ID: 492780
Sample Name: vZ1WZMpxTY
Cookbook: default.jbs
Time: 01:12:19
Date: 29/09/2021
Version: 33.0.0 White Diamond

Table of Contents

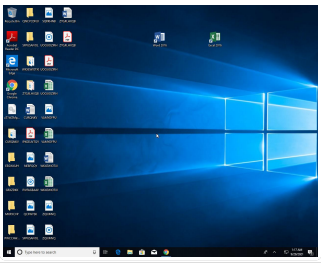
Windows Analysis Report vZ1WZMpxTY

Overview

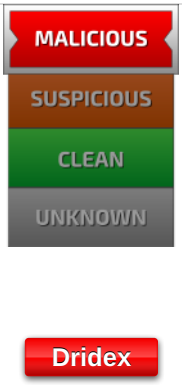
General Information

Sample Name:	vZ1WZMpxTY (renamed file extension from none to dll)
Analysis ID:	492780
MD5:	c10ee36fe08388f..
SHA1:	6477666e70f87ff...
SHA256:	d8bc15335ca8da..
Tags:	Dridex exe
Infos:	

Most interesting Screenshot:



Detection

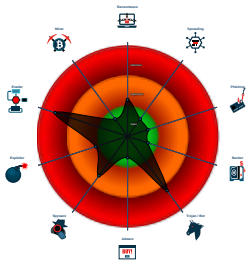


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Dridex unpacked file
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Changes memory attributes in foreig…
- Machine Learning detection for samp…
- Queues an APC in another process …
- Sigma detected: Regsvr32 Comman…
- Machine Learning detection for dropp…
- Uses Atom Bombing / ProGate to in…
- Queries the volume information (nam…
- Contains functionality to check if a d…
- Contains functionality to query locale…
- May sleep (evasive loops) to hinder …

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 6680 cmdline: loaddll64.exe 'C:\Users\user\Desktop\vZ1WZMpxTY.dll' MD5: E0CC9D126C39A9D2FA1CAD5027EBBD18)
  - cmd.exe (PID: 6236 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\vZ1WZMpxTY.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 4308 cmdline: rundll32.exe 'C:\Users\user\Desktop\vZ1WZMpxTY.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 4292 cmdline: regsvr32.exe /s C:\Users\user\Desktop\vZ1WZMpxTY.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - slui.exe (PID: 2680 cmdline: C:\Windows\system32\slui.exe MD5: 96A8EF9387619D17BB30B024DDF52BF3)
      - slui.exe (PID: 6376 cmdline: C:\Users\user\AppData\Local\qklwjLaE\slui.exe MD5: 96A8EF9387619D17BB30B024DDF52BF3)
      - FileHistory.exe (PID: 5972 cmdline: C:\Windows\system32\FileHistory.exe MD5: 989B5BDB2BEAC9F894BBC236F1B67967)
      - FileHistory.exe (PID: 5088 cmdline: C:\Users\user\AppData\Local\1QHnh\FileHistory.exe MD5: 989B5BDB2BEAC9F894BBC236F1B67967)
      - PresentationHost.exe (PID: 4780 cmdline: C:\Windows\system32\PresentationHost.exe MD5: E3053C73EA240F4C2F7971B3905A91CF)
      - PresentationHost.exe (PID: 5408 cmdline: C:\Users\user\AppData\Local\gKsll\PresentationHost.exe MD5: E3053C73EA240F4C2F7971B3905A91CF)
      - SystemPropertiesAdvanced.exe (PID: 5876 cmdline: C:\Windows\system32\SystemPropertiesAdvanced.exe MD5: 82ED6250B9AA030DDC13DC075D2C16E3)
      - SystemPropertiesAdvanced.exe (PID: 5952 cmdline: C:\Users\user\AppData\Local\rUhH1WSzx\SystemPropertiesAdvanced.exe MD5: 82ED6250B9AA030DDC13DC075D2C16E3)
      - Magnify.exe (PID: 6120 cmdline: C:\Windows\system32\Magnify.exe MD5: F97BE20B3744572366666607EE4BA7F7F)
      - Magnify.exe (PID: 5428 cmdline: C:\Users\user\AppData\Local\N8qUdj\Magnify.exe MD5: F97BE20B3744572366666607EE4BA7F7F)
      - omadmclient.exe (PID: 1624 cmdline: C:\Windows\system32\omadmclient.exe MD5: AD7C6CD7A8EEC95808AA77C5D7987941)
      - omadmclient.exe (PID: 5936 cmdline: C:\Users\user\AppData\Local\MfH2kGhD\omadmclient.exe MD5: AD7C6CD7A8EEC95808AA77C5D7987941)
      - msinfo32.exe (PID: 5684 cmdline: C:\Windows\system32\msinfo32.exe MD5: C471C6B06F47EA1C66E5FAA8DFCEF108)
      - msinfo32.exe (PID: 6296 cmdline: C:\Users\user\AppData\Local\3EDBT6em\msinfo32.exe MD5: C471C6B06F47EA1C66E5FAA8DFCEF108)
      - RdpSa.exe (PID: 1748 cmdline: C:\Windows\system32\RdpSa.exe MD5: 0795B6F790F8E52D55F39E593E9C5BBA)
      - RdpSa.exe (PID: 1460 cmdline: C:\Users\user\AppData\Local\px153\RdpSa.exe MD5: 0795B6F790F8E52D55F39E593E9C5BBA)
      - PasswordOnWakeSettingFlyout.exe (PID: 4308 cmdline: C:\Windows\system32\PasswordOnWakeSettingFlyout.exe MD5: F0C8675F98E397383A112CC8ED5B97DA)
      - PasswordOnWakeSettingFlyout.exe (PID: 1768 cmdline: C:\Users\user\AppData\Local\rM4q\PasswordOnWakeSettingFlyout.exe MD5: F0C8675F98E397383A112CC8ED5B97DA)
  - iexplore.exe (PID: 2288 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - iexplore.exe (PID: 6948 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2288 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - rundll32.exe (PID: 1352 cmdline: rundll32.exe C:\Users\user\Desktop\vZ1WZMpxTY.dll,BeginBufferedAnimation MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 4000 cmdline: rundll32.exe C:\Users\user\Desktop\vZ1WZMpxTY.dll,BeginBufferedPaint MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 3424 cmdline: rundll32.exe C:\Users\user\Desktop\vZ1WZMpxTY.dll,BeginPanningFeedback MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.365502864.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000026.00000002.632076850.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000020.00000002.565898043.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000003.00000002.445132804.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000017.00000002.484447780.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	

Click to see the 10 entries

Sigma Overview

System Summary:

Sigma detected: Regsvr32 Command Line Without DLL

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

E-Banking Fraud:

Yara detected Dridex unpacked file

System Summary:

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

Changes memory attributes in foreign processes to executable or writable

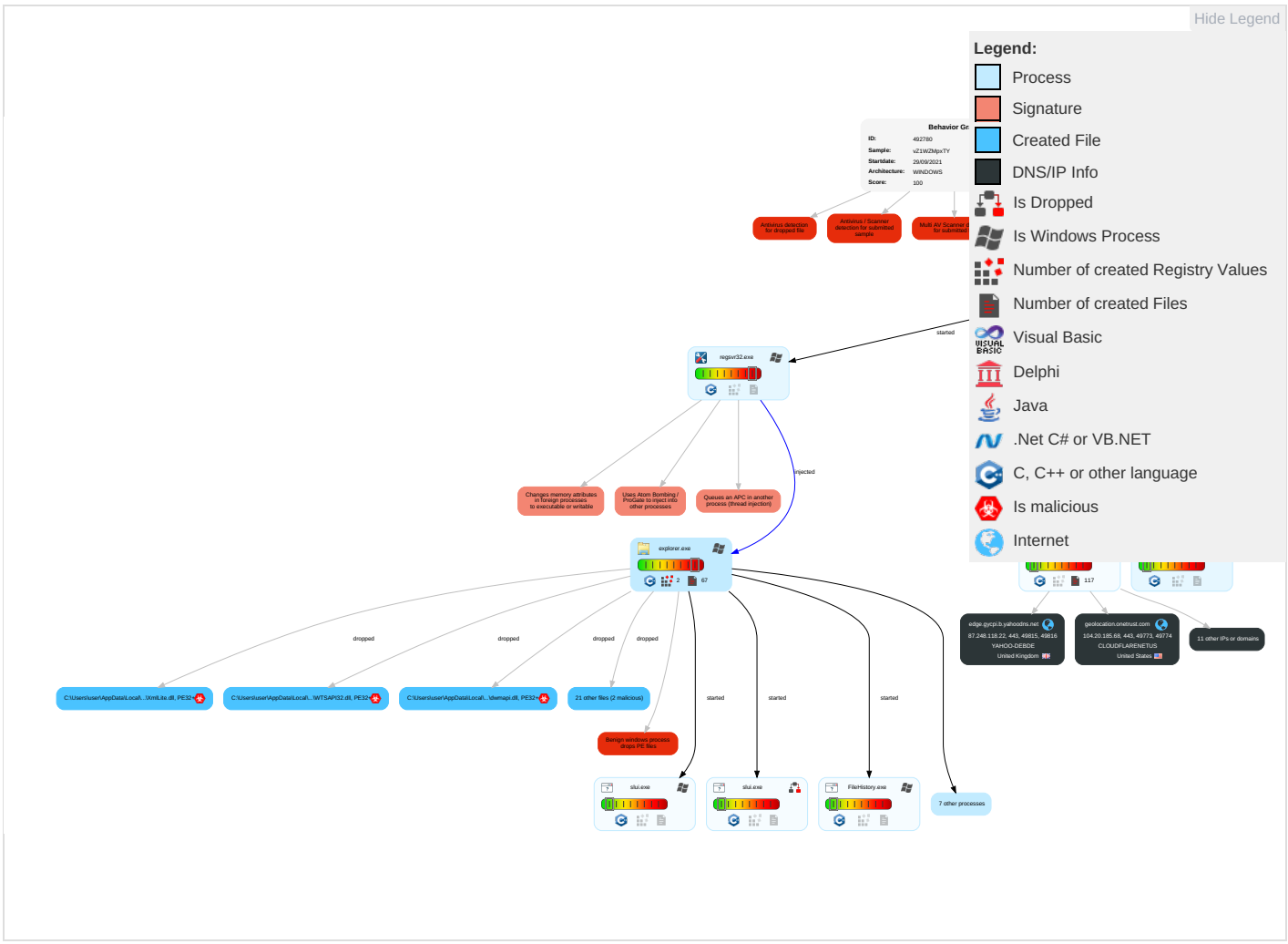
Queues an APC in another process (thread injection)

Uses Atom Bombing / ProGate to inject into other processes

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Valid Accounts 1	Exploitation for Client Execution 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Input Capture 2 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Scheduled Task/Job	Valid Accounts 1	Extra Window Memory Injection 1	Obfuscated Files or Information 2	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Encrypt Channe
Domain Accounts	At (Linux)	Logon Script (Windows)	Valid Accounts 1	Software Packing 2	Security Account Manager	System Information Discovery 3 5	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Applica Layer Protoco
Local Accounts	At (Windows)	Logon Script (Mac)	Access Token Manipulation 1	Timestomp 1	NTDS	Security Software Discovery 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applica Layer Protoco
Cloud Accounts	Cron	Network Logon Script	Process Injection 3 1 2	DLL Side-Loading 1	LSA Secrets	Virtualization/Sandbox Evasion 1	SSH	Keylogging	Data Transfer Size Limits	Fallbac Channe
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Extra Window Memory Injection 1	Cached Domain Credentials	Process Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commo Used P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Valid Accounts 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer P
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pr
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Access Token Manipulation 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoco
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Process Injection 3 1 2	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pro
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Regsvr32 1	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Rundll32 1	GUI Input Capture	Domain Groups	Exploitation of Remote Services	Email Collection	Commonly Used Port	Proxy

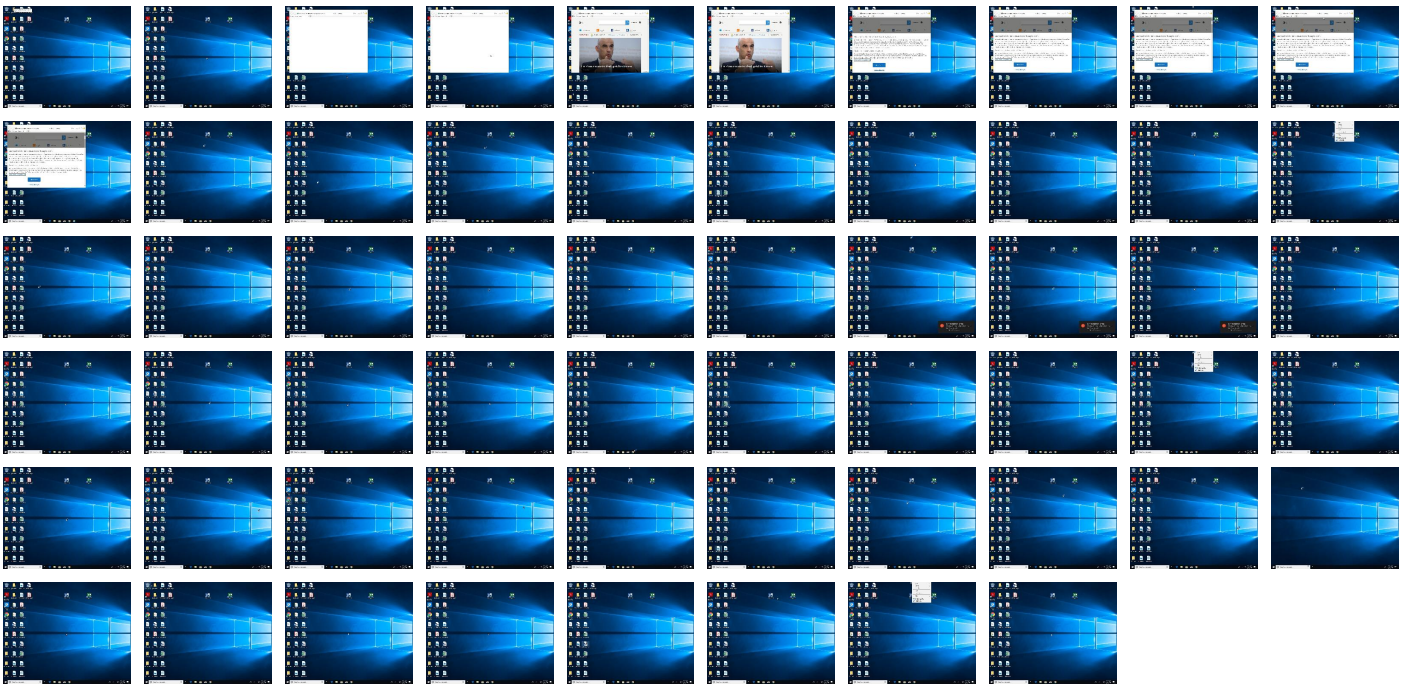
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
vZ1WZMpxTY.dll	66%	Virustotal		Browse
vZ1WZMpxTY.dll	63%	Metadefender		Browse
vZ1WZMpxTY.dll	76%	ReversingLabs	Win64.Infostealer.Dridex	
vZ1WZMpxTY.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
vZ1WZMpxTY.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\GXNcBGCPE\XmlLite.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\3EDBT6em\MFC42u.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\GXNcBGCPE\XmlLite.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\5vkpef\WTSAPI32.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\41zCY4W\dwmapi.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\1QHnh\UxTheme.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\GXNcBGCPE\XmlLite.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\3EDBT6em\MFC42u.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\GXNcBGCPE\XmlLite.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\5vkpef\WTSAPI32.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\41zCY4W\dwmapi.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\1QHnh\UxTheme.dll	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\1QHnh\FileHistory.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\1QHnh\FileHistory.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\1QHnh\FileHistory.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\3EDBT6em\msinfo32.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\3EDBT6em\msinfo32.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\41zCY4W\DisplaySwitch.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\41zCY4W\DisplaySwitch.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\5vkpef\BdeUISrv.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\5vkpef\BdeUISrv.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
32.2.Magnify.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.regsvr32.exe.140000000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
23.2.FileHistory.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.2.SystemPropertiesAdvanced.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll64.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.2.slui.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.2.PresentationHost.exe.1b521500000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://schemas.mi	0%	URL Reputation	safe	
http://https://btloader.com/tag?o=6208086025961472&upapi=true	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
contextual.media.net	23.54.113.52	true	false		high
hblg.media.net	23.54.113.52	true	false		high
lg3.media.net	23.54.113.52	true	false		high
btloader.com	104.26.6.139	true	false		high
geolocation.onetrust.com	104.20.185.68	true	false		high
edge.gycpi.b.yahoodns.net	87.248.118.22	true	false		high
s.yimg.com	unknown	unknown	false		high
web.vortex.data.msn.com	unknown	unknown	false		high
www.msn.com	unknown	unknown	false		high
srtb.msn.com	unknown	unknown	false		high
crcdn01.adnxs-simple.com	unknown	unknown	false		high
cvision.media.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location	false		high
http://https://btloader.com/tag?o=6208086025961472&upapi=true	false	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.20.185.68	geolocation.onetrust.com	United States		13335	CLOUDFLARENETUS	false
87.248.118.22	edge.gycpi.b.yahoodns.net	United Kingdom		203220	YAHOO-DEBDE	false
104.26.6.139	btloader.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	492780
Start date:	29.09.2021
Start time:	01:12:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 17m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	vZ1WZMpxTY (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	43
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:	mal100.troj.evad.winDLL@59/109@11/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 21.6% (good quality ratio 15.1%) • Quality average: 52.9% • Quality standard deviation: 41.5%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\1QHnh\FileHistory.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	246784
Entropy (8bit):	6.054877934071265
Encrypted:	false
SSDEEP:	3072:5WQz0maAVV604aFUxzYuVD8o+otIxAGQW7A70TshCbdmyTVulAyXRON:5WZmxPZUxzYuVD8ortIxAGJKSuCbd
MD5:	989B5BDB2BEAC9F894BBC236F1B67967
SHA1:	7B964642FEE2D6508E66C615AA6CF7FD95D6196E
SHA-256:	FF1DE8A606FDB6A932E7A3E5EE5317A6483F08712DE93603C92C058E05A89C0C
SHA-512:	0360C9FE88743056FD25AC17F12087DAD026B033E590A93F394B00EB486A2F5E2331EDCCA9605AA7573D892FBA41557C9E0EE4FAC69FCA687D6B6F144E5E524
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.s..k ..k ..k .hh!..k .^. ..k .ho!..k .hb!..k .hj!..k ..j #.k .hn!..k .h. ..k .h i!..k Rich..k .....PE..d....."....t...X.....{.....@..... .....\....`..... .....0..... ..8.....$... ...T..... .....H.....text...{m.....n..... ..`.nep.....r..... ..`.rdata...i.....j...x.....@..@.data... .....@....pdata..8.... ....@..@.rsrc.....0.....@..@.reloc..$.....@..B.....

C:\Users\user\AppData\Local\1QHnh\UxTheme.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2097152
Entropy (8bit):	3.6030901790339955
Encrypted:	false
SSDEEP:	12288:uVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:zfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	152E46C389FE180FA9994949FA664A06
SHA1:	4E2656B3A7CE47E8834DE7EB21E583DDC6A5E27E
SHA-256:	8528930AAE5DFA931BE2EAB8A0E0BEE905B248F6AD0C2C5DFF4687F700189FF4
SHA-512:	FECFF48E31BEEF968D07A880FE27EFB95FF561AB39AE2D5C5FCC7B4327E421039561E229F4BE4A267BFBE0C0841D32EEF1C028B35D99277C074274C13BE2BD5
Malicious:	**true**

C:\Users\user\AppData\Local\1QHnh\UxTheme.dll	
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.&..DN^....." .....p.....@..... .....@lx}..b.....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\3EDBT6em\MFC42u.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2121728
Entropy (8bit):	3.6345807361939917
Encrypted:	false
SSDEEP:	12288:CVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1YTjOh:ffP7fWsK5z9A+WGAW+V5SB6Ct4bnbW
MD5:	0A03F901938FEB852E5A4C5C1A658293
SHA1:	46D38D7E6610F3235DD07A03C2E133C05B98BCF1
SHA-256:	575F8EBFB8543E6DF7CC199A49D6F271FB33D98451C795237758460650B3408D
SHA-512:	71EB1C88774CF2596F8382995ACBC3F2D0B84A1DDC2086654B03B36E264BF4002075E28A32836BB148EFFFE449E5697E8C94F911DA7C0C3FB814BC80464FDC2
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.&..DN^....." .....@.....p.....@.....` .....@lx}..b.....\|...c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\3EDBT6em\msinfo32.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	370176
Entropy (8bit):	6.448503897594857
Encrypted:	false
SSDEEP:	6144:Uca2EiZg+uTUbSFWjSJiIOKZXcmg3GexhxiZEOHHrpm1XUZLxEZEOHHrpm1XUZLx:UB2PsUbSFWWAkZXcmkVx+tLpm1EwtLpr
MD5:	C471C6B06F47EA1C66E5FAA8DFCEF108
SHA1:	F8672A2B3B32956CBC948A954CEF236581045B78
SHA-256:	E2255751C1CF58596C8FE70C3093E099F8D71ED89580CFD0156FFCF0FED32861
SHA-512:	F7A2A31910CD4694B58FFCED83A2CCF633B5594859F178AFB9F67C02E3E664DA72701E7E45AA5590C4F1E1C99C82B665F0C0B80401506F0DFA49B61A8EEBD6EA
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|....y...y...y..yz...y..y}...y..y\|...y..yx...y...x...y..yp...y..y....y..y{...y.Rich..y.....PE..d....a....."....@.....0.....`..... .....$...h.....xJ.....(..... . ...P...T.....P.....P... .....text..... ..`.rdata..H*.....,.....@..@.data....k...@.....(.....@....pdata..(.....D.....@..@.rsrc...xJ.....L...V.....@..@.reloc.. ....@..B.....

C:\Users\user\AppData\Local\41zCY4W\DisplaySwitch.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1930224
Entropy (8bit):	1.9511202288226894
Encrypted:	false
SSDEEP:	3072:LvyYYIF4cmwcTigBmZWRHLxgMNnVYvkkVp66oB4E7p6:LvyYBF4R/igoZWRryMNnqz3
MD5:	97411B8A84E5980E509E500C3209E5C0
SHA1:	23398F8DA469DEAF10C32773062A6A62B7B004B4
SHA-256:	2C968556FCAD7EBB9A866B21A9F3F3DFCD0CA490CAF8F6B2ECDB423B9D24D3EF

C:\Users\user\AppData\Local\41zCY4W\DisplaySwitch.exe	
SHA-512:	1D5E598B51B37E8A92FA188A8D59C67B7522480B46AFB5D2033D4380A3C5A120D0DB2BE6FE62B636A23AD83F757B7A1803B77A0EA19DF3C51B9BD36B0F06CB(A
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... ..zd..)d..)d..)m.T)R..)...(g..)...(q..)...(c..)...(E..)d..)...)...({..)..8)e..)...(e..)Richd..).....PE..d....[~....."..... ....@.....`..... .....\.....(3.....d.....c...P..X.....T.....K..(....J.....K..x.....text..... ..... ..`.imrsiv.....0.....rdata..6....@.....$.....@..@.data...(.....@....pdata..d..... .@..@.rsrc...(3.....4.....@..@.reloc..X....P.....@..B..... .....

C:\Users\user\AppData\Local\41zCY4W\dwmapi.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2097152
Entropy (8bit):	3.5988848965545683
Encrypted:	false
SSDEEP:	12288:6VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1N:nfP7fWsK5z9A+WGAW+V5SB6Ct4bnbN
MD5:	B3F745E93C12EA4207A62A0C21FF46C1
SHA1:	C0505705A1C614FAED31C89E84B08C4645CA6C8C
SHA-256:	08BB889CC779BB5D208FF048B9F14C48044B31B667A1DDA097C45F551AF3CD9C
SHA-512:	582280D7A929ABED43C36B8D3F1B993E11C4488D7255A1CCDCC6E35D29AFF4907CE9CAB9AB5C2F20B9EEA00182E78ADB73EE5B55D2E3DB1FEB516B77D162(D27
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.& ..DN^....." .....p.....@..... .....@lx}..b.....&.....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\5vkpef\BdeUISrv.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	52736
Entropy (8bit):	5.7946530792580475
Encrypted:	false
SSDEEP:	768:NS51B2sZMD1mYu/Lr7p0dHkf9abpWnGjTopPjZdWC2bNrHuOKAh/4J99j4ktPUww:J/Yn/Lr7qwYb7/oRjeJh2991t8Yte
MD5:	25D86BC656025F38D6E626B606F1D39D
SHA1:	673F32CCA79DC890ADA1E5A2CF6ECA3EF863629D
SHA-256:	202BEC0F63167ED57FCB55DB48C9830A5323D72C662D9A58B691D16CE4DB8C1E
SHA-512:	D4B4BC411B122499E611E1F9A45FD40EC2ABA23354F261D4668BF0578D30AEC5419568489261FC773ABBB350CC77C1E00F8E7C0B135A1FD4A9B6500825FA6E0
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3..hw.;w.;w.;~.";u.;...t.;...`.;...:q.;...:d.;w.;..;...:..;..N;v.;...:v.;Richw.; .....PE..d...X....."....v...\.....0y.....@..... .....Db...`..... .....p.....x.....T..... .....text...At.....v..... ..`.rdata...3.....4...z.....@..@.data.....@....pdata.....@..@.rsrc.....@..@. reloc..x.....@..B..... .....

C:\Users\user\AppData\Local\5vkpef\WTSAPI32.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2097152
Entropy (8bit):	3.60071453018776
Encrypted:	false
SSDEEP:	12288:4VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:tfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	B0761FF56A5E4ABF5444BA58130778DC

C:\Users\user\AppData\Local\5vkpef\WTSAPI32.dll	
SHA1:	53EF27D1AC084B53D5377F8F49656408B19FB8B5
SHA-256:	0DE0CEEA86665BDC866264978A49FB7AC3E149B0371AC3DE1BCCC9C39FC97DBF
SHA-512:	147FC258F1868308D6CBCDFDB4E1F73F346D862E5E1BF4926C9D55AC49FFD635ECCC5F16862C14D036B756F20BB497FDB3EE23A1CFA104B965A46B43247E7CF
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.&..DN^......" .....p.....@..... .....@lx}..b.....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\GXNcBGCPE\XmlLite.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2097152
Entropy (8bit):	3.593383013578722
Encrypted:	false
SSDEEP:	12288:oVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:9fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	A3199F0B372CF1550C1920295358D76A
SHA1:	E019AE21159BE2F20BA243EEC0D319EE1494F5D3
SHA-256:	67E989ADB636DB5BC82E7CB4C37758427B6029E0A494529105ACE8BE45EB73D1
SHA-512:	AB92BADCC8F11F9FA18CF3CF58D65AA7C046E77E93B3A46F8F998A2699008496EDC04CCA0750597C2B568F903E82806EBB7E166FF9A715F93757F001A2B0BC8
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.&..DN^......" .....p.....@..... .....@lx}..b.....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\GXNcBGCPE\printfilterpipelinesvc.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	841728
Entropy (8bit):	6.098715724182093
Encrypted:	false
SSDEEP:	12288:JvOaQRxqg2DF9GOdw+UEx3OlRrd7p1dj6znesD0Xk++J:JvOaut2hf7r+lRZl6ak+
MD5:	4164BD4D8E23C672E40D203E4B4A38A7
SHA1:	7D7BC2BEB5B3669764EB0CA10E1C3E820413F8CA
SHA-256:	643F40ABCDA332944BBF92B4D2F846570A34B10BA0A0619B54F4FCF27AD116D0
SHA-512:	39969503FDF09107FD3B35F8A29CFB640B96E4A7DD257F9561F8BD34A22DC93B7246A424FC22D06EB1D7A01717CD05DCC3C5B00FB13F222F30D09D7F2EC31BA4
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....'...F...F...F...>I..F..".."...F.."...F.."...F...F...G..".^F..".."...F.."%..F.."...F..Rich.F.....PE..d...!.i....."......X.....b.....@.....`..... .....`/.....X....p...u.....h.....T.....(.....@.....text....W.....X..... ..`.rdata..>....p.....\.....@..@.data.....P.....8.....@....pdata...u...p...v...B.....@..@.rsrc...X.....@..@.reloc..h.....@..B.....

