fd fd fd fd fd fd fd 67 5f 0a 6d 06 02 8b 47 fd 34 53 1b 2b fd fd fd 07 fd 43 3b 66 fd 5c fd	3N{veP~3BqkHO wwTW,1~Bz/KOD/L; G2{4Vc&IPYLak*/wO{#\$4 }xb*=dv^b@ZR34* (3A:@g_mG4S+C;f\	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3\Extras_ReadMe_.txt	701	10	24 00 fd 00 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\Program Files (x86)\Autolt3\Extras_ReadMe_.txt	0	177	62 fd 5d fd fd fd 3f 3d fd fd fd fd 2c f8 4e fd 7c 1c fd fd 34 fd fd 0b 50 fd fd 36 70 fd 00 3c 02 1a 08 55 4b fd 3b 6f fd 77 fd fd 3a fd fd fd fd fd fd fd 44 6c 66 29 23 49 59 10 10 7d 75 fd 0e fc fd 0b fd 46 23 7b fd 48 41 3a fd 53 12 fd 03 25 46 00 40 74 57 fd fd fd fd 5c 02 5b 6a 35 fd 40 fd 48 2a fd 17 fd fd fd 41 3b fd 4b 47 fd 11 6a 6d fd 73 fd 49 3c fd fd 79 38 fd fd 27 64 56 1d 74 2c 47 fd 6c fd 67 4a fd 62 54 24 fd fd fd 2e 16 34 fd fd fd 38 fd 1e fd fd 2d fd 79 7b fd 03 0c 21 0f fd fd 51 fd	b]? =, 4P6<UK;o:DI{)#Y}uF# {HA:S%F@tW\ [j5@H*A;KGjmsl<y8'dVt, GlgJbT\$.48-y{!Q	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Autolt3\icons\lau3.ico	31526	524	fd 6d fd 7d 6f 5d 1f fd 1b fd fd 1a 71 01 fd fd fd 53 fd fd 3d fd fd 21 0d 34 57 32 30 fd 73 50 7b fd 5e fd fd fd 14 68 6c 6c 09 68 fd 49 fd 66 24 02 54 fd 30 fd 3f 2e fd 26 38 fd fd fd fd 08 14 fd 1e 76 51 04 0f 0d fd fd fd 7a fd 6c 6b 1b 32 fd 99 60 fd 45 41 fd 46 06 fd 48 fd 5c fd 0d 1e 25 15 7b 18 6e 2c 5a fd fd 47 fd fd fd 69 16 fd 26 fd fd 52 fd 02 fd 5e fd fd fd fd 06 fd 16 fd fd fd 2a fd 3b fd fd fd fd 6e 11 2e 69 fd 0e 5f 62 fd fd 0f 64 5f 5e 2d 21 fd fd 05 45 16 fd fd 17 fd 2e fd 67 fd 3e fd 0a fd fd 09 03 2d fd 70 27 fd fd 62 11 fd fd 6d fd fd fd 42 2a 1b fd 7f fd fd fd fd fd de fd 66 fd 20 fd 13 fd fd 0b 39 fd 2b fd 61 34 fd 19 55 fd fd 17 fd 76 0b 1b 18 48 fd fd 47 28 59 19 fd fd 7d fd 2b fd 18 1c fd	m)o]qS=I4W20sP{^hllhlf\$ T0?.&8vQzlk2'EAFH\% {n,ZGi&R^*;n.i_bd_^~ !E.g>-p'bmB*f 9+a4UvHG(Y)+	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3\icons\lau3.ico	32050	10	24 00 26 7b 00 00 00 00 00 00	\$&{	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3\lconslau3.ico	0	31526	5a fd 7d fd 04 19 fd 47 fd fd 44 55 fd fd fd fd fd fd 54 fd 5e 47 02 fd fd fd 0c fd fd 36 b5 e5 63 fd fd fd d5 fd 67 55 36 fd fd fd 0e fd 6b 12 2e 6a fd fd fd 77 0b 14 59 fd 06 69 2d fd 0d fd 6f 03 fd fd fd fd 13 6d 2b 7f 28 4d 7c fd 4c 74 41 3e fd fd 3a 64 fd 10 02 fd 24 56 fd 60 fd fd 5f fd fd 58 fd fd 00 0e e9 fd 7e fd fd fd fd 85 77 fd 06 2d 50 1a fd 01 33 07 7f fd fd 36 fd 0b fd fd fd 03 5e fd 45 fd 13 fd 4d 57 fd 4e fd 47 10 0f fd a2 fd 62 fd 33 fd 45 fd 38 3b fd 71 1f fd fd fd fd 47 fd 56 2e fd 3d fd fd fd 54 fd 31 43 16 26 fd fd 56 7f fd 11 10 3a fd 7f fd fd 6a 7d 48 fd fd 69 73 14 ad d0 db fd 1c fd fd 20 fd 5a de 1c fd fd 63 76 fd fd 71 2f 1b fd fd 7b fd fd fd 73 04 fd 33 4f fd fd	Z}GD^G6cgU6k.jwYi-om+(M LtA>:d\$V`_X~w-P36^EMWNGb3E8;qGV.=T1C&V:;)His Zcvq/{s3O	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Autolt3\lconslau3script_v10.ico	71546	524	36 fd fd fd fd 79 fd fd 0e fd 72 69 2b 79 fd fd fd fd 2b 68 5f 4c 65 fd 63 fd fd 5c fd 68 0b 12 fd fd fd c4 79 fd 54 d7 73 fd fd 05 40 fd 44 5f 7a 52 63 fd 0b fd fd fd 66 66 2b fd 50 4d 18 7d 45 fd fd fc 37 5a fd fd fd 05 63 fd 2d 79 fd 02 01 4f 14 a1 fd 73 3c fd 38 fd fd fd 42 fd 31 47 3f 0b fd 3b 3e fd 3c 71 fd 12 3f 17 11 71 17 fd 07 fd 76 27 fd fd 2a fd fd 31 78 fd fd 50 fd 3e fd 62 32 fd 09 fd 1b 63 fd fd fd 1d 79 2c 1b fd fd 47 fd d6 fd fd 65 6f fd fd 06 fd fd c4 7a 42 72 44 fd fd 57 fd 3b fd 27 fd 1f 29 76 fd fd 64 1d fd 2e fd fd fd 72 fd 4f fd 9f fd 10 fd 0c fd 15 3f 4e fd fd fd fd 43 50 49 fd fd 02 fd fd 00 6f fd 30 79 fd 22 7f fd 0a 6a fd 52 31 68 54 fd fd fd 1d 71 fd 0e fd fd 0d 74 60 51	6yri+y+h_Lec hyTs@D_zRcff+PM}E7Zc-yOs<8B1G?;><q?qv*1x>b2cy,GeozBrDW;')vd.rO?NCPlo0y"R1hTqt`Q	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3\lconslau3script_v10.ico	72070	10	24 00 7a 17 01 00 00 00 00 00	\$z	success or wait	1	F2CC68	WriteFile
C:\Program Files (x86)\Autolt3\lconslau3script_v10.ico	0	71546	19 fd 3a fd 76 13 fd 77 fd 46 fd fd fd 65 0b fd 43 fd 15 26 70 fd fd 63 fd 5c fd fd 7f fd fd 06 fd fd 70 64 fd 06 57 fd 62 c7 fd fd ee fd fd fd fd fd 4f 3b fd fd 36 11 05 07 fd fd fd 00 74 62 fd f3 1e fd fd 3c 2a fd 03 fd 30 31 48 fd fd b0 fd fd 13 fd 55 6e 63 fd 46 fd fd 75 fd 12 fd fd 0b 70 4c 01 1f 16 fd 2a 3e 2e 5e fd 4d ea 63 fd 26 4c 41 36 21 e0 15 fd 37 6f fd fd 2d 02 fd fd fd 03 fd 3c 05 6a 3d 4c fd fd 48 fd 04 fd fd fd fd fd 4f 56 68 1f fd 41 2c 42 fd 2c 7d 37 1a 32 4a 78 4c 04 0f fd fd b1 fd fd 64 fd fd 4e fd fd 44 fd fd 11 5c fd 5f fd 69 fd fd 5b 44 7d 7f fd fd 6d 04 fd 4a fd 47 fd 04 65 2b 6d 79 fd fd fd 34 fd 1a 3e d7 61 13 fd fd 5c fd 47 fd fd 34 22 78 76 fd 35 fd fd 1f fd fd 26 16 0b fd	:vwFeC&c dWbO;6tb<*01HUncFupL*>.^Mc&LA6!7o-<j=LHOVhA,B,}72JxLdND_i[D}mJGe+m4>a\G4"x5&	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3\Icons\lau3script_v9.ico	25214	524	25 25 5a fd fd 32 fd 78 fd 05 fd fd fd 5f 33 fd 79 fd 33 fd fd fd fd 37 fd fd fd 45 56 01 fd fd 2b 31 fd fd 75 fd 4d fd 65 fd 1b 58 fd fd fd 63 7f fd fd 22 6b fd 4a 40 47 27 5b 64 fd fd fd fd 2b fd 2f 15 fd fd fd 66 66 09 45 58 fd 62 4a fd 68 1d 7f 13 63 07 fd fd a9 68 fd 31 32 fd 51 46 5f 12 60 20 0b 42 62 fd 4c fd 08 fd 6d d7 3a fd 6c fd 45 fd fd fd fd 48 7a fd fd 2f fd fd fd 0e fd fd fd fd 47 fd 03 61 fd fd 32 2f 52 78 48 2a 43 7e fd fd 45 7b 52 fd 1a 14 fd 13 3f 69 48 57 fd fd 4f 40 1f fd e0 7b 27 62 12 0a fd 1e 21 fd e2 fd 2e 2a fd 7b 1d fd fd fd fd fd 13 05 02 1b 3b 3e fd 6f fd fd 2f fd 0e 27 56 fd fd 1d db fd 20 71 fd 68 28 33 39 fd 17 2f 14 fd 3e 52 fd 2b 37 30 72 7a 4e fd fd 4c 00 fd 5d 32 2d fd fd	%%Zx_3y37V+1uMeXc"k JG'[d+/ffEXbJhch12QF_` BbLEHz/Ga2/RxH*C~E {R?iHWO@{'b.*{;>o/^V qh(39/>R+70rzNL]2-	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3\Icons\lau3script_v9.ico	25738	10	24 00 7e 62 00 00 00 00 00 00	\$~b	success or wait	1	F2CC68	WriteFile