C:\Users\user\AppData\Local\MfH2kGhD\XmlLite.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2097152
Entropy (8bit):	3.593371737657062
Encrypted:	false
SSDEEP:	12288:GVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:bfP7fWsK5z9A+WGAW+V5SB6Ct4bnb

C:\Users\user\AppData\Local\MfH2kGhD\XmlLite.dll	
MD5:	E08951EEC08C440B9F4664A596B643D0
SHA1:	D60BD83E7805369BE0B23D7B4397E6200F2F6794
SHA-256:	09C9F6200B6A2823FC557F5ED7A6AEA2DBAFE971DFC617CEFCBD33A06C32E8AC
SHA-512:	145FCE12711F7CBE3E738FC15BDFA2625019BD965C29F053A79680DD0F1F8A9580A8D5E3581830E1035DED1BDE3508011A11F60F8F55C541D03BCC4113F2E23
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.& ..DN^....." .....p.....@..... .....@lx}..b.....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\MfH2kGhD\omadmclient.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	315904
Entropy (8bit):	6.1346795928867035
Encrypted:	false
SSDEEP:	6144:uwqIVaD9RkjUYNBDXEDBdcA1gBnbC03j0xjGKEgsQOQ25te8lG:XqIVaDrn6BD0NOA1gBnfj01QW
MD5:	AD7C6CD7A8EEC95808AA77C5D7987941
SHA1:	96985DDF5C2C30918F69CA4405D955BDD0C7E44E
SHA-256:	D7EED58A955ED6ADEF429FA78F82776BBC905C507E1ABE6D5CFCD5C8AC1B0AC9
SHA-512:	047EA8C542774045450B51BF367C75B4ED11E883553842BCACD9E6DFC4C27CDC8BE86A9BADFD5345DA068B4A881BC8522525BF9CEC72FEE1856E365E7CD20 5E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....`2.K$S~.$S~.$S~.-+..nS~.K7}.'S~.K7z.1S~.$S...R~.K7..=S~.K7{.)S ~.K7w..S~.K7..%S~.K7\|.%S~.Rich$S~.....PE..d...H..-.....".....d...x.....J.....@.....@.....`..... ....0.....T.....(.....8...8.....text....b.....d..... ..`.rdata..~4.....6...h.....@..@.data...l.....@....pdata... .....".....@..@.didat.....@....rsrc..... .....@..@.reloc.....0.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\FileHistory.exe.log	
Process:	C:\Users\user\AppData\Local\1QHnh\FileHistory.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	42
Entropy (8bit):	4.0050635535766075
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUy:Q3La/xwQ
MD5:	84CFDB4B995B1DBF543B26B86C863ADC
SHA1:	D2F47764908BF30036CF8248B9FF5541E2711FA2
SHA-256:	D8988D672D6915B46946B28C06AD8066C50041F6152A91D37FFA5CF129CC146B
SHA-512:	485F0ED45E13F00A93762CBF15B4B8F996553BAA021152FAE5ABA051E3736BCD3CA8F4328F0E6D9E3E1F910C96C4A9AE055331123EE08E3C2CE3A99AC2E177C E
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\EQAWN5DV\www.msn[2].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\EQAWN5DV\www.msn[2].xml	
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\IB42RK38\contextual.media[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2990
Entropy (8bit):	4.922341255712916
Encrypted:	false
SSDEEP:	48:L16161616z6z66z6zq46z6N6N6N6e6e36e6eMY6eMY76eMY7u6eMY76eMY7c2g6K:hiiss6ssfsOOOJJ3JJMYJMY7JMY7uJ+
MD5:	C1128B38CAE0054617A4E2C82A153DC1
SHA1:	2AB1351D679593D8EB66D2836FF7521D2EC1D399
SHA-256:	1AA6BBA5516DB3D62FFB233F3BB1980F643C0A00271E681AFFAE48678B60BEEE
SHA-512:	E7FF77FD8E5E0B12B524946A1EEEE67876AABB5249386A53AADD80D75050F4494FC00CE2425495129749E84E4F4FC7A4931CD852F5A8DF53F5FC1EA1048ACF8
Malicious:	false
Reputation:	unknown
Preview:	<root></root><root><item name="HBCM_BIDS" value="{}" ltime="3761547904" htime="30913801" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3761547904" htime="30913801" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3761547904" htime="30913801" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3761547904" htime="30913801" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3762027904" htime="30913801" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3762027904" htime="30913801" /><item name="mntest" value="mntest" ltime="3762027904" htime="30913801" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3762027904" htime="30913801" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3762027904" htime="30913801" /><item name="mntest" value="mntest" ltime="3765027904" htime="30913801" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3762027904" htime="30913801" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3768027904" htime="30913801"

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{1A69F8BE-20FD-11EC-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24152
Entropy (8bit):	1.7548561745265836
Encrypted:	false
SSDEEP:	48:IwAGcpr5GwpLSG/ap8MGIpctbGvnZpvt0GvHZp9tNGoSxqpvtaGo4es1pcjHGWSm:rkZzZ42cWWt7fOgtjes1WMkl
MD5:	BC0F9DA1844F1834836968175ACF991E
SHA1:	A3BBF2102D9FEEA5DD93AC6F6B5C996E2440D279
SHA-256:	7886964573DF7B3C6F060A57FEC9B110C3D3EE5ACD9FF479B560C77275612DAE
SHA-512:	84AE4EDCE084C6C2218B2DEDFA4092A92EFAED6C8EDC758A1ACC0CF4A3705AEAE939D16F067860C7615D8A795F81E816F7C6F571A3192C5ABEFCDE1F38B0 FF9
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1A69F8C0-20FD-11EC-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	198866
Entropy (8bit):	3.5870003074602694
Encrypted:	false
SSDEEP:	3072:0Z/2Bfcdmu5kgTzGtvZ/2Bfc+mu5kgTzGtV:NE0
MD5:	2A6EEDC822E9AF6CA10BAABD3D8B466B
SHA1:	1B14654D9BCF974270FBDD9CA78344E19D4B160F
SHA-256:	568583A726E8DEDA38703F959E82EE3E77E3C0F1E74CE03FF5666CF92CB5488A
SHA-512:	F05CCDE4041FD1D32B485850743B282E4178A615E644FA1B8CC383DC1E9E4175CBA68AFFD22E8A1A18033C6977847504C5D008BB50E3ED929C13B8AA8FE02C A
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.094887363548494
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEPBRnWimI002EtM3MHdNMNxOEPBRnWimI00OVbVbkEtMb:2d6NxOOSZHKd6NxOOSZ7V6b
MD5:	2C618CDBCB497A0B323FA38806622E4C
SHA1:	7E150CEA5B4F922D1C012E8C62E5F4E67ECC6305
SHA-256:	7903EC29ADFE60051AAC43BED8E925A817F18364B2BB709E8FDA8573282DF33D
SHA-512:	0DA4D12A9E589E07DCC1FF9069A8956576D95A11CC03DA7E3C6A2408A4FD01686D465E59A39521E1B261A2906F1D0AB57965A192B2E9098D9BEF1835D04DA99
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xf15f02b6,0x01d7b509</date><accdate>0xf15f02b6,0x01d7b509</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xf15f02b6,0x01d7b509</date><accdate>0xf15f02b6,0x01d7b509</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.123217718021022
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kPBRnWimI002EtM3MHdNMNxe2kPBRnWimI00OVbkak6EtMb:2d6NxruSZHKd6NxruSZ7VAa7b
MD5:	9B50940FB5ADD7DA1CAAA19F83DB18AD
SHA1:	DF2E26D29CEA73E45B88C18B629D428A2499784C
SHA-256:	62EFFFAB6571BDC6181815DA1C15FAF264410BD340B9A16762F9B5046376D6D2
SHA-512:	EFED5DB607EEDF7303D324C63E92ACDF0781D766F39A0C6AFACE4CD0250826F1D00EB51BD4C3DC5AE5640E4775E7ADFF352533C8CCDA2F95D6409553252DF67
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xf15f02b6,0x01d7b509</date><accdate>0xf15f02b6,0x01d7b509</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xf15f02b6,0x01d7b509</date><accdate>0xf15f02b6,0x01d7b509</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	665
Entropy (8bit):	5.143478469375462
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLjQynWimI002EtM3MHdNMNxvLjQynWimI00OVbmZEtMb:2d6NxvdSZHKd6NxvdSZ7Vmb
MD5:	CACE4BD8155B8D93A20D2D78A140BA49
SHA1:	1D41816CA82B14F44FE617C98FBEB4091D9B0AD9
SHA-256:	AA67F14DD4385A02734C40D91CFE5E6F0779C8617259461E68910F914A543885
SHA-512:	FD58A07B7471E96E14F0A13F14EBEAFE1FB62CBC1AAC266877EBCE931DEAA6770016AC31003579021794FB7E596CD52525BE5315DF23D99451718EB1FD40ACDE
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xf16742c8,0x01d7b509</date><accdate>0xf16742c8,0x01d7b509</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xf16742c8,0x01d7b509</date><accdate>0xf16742c8,0x01d7b509</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	650
Entropy (8bit):	5.110489474085417

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Encrypted:	false
SSDEEP:	12:TMHdNMNxiPBRnWimI002EtM3MHdNMNxiPBRnWimI00OVbd5EtMb:2d6NxESZHKd6NxESZ7VJjb
MD5:	E4440A485A12672EF35929B3BD0E4B93
SHA1:	03424B616404A382C9B06F6D6C8797FDF55C2F1C
SHA-256:	A7050E9C09AA29095C4AB6B34E136B9CBF471C140AAE6D7DEE67F89450D9A39F
SHA-512:	5BDCF485BD04916EA261D411D412F5177693960544153A270C5B1B75DF180FC6BDC92C6FB41152C09675D7A73408026F6DCF53BD9BFCD49CD14B4BFE204DDA
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xf15f02b6,0x01d7b509</date><acc date>0xf15f02b6,0x01d7b509</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xf15f02b6,0x01d7b509</date><accdate>0xf15f0 2b6,0x01d7b509</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.154694922040457
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwjQynWimI002EtM3MHdNMNxhGwjQynWimI00OVb8K075EtMb:2d6NxQUSZHKd6NxQUSZ7VYKajb
MD5:	60286CF6F10FDA7A88015CF26C068D9E
SHA1:	CC2565B314EE2B58621B76FD8C4BB3B70D9234DA
SHA-256:	17E2EC668B991D05CB2CA6B2F59632FF71460C89DBB0B5120B9BC8B84A82DEE6
SHA-512:	66EEDE3EAD2C28699BFEE53EE44AABD840FB867133C9FD89B3B45D6FC4A48E9207FCA202C2A25FD7390487636DDC9F1C3DF4BABCBB990B80A66436FF99ABF 70B
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xf16742c8,0x01d7b509</date>< accdate>0xf16742c8,0x01d7b509</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xf16742c8,0x01d7b509</date><accdate>0 xf16742c8,0x01d7b509</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.098698255707226
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nPBRnWimI002EtM3MHdNMNx0nPBRnWimI00OVbxEtMb:2d6Nx0LSZHKd6Nx0LSZ7Vnb
MD5:	85F5AB6D1F2943E3D06429D944AA89A7
SHA1:	7DDAD5D0A1817CEE48DE9B8AF08B02509BBBC3CD
SHA-256:	6F98FF741B789A84C49EC0FD7C4666709C64AA40A8D53379B1C05C253C7F1EF6
SHA-512:	2DD84CD50C333E51C2244C92257DE9520D038081FEA6B53A0EB5EA986314820E4AAF8C18F64572C031E2ECF7F5045FB2A966E5268D2970FB010480FEC7FDD5A
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xf15f02b6,0x01d7b509</date><accdate>0xf 15f02b6,0x01d7b509</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml vers ion="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xf15f02b6,0x01d7b509</date><accdate>0xf 15f02b6,0x01d7b509</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin202591677780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.134688465510693
Encrypted:	false
SSDEEP:	12:TMHdNMNxxPBRnWimI002EtM3MHdNMNxxPBRnWimI00OVb6Kq5EtMb:2d6Nx9SZHKd6Nx9SZ7Vob
MD5:	A34C81CB414C761A5B9BE5F8AD7D5943
SHA1:	C538DAB5F62BBF57E7C8BB90EE79F941591767DA
SHA-256:	25529D74D2FF6BCB2FEDA018280C9BA4C49F51159ECFB335F2127E22D4B06FD5

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
SHA-512:	52D207683E9C1A66A59F59ABA348A9EB23D3CB5BFE7A006AB5E89517821A6021084FD7697B3EC0B7FFEFAEE2EECB46D3691F36317C5716EBF67D0A4DBE835F66
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xf15f02b6,0x01d7b509</date><accdate>0xf15f02b6,0x01d7b509</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xf15f02b6,0x01d7b509</date><accdate>0xf15f02b6,0x01d7b509</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.1087133360324675
Encrypted:	false
SSDEEP:	12:TMHdNMNxcPBRnWimI002EtM3MHdNMNxcPBRnWimI00OVbVEtMb:2d6Nx2SZHKd6Nx2SZ7VDb
MD5:	F430D3E3D2BF384A1A8867C28ABEE415
SHA1:	0587038717E3C13AC63E51798471B0B65413EAFE
SHA-256:	D5D7AB7FBECAC098814E4EF85AEBF718EDEE2441443DABF149668EF1BEDC4DAC
SHA-512:	060B56C19305FAA7D2A8AA049D9B45DA7A23DD285D36E71D6CAC7CE5780A3B5BABF2FC6438CD3B33C15D3C0888E8F6A9D9DEE52793072D495B49E21BE8239421
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xf15f02b6,0x01d7b509</date><accdate>0xf15f02b6,0x01d7b509</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xf15f02b6,0x01d7b509</date><accdate>0xf15f02b6,0x01d7b509</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.09590925353469
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnPBRnWimI002EtM3MHdNMNxfnPBRnWimI00OVbe5EtMb:2d6NxTSZHKd6NxTSZ7Vijb
MD5:	805C2459EE87B7DEF6315A37D03455C9
SHA1:	1E94D47E59F3AE416AB95E43A90FBB26D9DB258C
SHA-256:	ABA7D191324A6A6F6B5677F894077C17C387B728262D54D42E5A4CA17FC8FF50
SHA-512:	C86BF27117B117EDC40E85E11DDAB72F288EB6BE6A6807D29086388D2D9B15EB85FF5D7EF94DE904B0C28459FC2F50E51DB0911073D3E6D4201753AA4C81304
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xf15f02b6,0x01d7b509</date><accdate>0xf15f02b6,0x01d7b509</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xf15f02b6,0x01d7b509</date><accdate>0xf15f02b6,0x01d7b509</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	934
Entropy (8bit):	7.029028188867423
Encrypted:	false
SSDEEP:	24:u6tWaF/6easyD/iCHLSWWqyCoTTdTc+yhaX4b9upGFpi:u6tWu/6symC+PTCq5TcBUX4brs
MD5:	1144AFB0E2BC599AA1142121884AC8B0
SHA1:	0C46F4BBCBD7F124F68041238E34D8394F30D5DD
SHA-256:	8179BFF39F01CC436DD502D0C1C04A086A9088C97035BAB293E3E37ADDD53127
SHA-512:	C470E4E8B4B4AEEAECC92033EDF5E8ECEFB2E8210FC1C23F175FA38A45D2F7C1AB0BDBABCFC29F8E79A38A027489737EFA9143DDCA08C7EEFEC6D01F7BA85BF8
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat	
Preview:	E.h.t.t.p.s.:.//.s.t.a.t.i.c.-.g.l.o.b.a.l.-.s.-.m.s.n.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.h.p.-.n.e.u./.s.c./.2.b./.a.5.e.a.2.1...i.c.o.....PNG.....IHDR... ... .pHYs..... .vpAg... ... .eIDATH...o.@../..MT..KY..P!9^....:UjS..T."P.(R.PZ.KQZ.S. ....,v2.^.....9/t....K..;_ }'.....~..qK..i.;.B..2.`.C...B.....<...CB.....).....;..Bx..2.}.. ._>w!..%B..{.d... LCgz..j/.7D.*.M.*.....'.HK..j%.!DOf7.....C.]._Z.f+..1.I+.;.Mf....L:Vhg..[.. ..O:..1.a....F..S.D...8<n.V.7M.....cY@.....4.D..kn%.e.A.@lA.,>\.Q|.N.P.....<.!....ip...y..U....J...9 ...R..mgp}vvn.f4$..X.E.1.T...?.....'.wz..U...../[...z..(DB.B(....-.....B.=m.3.....X...p...Y.....w..<.....8...3.;.0....(..I...A..6f.g.xF..7h.Gmq|....gz_Z...x..0F'.....x..=Y}.,jT..R..... .72w/...Bh..5..C...2.06`.....8@A..."zTXtSoftware..x.sL.OJU..MLO.JML.../.....M....IEND.B`. ... .# Ta....# Ta....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\1632725880101-6365[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 622x325, frames 3
Category:	dropped
Size (bytes):	97182
Entropy (8bit):	7.974305831456936
Encrypted:	false
SSDEEP:	1536:oUgpFYv6S6TW5ax4VczvDCUyIsCSp0lccFg2OOpGsF37T4GWxk92jSPApdpwMqcG:oV/s6S6TW5q4iv+UyTp0Vu2OYv4te8wT
MD5:	A843182FAD3657CA8B6AFA0CAAF9EF5A
SHA1:	2FFE112942E83324C8D6A8369F0756DFD47173BE
SHA-256:	9E01C150C28ECAE6D44A41ED2BCDFF91173AED209FAD20612DC3053BB8E53243
SHA-512:	22F4672A48F9DA56D6C771A3C7E07BEBCB979B478139CD3249F7A966653EE14D6092708BC71A18319B5D8B8011BBBE8D7637F6AD2D4D506E779A2DC45544191
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....(ICC_PROFILE.....mntrRGB XYZ .....acsp.....-.....desc.....trXYZ...d....gXYZ...x....bXYZ .....rTRC.....(gTRC.....(bTRC.....(wtpt.....cprt.....<mluc.....enUS...X.....s.R.G.B.....XYZ .....o...8.....XYZ .....b..... ....XYZ .....$.....para.....ff.....Y.....[.....XYZ .....-mluc.....enUS... .....G.o.o.g.l.e. .I.n.c... .2.0.1.6...C.....C..... .....E.n..".....J.....!...1.."A.2Qa#q..B.....R.....$3..Cbr.%4Sc.&5s.....A..... .!.1.A.."Qaq...2....#.$3BCR...45.r.DEb.....?..f,....T...A.....a.p.$y0T. .`..r ...@P.#.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\4996b9[2].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 45633, version 1.0
Category:	dropped
Size (bytes):	45633
Entropy (8bit):	6.523183274214988
Encrypted:	false
SSDEEP:	768:GiE2wcDeO5t68PKACfgVEwZfaDDxLQ0+nSEClr1X/7BXq/SH0Cl7dA7Q/B0WkAfO:82/DeO5M8PKASCZSvxQ0+TCPXtUSHF7c
MD5:	A92232F513DC07C229DDFA3DE4979FBA
SHA1:	EB6E465AE947709D5215269076F99766B53AE3D1
SHA-256:	F477B53BF5E6E10FA78C41DEAF32FA4D78A657D7B2EFE85B35C06886C7191BB9
SHA-512:	32A33CC9D6F2F1C962174F6CC636053A4BFA29A287AF72B2E2825D8FA6336850C902AB3F4C07FB4BF0158353EBBD36C0D367A5E358D9840D70B90B93DB2AE32
Malicious:	false
Reputation:	unknown
Preview:	wOFF.....A.....OS/2...p...`...`B.Y.cmap.....G.glyf.....,...,0..Hhead.....6...6....hhea...,...$...$....hmtx.....($LKloca...`...f...f....maxp...P... ... .name... .....IU..post..... ... .*.....I.A_.<..... .....d.*.....^...q.d.Z.....3.....3.....f.....HL .@...U...f..... .....\.d.\.d...d.e.d.Z.d.b.d.4.d.=.d.Y.d.c.d.].d.b.d.I.d.b.d.f.d._.d.^.d.(.d.b.d.^.d.b.d.b.d...d..._.d._.d...d...d.P.d.0.d.b.d.b.d.P.d.u.d.c.d.^.d._.d.q.d._.d.d.d.b.d._.d._.d. b.d.a.d.b.d.a.d.b.d...d...d.^.d.^.d.`.d.[.d...d...d.$.d.p.d...d...d.^.d._.d.T.d...d.b.d.b.d.b.d.b.d.i.d.d.d...d...d...d.7.d.^.d.X.d.].d.).d.l.d.l.d.b.d.b.d.,.d.,.d.b.d.b.d...d...d...d.7.d.b.d.1. d.b.d.b.d...d...d...d...d...d.A.d...d...d.(.d.`.d...d...d.^.d.r.d.f.d.,.d.b.d...d.b.d._.d.q.d...d...d.b.d.b.d.b.d.b.d.b.d...d.r.d.l.d._.d.b.d.b.d.b.d.V.d.Z.d.b.d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\5096d619-1503-4dc7-8fad-e2ece705fa8a[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 300x300, frames 3
Category:	dropped
Size (bytes):	53563
Entropy (8bit):	7.964566885828139
Encrypted:	false
SSDEEP:	768:G/Xmu+3tpeDse+cRsXU3ojcZMNOQ8m1wxi4ZDAnNTGnRX6rBstUXU7F3nh8oYMZz:umhMEE/U5L1wxiLNTG96rBs1FsM8y
MD5:	C611ADD2A8C6A087CB622C7715FD2031
SHA1:	2543F4F911BA4574194F082A05C6E6E3E06B47C7
SHA-256:	9EA50620C4AE82363FF2573F20C415CCB12348AFBCB8C9FBD677BE1EBBC991A4
SHA-512:	ED88C14AF65461C985D2B1C7EB2394BD0D8C87392D323B28FE623F324FECB1B49D225B022FC54882D5ED80E457EA7FBABD00363AC90BB836F0D1779AF8A0E42
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....C.....C.....,.,.."..... .....J.....!1..A.."Qa. 2q...#.....B...$3R..b.4Sr%Cc..&5T.....A.....!1...A.Qaq."..2.....#B..R...3$CSbr.T..Dc.....?...3E.!...2..u(.).(..C....[jN..R.w..j4.....<.RJ.#. Ue.ee$&L.{.l..l.;..\..\..%..c...../.....Vp.../9.L`.+.....-V.!r.R^ .W&..1B...M$....a.....2K..*XqI...W.U.....,...dT.+>.(.%..H=...*N.a.@1[~Z.RAuJ>.....$.v?f.)...W....W^....P....A( ..)..q.....Q...V.....q.N.....B..n.....Ma.....;5J...2....jud./...>.....S.~^U.R..~TOX.....=.^..U....`T.mB.b.YlZ6.4.JSJ.aCU.....n.sM....u.>W.[.l.&..QBJ.D....r..1%K$....?.T..'.Q.. .`."..a...sb|..s.....[.....+.C.t>.. .m.lA.Ud.....~%Yd..C.*;.n/Q.....@....1.+...\.....V.!f4F..t.... ....Y...X#...q]q.e..QR.x$X

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\89a22c36-158b-411c-9c2c-269457db6c00[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, progressive, precision 8, 1200x627, frames 3
Category:	dropped
Size (bytes):	436596
Entropy (8bit):	7.9862544867409335
Encrypted:	false
SSDEEP:	12288:OYROyuPELHV+6Wz/KN3Fv4sBclmpHyK2JyolQXBn:OYRLIEV+6Siv4sBccyVJywQXBn
MD5:	0F8FA892F54B49EB07C2AD015F5F3B6B
SHA1:	45496238EB99DBF5DAB4AFB8E25E59018FD7E649
SHA-256:	B1E339A5691768E9D1004083F148C238743B9F989C93CCA9F66FBE03AEA0C94A
SHA-512:	A78BA0410E60D6DCF2A6624C3B2E845940603E3EF9BE2D5916FAE4AF854141C72D5A316285E4D06550385B8446757130E618CE934E10470C788F7CEA31EA038F
Malicious:	false
Reputation:	unknown
Preview:	.....!Adobe.d@.....s...../..... .....!1. "2..#30A4.@$..PB%5.`C&6D8'7.....!.1.AQ..a".q.2#...B.....R3...br$. .C4.@.S%.0...D5&.P.cE6'7s...Tt..UuvG98.....!.1..AQaq..".....2. BRr#.0...b3@....CScs$.P`.4%...Dt.Td5u..v.....~k.Nq.'.<x....0.....8.....z.....z+..V.....5F...D".8...s.@.I]..$.?MUK.)$. ...jp..#.Vf.C..... 1L....q..R...&. .$S2..).C..1=.@.....!..%.z.7.0.....<.@.....0.x_.d..8.....@.2.R.-..jj...\.@`..1..X!..3..z..`.0..9Y...J.U `.5T "..z..f....L1S.....\fjz.....d.....#pZ9...Q.....!.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\AAKp8YX[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	497
Entropy (8bit):	7.3622228747283405
Encrypted:	false
SSDEEP:	12:6v/7YBQ24PosfCOy6itR+xmWHsdAmbDw/9uTomxQK:rBQ24LqOyJtR+xTHs+jUx9
MD5:	CD651A0EDF20BE87F85DB1216A6D96E5
SHA1:	A8C281820E066796DA45E78CE43C5DD17802869C
SHA-256:	F1C5921D7FF944FB34B4864249A32142F97C29F181E068A919C4D67D89B90475
SHA-512:	9E9400B2475A7BA32D538912C11A658C27E3105D40E0DE023CA8046656BD62DDB7435F8CB667F453248ADDCB237DAEAA94F99CA2D44C35F8BB085F3E005929E D
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..S=K.A.}{...3E..X.....`..S.A.k.I.....X..g.FTD,....&D...3.....^..of.....B....d....,.....P...#.P.....Y.~...8:..k..`.(.!1?.....]*.E. '.$.A&A.F..._~.I....L<7A{G.....W.(.Eei..1rq....K....c.@.d..zG..|.?.B.)....`.T+.4...X..P...V .^....1..../.6.z.L.`...d.|t...;.pm..X...P]..4...{..Y.3.no(....<..\I...7T.....U..G..,.a..N..b.t ..vwH#..qZ.f5;.K.C.f^L..Z..e`...lxW.....f...?..qZ....F.....>.t....e[.L...o..3.qX.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\AAOT1dh[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	dropped
Size (bytes):	2920
Entropy (8bit):	7.837352684963204
Encrypted:	false
SSDEEP:	48:QfAuETAimCtLOYcCqHYKqlGlmxs9HPlZNSGMnOjRvmNZvijEkWaB:Qf7EC0KYcIFlG8xs9HN3xMWvmWEa
MD5:	3B3B14572190A4316088EBBC77EF1612
SHA1:	5E49E6DBB4F4FB341DDA580F921793E6127F1B66
SHA-256:	E68A714235BAF89A3CCFF02A4E2949F096C4AE7FAB527649FD9462758BC05000
SHA-512:	0CBCBE42CB72D1BCDA4A8D50952EA388799B854CCFF567293AF7CAD59DAC8F210BD55DB3328B138167E673AA1E8D0C1CDEEB0533DB06F481D9E58482BDFEI 15C
Malicious:	false
Reputation:	unknown
Preview:	.....JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..[{.-.N..F{.b._0...2..S....F..v..**&.<..n'..{....sS.ZmH...Q...nT.W.I.>..5...fw0\.q.....C.T.5...x.W..}..O,.>.3m..6:.....A..(.....e.> ls.Z...i.l.iZ...p}+...J.gM..E.>n..%.'.i..4.d.e..U.o..ZZ.f.,...9.g~.%.s.a..c.K.....)=...r..p.Kb;}~...B1.X.6.(.Q.kX&..RzX.ma.G.....;..Y.M-..:.Y.nF..W.8...2kT..4.8.[,s.....Q....q.C.y.!.....+..6 ..48]gI..Z.Y%.....g<w?..R...*K....Q.o9....+