C:\Program Files (x86)\Autolt3\Icons\lau3script_v9.ico	0	25214	10 fd 74 fd 22 71 a4 fd 33 36 43 fd 40 78 0c 13 52 fd fd fd fb 2c 2c fd 53 4b fd 2d fd 52 fd 27 fd 5c 77 14 dc fd 6d fd 43 fd fd fd 0f fd fd fd 6a fd 61 fd 0d 5c fd fd fd fd 65 66 a8 fd fd 19 fd fd fd 68 11 5e 3f fd fd fd fd 38 7d fd fd fd 65 21 06 29 33 3e 3e 71 fd 51 fd fd fd 27 1e fd 45 fd 6a fd fd fd 76 fd 7d fd fd fd 42 0f fd 71 02 0e 04 fd 7c fd 3c 43 fd 73 fd fd 12 21 27 05 5f 76 fd 23 fd fd 5a 5d fd fd fd 13 23 fd fd fd 38 73 fd fd fd 14 fd fd fd 78 fd 62 7a 4f 16 18 fd 4a 58 34 01 0c 14 25 3a 3c 57 29 08 26 6d fd fd fd 0c 74 77 7e fd 01 32 fd 5c 02 25 fd 23 66 2e 7b fd 6e fd fd fd fd fd 63 fd fd 16 75 4e 2d 51 fd 02 26 53 fd fd fd 45 1e 7b 74 5b 55 5d fd 78 2e fd fd fd 76 fd 3f fd fd 3f fd d0 13 fd 1b fd fd fd fd 78 fd 31	t"q36C@xR.,SK- R"\wmCjalefh^?8} e!)3>>qQ'Ejv}Bq<Cs!_v# Z]#8sxzOJX4%: <W)&mtw~2\%#f.{ncuN- Q&SE{t[]x.v??x1	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Autolt3\Icons\filetype-blank.ico	33584	524	59 21 48 34 0b 34 11 4d fd 6d 1e 11 fd 3d 77 fd fd fd 4c fd 35 fd fd 58 fd 6d 32 fd fd 38 27 5d fd 5d 5d fd fd fd fd 33 2b 3a 4d fd fd fd fd 10 fd fd fd 4e fd 44 4a 0b fd fd fd 12 fd fd 1e 1b 71 fd fd 27 fd fd 28 fd fd fd 04 02 c6 4e fd 05 3c 07 2a 58 0b 35 00 25 71 fd fd fd 01 fd fd dc fd 6d 43 03 13 17 55 fd fd fd 28 fd 6f fd 1d 46 fd fd 49 04 44 fd 4b 05 fd 3f 66 4a 2a fd 02 fd 2f 57 70 39 fd 33 fd 01 06 21 fd 2f fd fd 3d 27 36 fd 4d fd 6c fd 65 31 77 fd 49 fd fd fd 59 2d 3e 13 fd fd fd 1d fd fd 02 fd 7b 1d fd 3e fd 67 fd fd 54 fd fd 62 5d fd fd ee 25 0e 14 78 fd fd 2c 78 6e 3d 2c fd fd fd 5e 18 fd fd 29 0e fd 1e 23 fd 5c 4d fd fd 03 33 27 fd 0e 01 61 0f fd fd 4d 52 fd 7d fd fd 36 7f fd 27 15 5a 44 6b 0e fd 3f fd 4b fd fd fd 74 fd	Y!H44Mmw5Xm28']]]3+: MNDJq'(N<*< X5%qmCU(oFIDK? fj*/Wp93I/='6Mle1wlY-> {>gTb]%x,xn=,^)#\M3'aM R}6'ZDk?Kt	success or wait	1	F2CBF8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3\icons\filetype-blank.ico	34108	10	24 00 30 fd 00 00 00 00 00 00	\$0	success or wait	1	F2CC68	WriteFile
C:\Program Files (x86)\Autolt3\icons\filetype-blank.ico	0	33584	0f 57 21 66 fd fd 10 fd 50 fd 41 fd 06 fd 18 3d 7c fd fd fd fd 48 5f 31 65 67 fd fd 2d 5c 50 19 fd 79 fd fd fd fd 1a 58 45 08 1c 38 fd 42 57 4b 48 05 fd 1f fd 0b fd 27 45 fd 2c fd 3e 79 5d 56 6d 17 35 51 5b 5f fd fd fd 50 58 14 13 fd 6c 1f 45 36 fd 40 2a 5c fd fd fd 02 56 fd 03 fd 5a 1f 46 64 05 fd 4f 32 fd fd fd fd 00 fd fd 30 fd 0e fd 07 73 fd 11 37 79 fd fd 3c fd fd fd 08 1c fd 48 5e fd 5d 04 fd 05 fd 28 fd 41 af 56 25 29 fd fd fd 5d 58 fd fd e1 fd 49 5e fd fd 3b 5b fd fd 5b 2e fd fd fd 2f 7d 60 61 fd fd fd fd 07 fd 2e fd 3a 0e fd 0d fd fd fd fd 0a 36 7d 76 0d fc fd 25 fd 44 4e fd fd fd 38 09 fd 26 fd 59 7e fd 32 fd fd 7e fd 79 14 fd 65 7d 32 fd 13 fd 1d fd fd 91 5f fd 72 fd fd fd 38 fd fd fd	W!fPA= H_1eg- \PyxE8BWKH'E,>y]V m5Q[_PXIE6@*\VZFO07 y<H^](AV%)X!"; [[./a.:6)v%Dn8&Y~2~ye} 2_r8	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Autolt3\icons\MyAutolt3_Blue.ico	7406	524	4f 4f 28 15 43 fd 44 70 7c fd fd 4f 33 52 fd 30 fd fd 5b fd fd fd fd fd 38 fd 24 4a fd fd 5b 38 fd fd fd 3e 34 fd 14 2b 5d fd 3f fd 5b 7d 5c 0e fd 07 fd fd 0a fd fd fd fd fd fd 79 fd 5a 2e 56 3a fd 22 66 01 fd 0e 74 19 fd fd 38 fd 1f fd fd fd 5a 21 1a 3d 24 13 37 61 4b 53 fd fd 35 ce 09 5f fd fd fd 16 25 fd 0d fd fd 78 40 fd fd 2e 7f 35 71 fd 21 fd fd 45 fd fd 48 fd fd 05 5f 78 38 4e 0e 58 fd fd fd fd 1d 36 fd fd 41 fd 49 44 fd fd 60 fd 62 fd fd fd fd 18 fd 0b fd 73 fd 25 fd fd 73 65 30 00 fd 32 41 35 4d fd fd 43 3f fd fd fd fd 58 32 67 5e fd 53 59 fd 6a 6e 2e 17 08 fd 75 70 2b 18 2e fd fd 2e fd 48 76 fd 74 4f 2c 0d fd 01 1e fd fd fd fd 3d fd fd 72 fd fd fd fd 22 05 fd 2b fd 32 15 0b fd 5a 21 4a 5b 7f 3f fd fd 4c	OO(CDp O3R[8\$J[8>4+]? []yZ.V:." t8Z!=\$7aKS5_%x@.5q!E Hx8NX6AID` bs%se02A5C? X2g^SYjn.up+...HvO,= r"+ZJ[?L	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3\icons\MyAutolt3_Blue.ico	7930	10	24 00 fd 1c 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\Program Files (x86)\Autolt3\icons\MyAutolt3_Blue.ico	0	7406	fd 42 68 25 cf fd fd 3d fd 7b fd fd 0f fd 7e fd 56 fd fd fd 79 64 4b fd fd 71 fd 28 fd 20 59 fd fd fd 1c 0a 37 fd fd fd 4c fd fd fd 1c fd 20 fd 27 0e 70 0b fd fd 42 d7 b5 0f fd fd fd fd 04 0e fd fd 4b 68 20 fd fd 44 fd fd 57 fd fd 31 b7 6b 08 fd fd 5e 44 fd fd fd fd 14 09 75 41 45 fd fd fd 7f fd 2a fd 4d fd fd 23 fd fd 17 4f fd 7a 4a fd 68 fd fd 3b 61 4c fd fd 08 7a fd 4b fd fd fd fd 25 fd 14 63 fd fd fd 50 0d 48 0e fd 57 fd fd 75 18 48 5b fd fd 7c 4e fd fd 33 01 fd fd fd fd fd 4f 2b 73 fd 35 2b fd fd fd 40 fd fd fd fd 36 35 15 fd fd fd 61 fd 35 6b 4a fd 1c fd 3a 41 42 69 1a 2e fd 21 78 45 28 fd 56 fd 43 fd fd 4e fd 76 62 72 fd 2c 1c fd 76 36 1e fd 54 77 6b fd fd 74 fd 2f 33 6d 66 36 fd fd fd fd 23 fd fd 7c 75 4d 76 00	Bh%={~VydKq(Y7L 'pBKh DW1k^Du AE*M#OzJh;aLzK%cPH WuH[]N3O+s5+ @65a5kJ:ABi.lxE(VCNvb r,v6Twkt/3mf6# uMv	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Microsoft.NET\Primary Interop Assemblies\IR3ADM3.txt	0	1290	20 5f 20 5f 5f 5f 5f 5f 20 20 5f 5f 5f 5f 20 20 5f 5f 5f 5f 5f 0d 0a 7c 20 5c 20 7c 20 7c 7c 20 5f 5f 5f 20 5c 2f 20 5f 5f 5f 7c 7c 20 20 5f 5f 5f 7c 0d 0a 7c 20 20 5c 7c 20 7c 7c 20 7c 5f 2f 20 2f 20 2f 5f 5f 5f 20 7c 5f 5f 5f 20 5c 0d 0a 7c 20 2e 20 60 20 7c 7c 20 5f 5f 5f 20 5c 20 5f 5f 5f 20 5c 20 20 20 20 5c 20 5c 0d 0a 7c 20 7c 5c 20 20 7c 7c 20 7c 5f 2f 20 2f 20 5c 5f 2f 20 7c 2f 5c 5f 5f 2f 20 2f 0d 0a 5c 5f 7c 20 5c 5f 2f 5c 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 5c 5f 5f 5f 5f 2f 0d 0a 0a 42 79 20 6e 6f 77 20 69 74 27 73 20 70 72 6f 62 61 62 6c 79 20 70 61 69 6e 66 75 6c 6c 79 20 61 70 70 61 72 65 6e 74 20 74 68 61 74 20 79 6f 75 72 20 65 6e 76 69 72 6f 6e 6d 65 6e 74 20 68 61 73 0d 0a 62 65 65 6e 20 69 6e 66 65 63 74 65 64 20 77 69 74 68 20 72	_ _ _ _ _ _ _ _ _ _ \\\n _ _ _ _ _ _ \\ \n// _ _ _ _ \\ . ` _ _ \\ _ _ \\ \\ _ _ / _ /\\ _ / _ _ \\ _ _ _ _ _ _ _ _ _ _ /By now it's probably painfully apparent that your environment has been infected with r	success or wait	1	F358DF	WriteFile
C:\Program Files (x86)\Autolt3\icons\MyAutolt3_Green.ico	7406	524	fd 37 fd 70 fd 61 fd 76 fd 52 fd 2f fd fd 4a fd 0a fd fd 4e fd 7c fd fd 4b 04 fd fd 0b fd fd 39 fd 50 24 1f 4f 22 51 fd 15 9b fd 14 31 59 fd 00 6b fd fd fd 6f 72 25 fd fd 2d 3e 19 1d fd 42 fd fd 02 fd fd cd 23 fd 06 fd fd fd 7e fd 4c 5f fd 4c 37 25 3e 0f 0d 1c fd 5d fd fd fd fd 71 32 12 5b 3f fd 24 fd 8c 55 fd 09 fd 20 fd fd 6b 02 fd fd 18 2c fd fd 41 fd 43 1e fd 46 76 7a 45 00 fd fd 25 60 fd fd fd 33 fd ad 47 1f 7c 4e 03 fd 6d 4b 42 fd 3f fd 5f d5 fd fd 6a fd 0c fd 03 7e fd fd 55 fd fd 6a fd 08 fd fd f9 7c 03 2e 1b 4e fd fd 19 2d 6e 2d 09 fd 33 fd ea fd 6f fd 40 10 41 44 fd 5a 46 30 fd fd fd 62 fd 71 fd 14 04 1e 66 1f 5a fd 28 55 fd 20 62 fd 0a fd fd fd fd 15 25 16 19 05 fd 00 fd fd 73 7b 34 5e fd fd 19 34 fd 54 fd fd	7pavR/JN K9P\$O"Q1Ykor%->B#~L_L7%>]q2[?\$Uk,ACFvzE%`3G NmKB?_j~Ujj.N-n-3o@DZF0bqfZ(U b%s[4^4T	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3\icons\MyAutolt3_Green.ico	7930	10	24 00 fd 1c 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3 Icons\MyAutolt3_Green.ico	0	7406	cd 77 fd 7d fd fd fd fd 01 13 24 08 fd 3a 7a fd 78 6f 5a 93 fd 6e 50 3d fd 34 5a fd 6d fd fd 15 37 fd 10 59 fd 69 fd fd fd 40 15 4c fd fd fd fd 47 fd 2a fd fd 4a fd fd fd 4d 0a fd 42 5f 70 fd 22 fd 0e 1a 3a fd fd 25 2f fd 5e fd fd fd fd 40 40 fd fd fd 07 0d fd 52 fd fd 0f fd fd fd fd fd fd 03 fd fd 3a fd 7e fd fd fd fd 06 77 5b a7 fd 37 05 fd 50 69 2f 0e fd fd fd fd 68 31 29 2b 6b fd fd 20 05 0d fd 72 fd fd 5c fd 73 fd 3d 74 22 4c 4f 15 0d fd 36 fd fd fd fd 27 4c 61 fd 0e 4c fd fd 08 fd fd 56 fd 5e fd fd 39 fd 4e 3f fd 60 fd fd 5d fd 24 3d fd 6f 7e 68 59 fd 3a fd 03 fd fd 43 3c fd 18 1d fd fd 51 fd 2b fd 3e fd fd 72 fd 2f fd fd fd fd d3 21 fd 7b 0c 14 fd 32 76 fd 3c 44 27 fd 72 fd 03 fd 72 2a 2a 2a f4 32 fd fd 0e	w)\$:zxoZnP=4ZmYi@LG *JM_p":%/^@ @R:~w[7Pi/h1)+k r!s=t"LO6!LaLV^9? `]\$=o~hY:C<Q+>r/! {2v<D'rr***2	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Autolt3 Icons\MyAutolt3_Red.ico	7406	524	5e 61 37 3f fd fd fd 47 fd 6f fd 56 fd 28 17 05 5c fd 1d fd 7a fd 03 fd fd 4f fd 61 fd 3a 3c fd 02 03 fd 7a fd 4c 08 f1 fd 56 19 fd fd 19 28 fd fd fd 68 fd 68 5b 41 58 48 fd 7a fd 16 39 18 fd a3 fd fd fd fd 18 1b fd 55 07 fd 11 fd 24 fd fd 76 58 22 31 0b fd 7d fd fd 72 71 02 fd fd 0e fd fd 43 fd fd 27 fd 0f fd 33 40 fd 02 fd 74 3a fd 13 fd 61 69 57 fd 17 fd 52 fd fd 3a 04 31 29 fd fd fd 6a 68 66 3c fd 7c fd fd 5e 05 fd fd 37 3f fd fd fd 17 3e fd fd d1 fd fd fd 16 72 1e 51 fd fd 79 fd 15 6b fd 53 6e fd fd 4d fd fd 34 20 4c 16 55 64 08 2d 0a 03 fd fd 32 fd fd 4f 79 fd 03 fd 05 61 fd 38 50 45 fd fd 79 fd 1f fd 41 fd fd 08 c7 49 fd 4e 4d fd 7c fd fd fd 39 06 fd 1d fd 52 fd 28 6c 50 37 25 6d 2f fd 3b fd fd 2d fd 28 db	^a7?GoV(\Oa: <zLVhh[AXHz9U\$vX"1 }rqC'3@:aiWR:1)jhf<^7? >rQykSnM4 LUD- 2Oya8PEyAINM 9R(IP7 %m/;-{(	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3 Icons\MyAutolt3_Red.ico	7930	10	24 00 fd 1c 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\Program Files (x86)\Autolt3 Icons\MyAutolt3_Red.ico	0	7406	45 3b 6d 7a fd 73 11 fd fd 1b 36 fd fd 11 fd 32 4c fd 10 fd fd 1e 3e cc fd fd 40 3b 3d 57 88 6d 5b 0a 54 fd 18 2a fd 64 3f 3e fd fd 5d 6b 78 fd fd 13 35 fd 78 2e fd fd 6a fd 03 6c 05 7f 48 fd fd 12 fd fd 5e fd 2a 3c 6a 4f 77 fd fd 41 1d 2e fd 10 fd 28 2c fd 3d fd fd 5e fd 25 fd 48 1a 54 fd 3a fd b2 14 fd a2 fd 11 26 71 62 fd 09 21 fd 7e fd fd 34 fd fd 74 18 3e 6a fd fd fd fd fd fd 67 fd fd 54 fd fd 5e fd 5f fd 3d 25 06 25 37 fd 79 fd fd fd 16 fd fd 01 fd 63 02 fd 33 fd fd fd fd fd fd 10 fd fd 0b 0a 16 41 fd fd 49 0a fd 5f fd 7f fd 94 50 6c 33 19 fd 0e 7c 44 59 fd fd fd fd 44 fd 14 1c 3c 04 0d fd fd fd 65 6a 3a 07 fd fd fd 02 2a 3b 61 fd fd 5d 2e df fd fd 6c 24 41 fd 51 4c fd 10 fd 3a fd fd fd 5e fd fd fd 66 40 1a	E;mzs62L>;=Wm[t*d? >]kx5x.jlH^*<JOWA. (,=^%HT:&qbl~4t>jgT^_= %% 7yc3AI_Pl3 DYD<ej*;a].l \$AQL:~f@	success or wait	1	F2C055	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3 Icons\MyAutolt3_Yellow.ico	7406	524	fd 03 fd fd 2e fd 69 6c 6b 50 34 0c 11 fd fd fd fd fd fd fd 3a fd 67 fd 06 fd 2e 17 fd 44 fd fd 28 fd fd fd fd fd fd 15 09 0a 24 fd 34 77 fd 60 fd ea fd 48 08 15 7e 6e fd 11 1a fd fd 6c 5c fd 3d 10 74 fd fd 4f 09 22 c2 73 fd 93 fd 34 3c fd fd fd 6a fd fd 18 6b 27 21 fd fd fd 48 6c fd 19 fd fd 1e fd fd 47 40 5f fd a4 fd 03 26 4e fd fd 6c fd 3d 7c fd 40 6c 16 fd fd 39 fd 17 fd 79 49 2a fd fd 1a 13 20 fd fd 4b fd 31 fd 5d 49 2e fd 16 fd 4f fd 28 68 fd fd 34 19 fd 64 33 fd 24 1c 7e fd fd 7c fd 5b fd 08 0e fd fd 65 fd 17 78 fd fd 1c 6c fd fd 0e 74 fd 58 5e 45 fd 71 fd fd 32 47 2d fd fd fd fd fd 32 49 7a fd 57 2b fd fd fd fd fd fd fd fd 26 fd 1d 3a fd fd fd 09 fd fd 05 21 fd fd fd 09 fd fd 2b fd fd 10 fd fd 1e 63 fd 50	.ilk4:g.D(\$4w' H~n\ =tO"s 4<jk'!HIG@_&NI= @!9y!* K1]!.O(h4d3\$~ [exltX^Eq2G- 2lzW+&:!:+cP	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3 Icons\MyAutolt3_Yellow.ico	7930	10	24 00 fd 1c 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile
C:\Program Files (x86)\Autolt3 Icons\MyAutolt3_Yellow.ico	0	7406	74 55 1b 0e 04 72 4e 09 02 b1 44 fd 79 fd 28 51 fd 53 fd 12 fd fd b1 1c 72 fd 0c fd fd fd 3f 67 5f 12 12 6b fd 10 32 fd 0c fd 51 fd fd fd 0b 16 fd 12 fd 3d fd fd 69 fd 05 52 fd 05 fd a6 35 fd 40 5a 51 05 64 16 55 fd fd fd 6b fd 7a fd 1f 60 77 fd 04 0f 9f 7f fd fd fd fd 58 62 5a fd 28 7c 43 21 73 4e fd 18 12 fd fd 62 fd fd 7b 1f fd fd 19 20 45 5a 12 fd fe 74 fd fd 64 fd 1e 12 fd 41 fd 77 1e 6e fd 31 75 68 fd fd 3b 78 55 fd fd 3a fd 07 5b 3c 3b 28 49 fd fd fd 54 fd fd 24 fd fd fd fd fd 03 fd 6a 14 7e fd fd 5b 7a 24 64 61 fd 29 45 57 21 39 fd 33 fd 0a fd 10 73 64 6d 71 fd fd 64 11 28 6f fd 1d 26 fd 1a fd fd fd fd fd a7 23 fd e0 b2 bb 9a 3f 21 41 fd fd fd 35 4c fd 66 5c 7d fd 10 fd 6d 20 fd 2e 0b fd a1	UrNDy(QSr? g_k2Q=iR5@ZQdUkzwX bZ{[C!sNb{ EZtdAwn1uh;xU:[:;(IT\$~ [z\$da)EW!93sdmqd(o&#? !A5Lf})m .	success or wait	1	F2C055	WriteFile