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\AAOU7uP[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	dropped
Size (bytes):	2286
Entropy (8bit):	7.762438974089825

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\AAOU7uP[1].jpg	
Encrypted:	false
SSDEEP:	48:QfAuETA4VXq5oXD0dngdaaL2/ypONS1nJQquK1U05C:Qf7EZRkoXY5gdrL2aON0nJ5NbA
MD5:	2CBDEB817AE9C5D2BDFCD5249DA1C8B3
SHA1:	7D5CF5648CBF4851C4621E44FFCDFD8FE4117B60
SHA-256:	718633983A34E937E6C2331DC7C76BD4B59F6FEECCB4BB44F624EA997724D41F
SHA-512:	ADDF9EE3422F06998E5D95311C1099B1AFCB7F4888796FA22C7A3E4864B8EC8F8FF36DC13EE80AAE37D807F0E15F45D2664507597049D9E7BC05EF7A76CAD9F 7
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......K.d..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?..|..<_..a..K...~G.....t?../m..?......yC.{C..}S...b...<...5..4 .....LO.e.i..4....gm.X..G...5...k..vv..l.]..#.#.s.Mf.Dr.8.}1R.i.%.6Cg.0 t.}..`.t.x..'..._=...y(..G.?._..G..gO......'.?.?.......P.........{E..}Q........?x....=......_....<..C.....}.=.{0................>b...}.......}.=.G..[...KQW..Y.9....5....[.:2JV..xNHb.S.XF.>....gv.ad.F.r.<T.. {2X...}.osE..gv.CbCp./.7F.Q....Z..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\AAOV2Ep[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	11727
Entropy (8bit):	7.835621315722319
Encrypted:	false
SSDEEP:	192:Q2vqXvd8+9CqK3l1CCS1hKClbrNbGlSuqJTeS7DwMz52JPyDglcH9atoY3Zujsj+:Nv6p9h0LCtOCldilSYS7D72QklcH9atg
MD5:	FAD42731F117ABA188BDB809934F8E73
SHA1:	DD4CFECFBD8E10397BE396672B150242D7772D94
SHA-256:	E048468C9B1E6C37B279FF3CC6907B42993077EC595AA500F9F74B87A95191DF
SHA-512:	644D714AE932DFC2E2C469442BED3DF60CA728BC86721C47739DD75542166369E5891AE843EC9174F811738562DDF2C3A119B15E9F75C6804B99B21A9702BB04
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......M.7..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?....-..`-...CL...i...`% ....@......P.@..%...P.@...@....P.@....P.P.L......(..H.4...P.....h...6....P.P...J.(.h.(........(.........b....).).(......(. (.....T.(..0.4.f..4.....J`% ..J.CL.........@.....{P...c........(.(.....b.C..(.S.(......(....-T...S.P...)...(.(.(......@%0....>.^f..{.i\.4..#..q...?/.5V&..k.(.8.k..4\,...Hy.)......25..E......J.d;2.........8.i....2f.H %h.B...OQHdt.P.@..%0.@..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\AAOVqW5[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	19742
Entropy (8bit):	7.795629570128694
Encrypted:	false
SSDEEP:	384:IkmuezunRyo4CyWCLFIhNz1iPX4vbKJXAEZjEiLl2u3u+fiX3NAHCTllU7/k/r:Ikmd56CBI1YovVggHu++E3Num47/o
MD5:	90C39A52F6F4E94EF7A35BAE15142FB5
SHA1:	F9946094116F7223B84BF36B2F44184D63039C31
SHA-256:	B4D5946082AA5E1D063C5ABA6986A9CC0B89D62A601067B48F69475B530C3C7D
SHA-512:	A7DD430E423202B845B7DC78506DE21E8248899AFBD7CC1AC3EEA2815118F49E23ABA16A56CF4777875B5F1C7A369D8D674E3E6F5D7B46CD1DB896056CAD91 1
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......p.n..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?...Z.Z.Z.(.h..........Z.(.h..........(..@. ..Z.....GSS&TU...n......S$.u8iH.8.f.o.b....-..P.......&S.Rb.v2.}+U....d...(l.*.....E.EY..c9 .Bb..&..c.].5M.^z...%..f.2"H.$.&.Z.0.H..mh..Z.........(......@....J.(......J@..P.@..%0..(.(...........@.@.@.h.(...!....Z.(.h............Z.(.h.h.........@..P...@.. .2.3<\ol....[..+B.,....+.U0 =hoB.)ubsX.Q.y.C..y.R.Bo."..B).V%I...*..-\q..4\V"i3..E.Ha..b.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\AAOVqW5[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	10806
Entropy (8bit):	7.841107890701649
Encrypted:	false
SSDEEP:	192:Q2LqdgRBh0PexN7uWyw1uveg6b8zJIxwRyHk44t2oLpgmJaP/5vaKXS9y:NLkW0GxNi0wWShROk4A2o9JaZv3C9y

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\AAOVqW5[2].jpg	
MD5:	FFF051180B47CECFEEB6887452CBEAFF
SHA1:	40C76A4C0B667C2C424CC0E9D02DFA0AE21D0ADE
SHA-256:	FDE0FE3B20C38DDE655761EEA8140FEFED1B497CC936DBC7750F7043237406F3
SHA-512:	988810EBCFA970F00AFFD2E74769E306D8229C12203B28A8F305FD0DC73206C151F1AF37CE9E6ED9461143C9267B103454ECE91507A7760937657B2E0F232494
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...Z@....P.....@..-...P.@.@....P.@.....P.@....P.@....P.@.@.....).P.@..6...Z.(.h.....(.h.....:....#.....c.,:....Q..s...)s.....Q.Ri.a....P.@....P.@....P.P.@..%...P.P.@.....Z.(.h.....r#9.&...A...nZC....l..3 .w.R.QcZ..$~...+..jvZ\.....x..a..&c.pkE39B..&N..jF|.*...(.....(.(.....J.(.....P.h.....Z.(.....<..>8..Ke$Y.E..-.b..J.td..r....Q.g=....U...X...e!VS.V

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB14hq0P[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	19135
Entropy (8bit):	7.696449301996147
Encrypted:	false
SSDEEP:	384:IHtFIzAsGkT2tP9ah048vTWjczBRfCghSyOaWLxyAy3FN5GU643lb1y6N0:INFIFTsEG46SjcbmaWLsR3FNY/Ayz
MD5:	01269B6BB16F7D4753894C9DC4E35D8C
SHA1:	B3EBFE430E1BBC0C951F6B7FB5662FEB69F53DEE
SHA-256:	D3E92DB7FBE8DF1B9EA32892AD81853065AD2A68C80C50FB335363A5F24D227D
SHA-512:	0AF92FBC8D3E06C3F82C6BA1DE0652706CA977ED10EEB664AE49DD4ADA3063119D194146F2B6D643F633D48AE7A841A14751F56CC41755B813B9C4A33B82E45C
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..h.h.....(.h.....(.h.....Z.(.....(.h.....TNY...W....q@..~..<..h.....dG.@.....F....L.@%}.....-K.F.9...c..O.7X9u,%.k.4..4..c.<p"...cp.-...U.J.n2..9.b.d.SphR.\V.5Q-./.LV.6...HM.V.d^E...F.q.*+7..a.m..VOA..qR.X.rx5&.(..Q..P.R..x..WM-.?.....V..GTi.(.(.....(.....J.(.(.....J.(.....Z.(.....Z.(.....Z.(.....(.h.....i..H.@...;..Y...q...0.<e+.B...[.v..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB7gRE[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	501
Entropy (8bit):	7.3374462687222906
Encrypted:	false
SSDEEP:	12:6v/71zYhg8gNX8GA3PhV8xJy4eOsEfOZbLjz:u8O9A/hSJ9lfkbb
MD5:	1FCA95AEED29D3219D0A53A78A041312
SHA1:	5A4661CCF1E9F6581F71FC429E599D81B8895297
SHA-256:	4B0F37A05AB882DA679792D483B105FDD820639C390FC7636676424ECFD418B9
SHA-512:	7E02CEB4A6F91B2D718712E37255F54DA180FA83008E0CE37080DADFE8B4D0D50BC0EA8657B87003D9BAD10FA5581DBB8C1C64D267B6C435DA48CBED3366CEA
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..RKN.A.}... ...e1(."le.....F\...@.."...|... ..ld.$.(.`..V.0].ghK....]SS...J.I.<@.O.{.....:WB8~....}Hr...P.....`I.N...N.....Z...'.3..;....3.B-....i...L.....b..{... ..Q.... .....L...=.d....n.....&.!..O....W1..."....gm5x....[.C.9^Q.BC.....O...../.(...|.~.0hv..S..7.....YBn..B..o.T<.....|.g&....U.....gm.. .....U..,.u..)\$.lN.w]Rm.....OZ.h.....zn.~...A.uy.....,.....3(.....z<....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BBPfCZL[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 50 x 50
Category:	dropped
Size (bytes):	2313
Entropy (8bit):	7.594679301225926
Encrypted:	false
SSDEEP:	48:5Zvh21Zt5SkY33fS+PuSsgSrrVi7X3ZgMjkCqBn9VKg3dPnRd:vkrrS333q+PagKk7X3ZgaI9kMpRd
MD5:	59DAB7927838DE6A39856EED1495701B
SHA1:	A80734C857BFF8FF159C1879A041C6EA2329A1FA
SHA-256:	544BA9B5585B12B62B01C095633EFC953A7732A29CB1E941FDE5AD62AD462D57
SHA-512:	7D3FB1A5CC782E3C5047A6C5F14BF26DD39B8974962550193464B84A9B83B4C42FB38B19BD0CEF8247B78E3674F0C26F499DAFCF9AF780710221259D2625DB86

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BBPfCZL[1].png	
Malicious:	false
Reputation:	unknown
Preview:	GIF89a2.2.....7..;..?..C..I..H..<..9.....8..F..7..E..@..C..@..6..9..8..J..*z.G..>..?..A..6..>..8..:..A..=..B..4..B..D..=..K..=..@..<..:..3~..B..D.....,|.4..2..6..:...J..;..G....Fl..1}.4..R....Y..E..>..9..5..X..A..2..P..J../|.9.....T.+Z.....+..<.Fq.Gn..V..;..7.Lr..W..C..<.Fp.]......A.....0{.L..E..H..@.....3..3..O..M..K....#[.3i..D..>.....I....<n..;..Z..1..G..8..E....Hu..1..>..T..a.Fs..C..8..0}....;..6..t.Ft..5.Bi..:.x...E.....'z^~.....[....8`.....;..@..B.....7.....<.....F.....6.....>..?.n.....g.....s...)a.Cm....'a.0Z..7....3f..<.:e.....@.q.....Ds..B....!P.n...J.....Li..=.....F.....B.....:r....w..|.....`..[}.g...J.Ms..K.Ft.....'..>.....Ry.Nv.n..]..Bl.....S..;....Dj.....=.....O.y.....6..J.....)V..g..5.....!..NETSCAPE2.0.....!...d...,...2.2.....3.`..9.(|.d.C .wH.("D...(D.....d.Y.....<.(PP.F...dL.@.&.28..$1S....*TP.....>...L..!T.X!.(..@a..IsgM..|..Jc(Q.+.....2.:.)y2.J.....W,..eW2.!....!....C.....d...zeh....P.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BBVuddh[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	316
Entropy (8bit):	6.917866057386609
Encrypted:	false
SSDEEP:	6:6v/lhPahmxj1eqc1Q1rHZI8lsCkp3yBPn3OhM8TD+8lzjpxVYSmO23KuZDp:6v/7j1Q1Q1ZI8lsfp36+hBTD+8pjpxy/
MD5:	636BACD8AA35BA805314755511D4CE04
SHA1:	9BB424A02481910CE3EE30ABDA54304D90D51CA9
SHA-256:	157ED39615FC4B4BDB7E0D2CC541B3E0813A9C539D6615DB97420105AA6658E3
SHA-512:	7E5F09D34EFBFCB331EE1ED201E2DB4E1B00FD11FC43BCB987107C08FA016FD7944341A994AA6918A650CEAFE13644F827C46E403F1F5D83B6820755BF1A4C13
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx....P..?E....U..E..|.....|...M.XD.`4YD...{.\6....s..0.;....?..&.../. .....$.\|Y....UU)gj...]..;x..(.."..$l.(.\.E.....4....y.....c...m.m.P...Fc...e.0.TUE....V.5..8..4..i.8.}.C0M.Y..w^G..t.e.l..0.h.6.|.Q...Q..i~.|....._...'..Q..."....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\a5ea21[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	758
Entropy (8bit):	7.432323547387593
Encrypted:	false
SSDEEP:	12:6v/792/6TCfasyRmQ/iyzH48qyNkWCj7ev50C5qABOTo+CGB++yg43qX4b9uTmMI:F/6easyD/iCHLSWWqyCoTTdTc+yhaX4v
MD5:	84CC977D0EB148166481B01D8418E375
SHA1:	00E2461BCD67D7BA511DB230415000AEFBD30D2D
SHA-256:	BBF8DA37D92138CC08FFEEC8E3379C334988D5AE99F4415579999BFBBB57A66C
SHA-512:	F47A507077F9173FB07EC200C2677BA5F783D645BE100F12EFE71F701A74272A98E853C4FAB63740D685853935D545730992D0004C9D2FE8E1965445CAB509C3
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR... ... .pHYs.....vpAg... ... .eIDATH...o.@../..MT..KY..P!9^....:UjS..T."P.(R.PZ.KQZ.S. ....,v2.^.....9/t....K..;_ }'.....~..qK..i.;.B..2.`.C...B.....<...CB.....).....;..Bx..2.}.. ._>w!..%B..{.d...LCgz..j/.7D.*.M.*.....'.HK..j%.!DOf7.....C.]._Z.f+..1.I+.;.Mf....L:Vhg..[.. ..O:..1.a....F..S.D...8<n.V.7M.....cY@.....4.D..kn%.e.A.@lA.,>\.Q|.N.P.....<.!....ip...y..U....J...9...R..mgp}vvn.f4$..X.E.1.T...?.....'.wz..U...../[...z..(DB.B(....-.....B.=m.3.....X...p...Y.....w..<.....8...3.;.0....(..I...A..6f.g.xF..7h.Gmq|....gz_Z...x..0F'.....x..=Y}.,jT..R.....72w/...Bh..5..C...2.06`.....8@A..."zTXtSoftware..x.sL.OJU..MLO.JML../.....M....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\iab2Data[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	242382
Entropy (8bit):	5.1486574437549235
Encrypted:	false
SSDEEP:	768:l3JqIW6A3pZcOkv+prD5bxLkjO68KQHamIT4Ff5+wbUk6syZ7TMwz:l3JqINA3kR4D5bxLk78KsIkfZ6hBz
MD5:	D76FFE379391B1C7EE0773A842843B7E
SHA1:	772ED93B31A368AE8548D22E72DDE24BB6E3855C
SHA-256:	D0EB78606C49FCD41E2032EC6CC6A985041587AAEE3AE15B6D3B693A924F08F2
SHA-512:	23E7888E069D05812710BF56CC76805A4E836B88F7493EC6F669F72A55D5D85AD86AD608650E708FA1861BC78A139616322D34962FD6BE0D64E0BEA0107BF4F4
Malicious:	false
Reputation:	unknown
Preview:	{"gvlSpecificationVersion":2,"tcfPolicyVersion":2,"features":{"1":{"descriptionLegal":"Vendors can:\n* Combine data obtained offline with data collected online in support of one or more Purposes or Special Purposes.","id":1,"name":"Match and combine offline data sources","description":"Data from offline data sources can be combined with your online activity in support of one or more purposes"},"2":{"descriptionLegal":"Vendors can:\n* Deterministically determine that two or more devices belong to the same user or household\n* Probabilistically determine that two or more devices belong to the same user or household\n* Actively scan device characteristics for identification for probabilistic identification if users have allowed vendors to actively scan device characteristics for identification (Special Feature 2)","id":2,"name":"Link different devices","description":"Different devices can be determined as belonging to you or your household in support of one or more of purposes."},"3":{"de

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\jquery-2.1.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	84249
Entropy (8bit):	5.369991369254365
Encrypted:	false
SSDEEP:	1536:DPEkjP+iADIOr/NEe876nmBu3HvF38NdTuJO1z6/A4TqAub0R4ULvguEhjzXpa9r:oNM2Jiz6oAFKP5a98HrY
MD5:	9A094379D98C6458D480AD5A51C4AA27
SHA1:	3FE9D8ACAAEC99FC8A3F0E90ED66D5057DA2DE4E
SHA-256:	B2CE8462D173FC92B60F98701F45443710E423AF1B11525A762008FF2C1A0204
SHA-512:	4BBB1CCB1C9712ACE14220D79A16CAD01B56A4175A0DD837A90CA4D6EC262EBF0FC20E6FA1E19DB593F3D593DDD90CFDFFE492EF17A356A1756F27F90376B50
Malicious:	false
Reputation:	unknown
Preview:	/*! jQuery v2.1.1 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */..!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k={},l=a.document,m="2.1.1",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return d.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a,b){return n.each(this,a,b)},map:function(a){return this.pushStack(n.map(this,funct

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\medianet[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	410470
Entropy (8bit):	5.48633977071712
Encrypted:	false
SSDEEP:	6144:zyTkYqP1vG2jnmuynGJ8nKM03VCuPbeEWpJi9Wmn:91vFjKnGJ8KMGxTPWmn
MD5:	E133E9ADE5E6E1E97EA8DD4678DB5C11
SHA1:	F6EE9B90DC2E8E4FEDAEA3B4FC96C48F5C96915C
SHA-256:	990F03EA23958069320F21E05DD22AD0F4689E135593138090DB2ABAFB909FC1
SHA-512:	A3445A5409EC0A80113B3D91083FEA37216D6DB0D49A6815B432F2C9F0802EEB6FA50745A85E6A129BAFB476194ACA77DC1643A7840DF7440213D3EA60E8825A
Malicious:	false
Reputation:	unknown
Preview:	<html>.<head></head>.<body style="margin: 0px; padding: 0px; background-color: transparent;">.<script language="javascript" type="text/javascript">window.mnjs=window.mnjs||{},window.mnjs.ERP=window.mnjs.ERP||function(){"use strict";for(var l="",s="",c="",f={},u=encodeURIComponent(navigator.userAgent),g=[],e=0;e<3;e++)g[e]=[];function d(e){void 0===e.logLevel&&(e={logLevel:3,errorVal:e}),3<=e.logLevel&&g[e.logLevel-1].push(e)}function n(){var e=0;for(a=0;a<3;a++)e+=g[a].length;if(0!==e){for(var n,r=new Image,o=f.lurl||"https://lg3-a.akamaihd.net/nerrping.php",t="",i=0,a=2;0<=a;a--){for(e=g[a].length,0;0<e;){if(n=1===a?g[a][0]:{logLevel:g[a][0].logLevel,errorVal:{name:g[a][0].errorVal.name,type:l,svr:s,servname:c,errId:g[a][0].errId,message:g[a][0].errorVal.message,line:g[a][0].errorVal.lineNumber,description:g[a][0].errorVal.description,stack:g[a][0].errorVal.stack}},n=n,!((n="object"!=typeof JSON||"function"!=typeof JSON.stringify?"JSON IS NOT SUPPORTED":JSON.stringify(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\medianet[4].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	410470
Entropy (8bit):	5.486293385384316
Encrypted:	false
SSDEEP:	6144:zyTkYqP1vG2jnmuynGJ8nKM03VCuPbQEWpJi9Wmn:91vFjKnGJ8KMGxThWmn
MD5:	506A65285091DB3D95F516D2A259DFAB
SHA1:	C17FCB855EE5DA4061322B2497AF119850631000
SHA-256:	D69CD5B68954BD114F5073D06B165195D28C37D4F3D7D47FA93BEF45D688B2D6
SHA-512:	8684D7F012C98246EEB4E3BE04DC41CFD117B09B85CB67D0B85E85989C96B105D1655FFC4D1C8BC9AAF0E6C514BB93E3CBF359BCF7205DB624E1335D1680D70
Malicious:	false
Reputation:	unknown
Preview:	<html>.<head></head>.<body style="margin: 0px; padding: 0px; background-color: transparent;">.<script language="javascript" type="text/javascript">window.mnjs=window.mnjs||{},window.mnjs.ERP=window.mnjs.ERP||function(){"use strict";for(var l="",s="",c="",f={},u=encodeURIComponent(navigator.userAgent),g=[],e=0;e<3;e++)g[e]=[];function d(e){void 0===e.logLevel&&(e={logLevel:3,errorVal:e}),3<=e.logLevel&&g[e.logLevel-1].push(e)}function n(){var e=0;for(a=0;a<3;a++)e+=g[a].length;if(0!==e){for(var n,r=new Image,o=f.lurl||"https://lg3-a.akamaihd.net/nerrping.php",t="",i=0,a=2;0<=a;a--){for(e=g[a].length,0;0<e;){if(n=1===a?g[a][0]:{logLevel:g[a][0].logLevel,errorVal:{name:g[a][0].errorVal.name,type:l,svr:s,servname:c,errId:g[a][0].errId,message:g[a][0].errorVal.message,line:g[a][0].errorVal.lineNumber,description:g[a][0].errorVal.description,stack:g[a][0].errorVal.stack}},n=n,!((n="object"!=typeof JSON||"function"!=typeof JSON.stringify?"JSON IS NOT SUPPORTED":JSON.stringify(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\otTCF-ie[1].js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\otTCF-ie[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	102879
Entropy (8bit):	5.311489377663803
Encrypted:	false
SSDEEP:	768:ONkWT0m7r8N1qpPVsjvB6z4Yj3RCjnugKtLEdT8xJORONTMC5GkkJ0XcJGk58:8kunecpuj5QRCjnrKxJg0TMC5ZW8
MD5:	52F29FAC6C1D2B0BAC8FE5D0AA2F7A15
SHA1:	D66C777DA4B6D1FEE86180B2B45A3954AE7E0AED
SHA-256:	E497A9E7A9620236A9A67F77D2CDA1CC9615F508A392ECCA53F63D2C8283DC0E
SHA-512:	DF33C49B063AEFD719B47F9335A4A7CE38FA391B2ADF5ACFD0C3FE891A5D0ADDF1C3295E6FF44EE08E729F96E0D526FFD773DC272E57C3B247696B79EE1168BA
Malicious:	false
Reputation:	unknown
Preview:	!function(){"use strict";var c="undefined"!=typeof window?window:"undefined"!=typeof global?global:"undefined"!=typeof self?self:{};function e(e){return e&&e.__esModule&&Object.prototype.hasOwnProperty.call(e,"default")?e.default:e}function t(e,t){return e(t={exports:{}},t.exports),t.exports}function n(e){return e&&e.Math==Math&&e}function p(e){try{return!!e()}catch(e){return!0}}function E(e,t){return{enumerable:!(1&e),configurable:!(2&e),writable:!(4&e),value:t}}function o(e){return w.call(e).slice(8,-1)}function u(e){if(null==e)throw TypeError("Can't call method on "+e);return e}function l(e){return l(u(e))}function f(e){return"object"==typeof e?null!==e:"function"==typeof e}function i(e,t){if(!f(e))return e;var n,r;if(t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;if("function"==typeof(n=e.valueOf)&&!f(r=n.call(e)))return r;if(!t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;throw TypeError("Can't convert object to primitive value")}function y(e,t){retur

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\55a804ab-e5c6-4b97-9319-86263d365d28[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2955
Entropy (8bit):	4.796538193381466
Encrypted:	false
SSDEEP:	48:Y9vlgmDHF6Bjb40UMRBrvdiZv5Gh8aZa6AyYAmHHPk5JKIcFerZjSaSZjfumjVT4:OymDwb40zrvdip5GHZa6AyQshjUjVjx4
MD5:	8FCB3F61085635194CE5A73516DE39F9
SHA1:	4EF7BB8362EE512BD497C48C168085738EE010C3
SHA-256:	CEC95B7811CBF927FD338529A08F6B1BBF12F5B78459D07D15DE92C60C12DD64
SHA-512:	DB60AF665E02724F527C6781396105C456E56D23691A64F57BDD452C0568EF43DE36F63D8B18702A5C5A6FA29C9C16CD6ADEBB74E28BA94AF7291EAC3095861
Malicious:	false
Reputation:	unknown
Preview:	{"CookieSPAEnabled":false,"MultiVariantTestingEnabled":false,"UseV2":true,"MobileSDK":false,"SkipGeolocation":false,"ScriptType":"LOCAL","Version":"6.4.0","OptanonDataJSON":"55a804ab-e5c6-4b97-9319-86263d365d28","GeolocationUrl":"https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location","RuleSet":[{"Id":"6f0cca92-2dda-4588-a757-0e009f333603","Name":"Global","Countries":["pr","ps","pw","py","qa","ad","ae","af","ag","ai","al","am","ao","aq","ar","as","au","aw","az","ba","bb","rs","bd","ru","bf","rw","bh","bi","bj","bl","bm","bn","bo","sa","bq","sb","sc","br","bs","sd","bt","sg","bv","sh","bw","by","sj","bz","sl","sn","so","ca","sr","ss","cc","st","cd","sv","cf","cg","sx","ch","sy","ci","sz","ck","cl","cm","cn","co","tc","cr","td","cu","tf","tg","cv","th","cw","cx","tj","tk","tl","tm","tn","to","tr","tt","tv","tw","dj","tz","dm","do","ua","ug","dz","um","us","ec","eg","eh","uy","uz","va","er","vc","et","ve","vg","vi","vn","vu","fj","fk","fm","fo","wf","ga","ws","gd","ge","gg","gh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\AAMqFmF[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	553
Entropy (8bit):	7.46876473352088
Encrypted:	false
SSDEEP:	12:6v/7kFXASpDCVwSb5I63cth5gCsKXLS39hWf98i67JK:PFXkV3lBKbSt8MVK
MD5:	DE563FA7F44557BF8AC02F9768813940
SHA1:	FE7DE6F67BFE9AA29185576095B9153346559B43
SHA-256:	B9465D67666C6BAB5261BB57AE4FC52ED6C88E52D923210372A9692A928BDDE2
SHA-512:	B74308C36987A45BC96E80E7C68AB935A3CC51CD3C9B4D0A8A784342B268715A937445DEB3AEF4CA5723FBC215B1CAD4E7BC7294EECEC04A2F1786EDE73E1A7
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx....RQ.....%AD.Vn$R...]n\.....Z..f.....\.A.~.f \H2(2.J.uT.i.u.....0P..s..}.....P.....l...*..P.....~...tb...f,.K.;.X.V...^..x<.b...lr8...bt.]..<.h.d2I.T2...sz...@.p8.x<..pH...g:...DX.Vt:.....eR..$...E.d2I..d..b.R.0...]. .j...v..A....j.....H...=....@.'Z^....E|>..tZv".^...#l.[yk(.B<j..#.H..dp.\..m....."#...b.l6.7.-.Q...l6.<.#.H.....|.....>/^.....eL.....9.z.....lwy....*.g..h?...<...zG...c\d.....q.3o9.Y.3.|..Jg...%.t.?>....+..6.0.m.....X.q.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\AAOUPbt[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	dropped
Size (bytes):	9932

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\AAOUPbt[1].jpg	
Entropy (8bit):	7.917912904881758
Encrypted:	false
SSDEEP:	192:QnupWATrmQU7ujYVHTLm8i12TGSrLlpK475jZ+m5x3FgMVCvnDY:0EmeQCJ2GWp/jZ+m/1fVC/k
MD5:	656C5D0C957B7D6F7F4099F9EE92ECD4
SHA1:	C3A31F8B06C89A4643033E0407258602F2C25503
SHA-256:	DCD15E6E43299265B3500D3827122AACC7883D4FCD794C8FDA2596BF87BE71DD
SHA-512:	5C4932020A0ADEF6AA07D2F0A6F0FE23D8BFB0C46D7045C822332EE0AD3A7EB4F74B7780765B2255C47923C6E00508AD9CDE9E44B863BA1B9C4E90CA639C0BD2
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...1TI.....e...[.q)..43Ts.Vf...>(.....F..-.g..`.<.GZf.1..''..t.'..p.P....E..}..z.L.m....''...i.bI.'Q.!...Bb.....(.A.w..''.f.....0.&.\(..Z....c.....*.-...4....'.D=3.M.#Z.....?..B(.pH.' .?.....=....N.v..46{f...Ns..?Q.f..@....P.@....P.@..0.b0.bq.?....ny...g<.....0q.,..Jn.E.....D.=.S1.)..X...9Q]...2.1....[[....y...nP.;.V-O..j...).....2..4.M3"H...qHddP.q@.''..h...E.q