C:\Program Files (x86)\Autolt3 Include\analysisistimer.au3	2551	524	fd 4e fd 10 64 36 1d fd a6 fd 39 08 32 0b fd 37 fd fd fd 1f 71 fd 42 fd 74 fd 71 fd fd 77 fd 1b 5c fd 01 51 59 7f 64 fd 37 fd 27 1c 7e 54 fd fd 88 6d fd 75 fd fd fd 0b 31 fd 21 fd 41 fd 7a 0d 50 19 fd 2f fd 51 76 fd f9 57 12 22 fd a6 16 0f fd fd 27 12 39 0b 40 23 fd 34 7e 56 0a 03 fd fd 38 2c fd fd 6a 47 fd fd fd 7a 6e fd fd fd e8 fd fd 7f fd fd fd 04 21 fd 22 fd fd 74 fd 6d 65 fd fd 53 fd 17 fd fd fd 53 4b fd 37 3c 11 fd fd 74 0d 3d 12 23 fd fd 0a 64 fd fd 4c 0b 3e 5c fd fd fd 5c 35 fd fd 34 84 7b 3a fd 18 1b fd fd fd 0e 16 4d fd 55 04 fd 7c fd fd 56 fd 0c 11 fd fd 61 0d 33 09 fd 69 fd 14 79 63 fd 64 2e fd 6c fd 9e fd fd 25 c7 37 fd fd 09 fd 32 fd 30 fd fd d6 40 fd 28 fd 5d 26 1a fd 04 74 fd fd	Nd6927qBtqwQYd7'~Tu 1!AzP/QvW" '9@#4~V8,jGzn!"tmeSSK 7<t=#dL>\ \54{;MU Va3iycd.l%720 @(&t	success or wait	1	F2CBF8	WriteFile
C:\Program Files (x86)\Autolt3 Include\analysisistimer.au3	3075	10	24 00 fd 09 00 00 00 00 00 00	\$	success or wait	1	F2CC68	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3\Include\analysisistimer.au3	0	2551	fd 21 0b 35 fd 64 0f 38 5a fd 3b 50 fd fd fd 5c 21 fd 44 20 72 fd 55 29 4b 37 11 77 fd fd 77 3c fd fd fd 5a 2d 3b 11 fd 50 66 fd ec 78 fd fd 7a fd fd 17 fd 32 32 5a 1d 5e fd fd 12 67 69 fd fd fd 46 5a 32 fd 37 fd 4b fd fd fd fd 4e 3d fd 44 03 fd fd fd fd 72 4c 26 73 95 55 fd 54 fd fd fd fd 44 fd fd 47 35 fd 25 fd 73 17 1c 6e 97 fd fd 4f 60 5d 69 4d 18 fd fd 15 5b 76 fd fd fd fd fd 56 07 fd 0a 15 fd 10 fd fd fd fd fd 4d fd 59 fd 75 fd fd fd fd 7a 31 fd fd 6a fd fd 21 fd 0c 1b fd fd fd fd 56 66 41 fd fd 74 64 03 fd fd fd fd fd 11 fd fd 0d 7c 29 31 fd fd fd 61 fd 3b 11 fd 3f fd fd fd 12 3b fd 47 fd fd 7f 61 6e fd 28 75 fd fd fd 1a fd 52 0e 12 fd 08 1a fd fd fd 06 fd 30 7c 78 fd fd fd 79 30 27 fd 15 39 fd 14 1a 69 fd fd 5b	!5d8Z;P\ID rU)K7ww<Z- ;Pfxz22Z^ giFZ27N=DrL&sUTDG% s nO`]iM[vVMY uz1j!VfAtd])1a;?;Gan(uR0 [xy'9i[	success or wait	1	F2C055	WriteFile

File Read								
File Path	Offset	Length	Completion	Count	Source Address	Symbol		
C:\bootTel.dat	unknown	80	success or wait	1	F2EC14	ReadFile		
C:\Program Files\desktop.ini	unknown	174	success or wait	1	F2EC14	ReadFile		
C:\Program Files (x86)\desktop.ini	unknown	174	success or wait	1	F2EC14	ReadFile		
C:\Users\desktop.ini	unknown	174	success or wait	1	F2EC14	ReadFile		
C:\Program Files (x86)\Autolt3\Au3Check.dat	unknown	12931	success or wait	1	F2EC14	ReadFile		
C:\Program Files (x86)\Autolt3\Autolt v3 Website.url	unknown	204	success or wait	1	F2EC14	ReadFile		
C:\Program Files (x86)\Autolt3\Autolt.chm	unknown	700540	success or wait	4	F2EA8E	ReadFile		
C:\ProgramData\Microsoft Help\MS.DATABASECOMPARE.16.1033.hxn	unknown	418	success or wait	1	F2EC14	ReadFile		
C:\ProgramData\Microsoft Help\MS.EXCEL.16.1033.hxn	unknown	350	success or wait	1	F2EC14	ReadFile		
C:\ProgramData\Microsoft Help\MS.GRAPH.16.1033.hxn	unknown	350	success or wait	1	F2EC14	ReadFile		
C:\ProgramData\Microsoft Help\MS.GROOVE.16.1033.hxn	unknown	356	success or wait	1	F2EC14	ReadFile		
C:\ProgramData\Microsoft Help\MS.LYNC.16.1033.hxn	unknown	344	success or wait	1	F2EC14	ReadFile		
C:\ProgramData\Microsoft Help\MS.LYNC_BASIC.16.1033.hxn	unknown	380	success or wait	1	F2EC14	ReadFile		
C:\ProgramData\Microsoft Help\MS.LYNC_ONLINE.16.1033.hxn	unknown	386	success or wait	1	F2EC14	ReadFile		
C:\ProgramData\Microsoft Help\MS.MSACCESS.16.1033.hxn	unknown	368	success or wait	1	F2EC14	ReadFile		
C:\ProgramData\Microsoft Help\MS.MSOUC.16.1033.hxn	unknown	350	success or wait	1	F2EC14	ReadFile		
C:\ProgramData\Microsoft Help\MS.MSPUB.16.1033.hxn	unknown	350	success or wait	1	F2EC14	ReadFile		
C:\ProgramData\Microsoft Help\MS.ONENOTE.16.1033.hxn	unknown	362	success or wait	1	F2EC14	ReadFile		
C:\ProgramData\Microsoft Help\MS.OUTLOOK.16.1033.hxn	unknown	362	success or wait	1	F2EC14	ReadFile		
C:\ProgramData\Microsoft Help\MS.POWERPNT.16.1033.hxn	unknown	368	success or wait	1	F2EC14	ReadFile		
C:\ProgramData\Microsoft Help\MS.SETLANG.16.1033.hxn	unknown	362	success or wait	1	F2EC14	ReadFile		
C:\ProgramData\Microsoft Help\MS.SKYPEFB.16.1033.hxn	unknown	362	success or wait	1	F2EC14	ReadFile		
C:\ProgramData\Microsoft Help\MS.SKYPEFB_BASIC.16.1033.hxn	unknown	398	success or wait	1	F2EC14	ReadFile		
C:\ProgramData\Microsoft Help\MS.SKYPEFB_ONLINE.16.1033.hxn	unknown	404	success or wait	1	F2EC14	ReadFile		
C:\ProgramData\Microsoft Help\MS.SKYPEFB_ONLINEG.16.1033.hxn	unknown	410	success or wait	1	F2EC14	ReadFile		
C:\ProgramData\Microsoft Help\MS.SPREADSHEETCOMPARE.16.1033.hxn	unknown	436	success or wait	1	F2EC14	ReadFile		
C:\ProgramData\Microsoft Help\MS.WINWORD.16.1033.hxn	unknown	362	success or wait	1	F2EC14	ReadFile		
C:\ProgramData\Microsoft Help\inslist.hxl	unknown	6262	success or wait	1	F2EC14	ReadFile		
C:\ProgramData\regid.1991-06.com.microsoft\regid.1991-06.com.microsoft Microsoft Office Professional Plus 2016.swidtag	unknown	1065	success or wait	1	F2EC14	ReadFile		
C:\ProgramData\regid.1991-06.com.microsoft\regid.1991-06.com.microsoft_Windows-10-Pro.swidtag	unknown	993	success or wait	1	F2EC14	ReadFile		
C:\Users\Default\NTUSER.DAT	unknown	262144	success or wait	1	F2EC14	ReadFile		
C:\Users\Default\NTUSER.DAT.LOG1	unknown	57344	success or wait	1	F2EC14	ReadFile		
C:\Users\Default\NTUSER.DAT{8ebe95f7-3dcb-11e8-a9d9-7cfe90913f50}.TM.blf	unknown	65536	success or wait	1	F2EC14	ReadFile		
C:\Users\Default\NTUSER.DAT{8ebe95f7-3dcb-11e8-a9d9-7cfe90913f50}.TMContainer00000000000000000001.regtrans-ms	unknown	524288	success or wait	1	F2EC14	ReadFile		

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Default\NTUSER.DAT{8ebe95f7-3dcb-11e8-a9d9-7cfe90913f50}.TMContainer000000000000000002.regtrans-ms	unknown	524288	success or wait	1	F2EC14	ReadFile
C:\Users\user\ntuser.ini	unknown	20	success or wait	1	F2EC14	ReadFile
C:\Users\Public\desktop.ini	unknown	174	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Office64WW.xml	unknown	4992	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\OWOW64WW.cab	unknown	3059210	success or wait	5	F2EA8E	ReadFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\pkeyconfig-office.xrm-ms	unknown	590523	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPlusWW.xml	unknown	17108	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW.cab	unknown	5242880	success or wait	30	F2EA8E	ReadFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ProPsWW2.cab	unknown	5242880	success or wait	20	F2EA8E	ReadFile
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\Setup.xml	unknown	27782	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelLR.cab	unknown	576950	success or wait	4	F2EA8E	ReadFile
C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\ExcelMUI.xml	unknown	1780	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0016-0409-0000-0000000FF1CE}-C\Setup.xml	unknown	2482	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PowerPointMUI.xml	unknown	1661	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\PptLR.cab	unknown	631010	success or wait	4	F2EA8E	ReadFile
C:\MSOCache\All Users\{90160000-0018-0409-0000-0000000FF1CE}-C\Setup.xml	unknown	2072	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PublisherMUI.xml	unknown	1662	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\PubLR.cab	unknown	1048576	success or wait	1	F2E82A	ReadFile
C:\MSOCache\All Users\{90160000-0019-0409-0000-0000000FF1CE}-C\Setup.xml	unknown	1795	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlkLR.cab	unknown	1048576	success or wait	1	F2E82A	ReadFile
C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\OutlookMUI.xml	unknown	2837	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-001A-0409-0000-0000000FF1CE}-C\Setup.xml	unknown	3870	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\Setup.xml	unknown	2772	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordLR.cab	unknown	1007970	success or wait	3	F2EA8E	ReadFile
C:\MSOCache\All Users\{90160000-001B-0409-0000-0000000FF1CE}-C\WordMUI.xml	unknown	2108	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Proofing.xml	unknown	1024	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-002C-0409-0000-0000000FF1CE}-C\Setup.xml	unknown	6067	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfLR.cab	unknown	1048576	success or wait	1	F2E82A	ReadFile
C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.xml	unknown	1230	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0044-0409-0000-0000000FF1CE}-C\Setup.xml	unknown	1795	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.cab	unknown	641590	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\DCFMUI.xml	unknown	1215	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0090-0409-0000-0000000FF1CE}-C\Setup.xml	unknown	1808	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.xml	unknown	1817	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\OneNoteLR.cab	unknown	1335470	success or wait	5	F2EA8E	ReadFile
C:\MSOCache\All Users\{90160000-00A1-0409-0000-0000000FF1CE}-C\Setup.xml	unknown	2175	success or wait	1	F2EC14	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveLR.cab	unknown	872962	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\GrooveMUI.xml	unknown	1126	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\Setup.xml	unknown	1640	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.cab	unknown	16813	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\OSMMUI.xml	unknown	1123	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-00E1-0409-0000-0000000FF1CE}-C\Setup.xml	unknown	2038	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\OSMUXMUI.cab	unknown	1048576	success or wait	1	F2E82A	ReadFile
C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\OSMUXMUI.xml	unknown	1458	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-00E2-0409-0000-0000000FF1CE}-C\Setup.xml	unknown	2454	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\branding.xml	unknown	336313	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeLR.cab	unknown	1170680	success or wait	5	F2EA8E	ReadFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeMUI.xml	unknown	5275	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OfficeMUISet.xml	unknown	1032	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\OffSetLR.cab	unknown	15708	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\pss10r.chm	unknown	14598	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\Setup.chm	unknown	82790	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\Setup.xml	unknown	8483	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0115-0409-0000-0000000FF1CE}-C\ShellUI.MST	unknown	10752	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUI.xml	unknown	1910	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Office64MUISet.xml	unknown	1036	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\OWOW64LR.cab	unknown	1048576	success or wait	1	F2E82A	ReadFile
C:\MSOCache\All Users\{90160000-0116-0409-1000-0000000FF1CE}-C\Setup.xml	unknown	3122	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\AccessMUISet.xml	unknown	1032	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-0117-0409-0000-0000000FF1CE}-C\Setup.xml	unknown	2584	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\LyncMUI.cab	unknown	1048576	success or wait	1	F2E82A	ReadFile
C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\LyncMUI.xml	unknown	1227	success or wait	1	F2EC14	ReadFile
C:\MSOCache\All Users\{90160000-012B-0409-0000-0000000FF1CE}-C\Setup.xml	unknown	1690	success or wait	1	F2EC14	ReadFile
C:\Program Files\internet explorer\SIGNUP\install.ins	unknown	452	success or wait	1	F2EC14	ReadFile
C:\Program Files\Microsoft Office\Office16\Custom.propdesc	unknown	1343	success or wait	1	F2EC14	ReadFile