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\AAOV8Yg[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	35862
Entropy (8bit):	7.95081760196589
Encrypted:	false
SSDEEP:	768:IZ3yGUGZHMa2sanr9JYdOKgVM31EZQhPxBdt9d+ciXZtli:IZ3xOaTanxJYwDK2QnBdncZXZri
MD5:	FC5DF80463B41DFBC89D1524BF2DE4CA
SHA1:	D6277B7EC42D960BD58B7CFA594539A333A0865D
SHA-256:	F8EBFFA1DDFD809E6FE9E16295D0BE476D23A539D62CC33A17046007DCEC093C
SHA-512:	6B152E91661C8546D71ABDB0A13985F73C0F417200119055A44AC06C71D1D7D316492C2B632456DCDD1F15FACB0C937B397B716BC878DB95442F018CCE91946
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..Bg.~.W.w.....".oP.X.Z..s..0~.Vb..i..F..b...y.....Aq1r.d..Y ..@...!.qL,4.k.2<.Vl..Z....I..".0."mf....W.1G+.b.S.4j....d.J....7."..1...qM$.e.{y..r..qT...R.y.$A1.@..q.W..l...b9..2.&.....).3+..*w'.j[bHdr.....>..._.....R.$8...L`z..(.....9=)...rH..6.Rj6...h...>V..EY<Af....|....\....a.....A...SS.~..@?.I.J9Wq]....<.....i..v3.W...6....Qt._.....9{..Z.J..s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\AAOVg6E[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	14459
Entropy (8bit):	7.926081343484909
Encrypted:	false
SSDEEP:	384:NV7pIgvD0ClDJOc4ThS46NobcJM7SaBqX6vr748gocyc:NVD5Kc4ONowaBxrE8gow
MD5:	059D037D2E78F28EFA9477F4521F424E
SHA1:	C1586C5FE9C3FE366E1BC46E80727238C7F9D2C4
SHA-256:	E9BB541B96960543796DD964C30CA1C6104944DA8F1A1430015570C0F97383C2
SHA-512:	CD5C86BC310D566A7102DE8D1E870D2D09921B1380DBD04FCDB5A044E507D64FEF7C8832D32EEE70FFFB740A01975C5F45BFB522AAC382A190E9954A31188A8
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..S.^m...U... ..].z..x....U\..d<.(.Xq..g.E..io....X.....).,,.i.)6.+....;..`.aa.p..4.8...@..).i.....te'.1...oQT!.S.E.@g].'...\,x....G..cP...=.ai.....A.t.<G...w..j.....:.{....,Fe.....,C....8..o.....O.~EK. ks.R.-.....-+._(7...t.M.+@\z.G.E.s.j.g..VH.....b..Y.4...,r....2h...O4..dc.L.Z..:f.....1.....@\g..94.....1..h..r....e.h..i....<..s@..[.4..H.' .`5Ve.i..y.q.`Dc..&..#

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\AAOVwgb[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	27567
Entropy (8bit):	7.969605306037314
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\AAOVwgb[1].jpg	
SSDEEP:	768:N69Gxl/1FRYB31ib+itac3BwSySHXGorTBOFhPtr:N69OjRfb+eyoGS9OFr
MD5:	40786A2A69103B5E4426A55464F81E4D
SHA1:	EB10CF39B97A07BC1E8D3CC7F2A4988ACE2796ED
SHA-256:	71AA6DFB987F76A78785E2BE89387DBEEB09B901BD48A56F6757CE9358A8A533
SHA-512:	D56FEA4EB4BF9B03B9E4D1D52A82AC0EB1FF79F6D2FE42B6477E4CD8CAD9B16470FD9E2784A10F3457CB4C5972C5257984CEA895FD25D766FEB4E916E3EA14 09
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..M..M..#..zW..j..K.....k.:..p.....Z.SMnD..R=NK.^{9!...U.rk...X.,1...h..Y.1b...Y.(....y....T.n...\..p..L2./..n...,...Pko...ur}..4... I ..i.%..Q....e*...'.q...(Geb\..i.#s.}*..V.D.m.gt.1.".<{...{D..K4.K....u"...,.w.H._....}G4..M.]].!o.X..i=..<R..4.....}..p.....MO..X..[.R..,.....K.I..]I|S...(.0D...C1.....K.....-6."...O.dx...N...;!...1 /,.=r.....E<](.E.A.y.^CL.s.n8..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1aXBV1[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1161
Entropy (8bit):	7.80841974432226
Encrypted:	false
SSDEEP:	24:zxxmempCXfPZq+DLeP1cRwZFIjvh3wuiFZMrFYzWkG4iD3w:zxRBXfB9k1cRuFIbJWsFYT/2w
MD5:	D858BE67BEA11BF5CEC1B2A6C1C1F395
SHA1:	6090B195BEF6AF1157654048EECEA81E2DCEC42A
SHA-256:	FC7CF2E8592C8E63CFF72530DA560E3293EC2DE3732823DBAEB4464609EA0494
SHA-512:	180FA05957A2FCF8192006D5F8E8D3E4DE1D79DD6F9F100D254C513068FC291B3086DE9A8897B3658D83FE3335FDEB4023F13AC3A6A8A507729AE22B621EC7D
Malicious:	false
Reputation:	unknown
Preview:	.PNG........IHDR.....................U....pHYs.....+.....;IDATx...}..c.....j...2..Y.l....i.<4.c...)..p...M..(4b.Z.r...."cDe..Bz..sw.g.9.....^..u}?....n[he.{..,u.....`.>.[.iE...[.1B.Tx..X.7......0.[... ..5.)p...x...d\...g.....WmE1.sl.....u....3K.[.....;.....f....W(.E3//6...2tG..AU...`7f.m. r;..r..{.~.X./.Q._..`.C...D.M.n.p%..U...0...HTe..1.....7.@.Tn.r.....C.k.../[..j.X..:.+Q.3.y.4. , E....g.Y...p^..c..:..#/...iES....E.w..op.... .9.W.....).+.1....A~.\...{...q.El..`.&;..o.&q:.K....|.....e.(..."9.z\.~.....G.h...\.';... G.....J....P.gy..<BeK.I..<..d..MF".O.uE...R..-...{..J...F ..*.a..lj...t\.W.....&.l]?...WvP...._o.c.....8..10;.q-"8L.2..~,....~V..|]..c..\.'...I.....u8.....Q.3..lB."..!LD.bs.K[..)0P0.9..'....K...W..g..,f.....S.....S..)N..D;....<.....7#..X2.ws.....H.vF '...,$l..R4.O/.~..j.'&..6.....!.D.m..].G.....W#.Uir..sT..m....h...UN.._V#..S.6.....i..M....[..?.J.....OL\..Q<{.G.n5).Ix.....<+7Ey.....W.].NR.o...._.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1cG73h[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1131
Entropy (8bit):	7.767634475904567
Encrypted:	false
SSDEEP:	24:lGH0pUewXx5mbpLxMkes8rZDN+HFlCwUntvB:JCY9xr4rZDEFC
MD5:	D1495662336B0F1575134D32AF5D670A
SHA1:	EF841C80BB68056D4EF872C3815B33F147CA31A8
SHA-256:	8AD6ADB61B38AFF497F2EEB25D22DB30F25DE67D97A61DC6B050BB40A09ACD76
SHA-512:	964EE15CDC096A75B03F04E532F3AA5DCBCB622DE5E4B7E765FB4DE58FF93F12C1B49A647DA945B38A647233256F90FB71E699F65EE289C8B5857A73A7E6AA0 6
Malicious:	false
Reputation:	unknown
Preview:	.PNG........IHDR.....................U....pHYs.....+.....IDATx..U=I.E.~3;w{..#].Dg!.SD...p...E....PEJ.....B4.RE. :h..B.0.-$.D"Q 8.(.;.r.{3...d...G.....7o..9....vQ.+...Q....."!#I.....x|...\...& .T6..~.....Mr.d.....K..&..}.m.c....`.`....AAA..,.F.?.v..Zk;...G...r7!..z.....^K...z.....y...._..E..S....!$...0...u.-.Yp...@;;;%BQa.j..A.<)..k..N.....9.?..]t.Y.`....o....[.~~..u.sX.L..tN..m1...u .....Ic....,7..(..&...t.Ka.]..,.T..g..".'...W.....q....:+t.?6....A..}...3h.BM/.....*..<.~..A.`m..:.....H...7.....{.....$... AL..^-...?5FA7'q..8jue...*.....?A...v..0...aS.*:.0.%.%".....[.=a.....X..j.. <725.C..@.\. ..`._....'...=....+.Sz.{.....JK.A...C|{.|r.$.=Y.#5.K6.!.....d.G...{.....$.-D*.z..{....@.!d.e...&..o...$Y...v.1.....w..(U...iyWg.$...\>..].N...L.n=.[.....QeVe..&h...`;=.w.e9..} a=.....(.A&..#.jM~4.1.sH.%...h...Z2".....RP....&.3.....a..&.I...y.m...XJK..'...a.....!.d.....Tf.yLo8.+.+...KcZ.....|K..T....vd....cH.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\a8a064[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 28 x 28
Category:	dropped
Size (bytes):	16360
Entropy (8bit):	7.019403238999426
Encrypted:	false
SSDEEP:	384:g2SEiHys4AeP/6ygbkUZp72i+ccys4AeP/6ygbkUZaoGBm:g2Tjs4Ae36kOpqi+c/s4Ae36kOaoGm
MD5:	3CC1C4952C8DC47B76BE62DC076CE3EB
SHA1:	65F5CE29BBC6E0C07C6FEC9B96884E38A14A5979

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\a8a064[1].gif	
SHA-256:	10E48837F429E208A5714D7290A44CD704DD08BF4690F1ABA93C318A30C802D9
SHA-512:	5CC1E6F9DACA9CEAB56BD2ECEEB7A523272A664FE8EE4BB0ADA5AF983BA98DBA8ECF3848390DF65DA929A954AC211FF87CE4DBFDC11F5DF0C6E3FEA8A5740EF7
Malicious:	false
Reputation:	unknown
Preview:	GIF89a.....dbd.....lnl.....trt.....!..NETSCAPE2.0.....!.....,.....+..I..8...`(.di.h..l.p,..(.....5H.....!.....,.....dbd.....lnl.....dfd...../..I..8...`(.di.h..l..e.....Q... ..-.3...r...!.....,.....dbd.....tvt.....*P.I..8...`(.di.h.v.....A<.. .....pH,.A..!.....,.....dbd.....|~|.....trt...ljl.....dfd..... .B`%.di.h..l.p,.t]S.....^..hD..F. .L..tJ.Z..l.080y..ag+...b.H...!.....,.....dbd.....ljl.....dfd.....lnl.....B.$.di.h..l.p.'J#.....9..Eq.l:..tJ.... ..E.B...#.....N...!.....,.....dbd.....tvt.....ljl.....dfd.....|~|.....D.$.di.h..l.NC.....C...0..)Q..t...L:..tJ.....T..%...@.UH...z.n.....!.....,.....dbd..... lnl.....ljl.....dfd.....trt...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\auction[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	6445
Entropy (8bit):	5.87552558421432
Encrypted:	false
SSDEEP:	96:8zfgn/omlMVYi7TFfA3F3P0elt90Hw5etubptIjFaNS1LzZpH/:Hkq3xP0el4btytIZjVF/
MD5:	0E0E8D125A126C138B6E6D3B2FE1323A
SHA1:	8912CBDE5D2362A68765DAAF1DBF99B54849B78F
SHA-256:	6468196DBA9781D4BB707CF30313D531FE5EC583AE9F4776DF7AD96E85E86C35
SHA-512:	E6A395E63888AE79520B58DF85F6F7B8968EF75F117A44671512820160B2E950E1A73DB7B06A2D645757B1CA692B29C8C05EA078FBF49A84D93FC34B7E10FA9E
Malicious:	false
Reputation:	unknown
Preview:	..<script id="sam-metadata" type="text/html" data-json="{"optout":{"msaOptOut":false,"browserOptOut":false},"taboola":{"sessionId":"v2_6aff4c5a3031328260c2463c51178b2a_903e8ea3-bba7-48cc-a96d-9fcb3d71cc0d-tuct84d2718_1632870808_1632870808_CIi3jgYQr4c_GNa9hPSMiYmZ5gEgASgBMCs4stANQMuIEEjTnt0DUP_____wFYAGAAaKKcqr2pwqnJjgFwAA"},"tbsessionid":"v2_6aff4c5a3031328260c2463c51178b2a_903e8ea3-bba7-48cc-a96d-9fcb3d71cc0d-tuct84d2718_1632870808_1632870808_CIi3jgYQr4c_GNa9hPSMiYmZ5gEgASgBMCs4stANQMuIEEjTnt0DUP_____wFYAGAAaKKcqr2pwqnJjgFwAA","pageViewId":"051f0e5a20c14b57a34074251f23c8b9","RequestLevelBeaconUrls":[]}">..</script>....<li class="single serversidenativead hasimage " data-json="{"tvb":[],"trb":[],"tjb":[],"p":"gemini","e":true}" data-provider="gemini" data-ad-region="infopane" data-ad-index="2" data-viewabil

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\checksync[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	21700
Entropy (8bit):	5.305011411091235
Encrypted:	false
SSDEEP:	384:VZAGcVXlblcqnzleZSweg2f5ng+7naMHF3OZOfQWwY4RXrqt:L86qhbS2RpF3OsfQWwY4RXrqt
MD5:	712460EA00FAF46836F259ADE169F255
SHA1:	7AB2E69D9931844A3F62BA22C5F195B8F27A5819
SHA-256:	5F493C20992ED790ECF1DA80F72F49F967C964AC4C0DF5085FF4A567937D90B7
SHA-512:	37749766A17F501635940085A519530A94561B95D4CF29BAD9514F3164EF80B01AB9A3B748F9FC099E6EA03E963FCB00D4F06C3D88377AD12902C68AA9C2316C
Malicious:	false
Reputation:	unknown
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":80,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"bs":{"name":"bs","cookie":"data-bs","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0},"ttd":{"name":"ttd","cookie":"data-ttd","isBl":1,"g":1,"cocs":0}},"ussyncmap":[],"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\checksync[4].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	21700
Entropy (8bit):	5.305011411091235
Encrypted:	false
SSDEEP:	384:VZAGcVXlblcqnzleZSweg2f5ng+7naMHF3OZOfQWwY4RXrqt:L86qhbS2RpF3OsfQWwY4RXrqt
MD5:	712460EA00FAF46836F259ADE169F255
SHA1:	7AB2E69D9931844A3F62BA22C5F195B8F27A5819
SHA-256:	5F493C20992ED790ECF1DA80F72F49F967C964AC4C0DF5085FF4A567937D90B7
SHA-512:	37749766A17F501635940085A519530A94561B95D4CF29BAD9514F3164EF80B01AB9A3B748F9FC099E6EA03E963FCB00D4F06C3D88377AD12902C68AA9C2316C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\checksync[4].htm	
Reputation:	unknown
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":80,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"bs":{"name":"bs","cookie":"data-bs","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0},"ttd":{"name":"ttd","cookie":"data-ttd","isBl":1,"g":1,"cocs":0}},"ussyncmap":[],"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\de-ch[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	79097
Entropy (8bit):	5.337866393801766
Encrypted:	false
SSDEEP:	768:olAy9XsiItnuy5zIux1whjCU7kJB1C54AYtiQzNEJEWlCgP5HVN/QZYUmftKCB:olLEJxa4CmdiuWlDxHga7B
MD5:	408DDD452219F77E388108945DE7D0FE
SHA1:	C34BAE1E2EBD5867CB735A5C9573E08C4787E8E7
SHA-256:	197C124AD4B7DD42D6628B9BEFD54226CCDCD631ECFAEE6FB857195835F3B385
SHA-512:	17B4CF649A4EAE86A6A38ABA535CAF0AEFB318D06765729053FDE4CD2EFEE7C13097286D0B8595435D0EB62EF09182A9A10CFEE2E71B72B74A6566A2697EAB1B
Malicious:	false
Reputation:	unknown
Preview:	{"DomainData":{"pclifeSpanYr":"Year","pclifeSpanYrs":"Years","pclifeSpanSecs":"A few seconds","pclifeSpanWk":"Week","pclifeSpanWks":"Weeks","cctId":"55a804ab-e5c6-4b97-9319-86263d365d28","MainText":"Ihre Privatsph.re","MainInfoText":"Wir verarbeiten Ihre Daten, um Inhalte oder Anzeigen bereitzustellen, und analysieren die Bereitstellung solcher Inhalte oder Anzeigen, um Erkenntnisse .ber unsere Website zu gewinnen. Wir geben diese Informationen auf der Grundlage einer Einwilligung und eines berechtigten Interesses an unsere Partner weiter. Sie k.nnen Ihr Recht auf Einwilligung oder Widerspruch gegen ein berechtigtes Interesse aus.ben, und zwar auf der Grundlage eines der folgenden bestimmten Zwecke oder auf Partnerebene .ber den Link unter jedem Zweck. Diese Entscheidungen werden an unsere Anbieter, die am Transparency and Consent Framework teilnehmen, signalisiert.","AboutText":"Weitere Informationen","AboutCookiesText":"Ihre Privatsph.re","ConfirmText":"Alle zulassen","AllowAll

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\location[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.55341170338059
Encrypted:	false
SSDEEP:	3:LUfGC48HptOE9HhE/fQ8I5CMnRMRU8x4URGQP22/9SM+nmyRHfHO:nCj4ElhEAjvRMmhUMQP2zjO
MD5:	A6B42B0E34A354029688094D2B66EB8A
SHA1:	400B86D37BB8C1F8EC364F98A780D981F1357E92
SHA-256:	6AC51762DD026703234ED9446F010135439C46DC525113BAF9D202F2CE199DBF
SHA-512:	A1096CAA2142AB0F7A1D0899BBBF468D1053D248B61EAD2D8B2F3D63B2CF37570202195D8CDCA0FFD49DEDB9C63588F8EFAF463EB07C640235AD0AF1D70BBD5
Malicious:	false
Reputation:	unknown
Preview:	jsonFeed({"country":"CH","state":"","stateName":"","zipcode":"","timezone":"Europe/Zurich","latitude":"47.14490","longitude":"8.15510","city":"","continent":"EU"});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\tag[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	10308
Entropy (8bit):	5.457068788802413
Encrypted:	false
SSDEEP:	192:4EamzdxOBoOBpxYzKhp5foeeXwhJTvlXQuzSqHEgiKGWdrBpOIztlomlRokr:4EamR7OrxYSLQdiMoHEgxGWdrz4+
MD5:	FAAE65A590E21D317489BA7A8ECB4A65
SHA1:	82369DE147E12C60BEB37EB87ECB5D1A73EA54F6
SHA-256:	B8D88C7C37CC39C30E5793572838005C2661C0AAB8FF8FB1E671F75F81E54CA2
SHA-512:	77C7910E1320BCD1D626BB6958978E38F9DE564CE9262F14CC35FD1207BCA3B63370039FB633DC8E4452DF19D41D3BE51AFB31F4E504232A7F9D087B781E849
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\tag[1].js	
Preview:	!function(){"use strict";function r(e,i,c,l){return new(c=c||Promise)(function(n,t){function o(e){try{r(l.next(e))}catch(e){t(e)}}function a(e){try{r(l.throw(e))}catch(e){t(e)}}function r(e){var t;e.done?n(e.value):((t=e.value)instanceof c?t:new c(function(e){e(t)})).then(o,a)}r((l=l.apply(e,i||[])).next())})}function i(n,o){var a,r,i,e,c={label:0,sent:function(){if(1 &i[0])throw i[1];return i[1]},trys:[],ops:[]};return e={next:t(0),throw:t(1),return:t(2)},"function"==typeof Symbol&&(e[Symbol.iterator]=function(){return this}),e;function t(t){return function(e){return function(t){if(a)throw new TypeError("Generator is already executing.");for(;c;)try{if(a=1,r&&(i=2&t[0]?r.return:t[0]?r.throw||((i=r.return)&&i.call(r),0):r .next)&&!(i=i.call(r,t[1])).done)return i;switch(r=0,i&&(t=[2&t[0],i.value]),t[0]){case 0:case 1:i=t;break;case 4:return c.label++,{value:t[1],done:!1};case 5:c.label++,r=t[1],t=[0];continue;case 7:t=c.ops.pop(),c.trys.pop();continue;default:if(!(i=0<(i=c.trys).length&&

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\AANcu7b[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	35530
Entropy (8bit):	7.959645305810465
Encrypted:	false
SSDEEP:	768:ItvbJFJEtBLCleym4zx18nET0uH/BL9Wnc1o+4G9x3:ItvbJEGley1vL9fBL0ncK+4uF
MD5:	C3466D21DA49B7AADE86135CAF672867
SHA1:	31B0546925A77686B4CAA3B1B8DDB3094BC80774
SHA-256:	353E0A946A167793ACC429264BB2AB11546A2775FF7E454B9A26A145CF63435A
SHA-512:	EF48B1BCE8A44F35B7859C863BA73E18917ACD6C8AB513843093149EEA95AE21C07F2FDACD1DCEE0F1822483DD117DD38BB23D2AFEED92B6568BCE50AFA1E 4F9
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....<V.....IEU.4...4..+rMH.7.M0,....hZ..T..8P"...e"D.+`R....@.\|S.JY2..IE+...E. K..w.j7..xk.#Io..@.....uiX...k...(.D,...i..... `g.4..._ .jC...'....H...S.9..Z..ct1.G1\|.....y.<..,....T..#...{b...m[$vY% ...V...b.=i_...n.&*....&.].z..'...d.G.'.qI.s.T..+.-.I*{.I.+X..Q.U.{..4CE.Z5.%.....B2j...E.....y..Z..ed.c.....*. I<...Y_.2..W ....dq0...i.lu.....sH.$...s.T..@.|....."..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\AANf6qa[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	432
Entropy (8bit):	7.252548911424453
Encrypted:	false
SSDEEP:	6:6v/lhPahm7saDdLbPvjAEQhnZxqQ7FULH4hYHgjtoYFWYooCUQVHyXRTTrYm/RTy:6v/79Zb8FZxqQJ4Yhro0Lsm96d
MD5:	7ED73D785784B44CF3BD897AB475E5CF
SHA1:	47A753F5550D727F2FB5535AD77F5042E5F6D954
SHA-256:	EEEA2FBC7695452F186059EC6668A2C8AE469975EBBAF5140B8AC40F642AC466
SHA-512:	FAF9E3AF38796B906F198712772ACBF361820367BDC550076D6D89C2F474082CC79725EC81CECF661FA9EFF3316EE10853C75594D5022319EAE9D078802D9C77
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....bIDATx..?..a..?.3.w`.x.&..d..Q.L..LJ^.o...,....DR,.$.O.....r.ws..<.<.\|..\|..x..?....^..j..r...F..v<.....t.d2.^...x<b6....\.WT...L".`8.R..... .m.N'..`0H.T..vc...@.H$..+..~..j....N.....~.O.Z%..+..T*.r...#.....F2..X,.Z.h4..R)z..6.s:...l2...l....N>...dB6.%..i...)....q...^..n.K&..^..X,>'..dT)..v:.0D.Q.y>.#.u:.,...Z..r..../h..u....#'.v .....\_&^....~..ol.#....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\AAOV2qA[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	modified
Size (bytes):	21409
Entropy (8bit):	7.956178661075971
Encrypted:	false
SSDEEP:	384:Ng/TiejnAE0p4dICjBs4diSokUzRFZd0BcDryJ9En9MfKRTfh6zrH5Y:NsA74dICLokUtFZd0KDmrEWfkfhiY
MD5:	203419243921B1C02DB93C3AD6166A71
SHA1:	2C34BCCF2600A0E5D10E62C6F8739D289912CCAC
SHA-256:	CAC75CA9837D6A69ECFFFDC0411A0960C806A8C8CB747948422B6E7839CA8B09
SHA-512:	DDE29A60D4C33874435325B592AD2A654A0E8767D437FAF2589A0F095F88093784C38E954D83355C56747DE090AFB55DE14FEF8BD4BC7E83396E69CD7DB8B28
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..& .. .H.2..D.z...5.D....i...1.p...'.@.V..I{.....G.$....M ..m...$t..$....(.U.d....w..{9l.7....2;....'.....2'..<;i....K.UHV.`8...J...my.mj.[E...6.. {#.....Q...../.j.4..x.c.8.<.....h. ..4....m..]NFC3..b..IA..X.B....eE..Q@...l.q.....J..9..s.%.Z...d..`...F{.%.....[....s.z~F..d[h....{.\....x.yS..T.5.n...+H.J..kg.*..:.....sr..q.T.....m.cP.. 0....j...j/r...8..=y.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\AAOV2qA[1].jpg	

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\AAOVrzQ[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	dropped
Size (bytes):	11211
Entropy (8bit):	7.9348237072689445
Encrypted:	false
SSDEEP:	192:Qn7krRXUrl9p0dQzD8PNsgcUdlcghbPUgAsXwbdmrROKMvzVQ9f/Oh:07kSk9nv6NsoeUzjwBYRTMvpQJ/Oh
MD5:	DD72BD402785EB8CC83690146EE1E3D9
SHA1:	B1C9B2998915AA16F04BFF367AF4F3353300ECB7
SHA-256:	E78765DCF17464B05FEFC37FD0A95E5AD13F94E04FB4E7283DB9DEF77B17F649
SHA-512:	A51CCD4CEEB65445A0DFB214C9623A00420AA7A9B45D78A987A2215111A10C942612D52DA24C88AAAEB2EE98017ECD1C088AF23FA5CF4C40361A3F69F84418 3
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....5v..1.p>..m#...h.(r03.`l...y..d..k.v.T..Mg*..N.O].r;8.....<]8.....j.2..CEM!s\.NZ...#.Q`.0.n.t..-tDJi".]..... ;..../..t!J6.9..... .._.Mw1%.b.....\\C4.Ic...(8.....-z.HJ.....5.!~..+..;.Z.Ux..V.>a...DJ.CV.(m.}. ....:.qM.4..:..A8<.C...W.....o.].<..hu...9a.*9...Xh.)L-.;...x...I..;..)b).H#v...m..g....g....V...<D...@.B D8...O.O..*..p...On.....Bn.u.....M..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB19vKWo[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	dropped
Size (bytes):	2131
Entropy (8bit):	7.639371518501625
Encrypted:	false
SSDEEP:	48:QfAuETA+42eKiIeQJQOayugeGVikTss8hvBj0PHOPG:Qf7E82iIzJZvikAhCHF
MD5:	71EFB6516B7F3DC52990EC9FFD95D8FA
SHA1:	54E3B79CB6E34B02350FF923B385032483EBBB17
SHA-256:	9203D2CC98C4861FF90E1DCA1008127C01783047ECC52608840B1CA8F09F70E9
SHA-512:	9F8213658865795DB9987C28EAE35D80087935437C93ACC909CA093002FA3DAE4E33D7533822273FA569BF58039CECBF16800537683EF0C2A0AA973EC0F1FAA5
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...!._*-.8.q..';....dz.....^q@.c$..Gy.L...#8.h...cA...$q...+.M.+.....`hcVo.;...p...K.,#T.)..rM...k(.C.....s.8R.....#X..i$.....(.....1.61. .....Gj..$.. .x.'.N.0"..0O....@...K....p....f../..y.....F..{....P.....!mx.`.1.`w.=h.KM-r...rc..#/..._..|hp.Q.v.G.....c..h....Q....#pl.....V:AH.on.n..@....i..u.]I..9...@.....K...b...Q..6...U.a...dg. '.?.....g.Q.8.....z|.L-}...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB1kMP0[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1198
Entropy (8bit):	7.799680025476214
Encrypted:	false
SSDEEP:	24:azZAfjKsQ7VZ/CRWAMUAOfemojmP8I4GNu8gtuK3uzFmrQoD:4Afjm7VUWA/Y67QYK+zM3D
MD5:	1CD1232E6BF6A22BF415CB2C4C767D52
SHA1:	83BD3437ACC73448C669634483201E5B48BFA05C
SHA-256:	1A9374FF802B1F5AE3D0A10D8C051C1EE4DC59CDE290F31E64A938E205592801
SHA-512:	D3E8255599706340EC64E3101DACB287D880369570F02FF026AA33757C4E63EE78D795E215ACD52FE0BDF9984CC7A43E7D08D963169C2E196FDEA76BB2609D1
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB1kMP0[1].png	
Preview:	.PNG.....IHDR.....;0.....pHYs.....+.....`IDATx..WkL.U.>3....Et..TD...)m...$.....?...0....6`..(1..VS.Gcb".".?0....h4VE#..k. ....f...-.....y.{.w.....$..!..P.....r.a....\.....m. .t....7....oCn.}R ~.!..z.q].@>...W.X+.u|.....*....@...'H.....->aU...3uX.?...W.d.....).1.y;".....\B.t..e..W....0)..).`0j....#..x.f..m..<.?.t...c.....(.....1..w...|i3Os%$..C...>..\.G..T}.b..... [....E &...>022r.....-.\|:.S/...[.....-'...~.$.}...By^W_UeeJZ.....)33.....$...<.....%g.....djF....S.....=s....O....8.ID....-/.D"o.....3.....:-.vj..NI.jk}..M'.#nw.....[n.{cFFF...&..... C...f.kg... /...W.=.f...\...t.....}>.9.N>..b.....w.....vOOO.....1/..9R..p..a.>(.A....x...((0YdY&.h...!Foo..}}}.a^.ll....Q...8Y...~///..#...K.....OlD...%.....n.h4.....el.....YVVv.H...h``. fgg?a.[....8C.....X.J..*MLL.....TPz..\.u..I<.TR%Y.oYQTES%..$.m.v.X.g@E..8....e5.S.....X.m.uuu....g.8....1..Q..t}.3.....:.d..[.}....@.'.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB7hjL[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	462
Entropy (8bit):	7.383043820684393
Encrypted:	false
SSDEEP:	12:6v/7FMgL0KPV1ALxcVgmgMEBXu/+vVIIMhZkdjWu+7cW1T4:kMgoyocsOmIZII+7cW1T4
MD5:	F810C713C84F79DBB3D6E12EDBCD1A32
SHA1:	09B30AB856BFFDB6AABE09072AEF1F6663BA4B86
SHA-256:	6E3B6C6646587CC2338801B3E3512F0C293DFF2F9540181A02C6A5C3FE1525A2
SHA-512:	236A88BD05EAF210F0B61F2684C08651529C47AA7DCBCD3575B067BEDCA1FBEE72E260441B4EAD45ABE32354167F98521601EA21DDF014FF09113EC4C0D9D7 8
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx...N.P...C.l...)...Mcb*qaC/..]..7..l...x.Z.....w....._....<....|....."FX.3.v.A.....1..Rt...}.....;....BT.....(X.....(....4...-...f ....0.8...|A.:P%.P..if.t..P..T.6..)s..H..~.C..(.7.s>....~...h..bz...Z.....D4Vm.T...2.5.U.P....q.6..1t~.ZU....7.i...".b.i.~...G.A!..&..+S.(<(...y._w..q.....Q.l..1...Tz...Q...r.....g...+.o.]. ..J...$.8:.F..I.....XT..k.v....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BBkwUr[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	436
Entropy (8bit):	7.255906495097201
Encrypted:	false
SSDEEP:	6:6v/lhPahm/BBjoPHhOVDqpp05cMxyHtGUmmozY7JE3R+hRMCzRPasXQc01UaVesl:6v/7MHQg25b8Ht3VEMNQ2w5
MD5:	01B5E74F991A886215461BF0057008C7
SHA1:	6A7347C3559814722D7AA4D491A0D754E157FCC5
SHA-256:	DB8A0C0A44AEE824F689A942D99802F95D7950758CB0739C7F179624A592CD51
SHA-512:	17820A7C90B35B0E45D0A07F5445D8C97BFD3098FD9E0F0283CD6CFC1DB2B33C651924D2F04EF398C147CEB8D7DEA3F591DBC19F9039279407C4E4231AC5F5 7
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....fIDATx.}..M.@.....0...Aa.....#0..."..0....a....<....<....y..qS.....m..k..%.'|.....`....Z.`x...X.....Np..x.....a%(..ab.....=.....j.[.. ..0}.>.O..R~..<@y....nV..:.q.....G.P.e.....?s....i^l.P..5.0....?...&.A.K..|+...X.h)....5K...Zx...[....G...0N<.~PC.@.X.O2..N..x...:?..7.xH.&.....C3..8....Q.*.>...W..~..].U..U>L/... .Le&.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\cfdbd9[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	740
Entropy (8bit):	7.552939906140702
Encrypted:	false
SSDEEP:	12:6v/70MpfkExg1J0T5F1NRlYx1TEdLh8vJ542irJQ5nnXZkCaOj0cMgL17jXGW:HMuXk5RwTTEovn0AXZMitL9aW
MD5:	FE5E6684967766FF6A8AC57500502910
SHA1:	3F660AA0433C4DBB33C2C13872AA5A95BC6D377B
SHA-256:	3B6770482AF6DA488BD797AD2682C8D204ED536D0D173EE7BB6CE80D479A2EA7
SHA-512:	AF9F1BABF872CBF76FC8C6B497E70F07DF1677BB17A92F54DC837BC2158423B5BF1480FF20553927ECA2E3F57D5E23341E88573A1823F3774BFF8871746FFA51
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....U....sBIT....|.d.....pHYs.....~.....tEXtSoftware.Adobe Fireworks CS6.....tEXtCreation Time.07/21/16.~y....<IDATH..;k.Q....;.;..&..#...4..2... ..V,...X..~.{..|.Cj.....B$.%.nb....c1...w.YV....=g.....!..&.$.mI...I.$M.F3.}W,e.%..x,,..c..0.*V....W.=0.uv.X...C....3`....s.....c.....2]E0.....M...^i...[..]5.&...g.z5]H....gf....I... .u....:uy.8"....5...0.....z.....o.t...G..".....3.H....Y....3..G....v..T....a.&K.....,T.\.[..E.....?.....D.....M..9...ek..kP.A.`2.....k...D.}.\...V%.\..vIM..3.t....8.S.P.....9.....yI.<...9... ..R.e.!`..-@.....+.a..*x..0.....Y.m.1..N.I...V.'..,.V..a.3.U....,.1c.-.J<..q.m-1...d.A..d.`.4.k..i.....SL.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\checksync[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\checksync[2].htm	
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	21700
Entropy (8bit):	5.305011411091235
Encrypted:	false
SSDEEP:	384:VZAGcVXlblcqnzleZSweg2f5ng+7naMHF3OZOfQWwY4RXrqt:L86qhbS2RpF3OsfQWwY4RXrqt
MD5:	712460EA00FAF46836F259ADE169F255
SHA1:	7AB2E69D9931844A3F62BA22C5F195B8F27A5819
SHA-256:	5F493C20992ED790ECF1DA80F72F49F967C964AC4C0DF5085FF4A567937D90B7
SHA-512:	37749766A17F501635940085A519530A94561B95D4CF29BAD9514F3164EF80B01AB9A3B748F9FC099E6EA03E963FCB00D4F06C3D88377AD12902C68AA9C2316C
Malicious:	false
Reputation:	unknown
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":80,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"bs":{"name":"bs","cookie":"data-bs","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0},"ttd":{"name":"ttd","cookie":"data-ttd","isBl":1,"g":1,"cocs":0}},"ussyncmap":[],"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\checksync[3].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	21700
Entropy (8bit):	5.305011411091235
Encrypted:	false
SSDEEP:	384:VZAGcVXlblcqnzleZSweg2f5ng+7naMHF3OZOfQWwY4RXrqt:L86qhbS2RpF3OsfQWwY4RXrqt
MD5:	712460EA00FAF46836F259ADE169F255
SHA1:	7AB2E69D9931844A3F62BA22C5F195B8F27A5819
SHA-256:	5F493C20992ED790ECF1DA80F72F49F967C964AC4C0DF5085FF4A567937D90B7
SHA-512:	37749766A17F501635940085A519530A94561B95D4CF29BAD9514F3164EF80B01AB9A3B748F9FC099E6EA03E963FCB00D4F06C3D88377AD12902C68AA9C2316C
Malicious:	false
Reputation:	unknown
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":80,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"bs":{"name":"bs","cookie":"data-bs","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0},"ttd":{"name":"ttd","cookie":"data-ttd","isBl":1,"g":1,"cocs":0}},"ussyncmap":[],"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\e151e5[2].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.122191481864228
Encrypted:	false
SSDEEP:	3:CUTxls/1h/:7lU/
MD5:	F8614595FBA50D96389708A4135776E4
SHA1:	D456164972B508172CEE9D1CC06D1EA35CA15C21
SHA-256:	7122DE322879A654121EA250AEAC94BD9993F914909F786C98988ADBD0A25D5D
SHA-512:	299A7712B27C726C681E42A8246F8116205133DBE15D549F8419049DF3FCFDAB143E9A29212A2615F73E31A1EF34D1F6CE0EC093ECEAD037083FA40A075819D2
Malicious:	false
Reputation:	unknown
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\fefc2984-60ee-407b-a704-0db527f30f53[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 300x300, frames 3
Category:	dropped
Size (bytes):	68315
Entropy (8bit):	7.9756456950150305
Encrypted:	false
SSDEEP:	1536:Mf2o1r4LXC+2YgZCQ7t3vOvuIl80nlOf+9w32cilcTqvMSoCXf9zM:MBr4zC+2O6VeJlNnlOGY2c2ghSZK
MD5:	9825025914DDDB50A9ABF954276E9631

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\fefc2984-60ee-407b-a704-0db527f30f53[1].jpg	
SHA1:	BBDA4E7E92A5FDA3504216B63441C94EB7F7F9AE
SHA-256:	447ECC4AE7E9B16037B19681709BA178848FB2971B511DBDE5B3A44D9A34B79D
SHA-512:	09A19D543DB620226B064E977A15A221078BE3C896C9E1D43C356784626B654DAC158915B6523698BC2AD45FCB86FF832D2E50BC6CEBCCB99311688D12DF35E
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....C.....C.....,.,.."..... .....A.....!..1.."..2A #Qa.Bq.$3R....C.%4br..S.....A.....!1.A."Q.2aq.....#BR....3b..$r..%4CD.....?...^.),...|..N.hl...$.....k.3...\G.k.QYA...../.}b..V...CV&.E3.S.!. {.kEI.....=.F..h..Fp...WX..8.....h..}b..MW.....Q....qKW....i.....+..$k..s..#.T1.M..n...'d.r.^<..Y.....U.2YJw....hl.....FF..%z.+...2L4.....M.....R..w..o.Xp.\.V..jlZ...:..[2F....jBG.F. .Y.idg..D...#..~..]...;.?.Cx...ZR.....D#e.u.e?..^.M.....F>.O5....P.<.....R"r)*.?....^mW....3^.O..".....B).. ..!+..w..#..}J.c...7a..B$..Q|..F..A.....>~=.-.l...:X2....2%"..SM TO .B..v...)d.....4.H..ln....U.....X.j...t...\...lbk....?..C.W.....].+@.U....[...<..c..Q...8H.Z+.....A....#...V..Z...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\nrrV52473[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	90596
Entropy (8bit):	5.421672617333306
Encrypted:	false
SSDEEP:	1536:uEuukXGs7RiUGZFVgRdillDx5Q3YzuZp9ojuvby3TdXPH6viqQDkjs2i:atiX0di3M8ulMfHgjg
MD5:	F65442DA5F1A08238578462C9D90FFF0
SHA1:	3B959556D6B4FEABC4D8FD3C8610616B0104F3AD
SHA-256:	518299B805889F3C6AEDA8EA7D79C661A3C7C5E32C15DDA51D2EA5835C8554A8
SHA-512:	B567278E529F31934DA1947F56E8B884E023A565E9FD55CE09178A74C2DEE832F11B857FDE5DFEBF5F53442D8A5A62B339FB309BE48898062E5B1DFBFCA419C
Malicious:	false
Reputation:	unknown
Preview:	var _mNRequire,_mNDefine;!function(){"use strict";var c={},u={};function a(e){return"function"==typeof e}_mNRequire=function e(t,r){var n,i,o=[];for(i in t)t.hasOwnProper ty(i)&&("object"!=typeof(n=t[i])&&void 0!==n?(void 0!==c[n]||(c[n]=e(u[n].deps,u[n].callback)),o.push(c[n])):o.push(n));return a(r)?r.apply(this,o):o},_mNDefine=function(e,t,r) {if(a(t)&&(r=t,t=[]),void 0===(n=e)||""===n||null===n||(n=t,"[object Array]"!==Object.prototype.toString.call(n))||!a(r))return!1;var n;u[e]={deps:t,callback:r}}}();_mNDefine ("modulefactory",[],function(){"use strict";var r={},e={},o={},i={},t={},n={},a={},d={},c={},l={};function g(r){var e=!0,o={};try{o=_mNRequire([r])[0]}catch(r){e=!1}return o.isReso lved=function(){return e},o}return r=g("conversionpixelcontroller"),e=g("browserhinter"),o=g("kwdClickTargetModifier"),i=g("hover"),t=g("mraidDelayedLogging"),n =g("macrokeywords"),a=g("tcfdatamanager"),d=g("l3-reporting-observer-adapter"),c=g("editorial_blocking"),l=g("debuglogs"),{conversionPixelCo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\otBannerSdk[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	374818
Entropy (8bit):	5.338137698375348
Encrypted:	false
SSDEEP:	3072:axBt4stoUf3MiPnDxOFvxYyTcwY+OiHeNUQW2SzDZTpl1L:NUfbPnDxOFvxYyY+Oi+yQW2CDZTn1L
MD5:	2E5F92E8C8983AA13AA99F443965BB7D
SHA1:	D80209C734F458ABA811737C49E0A1EAF75F9BCA
SHA-256:	11D9CC951D602A168BD260809B0FA200D645409B6250BD8E8996882EBE3F5A9D
SHA-512:	A699BEC040B1089286F9F258343E012EC2466877CC3C9D3DFEF9D00591C88F976B44D9795E243C7804B62FDC431267E1117C2D42D4B73B7E879AEFB1256C644E
Malicious:	false
Reputation:	unknown
Preview:	/** .. * onetrust-banner-sdk.. * v6.13.0.. * by OneTrust LLC.. * Copyright 2021 .. */..!function(){"use strict";var o=function(e,t){return(o=Object.setPrototypeOf||{__proto__:[]}in stanceof Array&&function(e,t){e.__proto__=t}||function(e,t){for(var o in t)t.hasOwnProperty(o)&&(e[o]=t[o])})(e,t)};var r=function(){return(r=Object.assign||function(e){for(var t,o=1,n=arguments.length;o<n;o++)for(var r in t=arguments[o])Object.prototype.hasOwnProperty.call(t,r)&&(e[r]=t[r]);return e}).apply(this,arguments)};function a(s,i,l,a){ret urn new(l=l||Promise)(function(e,t){function o(e){try{r(a.next(e))}catch(e){t(e)}}function n(e){try{r(a.throw(e))}catch(e){t(e)}}function r(t){t.done?e(t.value):new l(function(e){e (t.value)}).then(o,n)}r((a=a.apply(s,i|\[])).next())})}function d(o,n){var r,s,i,e,l={label:0,sent:function(){if(1&i[0])throw i[1];return i[1]},trys:[],ops:[]};return e={next:t(0),throw:t(1) ,return:t(2)},"function"==typeof Symbol&&(e[Symbol.iterator]=function(){return this}),e;function t(t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\17-361657-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1238
Entropy (8bit):	5.066474690445609
Encrypted:	false
SSDEEP:	24:HWwAaHZRRIYfOeXPmMHUKq6GGiqIlQCQ6cQflgKioUInJaqzrQJ:HWwAabuYfO8HTq0xB6XfyNoUiJaD
MD5:	7ADA9104CCDE3FDFB92233C8D389C582
SHA1:	4E5BA29703A7329EC3B63192DE30451272348E0D
SHA-256:	F2945E416DDD2A188D0E64D44332F349B56C49AC13036B0B4FC946A2EBF87D99
SHA-512:	2967FBCE4E1C6A69058FDE4C3DC2E269557F7FAD71146F3CCD6FC9085A439B7D067D5D1F8BD2C7EC9124B7E760FBC7F25F30DF21F9B3F61D1443EC3C214E3F F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\17-361657-68ddb2ab[1].js	
Malicious:	false
Reputation:	unknown
Preview:	define("meOffice",["jquery","jqBehavior","mediator","refreshModules","headData","webStorage","window"],function(n,t,i,r,u,f,e){function o(t,o){function v(n){var r=e.local Storage,i,t,u;if(r&&r.deferLoadedItems)for(i=r.deferLoadedItems.split(","),t=0,u=i.length;t<u;t++)if(i[t]&&i[t].indexOf(n)!==-1){f.removeItem(i[t]);break}}function a(){var i=t.find ("section li time");i.each(function(){var t=new Date(n(this).attr("datetime"));t&&n(this).html(t.toLocaleString())})}function p(){c=t.find("[data-module-id]").eq(0);c.length&&(h=c. data("moduleId"),h&&(l="moduleRefreshed-"+h,i.sub(l,a)))}function y(){i.unsub(o.eventName,y);r(s).done(function(){a();p()})}var s,c,h,l;return u.signedin||(t.hasClass("of fice")?v("meOffice"):t.hasClass("onenote")&&v("meOneNote")),{setup:function(){s=t.find("[data-module-deferred-hover], [data-module-deferred]").not("[data-sso-de pendent]");s.length&&s.data("module-deferred-hover")&&s.html("<p class='meloading'><\/p>");i.sub(o.eventName,y)},teardown:function(){h&&i.un

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\2d-0e97d4-185735b[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	251398
Entropy (8bit):	5.2940351809352855
Encrypted:	false
SSDEEP:	3072:FaPMULTAHEkm8OUdvUvJZkrqq7pjD4tQH:Fa0ULTAHLOUdvwZkrqq7pjD4tQH
MD5:	24D71CC2CC17F9E0F7167D724347DBA4
SHA1:	4188B4EE11CFDC8EA05E7DA7F475F6A464951E27
SHA-256:	4EF29E187222C5E2960E1E265C87AA7DA7268408C3383CC3274D97127F389B22
SHA-512:	43CF44624EF76F5B83DE10A2FB1C27608A290BC21BF023A1BFDB77B2EBB4964805C8683F82815045668A3ECCF2F16A4D7948C1C5AC526AC71760F50C82AADE2 B
Malicious:	false
Reputation:	unknown
Preview:	/*! Error: C:/a/_work/1/s/Statics/WebCore.Statics/Css/Modules/ExternalContentModule/Uplevel/Base/externalContentModule.scss(207,3): run-time error CSS1062: Expe cted semicolon or closing curly-brace, found '@include.multiLineTruncation' */....@charset "UTF-8";div.adcontainer iframe[width='1']{display:none}span.nativead{font-weigh t:600;font-size:1.1rem;line-height:1.364}div:not(.ip) span.nativead{color:#333}.todaymodule .smalla span.nativead,.todaystripe .smalla span.nativead{bottom:2rem ;display:block;position:absolute}.todaymodule .smalla a.nativead .title,.todaystripe .smalla a.nativead .title{max-height:4.7rem}.todaymodule .smalla a.nativead .caption, .todaystripe .smalla a.nativead .caption{padding:0;position:relative;margin-left:11.2rem}.todaymodule .mediuma span.nativead,.todaystripe .mediuma span.nativead {bottom:1.3rem}.ip a.nativead span:not(.title):not(.adslabel),.mip a.nativead span:not(.title):not(.adslabel){display:block;vertical-align:top;color:#a0a0a0}.ip a.nativead .captio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\52-478955-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	396806
Entropy (8bit):	5.324117607788422
Encrypted:	false
SSDEEP:	6144:YXP9M/wSg/jgyYZw44K7hmnidDWPqIjHSjaICr1BgxO0DkV4FcjtIuNK:CW/VcnidDWPqIjHdB16tbcjut
MD5:	A01F715D94D664BFFD387E3EB04AE159
SHA1:	5E80CAB36F0E0CBE231C8E85D5D0E591FDF0107D
SHA-256:	7959B1DA9C26C84C6D6FC46614D53C1BC095676AC21CEA64B58166D6E5198458
SHA-512:	8F77BB672BADCC0D36C92C3D9A35B01CFEDC5684BAB0F7626D8256EB068F2C0556903E4548EDB06E1965968CDBEC1632FBAA67C6ED1046EB204DF1DD01859 BC
Malicious:	false
Reputation:	unknown
Preview:	var awa,behaviorKey,Perf,globalLeft,Gemini,Telemetry,utils,data,MSANTracker,deferredCanary,g_ashsC,g_hsSetup,canary;window._perfMarker&&window._perfMa rker("TimeToJsBundleExecutionStart");define("jqBehavior",["jquery","viewport"],function(n){return function(t,i,r){function u(n){var t=n.length;return t>1?function(){for(var i=0;i<t;i++)n[i]()}:t?n[0]:f}function f(){}if(typeof t!="function")throw"Behavior constructor must be a function";if(i&&typeof i!="object")throw"Defaults must be an object or nu ll";if(r&&typeof r!="object")throw"Exclude must be an object or null";return r=r||{},function(f,e,o){function c(n){n&&(typeof n.setup=="function"&&l.push(n.setup),typeof n.teardown=="function"&&a.push(n.teardown),typeof n.update=="function"&&v.push(n.update))}var h;if(o&&typeof o!="object")throw"Options must be an object or null";var s=n.extend(!0,{},i,o),l=[],a=[],v=[],y=!0;if(r.query){if(typeof f!="string")throw"Selector must be a string";c(t(f,s))}else h=n(f,e),r.each?c(t(h,s)):(y=h.length>0,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\AAOQ0Q5[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 300x250, frames 3
Category:	dropped
Size (bytes):	11863
Entropy (8bit):	7.927704017701038
Encrypted:	false
SSDEEP:	192:QtQSJRe7t3x7fdIts70jIPbxN6q4nWnNpn2v0uCvmfpW8UpYrkjdfSe4gQ4DBpit:+pJItx7fdIGo8L6q4nWp2UuAArid6ef8
MD5:	7EFA3908B23DA76AD963B7D859243F2B
SHA1:	9A4605DAA61556215F925F324B40DE1CCED89604
SHA-256:	8DC8DFC03B572F99AFF783F2A5DAC3081E754BA3C155FF905B8124C6615479FC
SHA-512:	DF8B3F164C22BDC1E3F4C01DEB21EB685C48F12FC5577AC6D91746C1D4B3A7E68FF5DAC2F4681CB078E68269BA859C412F86C9C129E6FB3487700C2A0A80C7 9
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\AAOQ0Q5[1].jpg	
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....,.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..*J.....).P.L....).S.....(.....(.....(.....@..3.5.+Y.E..?.Fp~..4.).....k...h..]S.....+.).k{ov..@..;.....C@.@..A@.L....(.....(.....(.....(.....(.....(.(.h.(.....\l.....#.....L.v.,.C$....|.....mm..#"..9...9.Sj.B.(..M...@....f. ...r..L...h..j1.o.d....fmX. ... .(.....(.....J.Z.(.....(.....(.(.....@..T...:g$TM.6...1.D>....B..z.y...).K Fv.z..7....z