C:\Program Files\Microsoft Office\Office16\Mso Example Setup File A.txt	unknown	78	success or wait	1	F2EC14	ReadFile
C:\Program Files\Microsoft Office\Office16\VisioCustom.propdesc	unknown	1156	success or wait	1	F2EC14	ReadFile
C:\Program Files\UNP\Log\UpdateNotificationPipeline.001.etl	unknown	131072	success or wait	1	F2EC14	ReadFile
C:\Program Files\UNP\Log\UpdateNotificationPipeline.002.etl	unknown	131072	success or wait	1	F2EC14	ReadFile
C:\Program Files\UNP\Log\UpdateNotificationPipeline.003.etl	unknown	131072	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Adobe\Acrobat Reader DC\ReadMe.htm	unknown	16633	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX.chm	unknown	200478	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX.psd1	unknown	26418	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX3.Assembly.xml	unknown	49518	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX3_DLL.h	unknown	12993	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX3_DLL.lib	unknown	28976	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\AutoltX\AutoltX3_x64_DLL.lib	unknown	27546	success or wait	1	F2EC14	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3\Examples\calculator.au3	unknown	1405	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Examples\count-do.au3	unknown	1177	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Examples\count-for.au3	unknown	964	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Examples\count-while.au3	unknown	1169	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Examples\functions.au3	unknown	1157	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Examples\inputbox.au3	unknown	1692	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Examples\msgbox.au3	unknown	459	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Examples\notepad1.au3	unknown	1701	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Examples\notepad2.au3	unknown	1415	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Examples_ReadMe_.txt	unknown	207	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Extras_ReadMe_.txt	unknown	177	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\icons\au3.ico	unknown	31526	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\icons\au3script_v10.ico	unknown	71546	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\icons\au3script_v11.ico	unknown	41287	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\icons\au3script_v9.ico	unknown	25214	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\icons\filetype-blank.ico	unknown	33584	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\icons\MyAutolt3_Blue.ico	unknown	7406	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\icons\MyAutolt3_Green.ico	unknown	7406	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\icons\MyAutolt3_Red.ico	unknown	7406	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\icons\MyAutolt3_Yellow.ico	unknown	7406	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\analysis\timer.au3	unknown	2551	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\APIComConstants.au3	unknown	971	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\APIConstants.au3	unknown	1748	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\APIDiagConstants.au3	unknown	2906	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\APIDlgConstants.au3	unknown	10755	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\APIErrorsConstants.au3	unknown	309461	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\APIFilesConstants.au3	unknown	27433	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\APIGdiConstants.au3	unknown	19422	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\APILocaleConstants.au3	unknown	7757	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\APIMiscConstants.au3	unknown	1879	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\APIProcConstants.au3	unknown	5111	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\APIRegConstants.au3	unknown	4559	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\APIResConstants.au3	unknown	6485	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\APIShellExConstants.au3	unknown	33109	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\APIShPathConstants.au3	unknown	3171	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\APISysConstants.au3	unknown	16212	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\APIThemeConstants.au3	unknown	11852	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\Array.au3	unknown	81061	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\ArrayDisplayInternals.au3	unknown	33030	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\AutoltConstants.au3	unknown	13223	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\AVIConstants.au3	unknown	1583	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\BorderConstants.au3	unknown	2120	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\ButtonConstants.au3	unknown	4451	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\cleanup.au3	unknown	1346	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\Clipboard.au3	unknown	18982	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\Color.au3	unknown	9958	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\ColorConstants.au3	unknown	2605	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\ComboConstants.au3	unknown	7771	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\Constants.au3	unknown	4233	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\Crypt.au3	unknown	27295	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\CUIAutomation2.au3	unknown	47661	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\Date.au3	unknown	82884	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\DateTimeConstants.au3	unknown	7054	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\Debug.au3	unknown	26886	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\DirConstants.au3	unknown	1095	