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\AAOUGsI[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	dropped
Size (bytes):	1931
Entropy (8bit):	7.685428596916561
Encrypted:	false
SSDEEP:	48:QfAuETAWi6K2TtNLPXaxUhAtCdLbnNucZIpu7FS88:Qf7ELize9PKx9tmXnNHIpu5D8
MD5:	AF6D6F6C1169BE5212778003B781D993
SHA1:	93A1332A7A1219652732243903629EC1A2E110F6
SHA-256:	037DA90D4B98E5A0E8F30D5BCF4CC0A74391D34F9D1575B6C5814AF7267B83E4
SHA-512:	FB46C8998D2712876545E5D722308A257A2F1E917D3031EB1DB4BE7BB8C4EC4D080195C04C3930B27966C57089FA0A5ADA107286EE220DC3AF09969D2D2C69E
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....n;..Z...?u.....Q.BO...F.(.....9..sO@..^...].....d>I..d...3.wB.B.....]..C.1.....2..<g..O5@.y.].y....]...p)]....^.h...F.!O...@.....@ 8....94.Vi.s0Q..?.c9jtS.<..(+.[..F.!....,:.QW...(.&B>.....88$.....H?....\.J.....X...0...<.....<...Q.....y.q.....p.-.C.;..1..r..n.a,._.y.inu.bf..d.*J+..8... g=..e;G...1..t\.j.....J.!<.?..c.;.r.. ..B...N}..c..q.)\..79CE.]...#..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\AAOVfsv[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 300x250, frames 3
Category:	dropped
Size (bytes):	17463
Entropy (8bit):	7.9592305311599025
Encrypted:	false
SSDEEP:	384:+FvXo7KbarNWRr8+2SnphMl1rp813FlPk22TVg3tUidykRlZTX4qvCeOV:+xXok+Nn+2SpEpulj2Mt1ykRrX48NOV
MD5:	DF68AD56D8922FF005964CD4C1D861FC
SHA1:	DA671E3C2F053062EF307A3EB47D42E5F0D87AC5
SHA-256:	EC745BB874A1C3B1E2F3402DEDC88BC9180DC1BE6BE32E5943EFEBB461C64F7F
SHA-512:	6C020322132C00DC380190E21F7E406BD74729F8EDE55BDFA9F53B4C9775C887FEEB7EDC23363377D91927F8BFBEDED9E01E274156059BF1998DBD122A2CA99
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....,.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....,.8..p..y.-.S..HfT.....H.T.....(.Y[....@9...S....~..".^.t.i.o9[r....$.W..M....imo$.&i-.p.~...q...:..qum".....@.4.c..h..p...z~.}m... .0*..p...}j.%.....l.lt%.....w.@...pH.....Yn^GR.F..b)...G4....a.'.g...9._._..m.0W.>..!..0]\6...<c~y8..2..p....y%h..p-#.2@Os.(..5;q.....U.5.X.....I....p.H..i..Mh'..el#.IrS..v<..*....d. ,...V..Z@HJ...2..@<.....%..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\AAOVowX[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	48199
Entropy (8bit):	7.964167583002753
Encrypted:	false
SSDEEP:	768:IkCZ4x0Pc+XYVq1tbsUuBE5OjSXUEZdXwaT501f7WGQ+zErm/jxWTQE3N+:I9ixOc+IVcb96+OWXUEZdAatqfiYqm/1
MD5:	7B13FBEE25411309F9F418591F36D433
SHA1:	2DE876D76D64C189F270D1916E5F7723ED2FB646
SHA-256:	4D796BFA0409FDA6A10106AEA52BC969E72932641A78F9AF515AEE355971A066
SHA-512:	2A8360702CBDFCF6DDD94A1A3E187D87532F946F6B90FCE373BEF7E2C30D1018DAFD77D6D6694A393532003A92D2B40D724875C6A7C0B20CE0BD72C300B1E43
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\AAOVowX[1].jpg	
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.t... `..1..#.u....j.q..&.....)[...].c.#<.I.4?.....ri..... " .-...>.^.Nfv.,....3.j.!.....cU=M&..a .....U.X.{t mc...&..J..n.w$.)=...W..[U.u..* \..Z).....P..JB.:..sE...$.`.{6)....^...!.Nz.YKsX.VO0o....). ...0..1.RcC\.LT.F.D..{.qLD.ZL...*.m.....W...`.....0$...7..c..L...Eut....3.(.+O...4,...dr..h..6.!.+..d.Z,.".R..\..T#...WK..r. 6n.pj.....+..Cg=.RZ..v..A..jv.{i..*...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\AAOVte1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	33347
Entropy (8bit):	7.876176789934141
Encrypted:	false
SSDEEP:	768:IZvYWrngj/RpJHG2TCxKAZfVOHXGQKNvxOF1mUSi+:IZv3rnsRvs1ZkHY9xOF1F5+
MD5:	EEE3FF54DC48917DF698BFC7478993FF
SHA1:	0D5DB57829C9E046D029F09CC09811D65850EE83
SHA-256:	530A142B9BD003A2EF84BF01897F311F6AD36E57193B4AE304748D6973E84D33
SHA-512:	DB40F00EDE9FFB2227756895F33759C384D9EB234BB18D8B8192AA0555BE314769B4E7DE768F6EB90B7F896D6EA19C0AAD952722A85057BEFFCA3E9B89FCCB3 3
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..H]U..$v.SD.v6.u.RB.bX....3..T.q...Z.R....8.*.I.-.__.|.of.%.J.1CV..vzO..j.4..U...p...If..Z...'.Jo?....&.2.Q....W6...P|..@.."....u..$ .....vTu.G-.....?...|/.P...}s._\.r.x.%\`.7...M...Q.1.-..G...[.....Q`....H.....o.....@....:....$.....f.0...V-b.85..5.....i.....K.S..27.....fO.(...Y.....t.:}(.;...G....4..m.>....O..(....^.. ..%Yc..C....c.@.:MWQ.m{..{..#.fe..,v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\BB14EN7h[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	13764
Entropy (8bit):	7.273450351118404
Encrypted:	false
SSDEEP:	384:IfOm4cIa37nstlEM15mv7OAkrIh4McOD07+8n0GoJdxFhEh8:I2m4pa37stlTgqAjS0GoJd3yK
MD5:	DA6531188AED539AF6EAA0F89912AACF
SHA1:	602244816EA22CBE39BBD4DB386519908745D45C
SHA-256:	C719BE5FFC45680FE2A18CDB129E60A48A27A6666231636378918B4344F149F7
SHA-512:	DF03FA1CB6ED0D1FFAC5FB5F2BB6523D373AC4A67CEE1AAF07E0DA61E3F19E7AF43673B6BEFE7192648AC2531EF64F6B4F93F941BF014ED2791FA6F46720C7 DB
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....5.D..gJ.ks@..(...@.....l..pE..iT...t&..V.M..h....4.m.-.!...:.....*...a...CQ...c....Fj....F(...5 ..<.....J..E.0."..].6...B.K... .....k.t.A'p..KJ..*A....(.....(.....(.....(.....(.....(.....(.....(.....(.....(.....K1.....:...0.....I...M.9..n..d.Z.e.Q..HfE....I^...h.h.t....(.9:.2....z...@.....:...3..w.@.P4Ac1.a.@...A#.P1... ..4..@.@. (.h.h.(....0....Y..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\BB1cEP3G[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	1088
Entropy (8bit):	7.81915680849984
Encrypted:	false
SSDEEP:	24:FCGPRm4XxHvhNBb6W3bc763IU6+peaq90IUkiRPfoc:/pXBvkW3bc7k1FqWIUkSfB
MD5:	24F1589A12D948B741C2E5A0C4F19C2A
SHA1:	DC9BB00C5D063F25216CDABB77F5F01EA9F88325
SHA-256:	619910A3140A45391D7D3CB50EC4B48F0B0C8A76DC029576127648C4BD4B128C
SHA-512:	5D7A17B05E1FD1BC02823EC2719D30BC27A9FA03BCFFE30F3419990E440845842F18797C9071C037417776641AB2CDB86F1F6CD790D70481B3F863451D3249EE
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\BB1cEP3G[1].png	
Preview:	.PNG.....IHDR.....U....pHYs.....+.....IDATx...]..U.....d..6YwW(.UV\.v.>.>..`.K}X).i..Tj...C..RD. ..AEXP.....]).vQ../$.%.l2.....dH&.YiOr93.....~..u.S...5.....J. &..;.JN..z....2..;q.4..I .....c!....2;*J.....I(.....?.m+.....V...g3.0.....C..GB.$..M.....jl.M..~6?...../a%...;....E.by.J..1.$...".&.DX..W..jh.....=...aK...[.#....]. ....:Q....X.....uk.6 .0...e7..RZ..@@H..k.....#.....[..C.-.AbC.fK.(a.<.^p.j`...._>{<...`.....%.L...q.G...).2oc{....vQ...N5..%m-ky19..F.S....&..../..F.....y.(.8.1..>?Zr.....Q.`.e.\|0.&m.E....=[aN..r.+... .2B/f8.v..n...N..=.....i.^....s&..Hr.z.....M.....:.....EF.....0.. .N.x.....N.pO.#2...df=...Fa..B#2yU....O.;.g....b.}ct.&.7x*..t.Y..yg....]..){.,.v.F.e.ZF.z..Ur+..^..].#.]....~..}..{g.W0? ....&....6n....p\.=.]..X...F.]...\s5OK.3Wb.#.M/fT...:^.M}...:t.....!..g.....0t.h..8..4cB....px.....1.!...}=...Qb$W.*..."....V....!.y.....<H

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\BB1ftEY0[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	497
Entropy (8bit):	7.316910976448212
Encrypted:	false
SSDEEP:	12:6v/7YEtTvpTjO7q/cW7Xt3T4kL+JxK0ew3Jw61:rEtTRTj/XtjNSJMkJw61
MD5:	7FBE5C45678D25895F86E36149E83534
SHA1:	173D85747B8724B1C78ABB8223542C2D741F77A9
SHA-256:	9E32BF7E8805F283D02E5976C2894072AC37687E3C7090552529C9F8EF4DB7C6
SHA-512:	E9DE94C6F18C3E013AB0FF1D3FF318F4111BAF2F4B6645F1E90E5433689B9AE522AE3A899975EAA0AECA14A7D042F6DF1A265BA8BC4B7F73847B585E3C12C26 2
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx....N.A..=.....bC...RR..`'.....v.{:.^..... ."1.2....P..p.....nA.....o.....1...N4.9.>..8....g.,...|."...nL.#..vQ.....C.D8.D.0*.DR).... kl..|.....m...T..=.tz...E..y..... ..S.i>O.x.l4p~w.....{...U..S....w<.;.A3...R*..F..S1..j..%...1.|.3.mG..... f+.,x....5.e..]lz..*.).1W..Y(..L`.J...xx.y{.*.\. ...L..D..\N.....g..W...}w:.....@].j ._$.LB.U..w'..S.....R...:^..[\.^@....j..t...?..<.....M..r..h....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\BB7hg4[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	470
Entropy (8bit):	7.360134959630715
Encrypted:	false
SSDEEP:	12:6v/7TIG/Kupc9GcBphmZgPEHfMwY7yWQtygnntrNKKBBN:3KKEc9GcXhmZwM9LtyGJKKBBN
MD5:	B6EA6C62BAEBF35525A53599C0D6F151
SHA1:	4FFEFB243AAEC286D37B855FBE33C790795B1896
SHA-256:	71CC7A3782241824ACDC2D6759E455399957E3C7C9433A1712C3947E2890A4D4
SHA-512:	0E4E87A66CF6E01750BC34D2D1EC5B63494A7F5C4B831935DD00E1D825CDB1CFD3C3E90F29D1D4076E7F24C9C287E59BE23627D748DB05FB433A3A535F1154
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..QKN.A....(..1a.....p...o..T...../.....$..n\...V.C .b2.....qe'.T.1.1h8./.....$:Y6...w}_>...P.o$.n....X,<...R..y....$p.P..c.\.7.. f...H.vm...I.....b..K..3.....R..u...Z'.?..$.B...l.r....H.1....MN).c.K1H.....t...9.....d.$.....:..8..8@t._...1.".@C....i&Z.'...A1...!....R....}.w.E4.|_..N.....b...(.^.vH.....j.....s...h. ..9.p!... ..gT.=B.|..,=v.....G..c.5.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\BBX2afX[2].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	879
Entropy (8bit):	7.684764008510229
Encrypted:	false
SSDEEP:	24:nbwTOG/D9S9kmVgvOc0WL9P9juX7wlA3lrvfFRNa:bwTOk5S96vBB1jGwO3lzfxa
MD5:	4AAAEC9CA6F651BE6C54B005E92EA928
SHA1:	7296EC91AC01A8C127CD5B032A26BBC0B64E1451
SHA-256:	90396DF05C94DD44E772B064FF77BC1E27B5025AB9C21CE748A717380D4620DD
SHA-512:	09E0DE84657F2E520645C6BE20452C1779F6B492F67F88ABC7AB062D563C060AE51FC1E99579184C274AC3805214B6061AEC1730F72A6445AEBDB7E9F255755F
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....U....pHYs.....+.....!IDATx...K.Q..wfv.u.....*.,l"...)...z.....>.OVObQ.....d?|.....F.Ql$....qf.s....">y`.....{~.6.Z.`.D[&.cV`..-8i...J.S.N..xf.6@.v.(E..S. ....&...T...?.X)${.....s.l."V..r...PJ*!..p.4b}.=2...[.....:.....LW3...A.eB.;...2...~...s_z.x|..o....+..x....KW.G2..9.....<.\....gv...n..1..0...1}....Ht_A.x...D..5.H.....W..$_\G.e;./.1R+v....j.6v... .....z.k.....&..(....,F.u8^..v...d-.j?.w..;..O.<9$..A..f.k.Kq9..N..p.rP2K.0.).X.4..Uh[..8..h....O..V.%.f.....G..U.m.6$.....X...../.=....f:.....\|c(,.....I.\..<./..6...!...z(.....# "S..f .Q.N=.0VQ._..\|....>@....P.7T.$./)s....Wy..8..xV.....D....8r."b@...:.E.E....._(....4w....Ir..e-5..zjg...e?./...|X..."!..'*/.....OI..J"I.MP....#...G.Vc..E..m.....wS.&.K<...K*q..\...A..$.K .....,...[..D...8.?..)..3....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\de-ch[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\de-ch[1].htm	
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	429699
Entropy (8bit):	5.442578112008925
Encrypted:	false
SSDEEP:	3072:4fbmJUBxx+uAkJ8i/NycyIRX8QVYrxtudnE6jHkPLgmTceV45IfA+JxLf:4fiIOujXkdTLEmTXysJh
MD5:	73DABCDA8565E0429191B5B49912BD8F
SHA1:	041DD102D79B0AD9D631F2CBE69BA7509E323E5B
SHA-256:	8F3DD1B47A07A73215190854166FD542CC0C6A0565E4A99420989AFCF211920E
SHA-512:	951104F05376DFC67A07916C7020B722C4C867B9027185401E39EFC33303BE82EF06EF3A0BAF6A5E5B4E7E5C7642DE788D2BDCE05190F0817CFC9651BD0B928
Malicious:	false
Reputation:	unknown
Preview:	<!DOCTYPE html><html prefix="og: http://ogp.me/ns# fb: http://ogp.me/ns/fb#" lang="de-CH" class="hiperf" dir="ltr" >.. <head data-info="v:20210928_247027 32;a:051f0e5a-20c1-4b57-a340-74251f23c8b9;cn:10;az:{did:951b20c4cd6d42d29795c846b4755d88, rid: 10, sn: neurope-prod-hp, dt: 2021-09-28T23:04:40.1223713Z, bt: 2021-09-28T00:15:28.3963579Z};ddpi:1;dpio:;dpi:1;dg:tmx.pc.ms.ie10plus;th:start;PageName:startPage;m:de-ch;cb:;l:de-ch;mu:de-ch;ud:{cid:,vk:homepage,n:,l:de-ch,ck :};xd:BBqgbZW;ovc:f;al:;fxd:f;xdpub:2021-08-11 10:21:32Z;xdmap:2021-09-28 23:12:06Z;axd:;f:msnallexpusers,muidflt9cf,muidflt11cf,muidflt13cf,muidflt14cf,muidflt 19cf,audexedge3cf,pnehz2cf,gallery5cf,onetrustpoplive,1s-bing-news,vebudumu04302020,bbh20200521msncf,weather4cf,prg-1sw-h5ctp6,prg-1sw-h5ucrd-com,prg-1sw-sixh6top,prg-whp-shabst25,prg-adspeek,1s-br30min,btrecrow1,1s-winauthservice,prg-castapi1,prg-1sw-setcogt,prg-wpo-hpolypc,weather7cf,prg-1sw-halfwea,prg-bra ndupwhp,prg-1sw-wosa-t,prg-1sw-wosauth,prg-osanon3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\otFlat[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	12282
Entropy (8bit):	5.246783630735545
Encrypted:	false
SSDEEP:	192:SZ1Nfybp4gtNs5FYdGDaRBYw6Q3OEB+q5OdjM/w4lYLp5bMqEb5PenUpoQuQJYQj:WNejbnNP85csXfn/BoH6iAHyPtJJAk
MD5:	A7049025D23AEC458F406F190D31D68C
SHA1:	450BC57E9C44FB45AD7DC826EB523E85B9E05944
SHA-256:	101077328E77440ADEE7E27FC9A0A78DEB3EA880426DFFFDA70237CE413388A5
SHA-512:	EFBEFAF0D02828F7DBD070317BFDF442CAE516011D596319AE0AF90FC4C4BD9FF945AB6E6E0FF9C737D54E05855414386492D95ABFC610E7DE2E99725CB1A9 6
Malicious:	false
Reputation:	unknown
Preview:	.. {.. "name": "otFlat",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtYmFubmVyLXNkayIgY2xhc3M9Im90RmxhdCIgcm9sZT0iZGlhbG9nIiBhcml hLWRlc2NyaWJlZGJ5PSJvbmV0cnVzdC1wb2xpY3ktdGV4dCI+PGRpdiBjbGFzcz0ib3Qtc2RrLWNvbnRhaW5lciI+PGRpdiBjbGFzcz0ib3Qtc2RrLXJvdyI+PGRpdiBpZ D0ib25ldHJ1c3QtZ3JvdXAtY29udGFpbmVyIiBjbGFzcz0ib3Qtc2RrLWVpZ2h0IG90LXNkay1jb2x1bW5zIj48PC9kaXY+PGR pdiBpZD0ib25ldHJ1c3QtcG9saWN5Ij48aDMgaWQ9Im9uZXRydXN0LXBvbGljeS0xRsZSI+VGl0bGU8L2gzPjxwIGlkPSJvbmV0cnVzdC1wb2xpY3ktdGV4dCI+dGl0b GU8L3A+PGRpdiBjbGFzcz0ib3QtZHBkLWNvbnRhaW5lciI+PGgzIGNsYXNzPSJvdC1kcGQtdGl0bGUiPldlIGNvbGxlY3QgZGF0YSBpbiBvcmRlciB0byBwcm92aWRlOjwv vaDM+PGRpdiBjbGFzcz0ib3QtZHBkLWNvbnRlbnQiPjxwIGNsYXNzPSJvdC1kcGQtZGVzYyI+ZGVzY3JpcHRpb248L3A+PC9kaXY+PC9kaXY+PC9kaXY+PC9 kaXY+PGRpdiBpZD0ib25ldHJ1c3QtYnV0dG9uLWdyb3VwLXBhcmVudCIgY2xhc3M9Im90LXNkay10aHJlZSBvdC1zZGstY29sdW1ucyI+PGRpdiBpZD0ib25ldHJ1c3QtY nV0dG9uLWdyb3Vwlj48YnV0dG9uIGlkPSJvbmV0cnVzdC1wYy1idG4taGFuZGxlciI+Y2h

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\otPcCenter[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	47714
Entropy (8bit):	5.565687858735718
Encrypted:	false
SSDEEP:	768:4zg/3JXE9ZSqN76pW1lzZzic18+JHoQthI:4zCBceUdZzic18+5xI
MD5:	8EC5B25A65A667DB4AC3872793B7ACD2
SHA1:	6B67117F21B0EF4B08FE81EF482B888396BBB805
SHA-256:	F6744A2452B9B3C019786704163C9E6B3C04F3677A7251751AEFD4E6A556B988
SHA-512:	1EDC5702B55E20F5257B23BCFCC5728C4FD0DEB194D4AADA577EE0A6254F3A99B6D1AEDAAAC7064841BDE5EE8164578CC98F63B188C1A284E81594BCC0F20 68
Malicious:	false
Reputation:	unknown
Preview:	.. {.. "name": "otPcCenter",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtcGMtc2RrIiBjbGFzcz0ib3RQY0NlbnRlciBvdC1oaWRlIG90LWZhZGUta W4iIGFyaWEtbW9kYWw9InRydWUiIHJvbGU9ImRpYWxvZyIgYXJpYS1sYWJlbGxlZGJ5PSJvdC1wYy10aXRsZSI+PCEtLSBDbG9zZSBCdXR0b24gLS0+PGRpd iBjbGFzcz0ib3QtcGMtaGVhZGVyIj48IS0tIExvZ28gVGFnIC0tPjxkaXYgY2xhc3M9Im90LXBjLWxvZ28iIHJvbGU9ImltZyIgYXJpYS1sYWJlbD0iQ29tcGFueSBMb2d vIj48L2Rpdj48YnV0dG9uIGlkPSJjbG9zZS1wYy1idG4taGFuZGxlciIgY2xhc3M9Im90LWNsb3NlLWljb24iIGFyaWEtbGFiZWw9IkNsb3NlIj48L2J1dHRvbj48L2Rpdj4xsYmFyIj48aDMgaWQ9Im90LXBjLXRpdGxlIj5Zb3VyIFByaXZhY3k8L 2gzPjxkaXYgaWQ9Im90LXBjLWRlc2MiPjwvZGl2PjxidXR0b24gaWQ9ImFjY2VwdC1yZWNvbW1lbmRlZC1idG4taGFuZGxlciI+QWxsb3cgYWxsPC9idXR0b24+PHNlY3R pb24gY2xhc3M9Im90LXNkay1yb3cgb3QtY2F0LWdycCI+PGgzIGlkPSJvdC1jYXRlZ29yeS10aXRsZSI+TWFuYWdlIENvb2tpZSBQcmVmZXJlbmNlczwvaDM+PGRpdiBjb GFzc0ib3QtcGxpLWhkciI+PHNwYW4gY2xhc3M9Im90LWxpLXRpdGxlIj5Db25zZW50PC9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\otSDKStub[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16853
Entropy (8bit):	5.393243893610489
Encrypted:	false
SSDEEP:	192:2Qp/7PwSgaXIXbci91iEBadZH8fKR9OcmIQMYOYS7uzdwnBZv7iIHXF2FsT:FRr14FLMdZH8f4wOjawnTvuIHVh
MD5:	82566994A83436F3BDD00843109068A7
SHA1:	6D28B53651DA278FAE9CFBCEE1B93506A4BCD4A4
SHA-256:	450CFBC8F3F760485FBF12B16C2E4E1E9617F5A22354337968DD661D11FFAD1D
SHA-512:	1513DCF79F9CD8318109BDFD8BE1AEA4D2AEB4B9C869DAFF135173CC1C4C552C4C50C494088B0CA04B6FB6C208AA323BFE89E9B9DED57083F0E8954970EF822
Malicious:	false
Reputation:	unknown
Preview:	var OneTrustStub=function(e){"use strict";var t,o,n,i,a,r,s,l,c,p,u,d,m,h,f,g,b,A,C,v,y,I,S,w,T,L,R,B,D,G,E,P,_,U,k,O,F,V,x,N,H,M,j,K=new function(){this.optanonCookieName="OptanonConsent",this.optanonHtmlGroupData=[],this.optanonHostData=[],this.genVendorsData=[],this.IABCookieValue="",this.oneTrustIABCookieName="eupubconsent",this.oneTrustIsIABCrossConsentEnableParam="isIABGlobal",this.isStubReady=!0,this.geolocationCookiesParam="geolocation",this.EUCOUNTRIES=["BE","BG","CZ","DK","DE","EE","IE","GR","ES","FR","IT","CY","LV","LT","LU","HU","MT","NL","AT","PL","PT","RO","SI","SK","FI","SE","GB","HR","LI","NO","IS"],this.stubFileName="otSDKStub",this.DATAFILEATTRIBUTE="data-domain-script",this.bannerScriptName="otBannerSdk.js",this.mobileOnlineURL=[],this.isMigratedURL=!1,this.migratedCCTID="[[OldCCTID]]",this.migratedDomainId="[[NewDomainId]]",this.userLocation={country:"",state:""}};(o=t=t||{})[o.Unknown=0]="Unknown",o[o.BannerCloseButton=1]="BannerCloseButton",o[o.ConfirmChoiceButton

C:\Users\user\AppData\Local\N8qUdj\Magnify.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	809472
Entropy (8bit):	6.649005640850081
Encrypted:	false
SSDEEP:	6144:g4yELxB+4i7juGW9ku9gi9m5SBo3BZHgnlWXL1ogREJwkz5gzNOx8XA08bAhMWUy:1tLvDNhg0Pnomt8XOykpyk
MD5:	F97BE20B3744572366666607EE4BA7F7F
SHA1:	378D5ADAB450032CBD086A419C07DF8278FF4F32
SHA-256:	72A31AEB7655343C7112085DFD49A2D5F1A6F1191D8F91A96BC446DE932724EA
SHA-512:	62C8875A9ECB710CCE5CACBEFF3615A9771913F0C7A7CD42FFFE1D00F9B9E26D01139501635F1578F1B63E03682B52312E776A7191F291B86960B1D7464AB216
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._T..>:D.>:D.>:D.F.D.>:D.Z>E.>:D.Z9E.>:D.Z?E.>:D.Z;E.>:D.>;D.8:D.Z3E.>:D.Z.D.>:D.Z.D.>:D.Z8E.>:DRich.>:D.....PE..d...U....."..... .....@.....`.....  .....8.....0..@G.....-.....8...P"..T.....  ...(...  .....H...(.....text...*.....  ..`.rdata..t(.....*.....@..@.data.....@....pdata...-.....@..@.rsrc...@G...0...H.....@..@.reloc..8.....T.....@..B.....

C:\Users\user\AppData\Local\N8qUdj\OLEACC.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2097152
Entropy (8bit):	3.5956755819217476
Encrypted:	false
SSDEEP:	12288:oVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:9fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	F64C766BCDFF1514609281F6ACF86D6A
SHA1:	2FE64A164EC497996CDC09745C803325DD7E625B
SHA-256:	8283A0D7096251F44DF92649B97D84358857A20096082F6EC9B582605A531EAD
SHA-512:	F03627DDE81E76F1136DE300EBCD9A35607E2A33A04ED0DBBD94BC409DCD5A6FC8737EEA953BD49FE32E1CC1D922E55E733AA814AEAD43CA8AA375F33BB3DA38
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|...|...|....K.#}...'...}.....{}....X.#}....f..|....g..}..*...a|.....}....N..}..*...E}..[.I.E|...'..U}....N.+}..[.K.P|..[.K./}...I.h}..u.Y.k|.....|..W"...|..b.L.t|...|...}.....N|..2%...|..Rich.|.....PE..d.&..DN^....."..... .....p.....@..... .....@lx}..b.....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\Temp\~DF843FC6B68D0B177F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Temp\~DF843FC6B68D0B177F.TMP	
Size (bytes):	196628
Entropy (8bit):	3.1365124225892194
Encrypted:	false
SSDEEP:	3072:lZ/2Bfcdmu5kgTzGtvZ/2Bfc+mu5kgTzGt:ME
MD5:	E8E0BA88E0C207F6FD42DDA7021E2DBE
SHA1:	0FFF593C36A8B68A2121F7664CECC0716EF5BE81
SHA-256:	BCA57AC19B322F79B4BC48CAD20D08B55E87190818BA4FF7C60F5634B4A9ECFB
SHA-512:	204A5E8A93758ED956E28AD5D6BD2F7D5D581E00877AB7CA3FE7B9C3A237F7F5576F6D58A2680968C2EF527106207BAF09A326ADEE0AAD589AB93CD2ADBF37F0
Malicious:	false
Reputation:	unknown
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF9E1A0A52EBCE6F97.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12965
Entropy (8bit):	0.41733495032567686
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loh9loB9lWVMz+F+ZGdq:kBqoIKUNoOq
MD5:	240A815D3A999BAA3BBEDCCCE838AC32
SHA1:	16F15CAF9CB2788C5D6A816535493B7F03B3AC1D
SHA-256:	C73E01EA17378D5BD6CF158D3B6C7A83C1A744084F1480A40D94C0FF71EDBC9E
SHA-512:	D121FE4746820C6222C78017425B792D96A95B0C29F5E1F8BBD8532FD4A4D8F72FC633EC58C125F25C6F1FA410645E59875F1CADEC6D1AD78A35549366550A98
Malicious:	false
Reputation:	unknown
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\gKsll\PresentationHost.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	259072
Entropy (8bit):	6.5074250085194665
Encrypted:	false
SSDEEP:	6144:8kfs4/kfxzJTbHfyH5KNXwy3Odjp19k5KNXf:fs4ixzJTbHmKVwy3OdLaKV
MD5:	E3053C73EA240F4C2F7971B3905A91CF
SHA1:	1848AD66BD55E5484616FB85E80BA58BE1D5BA4B
SHA-256:	0BACCDB2B5ACB7B3C2E9085655457532964CAFFF1AE250016CE1A80E839B820C
SHA-512:	167BCC3E2552286F7D985A65674DA2FF0D0AA6A7F0C4C3B43193943B606E0133C06EEB33656EFBB8B827AC9221FB1BA00A49ADCC2489BD4F38DF62A015806DE3
Malicious:	false
Reputation:	unknown
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.........3/.]\|.]\|.]\|...\|.]\|...\|..]\|..^}.]\|..Y}.]\|.\\|..]\|..\}.]\|..T}..]\|..X}.]\|..\|.]\|.._}.]\|Rich.]\|. ....PE..d..../............"..........&.................@.............................0............`.......... ......................................p..,........j......l............ ..,....d..T...........................#......... ......$...............................text...o........................... ..`.rdata..............................@..@.data................r.............@....pdata..l............t.............@..@.rsrc....j.......l...~........... ...@..@.reloc..,.... ....@..B.. ....

C:\Users\user\AppData\Local\gKsll\VERSION.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2097152
Entropy (8bit):	3.5942311342114386
Encrypted:	false
SSDEEP:	12288:YVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:NfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	A389ABF74E0D18E6A236BB497BB9AEF4
SHA1:	CD380200F838247EA79BD56ED7E0900F05D04754

C:\Users\user\AppData\Local\gKsll\VERSION.dll	
SHA-256:	1EB74EDBF6B692396BF218B446A6F93D2FEFEFB336DC2D3563E2FFDE0840D023
SHA-512:	9CFA3081ADBFF3335002C27168F6C195164359D2460AF0A3D4CBA544D6F88F223F28835712BDD7096A11D03D669F9BC8765C8F1DFE07CBC096B2DCBB122D2A6
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.& ..DN^....." .....p.....@..... .....@lx}..b.....+....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

Static File Info

General

File type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Entropy (8bit):	3.608861528309905
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 86.43% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	vZ1WZMpxTY.dll
File size:	2093056
MD5:	c10ee36fe08388fce375f320660bc91c
SHA1:	6477666e70f87ff53040e98f324660a5167eb4f4
SHA256:	d8bc15335ca8daa9a8a67fc2261636775be4dde332d8a0944017676926236da3
SHA512:	9fa8df612db5d4da32d2a5531e752b668a503fc49c45aecb9a2df4f95964671712f410a74a76cd677aba005bd4f119070893fc6d6fbaff66d9617cbf45764587
SSDEEP:	12288:xVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ17:AfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|...|...|....K.#}...'...}.....{}....X.#}....f..|....g..}..*...a|.....}....N..}..*...E}..[.I.E|...'..U}....N.+}..[.K.P|.

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x140041070
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x140000000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x5E4E44CC [Thu Feb 20 08:35:24 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0

General

Import Hash:	6668be91e2c948b183827f040944057f

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x40796	0x41000	False	0.776085486779	data	7.73364605679	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x42000	0x64fd0	0x65000	False	0.702390160891	data	7.86574512659	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa7000	0x178b8	0x18000	False	0.0694580078125	data	3.31515306295	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0xbf000	0x12c	0x1000	False	0.06005859375	PEX Binary Archive	0.581723022719	IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xc0000	0x880	0x1000	False	0.139892578125	data	1.23838501563	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc1000	0x2324	0x3000	False	0.0498046875	data	4.65321444248	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.qkm	0xc4000	0x74a	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.cvjb	0xc5000	0x1e66	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tlmkv	0xc7000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wucsxe	0xc8000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fltwtj	0x10e000	0x1267	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.sfplio	0x110000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rpg	0x111000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bewzc	0x157000	0x1124	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vksvaw	0x159000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wmhg	0x15a000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nfuu	0x15c000	0x451c2	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.cqcgue	0x1a2000	0x1f7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.edydzn	0x1a3000	0x21b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fgoks	0x1a4000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fdf	0x1a5000	0x1e66	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.vlyui	0x1a7000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.onihaq	0x1a8000	0x322	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.dnoygv	0x1a9000	0x21b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ejopd	0x1aa000	0xd33	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ech	0x1ab000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.euhsb	0x1ac000	0xd57	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tym	0x1ad000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nhtbzp	0x1ae000	0x1f87	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ujern	0x1b0000	0x128f	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.cuhy	0x1b2000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qqrro	0x1b4000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.mcqw	0x1b5000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xvhbg	0x1b6000	0x5a7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pjphmh	0x1b7000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.lgwynn	0x1b8000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.dyw	0x1fe000	0xbde	0x1000	False	0.396240234375	data	4.69322421882	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 29, 2021 01:13:22.043632030 CEST	192.168.2.6	8.8.8.8	0x5947	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Sep 29, 2021 01:13:24.300904036 CEST	192.168.2.6	8.8.8.8	0x5945	Standard query (0)	web.vortex .data.msn.com	A (IP address)	IN (0x0001)
Sep 29, 2021 01:13:24.645220041 CEST	192.168.2.6	8.8.8.8	0xf72a	Standard query (0)	geolocatio n.onetrust.com	A (IP address)	IN (0x0001)
Sep 29, 2021 01:13:24.676326036 CEST	192.168.2.6	8.8.8.8	0x9e49	Standard query (0)	contextual .media.net	A (IP address)	IN (0x0001)
Sep 29, 2021 01:13:24.905611992 CEST	192.168.2.6	8.8.8.8	0x4755	Standard query (0)	btloader.com	A (IP address)	IN (0x0001)
Sep 29, 2021 01:13:26.447161913 CEST	192.168.2.6	8.8.8.8	0xd5c3	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Sep 29, 2021 01:13:26.793878078 CEST	192.168.2.6	8.8.8.8	0x2ecb	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Sep 29, 2021 01:13:27.963073015 CEST	192.168.2.6	8.8.8.8	0x3af6	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
Sep 29, 2021 01:13:28.457707882 CEST	192.168.2.6	8.8.8.8	0xaee9	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)
Sep 29, 2021 01:13:29.557205915 CEST	192.168.2.6	8.8.8.8	0x8184	Standard query (0)	s.yimg.com	A (IP address)	IN (0x0001)
Sep 29, 2021 01:13:29.576272011 CEST	192.168.2.6	8.8.8.8	0xf66b	Standard query (0)	crcdn01.adnxs-simple.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 29, 2021 01:13:22.057722092 CEST	8.8.8.8	192.168.2.6	0x5947	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Sep 29, 2021 01:13:24.332098961 CEST	8.8.8.8	192.168.2.6	0x5945	No error (0)	web.vortex .data.msn.com	web.vortex.data.microsoft .com		CNAME (Canonical name)	IN (0x0001)
Sep 29, 2021 01:13:24.667232990 CEST	8.8.8.8	192.168.2.6	0xf72a	No error (0)	geolocatio n.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
Sep 29, 2021 01:13:24.667232990 CEST	8.8.8.8	192.168.2.6	0xf72a	No error (0)	geolocatio n.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Sep 29, 2021 01:13:24.691529989 CEST	8.8.8.8	192.168.2.6	0x9e49	No error (0)	contextual .media.net		23.54.113.52	A (IP address)	IN (0x0001)
Sep 29, 2021 01:13:24.928081989 CEST	8.8.8.8	192.168.2.6	0x4755	No error (0)	btloader.com		104.26.6.139	A (IP address)	IN (0x0001)
Sep 29, 2021 01:13:24.928081989 CEST	8.8.8.8	192.168.2.6	0x4755	No error (0)	btloader.com		104.26.7.139	A (IP address)	IN (0x0001)
Sep 29, 2021 01:13:24.928081989 CEST	8.8.8.8	192.168.2.6	0x4755	No error (0)	btloader.com		172.67.70.134	A (IP address)	IN (0x0001)
Sep 29, 2021 01:13:26.462439060 CEST	8.8.8.8	192.168.2.6	0xd5c3	No error (0)	lg3.media.net		23.54.113.52	A (IP address)	IN (0x0001)
Sep 29, 2021 01:13:26.808794975 CEST	8.8.8.8	192.168.2.6	0x2ecb	No error (0)	hblg.media.net		23.54.113.52	A (IP address)	IN (0x0001)
Sep 29, 2021 01:13:27.999878883 CEST	8.8.8.8	192.168.2.6	0x3af6	No error (0)	cvision.me dia.net	cvision.media.net.edgeke y.net		CNAME (Canonical name)	IN (0x0001)
Sep 29, 2021 01:13:28.471856117 CEST	8.8.8.8	192.168.2.6	0xaee9	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Sep 29, 2021 01:13:28.471856117 CEST	8.8.8.8	192.168.2.6	0xaee9	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Sep 29, 2021 01:13:29.571511030 CEST	8.8.8.8	192.168.2.6	0x8184	No error (0)	s.yimg.com	edge.gycpi.b.yahoodns.n et		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 29, 2021 01:13:29.571511030 CEST	8.8.8.8	192.168.2.6	0x8184	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.22	A (IP address)	IN (0x0001)
Sep 29, 2021 01:13:29.571511030 CEST	8.8.8.8	192.168.2.6	0x8184	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.23	A (IP address)	IN (0x0001)
Sep 29, 2021 01:13:29.596576929 CEST	8.8.8.8	192.168.2.6	0xf66b	No error (0)	crcdn01.adnxs-simple.com	crcdn01.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Sep 29, 2021 01:13:29.596576929 CEST	8.8.8.8	192.168.2.6	0xf66b	No error (0)	crcdn01.adnxs.com	secure-adnxs.edgekey.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- https:
  - geolocation.onetrust.com
  - btloader.com
  - s.yimg.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49774	104.20.185.68	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 23:13:24 UTC	0	OUT	GET /cookieconsentpub/v1/geo/location HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: geolocation.onetrust.com Connection: Keep-Alive
2021-09-28 23:13:24 UTC	0	IN	HTTP/1.1 200 OK Date: Tue, 28 Sep 2021 23:13:24 GMT Content-Type: text/javascript Content-Length: 164 Connection: close Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Server: cloudflare CF-RAY: 6960a981aae601db-ZRH
2021-09-28 23:13:24 UTC	0	IN	Data Raw: 6a 73 6f 6e 46 65 65 64 28 7b 22 63 6f 75 6e 74 72 79 22 3a 22 43 48 22 2c 22 73 74 61 74 65 22 3a 22 22 2c 22 73 74 61 74 65 4e 61 6d 65 22 3a 22 22 2c 22 7a 69 70 63 6f 64 65 22 3a 22 22 2c 22 74 69 6d 65 7a 6f 6e 65 22 3a 22 45 75 72 6f 70 65 2f 5a 75 72 69 63 68 22 2c 22 6c 61 74 69 74 75 64 65 22 3a 22 34 37 2e 31 34 34 39 30 22 2c 22 6c 6f 6e 67 69 74 75 64 65 22 3a 22 38 2e 31 35 35 31 30 22 2c 22 63 69 74 79 22 3a 22 22 2c 22 63 6f 6e 74 69 6e 65 6e 74 22 3a 22 45 55 22 7d 29 3b Data Ascii: jsonFeed({"country":"CH","state":"","stateName":"","zipcode":"","timezone":"Europe/Zurich","latitude":"47.14490","longitude":"8.15510","city":"","continent":"EU"});

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49786	104.26.6.139	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 23:13:25 UTC	0	OUT	GET /tag?o=6208086025961472&upapi=true HTTP/1.1 Accept: application/javascript, */*;q=0.8 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: btloader.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-09-28 23:13:25 UTC	1	IN	HTTP/1.1 200 OK Date: Tue, 28 Sep 2021 23:13:25 GMT Content-Type: application/javascript Content-Length: 10308 Connection: close Access-Control-Allow-Origin: * Cache-Control: public, max-age=1800, must-revalidate Etag: "d8733c72977f7f00ebdfe201a7976112" Vary: Origin Via: 1.1 google CF-Cache-Status: HIT Age: 1917 Accept-Ranges: bytes Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=9Ku3ATEEc0stA%2BG0KjTm7jTsDuSkLwIlYgPuSFl6KukxN5M85k%2F6H6KvLjozahdDK5uoh2If8ERdlf0BJplpxq218QYm9jXs9xOsnjRoYX3f33Be0GH1EGSuLxq96w%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6960a9838da13757-MXP
2021-09-28 23:13:25 UTC	1	IN	Data Raw: 21 66 75 6e 63 74 69 6f 6e 28 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 66 75 6e 63 74 69 6f 6e 20 72 28 65 2c 69 2c 63 2c 6c 29 7b 72 65 74 75 72 6e 20 6e 65 77 28 63 3d 63 7c 7c 50 72 6f 6d 69 73 65 29 28 66 75 6e 63 74 69 6f 6e 28 6e 2c 74 29 7b 66 75 6e 63 74 69 6f 6e 20 6f 28 65 29 7b 74 72 79 7b 72 28 6c 2e 6e 65 78 74 28 65 29 29 7d 63 61 74 63 68 28 65 29 7b 74 28 65 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 61 28 65 29 7b 74 72 79 7b 72 28 6c 2e 74 68 72 6f 77 28 65 29 29 7d 63 61 74 63 68 28 65 29 7b 74 28 65 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 72 28 65 29 7b 76 61 72 20 74 3b 65 2e 64 6f 6e 65 3f 6e 28 65 2e 76 61 6c 75 65 29 3a 28 28 74 3d 65 2e 76 61 6c 75 65 29 69 6e 73 74 61 6e 63 65 6f 66 20 63 3f 74 3a 6e 65 77 20 63 28 66 75 6e 63 74 69 6f Data Ascii: !function(){"use strict";function r(e,i,c,l){return new(c=c||Promise)(function(n,t){function o(e){try{r(l.next(e))}catch(e){t(e)}}function a(e){try{r(l.throw(e))}catch(e){t(e)}}function r(e){var t;e.done?n(e.value):((t=e.value)instanceof c?t:new c(functio
2021-09-28 23:13:25 UTC	2	IN	Data Raw: 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 74 29 7b 69 66 28 61 29 74 68 72 6f 77 20 6e 65 77 20 54 79 70 65 45 72 72 6f 72 28 22 47 65 6e 65 72 61 74 6f 72 20 69 73 20 61 6c 72 65 61 64 79 20 65 78 65 63 75 74 69 6e 67 2e 22 29 3b 66 6f 72 28 3b 63 3b 29 74 72 79 7b 69 66 28 61 3d 31 2c 72 26 26 28 69 3d 32 26 74 5b 30 5d 3f 72 2e 72 65 74 75 72 6e 3a 74 5b 30 5d 3f 72 2e 74 68 72 6f 77 7c 7c 28 28 69 3d 72 2e 72 65 74 75 72 6e 29 26 26 69 2e 63 61 6c 6c 28 72 29 2c 30 29 3a 72 2e 6e 65 78 74 29 26 26 21 28 69 3d 69 2e 63 61 6c 6c 28 72 2c 74 5b 31 5d 29 29 2e 64 6f 6e 65 29 72 65 74 75 72 6e 20 69 3b 73 77 69 74 63 68 28 72 3d 30 2c 69 26 26 28 74 3d 5b 32 26 74 5b 30 5d 2c 69 2e 76 61 6c 75 Data Ascii: return function(e){return function(t){if(a)throw new TypeError("Generator is already executing.");for(;c;)try{if(a=1,r&&(i=2&t[0]?r.return:t[0]?r.throw||((i=r.return)&&i.call(r),0):r.next)&&!(i=i.call(r,t[1])).done)return i;switch(r=0,i&&(t=[2&t[0],i.valu
2021-09-28 23:13:25 UTC	3	IN	Data Raw: 69 6e 64 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 29 2e 61 70 70 65 6e 64 43 68 69 6c 64 28 65 29 7d 29 7d 76 61 72 20 75 2c 61 2c 64 2c 62 2c 6d 3b 75 3d 22 36 32 30 38 30 38 36 30 32 35 39 36 31 34 37 32 22 2c 61 3d 22 62 74 6c 6f 61 64 65 72 2e 63 6f 6d 22 2c 64 3d 22 61 70 69 2e 62 74 6c 6f 61 64 65 72 2e 63 6f 6d 22 2c 62 3d 22 32 2e 30 2e 32 2d 32 2d 67 66 64 63 39 30 35 34 22 2c 6d 3d 22 22 3b 76 61 72 20 6f 3d 7b 22 6d 73 6e 2e 63 6f 6d 22 3a 7b 22 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 22 3a 74 72 75 65 2c 22 6d 6f 62 69 6c 65 5f 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 22 3a 66 61 6c 73 65 2c 22 77 65 62 73 69 74 65 5f 69 64 22 3a 22 35 36 37 31 37 33 37 33 38 38 36 39 35 35 35 32 22 7d 7d 2c 77 Data Ascii: indow.document.documentElement).appendChild(e)})}var u,a,d,b,m;u="6208086025961472",a="btloader.com",d="api.btloader.com",b="2.0.2-2-gfdc9054",m="";var o={"msn.com":{"content_enabled":true,"mobile_content_enabled":false,"website_id":"5671737388695552"}},w
2021-09-28 23:13:25 UTC	5	IN	Data Raw: 4f 66 28 6e 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 29 29 26 26 28 74 3d 21 30 2c 70 2e 77 65 62 73 69 74 65 49 44 3d 6f 5b 6e 5d 2e 77 65 62 73 69 74 65 5f 69 64 2c 70 2e 63 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 6f 5b 6e 5d 2e 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 2c 70 2e 6d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 6f 5b 6e 5d 2e 6d 6f 62 69 6c 65 5f 63 6f 6e 74 65 6e 74 5f 65 6e 61 62 6c 65 64 29 3b 74 7c 7c 28 28 6e 65 77 20 49 6d 61 67 65 29 2e 73 72 63 3d 22 2f 2f 22 2b 64 2b 22 2f 6c 3f 65 76 65 6e 74 3d 75 6e 6b 6e 6f 77 6e 44 6f 6d 61 69 6e 26 6f 72 67 3d 22 2b 75 2b 22 26 64 6f 6d 61 69 6e 3d 22 2b 65 29 7d 28 29 2c 77 69 6e 64 6f 77 2e 5f 5f 62 74 5f 74 61 67 5f 64 3d 7b 6f 72 67 49 44 3a 75 2c 64 6f 6d 61 69 6e Data Ascii: Of(n.toLowerCase()))&&(t=!0,p.websiteID=o[n].website_id,p.contentEnabled=o[n].content_enabled,p.mobileContentEnabled=o[n].mobile_content_enabled);t||((new Image).src="//"+d+"/l?event=unknownDomain&org="+u+"&domain="+e)}(),window.__bt_tag_d={orgID:u,domain
2021-09-28 23:13:25 UTC	6	IN	Data Raw: 29 7b 76 61 72 20 74 3d 63 2e 62 75 6e 64 6c 65 73 5b 65 5d 3b 69 5b 65 5d 3d 7b 6d 69 6e 3a 4d 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 2b 6f 2b 30 29 29 2c 6d 61 78 3a 4d 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 2b 6f 2b 30 2b 74 29 29 7d 2c 6f 2b 3d 74 7d 29 7d 76 61 72 20 6c 3d 74 5b 30 5d 3b 69 66 28 6e 75 6c 6c 21 3d 6c 26 26 6c 2e 62 75 6e 64 6c 65 73 29 7b 76 61 72 20 73 3d 6f 2c 75 3d 31 2d 6f 3b 4f 62 6a 65 63 74 2e 6b 65 79 73 28 6c 2e 62 75 6e 64 6c 65 73 29 2e 73 6f 72 74 28 29 2e 66 6f 72 45 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 6c 2e 62 75 6e 64 6c 65 73 5b 65 5d 3b 69 5b 65 5d 3d 7b 6d 69 6e 3a 4d 61 74 68 2e 74 72 75 6e 63 28 31 30 30 2a 28 73 2b 75 2a 61 29 29 2c 6d 61 78 3a 4d 61 74 68 2e 74 72 75 6e Data Ascii:){var t=c.bundles[e];i[e]={min:Math.trunc(100*(+o+0)),max:Math.trunc(100*(+o+0+t))},o+=t})}var l=t[0];if(null!=l&&l.bundles){var s=o,u=1-o;Object.keys(l.bundles).sort().forEach(function(e){var t=l.bundles[e];i[e]={min:Math.trunc(100*(s+u*a)),max:Math.trun
2021-09-28 23:13:25 UTC	7	IN	Data Raw: 77 2e 64 69 73 70 61 74 63 68 45 76 65 6e 74 28 6f 29 7d 63 61 74 63 68 28 65 29 7b 7d 76 61 72 20 61 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 76 65 6e 74 28 22 43 75 73 74 6f 6d 45 76 65 6e 74 22 29 3b 61 2e 69 6e 69 74 43 75 73 74 6f 6d 45 76 65 6e 74 28 74 2c 6e 2e 62 75 62 62 6c 65 73 2c 6e 2e 63 61 6e 63 65 6c 61 62 6c 65 2c 6e 2e 64 65 74 61 69 6c 29 2c 77 69 6e 64 6f 77 2e 64 69 73 70 61 74 63 68 45 76 65 6e 74 28 61 29 7d 66 3d 7b 22 35 36 37 31 37 33 37 33 38 38 36 39 35 35 35 32 22 3a 7b 22 64 69 67 65 73 74 22 3a 36 32 38 31 36 37 38 39 32 31 31 33 38 31 37 36 2c 22 62 75 6e 64 6c 65 73 22 3a 7b 22 36 32 38 31 36 37 38 39 32 31 31 33 38 31 37 36 22 3a 31 7d 7d 2c 22 67 6c 6f 62 61 6c 22 3a 7b 22 64 69 67 65 73 74 22 3a 36 32 36 30 30 Data Ascii: w.dispatchEvent(o)}catch(e){}var a=document.createEvent("CustomEvent");a.initCustomEvent(t,n.bubbles,n.cancelable,n.detail),window.dispatchEvent(a)}f={"5671737388695552":{"digest":6281678921138176,"bundles":{"6281678921138176":1}},"global":{"digest":62600

Timestamp	kBytes transferred	Direction	Data
2021-09-28 23:13:25 UTC	9	IN	Data Raw: 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 2e 69 6e 64 65 78 4f 66 28 22 62 74 5f 64 65 62 75 67 3d 74 72 75 65 22 29 7c 7c 22 74 72 75 65 22 3d 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 6c 53 74 6f 72 61 67 65 2e 67 65 74 49 74 65 6d 28 22 62 74 5f 64 65 62 75 67 22 29 29 26 26 28 70 2e 63 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 22 74 72 75 65 22 3d 3d 6c 6f 63 61 6c 53 74 6f 72 61 67 65 2e 67 65 74 49 74 65 6d 28 22 66 6f 72 63 65 43 6f 6e 74 65 6e 74 22 29 7c 7c 70 2e 63 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 2c 70 2e 6d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 45 6e 61 62 6c 65 64 3d 22 74 72 75 65 22 3d 3d 6c 6f 63 61 6c 53 74 6f 72 61 67 65 2e 67 65 74 49 74 65 6d 28 22 66 6f 72 63 65 4d 6f 62 69 6c 65 43 6f 6e 74 65 6e 74 22 29 7c 7c 70 2e 6d 6f 62 Data Ascii: dow.location.href.indexOf("bt_debug=true")||"true"==window.localStorage.getItem("bt_debug"))&&(p.contentEnabled="true"==localStorage.getItem("forceContent")||p.contentEnabled,p.mobileContentEnabled="true"==localStorage.getItem("forceMobileContent")||p.mob
2021-09-28 23:13:25 UTC	10	IN	Data Raw: 2f 29 7c 6b 6c 6f 6e 7c 6b 70 74 20 7c 6b 77 63 5c 2d 7c 6b 79 6f 28 63 7c 6b 29 7c 6c 65 28 6e 6f 7c 78 69 29 7c 6c 67 28 20 67 7c 5c 2f 28 6b 7c 6c 7c 75 29 7c 35 30 7c 35 34 7c 5c 2d 5b 61 2d 77 5d 29 7c 6c 69 62 77 7c 6c 79 6e 78 7c 6d 31 5c 2d 77 7c 6d 33 67 61 7c 6d 35 30 5c 2f 7c 6d 61 28 74 65 7c 75 69 7c 78 6f 29 7c 6d 63 28 30 31 7c 32 31 7c 63 61 29 7c 6d 5c 2d 63 72 7c 6d 65 28 72 63 7c 72 69 29 7c 6d 69 28 6f 38 7c 6f 61 7c 74 73 29 7c 6d 6d 65 66 7c 6d 6f 28 30 31 7c 30 32 7c 62 69 7c 64 65 7c 64 6f 7c 74 28 5c 2d 7c 20 7c 6f 7c 76 29 7c 7a 7a 29 7c 6d 74 28 35 30 7c 70 31 7c 76 20 29 7c 6d 77 62 70 7c 6d 79 77 61 7c 6e 31 30 5b 30 2d 32 5d 7c 6e 32 30 5b 32 2d 33 5d 7c 6e 33 30 28 30 7c 32 29 7c 6e 35 30 28 30 7c 32 7c 35 29 7c 6e 37 28 30 Data Ascii: /)|klon|kpt |kwc\-|kyo\(c|k\)|le\(no|xi\)|lg\(g|\/\(k||u\)|50|54|\-\[a\-w\]\)|libw|lynx|m1\-w|m3ga|m50\/|ma\(te|ui|xo\)|mc\(01|21|ca\)|m\-cr|me\(rc|ri\)|mi\(o8|oa|ts\)|mmef|mo\(01|02|bi|de|do|t\(\-| |o|v\)|zz\)|mt\(50|p1|v \)|mwbp|mywa|n10\[0\-2\]|n20\[2\-3\]|n30\(0|2\)|n50\(0|2|5\)|n7\(0
2021-09-28 23:13:25 UTC	11	IN	Data Raw: 74 2b 22 26 22 2b 6d 29 3b 72 65 74 75 72 6e 20 74 7d 28 6f 29 29 2c 5b 32 5d 3b 74 72 79 7b 44 28 7b 65 76 65 6e 74 4e 61 6d 65 3a 22 41 63 63 65 70 74 61 62 6c 65 41 64 73 49 6e 69 74 22 2c 70 61 79 6c 6f 61 64 3a 7b 64 65 74 61 69 6c 3a 21 31 7d 7d 29 2c 44 28 7b 65 76 65 6e 74 4e 61 6d 65 3a 22 75 70 6f 6e 69 74 49 6e 69 74 22 2c 70 61 79 6c 6f 61 64 3a 7b 64 65 74 61 69 6c 3a 21 31 7d 7d 29 7d 63 61 74 63 68 28 65 29 7b 7d 72 65 74 75 72 6e 5b 32 5d 7d 7d 29 7d 28 29 7d 63 61 74 63 68 28 65 29 7b 7d 7d 28 29 3b 0a Data Ascii: t+"&"+m);return t}(o)),[2];try{D({eventName:"AcceptableAdsInit",payload:{detail:!1}}),D({eventName:"uponitInit",payload:{detail:!1}})}catch(e){}return[2]}}}}}()}catch(e){}}();

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49816	87.248.118.22	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 23:13:29 UTC	12	OUT	GET /lo/api/res/1.2/0XpuUmHG5cpKtbzOUv9Rmg--~A/Zmk9Zml0O3c9NjIyO2g9MzY4O2FwcGlkPWdlbWluaTtxPTEwMA--/https://s.yimg.com/av/ads/1632725880101-6365.jpg HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://www.msn.com/de-ch/?ocid=iehp Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: s.yimg.com Connection: Keep-Alive
2021-09-28 23:13:29 UTC	12	IN	HTTP/1.1 200 OK Content-Length: 97182 Access-Control-Allow-Headers: X-Requested-With Access-Control-Allow-Origin: * Cache-Control: public, max-age=2592000 Content-Type: image/jpeg Edge-Cache-Tag: 451278680546267930714637994953532079223,444071775025019603777525119764716296813,ae7a14591aaf8d474cdb3f92111c923e Etag: "a843182fad3657ca8b6afa0caaf9ef5a" Last-Modified: Mon, 27 Sep 2021 13:36:04 GMT Server: ATS Status: 200 OK Timing-Allow-Origin: * X-Request-Id: 0348b2ec8a87feda93d35f19c9c3e475 Accept-Ranges: bytes Date: Mon, 27 Sep 2021 13:36:30 GMT X-Served-By: cache-wdc5565-WDC X-Cache: MISS X-Cache-Hits: 0 X-Timer: S1632749790.079551,VS0,VE393 Age: 121019 Strict-Transport-Security: max-age=15552000 Referrer-Policy: no-referrer-when-downgrade X-Frame-Options: SAMEORIGIN cld_cache: MISS cld_hits: 0 cld_id: 0348b2ec8a87feda93d35f19c9c3e475 cld_by: cache-wdc5565-WDC cld_latency: 393 Connection: close Expect-CT: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only" X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff