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\EditConstants.au3	unknown	4834	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\EventLog.au3	unknown	31728	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\Excel.au3	unknown	57620	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\ExcelConstants.au3	unknown	19617	success or wait	1	F2EC14	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3\Include\File.au3	unknown	43954	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\FileConstants.au3	unknown	6681	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\FontConstants.au3	unknown	3606	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\FrameConstants.au3	unknown	2068	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\FTPEx.au3	unknown	45602	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GDIPlus.au3	unknown	304821	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GDIPlusConstants.au3	unknown	28033	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GuiAVI.au3	unknown	11250	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GuiButton.au3	unknown	28493	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GuiComboBox.au3	unknown	41625	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GuiComboBoxEx.au3	unknown	49337	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GUIConstants.au3	unknown	1009	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GUIConstantsEx.au3	unknown	4049	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GuiDateTimePicker.au3	unknown	15543	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GuiEdit.au3	unknown	54035	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GuiHeader.au3	unknown	44305	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GuiImageList.au3	unknown	31626	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GuiIPAddress.au3	unknown	12769	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GuiListBox.au3	unknown	44090	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GuiListView.au3	unknown	225813	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GuiMenu.au3	unknown	61910	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GuiMonthCal.au3	unknown	45407	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GuiReBar.au3	unknown	69800	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GuiRichEdit.au3	unknown	209177	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GuiScrollBars.au3	unknown	24716	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GuiSlider.au3	unknown	26774	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GuiStatusBar.au3	unknown	31347	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GuiTab.au3	unknown	41467	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GuiToolBar.au3	unknown	89416	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GuiToolTip.au3	unknown	48537	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\GuiTreeView.au3	unknown	125305	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\HeaderConstants.au3	unknown	7013	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\helper.au3	unknown	20799	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\htmlfetcher.au3	unknown	5192	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\ie.au3	unknown	153545	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\ImageListConstants.au3	unknown	1745	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\inet.au3	unknown	15121	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\inetConstants.au3	unknown	1296	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\IPAddressConstants.au3	unknown	1374	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\ListBoxConstants.au3	unknown	5024	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\ListViewConstants.au3	unknown	23220	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\liveprocess.au3	unknown	2648	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\Math.au3	unknown	4647	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\MathConstants.au3	unknown	926	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\Memory.au3	unknown	17350	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\MemoryConstants.au3	unknown	2433	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\MenuConstants.au3	unknown	4894	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\Misc.au3	unknown	31966	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\MsgBoxConstants.au3	unknown	4120	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\NamedPipes.au3	unknown	14025	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\NetShare.au3	unknown	45807	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\NTSTATUSConstants.au3	unknown	240674	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\PowerPoint.au3	unknown	57717	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\PowerPointConstants.au3	unknown	7161	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\Process.au3	unknown	3821	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\ProcessConstants.au3	unknown	1469	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\ProgressConstants.au3	unknown	2067	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\RebarConstants.au3	unknown	6419	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\RichEditConstants.au3	unknown	14375	success or wait	1	F2EC14	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolt3\Include\ScreenCapture.au3	unknown	11029	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\ScrollBarConstants.au3	unknown	498	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\ScrollBarsConstants.au3	unknown	1961	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\Security.au3	unknown	18076	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\SecurityConstants.au3	unknown	7958	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\SendMessage.au3	unknown	2380	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\SliderConstants.au3	unknown	4264	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\Sound.au3	unknown	22948	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\SQLite.au3	unknown	56601	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\StaticConstants.au3	unknown	1977	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\StatusBarConstants.au3	unknown	3216	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\String.au3	unknown	8310	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\StringConstants.au3	unknown	2854	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\StructureConstants.au3	unknown	64285	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\TabConstants.au3	unknown	6193	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\Timers.au3	unknown	11852	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\ToolBarConstants.au3	unknown	13733	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\ToolTipConstants.au3	unknown	5526	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\TrayConstants.au3	unknown	2662	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\TreeViewConstants.au3	unknown	9401	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\UDFGlobalID.au3	unknown	6689	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\UIAWrappers.au3	unknown	110041	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\UpDownConstants.au3	unknown	1151	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\Visa.au3	unknown	39973	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPI.au3	unknown	1520	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPICom.au3	unknown	9552	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPIConstants.au3	unknown	5273	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPIConv.au3	unknown	29137	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPIDiag.au3	unknown	32900	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPIDlg.au3	unknown	39024	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPIError.au3	unknown	11902	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPIEx.au3	unknown	1607	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPIFiles.au3	unknown	95747	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPIGdi.au3	unknown	203649	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPIGdiDC.au3	unknown	20015	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPIGdiInternals.au3	unknown	29558	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPIHObj.au3	unknown	13115	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPIIcons.au3	unknown	24069	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPIInternals.au3	unknown	18871	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPIlangConstants.au3	unknown	8317	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPILocale.au3	unknown	20847	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPIMem.au3	unknown	21490	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPIMisc.au3	unknown	14256	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPIProc.au3	unknown	76320	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPIReg.au3	unknown	31923	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPIRes.au3	unknown	37968	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPIShellEx.au3	unknown	42670	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPIShPath.au3	unknown	44447	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPISys.au3	unknown	77683	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPISysinfoConstants.au3	unknown	9018	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPISysInternals.au3	unknown	28131	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPISysWin.au3	unknown	58221	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPITheme.au3	unknown	41505	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinAPIvkeysConstants.au3	unknown	6259	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WindowsConstants.au3	unknown	33410	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WinNet.au3	unknown	46240	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\Word.au3	unknown	32921	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include\WordConstants.au3	unknown	11668	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Autolt3\Include_ReadMe_.txt	unknown	214	success or wait	1	F2EC14	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Autolr3\SciTE\au3.keywords.properties	unknown	91311	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Common Files\DESIGNER\MSADDNDR.OLB	unknown	14552	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Google\Update\GoogleUpdate.bk	unknown	156104	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Internet Explorer\SIGNUP\install.ins	unknown	452	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\COPYRIGHT	unknown	3244	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\LICENSE	unknown	44	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\README.txt	unknown	46	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\release	unknown	425	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\THIRDPARTYLICENSEREADME-JAVAFX.txt	unknown	112748	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\THIRDPARTYLICENSEREADME.txt	unknown	149725	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\Welcome.html	unknown	955	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	256	success or wait	1	F2EC14	ReadFile
C:\Program Files (x86)\Microsoft Office\Document Themes 16\Facet.thmx	unknown	738429	success or wait	1	F2EC14	ReadFile

Registry Activities											
There is hidden Windows Behavior. Click on Show Windows Behavior to show it.											
Key Path					Completion		Count	Source Address	Symbol		
Key Path		Name	Type	Data		Completion		Count	Source Address	Symbol	
Key Path		Name	Type	Old Data		New Data		Completion	Count	Source Address	Symbol

Disassembly								
 No disassembly								