Timestamp	kBytes transferred	Direction	Data
2021-09-28 23:13:29 UTC	13	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 96 00 96 00 00 ff e2 02 28 49 43 43 5f 50 52 4f 46 49 4c 45 00 01 01 00 00 02 18 00 00 00 00 02 10 00 00 6d 6e 74 72 52 47 42 20 58 59 5a 20 00 00 00 00 00 00 00 00 00 00 00 00 61 63 73 70 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 01 00 00 f6 d6 00 01 00 00 00 00 d3 2d 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 00 00 00 00 00 00 00 09 64 65 73 63 00 00 00 f0 00 00 00 74 72 58 59 5a 00 00 01 64 00 00 00 14 67 58 59 5a 00 00 01 78 00 00 00 14 62 58 59 5a 00 00 01 8c 00 00 00 14 72 54 52 43 00 00 01 a0 00 00 00 28 67 54 52 43 00 00 01 a0 00 00 00 28 62 54 52 43 00 00 01 a0 00 00 00 28 77 Data Ascii: JFIF(ICC_PROFILEmntrRGB XYZ acsp-desctrXYZdgXYZxbXYZrTRC(gTRC(bTRC(w
2021-09-28 23:13:29 UTC	14	IN	Data Raw: b3 0f 70 4f d7 81 87 62 59 ae a6 e3 13 8a 91 6b 59 97 70 47 bf e7 bf 04 44 82 4a 9b d8 0e eb 88 37 3f 5b f7 04 7b 6f 6f b7 13 13 96 59 6d 60 31 20 10 08 3b b0 3b 1c 8a fa 77 b8 b1 d8 71 31 39 65 93 5a d6 c6 fe 93 f9 8b 7b 7b 6f c4 61 be 44 b5 82 ee 2f 70 2c 72 c8 2f f8 ad b7 7e dc 11 42 37 2c 4e d6 1b 10 36 c7 22 48 36 be f9 6e 0d c6 c2 d6 37 26 ea 78 9c 9b 96 38 65 75 36 1b 5c 01 88 00 0f ce e4 93 c4 8a 03 29 c8 86 08 6c 3d 5d ac b7 be 23 d9 9b 20 0b 7d 14 7d 38 d4 55 02 06 0a 48 07 b0 bd c2 ec 05 94 7b 0d af 6f ad cf bf 04 45 57 10 45 f6 c8 95 01 55 42 a9 b7 a4 05 00 58 1b 9b da f7 26 f7 3b f0 a2 d1 fc cd 7b f6 b8 51 d8 93 ed 6b f7 b7 e4 07 13 e4 f7 2d 76 2d ea 24 d8 6d e9 1d fd 23 d8 7b 71 8f 27 b6 ec 77 63 76 39 1d ed ee 77 b0 ec 07 b0 b7 04 51 6e 54 Data Ascii: pObYkYpGDJ7?[{ooYm`1 ;;wq19eZ{{oaD/p,r/~B7,N6"H6n7&x8eu6\)l=]# }}8UH{oEWEUBX&;{Qk-v-$m#{ q'wcv9wQnT
2021-09-28 23:13:29 UTC	16	IN	Data Raw: 85 19 d7 60 c7 12 c6 de e0 ce 61 58 d7 af d2 28 64 89 54 4b 86 26 66 60 21 c7 35 64 cc c8 46 02 c0 df e5 60 c0 70 26 68 54 c0 26 e9 e4 d3 2a 42 24 c6 e6 62 8e 40 8f 2b 1e a6 21 ec 41 56 c7 2d fb 82 45 1e 38 1a 58 64 90 46 66 4e af 41 98 af 51 73 4b 4b d2 17 04 9c 0d a4 c4 35 93 1f 6b f1 30 80 d4 a4 8e 23 f3 6b 0b ac 77 23 aa 20 66 8d a4 0a 32 bf 4f 31 1e 64 2d b2 28 6f ea e1 1d a9 fa b0 09 3a 5d 66 32 9a 6c 80 cc 95 45 eb 18 4d d9 93 f0 c0 12 11 7f 45 8b 90 e7 12 d9 d3 0a 98 e3 bc 7e 68 c1 23 a0 21 7a dd 01 22 2c 98 92 33 e8 f5 0a 76 22 e7 12 45 87 04 51 62 a7 5a b9 25 02 3f 35 24 11 ac 96 62 65 e8 ab bf 4b 35 ca cb 19 63 21 4f 4f a8 8e f7 e1 22 8e 95 2a 2a e4 85 63 13 c8 d0 9a c2 84 19 59 92 10 20 69 01 2c 46 11 0b 46 02 ad c1 3f 99 b1 5a 98 d5 48 a0 c5 Data Ascii: `aX(dTK&f`!5dF`p&hT&*B$b@+!AV-E8XdFfNAQsKK5k0#kw# f2O1d-(o:]f2lEME~h#!z",3v"EQbZ%?5$beK5 c!OO"**cY i,FF?ZH
2021-09-28 23:13:29 UTC	17	IN	Data Raw: 99 63 25 0d 30 08 8b 70 2e 50 c6 42 8b 58 86 3b 5c e5 ea 6f a3 c3 1d 21 d5 bc b9 8d ea e9 92 8f cc 45 d4 41 58 e4 8a 5e 92 a8 71 98 37 08 c9 e8 40 3d 52 06 24 70 44 f5 50 50 4b 2d 03 d6 ac 5d 78 aa 7a 94 25 d8 23 8a 90 ad 6e 98 c9 73 6c 6f 70 72 36 f6 f6 e1 aa 21 a0 6a da 39 a6 11 1a e8 84 de 50 34 85 65 c0 ad a6 e9 26 40 3f a1 89 6b 83 60 3d f6 e2 da c9 34 f4 92 90 56 88 7a ef 50 45 0f 5a 3c 9c 55 60 5a d0 9e 9b e1 27 4b 21 96 4a 3b 8b dc 03 c5 13 b5 08 ae a4 59 fa 02 b5 c4 de 4c bc 61 a7 c5 55 0c e2 16 28 d8 5d 4a e6 4b 2d c6 df 5e 08 94 c7 43 e7 d6 7b c4 75 21 4a ca 9f 88 bd 7f 2c 58 b3 37 4c ba 96 40 c4 9c b1 36 07 f7 71 22 86 80 6a 13 cd 18 8b f5 8b c3 0a 54 d9 d8 cc d0 a0 0b 1f 52 3b e2 15 b1 50 18 0b 93 b1 3c 58 65 a1 f3 e9 11 58 4e a3 e5 59 d7 6b Data Ascii: c%0p.PBX;\o!EAX^q7@=R$pDPPK-]xz%#nslopr6!j9P4e&@?k`=4VzPEZ<U`Z'K!J;YLaU(]JK-^C{u!J,X7L@6 q"jTR;P<XeXNYk
2021-09-28 23:13:29 UTC	18	IN	Data Raw: 4a e5 65 f9 80 37 bf 15 38 0a f2 05 c5 5f ff 00 76 d6 07 22 bb 17 b6 f9 63 8f cd be 36 f6 b7 04 4a cc a3 25 02 d7 62 dd c9 20 9b 5e f7 ed f5 0a 36 1f bf 8a 88 b0 16 16 07 2b 6f 70 77 24 db df b9 b9 fa 13 6f 6e 02 a0 f5 61 8d f3 39 e3 ff 00 ed 36 cb 2b 0f 9f b6 57 f5 76 bf b7 11 30 55 16 c4 a9 be 21 31 20 6e 72 22 db 0b b5 c1 f7 c8 30 60 08 e0 89 c0 01 02 6d 60 0a 85 c8 de c7 60 0b 5e f7 1b ef 7f a6 fb 70 81 41 56 04 5c 00 3b 12 0e c7 eb ed db 7f f7 e0 59 70 d9 93 a5 85 ae 18 74 fa 56 26 ff 00 4e 95 81 dc 7a 78 2f d3 65 df 10 9b 5f 20 30 37 23 1b f7 1d f7 17 db 6b f0 45 2f 7c 89 17 07 73 6b 83 f5 b0 b6 e2 e7 db df b7 7e 11 ae db b6 c2 f7 d8 91 6f a5 fe de dc 19 0a 0f 9c ad b2 50 32 22 cc f7 f4 d8 9d b2 2d ba 92 46 fb de fc 03 8e d7 0b b1 f4 df 11 63 63 db Data Ascii: Je78_v"c6J%b ^6+opw$ona96+Wv0U!1 nr"0`m``^pAV\;YptV&Nzx/e_ 07#kE/|sk~oP2"-Fcc
2021-09-28 23:13:29 UTC	19	IN	Data Raw: 34 aa 83 49 76 61 d1 9e 83 96 46 b1 5c 95 64 0c d1 04 44 62 42 96 b9 3c 76 b3 92 3f e1 f5 f1 6b 57 68 53 9e 3e 25 7c 36 d0 63 66 56 98 72 bf 29 f3 1f 30 c8 21 0c c9 2b d1 54 ea b3 e8 34 95 72 47 22 88 dc 33 24 28 49 bb d8 80 d1 1d 78 b5 31 a4 be ae 33 8c 70 0e ec 9f 81 6f 07 90 71 87 10 7d e5 7c f7 a9 3d 33 fd 17 34 9b a5 8a e3 d6 2d 1f 3c d1 67 74 56 69 aa 75 1c 98 63 83 5e 07 dc 74 d5 f1 bd ed 70 23 63 24 73 83 c0 69 0d 2e 0b 44 e6 6f f8 89 bf 4b 0f 32 75 0c 9f 16 53 e8 71 3b 6d 1f 2b 78 59 e1 4e 90 23 41 dd 63 9a 0e 51 6a 81 70 06 fd 5c cf cd 96 47 2e 38 6b 53 fd 38 df a5 1b 53 32 49 2f c7 27 8d 91 bb b5 88 d3 f5 0d 2f 49 58 c5 ef f8 11 69 fa 54 11 45 ec 07 4d 52 db f7 02 dc 7a 0f a6 7f c3 f5 e0 cd 05 25 2a 73 1f c4 ef 89 ba c5 54 75 8b 2e a7 53 a3 72 Data Ascii: 4IvaF\dDbB<v?kWhS>%|6cfVr)0!+T4rG"3$(Ix13poq}\|=34-<gtViuc^tp#c$si.DoK2uSq;m+xYN#AcQjp\G. 8kS8S2I/'/IXiTEMRz%*sTu.Sr
2021-09-28 23:13:29 UTC	21	IN	Data Raw: b2 0c 01 b9 52 42 10 55 ac 76 e1 c4 97 95 a2 e9 ca 31 45 71 29 5f c1 62 e5 86 0a f7 b9 91 42 64 cb 88 01 4a 9b 9e c0 2c b9 49 2a 18 a5 4e 91 40 24 74 02 39 7a 8b 91 30 be 47 25 4b 63 21 21 71 61 6d c0 b8 22 58 a7 82 53 38 45 6f c2 99 a2 97 28 99 01 90 2a 16 37 60 03 ad 8a d9 d7 20 d6 d8 ed c4 82 a2 39 a3 69 63 0e 11 64 95 0e 71 bc 6d 94 32 32 48 42 b0 0c 46 6a d6 60 08 7f 99 6f 71 73 1c c2 43 28 30 cd 13 47 29 8e d2 c6 13 ab 60 84 c9 11 b9 0f 1f a8 00 f7 17 2a 76 d8 5e 41 3f 5a 36 90 43 34 58 bc b1 e1 2a 04 73 d2 76 4c 95 43 30 28 f8 e5 19 b8 c9 48 24 29 b8 04 49 1d 4c 32 52 79 95 57 10 74 9e 4c 5a 17 57 c1 01 c9 7a 05 44 97 f4 90 13 0c 9b d8 1b 8b ac 95 74 e9 44 6a dd 64 34 c2 15 94 a2 c0 ef 20 89 82 90 3c b8 5c ff 00 6d 46 18 dc 1b ed b1 e2 c8 ea 3a 94 Data Ascii: RBUv1Eq)_bBdJ,I*N@$t9z0G%Kc!!qam"XS8Eo(*7` 9icdqm22HBFj`oqsC(0G)`*v^A?Z6C4X*svLC0(H$)IL2 RyWtLZWzDtDjd4 <\mF:
2021-09-28 23:13:29 UTC	22	IN	Data Raw: 1b c6 18 94 3b 90 3b f0 eb 57 7a d9 e8 45 3d 4a 88 29 e2 a8 f3 92 46 12 91 cc 8e cb d1 86 62 c1 9a 55 c6 f2 26 0a 00 22 cc 4e dc 2c 35 86 6a 8a a8 3c ad 54 1e 58 c2 3a d2 c7 85 3d 47 55 33 bd 2b e4 5a 41 18 f4 ca 4a 8c 5a e0 64 37 24 46 09 e9 e4 a9 ab 86 34 61 35 34 91 a5 4b 18 59 15 99 93 34 c6 42 a0 4d 64 d8 95 24 2d c0 be fc 3c 73 19 24 9d 4c 52 c7 d1 90 46 b2 48 a0 24 e0 a8 6e a4 26 e5 99 01 f4 12 42 d9 94 8f 6e 1c 4b 33 cb 2a 3c 25 62 8c 46 62 9f 35 2b 3b 38 6e a2 84 1e b5 68 71 40 c5 cf ab 31 88 18 9e 2c 80 bc cf 3a c9 01 89 22 75 58 a4 2e ad d7 05 01 67 08 b6 31 05 6f 4e 2c 32 b8 26 e7 82 2a ef 78 c4 86 37 00 ae 58 3a 63 20 04 12 09 8d ac ea 5a db 02 05 ee 3e a3 8a ba c9 d2 33 74 e4 b0 8f aa 53 a4 7a b6 c7 2c 7a 5f 3f 50 76 29 6c b2 ba da fb 71 97 Data Ascii: ;;WzE=J)FbU&"N,5j<TX:=GU3+ZAJZd7$F4a54KY4BMd$-<s$LRFH$n&BnK3*<%bFb5+;8nhq@1,:" uX.g1oN,2&*x7X:c Z>3tSz,z_?Pv)lq
2021-09-28 23:13:29 UTC	23	IN	Data Raw: ed da fc 46 20 00 48 27 d4 00 b0 be e7 60 7f df e9 c0 2e 14 21 b1 b3 10 36 52 6c 31 24 5e df 28 16 ee 76 06 c3 df 82 25 91 85 c2 93 ea 3e af af b6 fb fd 6c 57 f7 11 c5 7b 5f da ff 00 cc 8f f4 1c 4c b7 1d ce 44 d8 f7 07 60 c4 df f7 ed fc b8 19 28 60 a7 dc 16 36 1e ca 6c 45 fe bf 6f 71 c1 15 32 90 cd 80 3e a0 01 20 fd 37 df f9 f1 58 21 43 0b 5c a8 bb 58 76 b6 e0 9b db db b7 e5 f6 e2 36 4c ed 6b fd 46 fe d7 b0 03 7f 6f 71 c2 9e c4 1e e4 ef f5 b1 1f 5f f7 e0 89 2f 7b 90 7d f7 3f 7b fa af f7 fb f1 4b 10 49 37 b8 1f e4 37 e2 e1 6e e3 df 8a e3 47 9a 42 88 a4 b1 63 60 47 61 b6 e7 ec 0f f9 f0 45 50 8d a7 74 8e 21 76 27 e9 6b 0b 8c 89 3e c0 0e ff 00 5e c2 e7 6e 37 15 2d 24 74 e9 b0 2c c7 e7 92 e0 13 6d ed 6f f0 8f 60 2d 7f b5 f8 34 b4 cb 02 96 b5 c9 17 76 b5 89 2b Data Ascii: F H'`.!6Rl1$^(v%>lW{_LD`(`6lEoq2> 7X!C\Xv6LkFoq_/{}?{Kl77nGBc`GaEPt!v'k>^n7-$t,mo`-4v+

Timestamp	kBytes transferred	Direction	Data
2021-09-28 23:13:29 UTC	24	IN	Data Raw: 99 62 82 18 a9 3a 68 c9 0a 44 d4 e1 55 a3 91 0a dc 7a 78 e3 ba 19 ab 2a 96 a3 35 d4 eb ea 22 a8 77 63 4e 89 4f a4 da 75 3d 6a 51 58 25 55 8d 29 e5 39 39 eb a5 cb 3c 7b a6 eb ac 0a 1d 6d 63 65 97 4e 9a 18 96 9a 00 d2 c3 52 24 82 21 42 e0 41 53 25 4b da 8e 19 69 d1 84 42 69 2b 80 92 9f 15 95 99 51 4f 18 67 54 cb 39 0e 96 67 c9 23 bb 87 17 38 9f 21 9c 64 3b 38 c9 ee 4f 04 82 57 c3 da 8b 50 ea ad 57 70 96 af 53 df ef fa 86 e3 51 ec c9 59 75 ba dc 6e 95 73 36 4f 0c 92 25 aa 99 f2 c8 d8 c4 8d 01 ce 18 88 cb 23 49 01 d9 76 eb 48 2b 28 cc 50 ca f1 cd 5f 54 cb 24 cb 2b cb 39 98 c6 dd 47 78 db 29 57 a4 ad 75 e9 82 49 0c c1 97 15 17 d4 d2 96 aa ba 69 44 55 11 1a 08 e2 11 35 14 71 b4 32 52 4c 18 a3 a8 06 dd 1a 73 1b c4 f2 63 6b b0 c7 bb 71 c6 9a ff 00 3c e9 9a 0d 4e Data Ascii: b:hDUzx*5"wcNOu=jQX%U)99<{mceNR$!BAS%KiBi+QOgT9g#8!d;8OWPWpSQYuns6O%#IvH+(P_T$ +9Gx)WuIiDU5q2RLsckq<N
2021-09-28 23:13:29 UTC	26	IN	Data Raw: 19 78 77 cb b5 15 ba 9e 85 c8 bc 99 cb 7c a1 a1 4f a8 4f e6 35 16 d0 b9 7e 82 9f 48 d2 e3 aa a9 91 89 a9 92 87 4c a3 a7 a5 69 a4 63 35 41 87 ad 23 b4 b2 b9 e3 94 9d 99 7a 76 42 e0 ba 86 65 74 5e 98 b1 3d 4f 59 5c ec c1 40 0a 0b 5c 86 b5 94 db ac bf 0a fe 38 72 f7 8e 5e 15 69 bc c1 cb ca b1 d4 e9 92 9d 3f 54 d3 de b2 9e b1 21 fc 69 9a 0a aa 5a fa 54 96 9e b2 8e aa 05 32 d2 4d 12 ad ec d0 c8 90 4f 14 aa 3b 33 23 c8 a1 0c 6a 0d d8 87 25 ca 14 43 1b d9 94 04 70 ec 1f 11 83 62 b6 25 b2 ba 80 76 ca 5f 1b d5 e0 15 2d 73 6a 1b 14 6d 9c 3f f1 78 ad 63 5b 21 ec 01 cb 81 39 1c 1c f0 4f 75 fb 45 a7 64 aa 96 c3 67 92 ba 27 c1 5c 6d b4 42 b6 19 0e 64 8a ad b4 f1 b6 a6 37 9d cf cb 99 38 91 a4 ee 76 71 9c f2 95 d9 b3 4f 43 62 d9 67 32 94 1d 12 02 b8 0e a4 16 75 90 9c 7d Data Ascii: xw|OO5~HLic5A#zvBet^=OY\@\8r^i?T!iZT2MO;3#j%Cpb%v_-sjm?xc[!9OuEdg'\mBd78vqOCbg2u}
2021-09-28 23:13:29 UTC	27	IN	Data Raw: e2 25 33 95 57 2b 22 ac 45 fd 16 4c 98 0b e3 c1 69 35 1f d5 bd 4f 2d 4e 75 3f 2a 1b ca 79 96 f2 de 6b 0f fb 3e 68 c5 9f 4b 3f 49 93 a7 96 3e f7 f5 f0 44 95 55 15 11 52 2c f0 d1 49 55 51 f8 37 a3 12 c2 ac 0c 84 09 af 2b 5a 22 60 04 b3 e2 c0 b0 5c 41 b3 5b 86 aa a9 a9 85 60 f2 d4 52 56 b4 95 10 43 2a 45 2c 49 d1 82 46 c6 5a 92 ef 74 65 84 28 2c 83 12 c1 8d 86 fb b5 53 57 0a 4e a5 35 3d 3c b5 a4 40 c6 09 a7 74 83 32 f1 75 ad 28 46 36 8d 3a 86 3f 45 98 aa 82 05 f6 35 86 b1 56 2f 27 04 13 93 51 0a cc 93 4c 62 54 a6 66 2b 34 c8 dd 37 2f 2c 48 91 34 71 90 8a e4 90 48 df 82 21 24 d3 25 55 2c 31 d3 34 b1 4d d4 eb d5 2c b1 a4 74 bd 38 c3 c7 d4 89 8f 51 cc ee 4c 71 84 f9 58 82 76 02 d7 34 d5 0b 5d 0d 3a 52 b9 a6 6a 67 9a 4a e1 24 62 34 94 3d 92 99 a2 62 24 67 91 2e Data Ascii: %3W+"ELi5O-Nu?*yk>hK?I>DUR,IUQ7+Z"`\A[`RVC*E,IFZte(,SWN5=<@t2u(F6:?E5V/'QLbTf+47/,H4qH!$ %U,14M,t8QLqXv4]:RjgJ$b4=b$g.
2021-09-28 23:13:29 UTC	28	IN	Data Raw: 13 d5 0a 4c 81 42 63 80 27 30 4d b8 b9 95 c3 46 12 3c e3 61 29 92 4c 94 14 60 10 46 30 22 ee 1e ed ba 9f 4f 4e ec 77 03 8c 77 2c 27 09 87 e1 88 c3 67 90 b1 72 4a e0 53 1c c9 00 e6 1c b6 02 d6 ee 78 22 a3 d7 d4 75 64 20 00 18 48 c1 70 60 d9 dd 50 dc e4 c9 88 ea 29 50 14 48 86 e4 16 01 55 81 32 26 0e 98 b6 20 b0 01 64 ba 8f 54 76 27 d3 ed ba ae e0 fa 6d b9 b8 f5 0b b8 68 ed 18 55 22 4c 94 96 24 bd d3 0d 88 11 e2 ac 58 9f 56 76 02 eb 71 8d 2c 8c ce f9 28 52 1b 14 6c af 9a d9 7d 44 00 4a 6e 59 6c 6e db 6d ec 38 22 1d 60 43 e2 ac 84 3b 2d d9 54 06 c4 01 75 0a 58 61 7f 96 f6 3d ee 07 14 2c 8e c3 32 ac 85 af 75 70 97 f4 9c 77 2b 75 37 00 10 7b 90 46 5b df 80 a5 8f cc b8 e2 4a 8b b6 59 aa 9d 9e c0 fa 72 1f b3 7b 8b 7d f8 21 99 d4 16 5c 0d db d3 70 c4 00 6c 2e c3 Data Ascii: LBc'0MF<a)L`F0"ONww,'grJSx"ud Hp`P)PHU2& dTv'mhU"L$XVvq,(Rl}DJnYlnm8"`C;-TuXa=,2upw+u7{F [JYr{}!\pl.
2021-09-28 23:13:29 UTC	30	IN	Data Raw: e8 d9 ca c1 48 c4 82 a4 c6 b7 95 81 cd a4 28 00 e2 f7 7d 59 5f 76 7b b7 4c d8 29 f7 65 b4 d1 bb 63 5b 8d bb 4b e4 38 f1 1f df d9 e1 a7 c8 0f 6b 3f 81 fd 7e f4 be ea af a4 15 4c f4 57 5b 84 ba 67 42 3a 60 ea 1d 17 64 9a 78 68 24 66 0b e0 17 ca d6 08 ea 2f 55 04 38 3a 59 2a 1c 68 1b 2b 47 a8 db e9 b6 b9 cb 75 d4 55 d6 eb 53 4d e7 1a b2 ae b6 69 56 4a 4a 49 91 29 3c 84 53 62 c8 35 1a a7 25 a1 69 9c 91 2c 53 4a af eb 8e 33 1b 4c 18 8b 69 5e a2 87 54 33 4a 61 d5 69 b5 0a 2a ad 2b 57 d1 34 e8 a4 fd 54 94 f5 14 e6 9e 71 53 58 d7 89 3a d1 b2 bc 32 b3 41 1c 35 70 a3 aa 3b 2d 9b 87 39 eb c5 5e 4b f0 c7 4e 86 ab 9c b5 95 e5 81 55 3d 1c 3d 39 8d 46 a1 cc 9a b4 da 84 c9 a7 d1 d4 9d 2a 9d 96 a6 97 49 9e b6 78 69 24 d5 25 14 9a 55 1b cf d6 a9 60 cc 58 f5 92 b3 e2 ef 5a Data Ascii: H{}Y_v{L)ec[K8k?~LW[gB:`dxh$f/U8:Y*h+GuUSMiVJJI)<Sb5%i,SJ3Li^T3Jai*+W4TqSX:2A5p;-9^KNU== 9F*Ixi$%U`XZ
2021-09-28 23:13:29 UTC	31	IN	Data Raw: d7 bb 55 6b ab 86 b8 b8 dc 25 86 5f 12 7b 2d 92 c3 6b b4 88 9a f0 68 ec 96 db 4d 2b 25 86 92 43 21 74 9f 79 5c 2e 95 6e 73 23 c5 50 6e e6 9d 91 47 a8 d5 50 4b 3b e9 1a ae a1 43 51 15 5d 14 95 02 8a a6 a6 95 5e 7d 36 ae 3a ed 3e 6a 84 8c a4 55 89 45 59 1c 75 74 32 4a b2 2d 3d 44 42 78 71 74 56 16 55 1a ed 67 53 ad d6 35 9a fa ed 5f 57 d5 6a a4 ae d4 b5 4d 4a a6 6a cd 43 50 ab 9d 83 4b 53 57 55 33 34 b5 13 ca ca a5 e5 91 d9 9e c0 33 1b 01 c5 a3 4f 6a 69 6d 22 49 1b 32 b5 3a 53 b4 8d 38 8e 2a 56 68 d2 4c c8 00 67 19 17 36 bf 7d f6 bf 19 71 a9 8e c5 bb 0e df 6d c6 c3 bf df f9 f1 3c 37 8c 13 e7 90 41 f9 61 74 30 1b 9c b8 67 1d b8 19 e4 60 fe 63 83 ef 0b 3e 0a 50 ca 11 53 df 32 a1 02 9c ad 6c b6 20 dc d8 02 47 7d ef ef c6 3c b1 a8 ce e8 09 66 de db 2e c6 e1 7b Data Ascii: Uk%_{-khM+%C!ty\.ns#PnGPK;CQ]^}6:>jUEYut2J-=DBxqtVUgS5_WjMJjCPKSWU343Ojim"I2:S8*VhLg6}qm <7Aat0g`c>PS2l G}<f.{
2021-09-28 23:13:29 UTC	32	IN	Data Raw: ef c0 e9 cc d2 42 52 70 88 ac fd 78 fa 6a c6 75 68 d9 55 43 92 3a 58 39 59 0b 2a b1 6c 71 36 07 7b 16 29 5a a1 64 59 c0 a7 48 dd 64 80 46 a7 a9 29 c4 a3 89 89 cd 30 01 ae b8 d8 e5 bf 61 62 27 09 54 27 b9 68 4d 27 49 40 5c 5f cc 89 f3 7c cb 30 3d 33 0f 4f 00 00 f5 66 1c 93 62 38 cb a7 8a a8 54 4c d2 b4 0d 48 44 02 95 51 5c 4e ad 8b 1a 8e b3 31 c1 81 38 f4 f0 00 81 90 37 bf 15 c7 1c ed 53 d4 33 86 a7 30 aa 0a 7e 9a 5c 4d 99 66 9b ae 08 2c 1a 36 48 fa 78 e2 0a e5 96 57 1c 65 c3 1c eb 3c cf 24 d9 53 b8 8b cb c1 d1 08 60 64 42 b3 13 36 45 a5 ea 9b 30 0c a3 0b 7a 4d 9a c0 8a ea 58 6a f3 aa f3 26 02 86 62 69 3a 21 c3 8a 7c 07 a6 a0 b9 2a d2 f5 72 b1 8c 05 e9 95 04 16 04 8c 8a 64 ab 11 ba d5 18 19 c5 44 c6 1e 80 70 a2 97 a9 f8 0a fd 46 24 cc 22 b0 94 a9 c0 c9 ba Data Ascii: BRpxjuhUC:X9Y*lq6{}ZdYHdF)0ab'T'hM'I@_|0=3Ofb8TLHDQ\N187S30~\Mf,6HxWe<$S`dB6E0zMXj&bi:! \|*rdDpF$"
2021-09-28 23:13:29 UTC	33	IN	Data Raw: 6c 81 e9 e4 71 2d 7d c3 15 b1 60 2e 01 bd 86 dc 65 d3 d2 4d 2c 66 4e 98 ba c6 4e 01 c8 59 25 01 8a a4 72 30 b0 05 82 ab 3b 0b 2d f7 00 90 38 cb a3 a3 79 9a 43 25 99 33 24 36 24 59 4e e1 06 fe a6 03 62 fd 89 b9 b0 b5 b8 d5 c4 52 a5 3d 93 a2 65 44 6c 12 ef 1c 19 82 71 dc a3 38 0c 31 ca d7 7b e4 c5 47 a4 70 45 51 5c 23 bc 70 86 61 8d a2 0e b1 8d d8 06 f5 9f 4f a4 16 6b 91 76 c6 dd c8 e0 ca b2 2c 6c 69 c4 4f 28 23 01 33 48 88 54 b8 0e 4b 22 39 0c 23 2c c8 31 20 b8 55 62 01 27 8b da 19 5e 17 11 b2 c5 39 5f 43 b2 b4 b1 a3 9f 7c 01 46 91 6f ed 92 9b 7b 8e 16 78 67 31 11 4e f1 a4 d7 8f 19 26 46 78 80 cd 7a 99 2a 32 b0 c9 32 0b ea f4 b1 5b e5 62 09 16 3c eb 3d d0 c0 23 7b c8 82 4e ab b4 78 c4 4f e2 32 61 14 99 48 aa 3d 11 b1 44 63 b1 98 7b 24 ab 36 71 2c 62 32 85 Data Ascii: lq-}`.eM,fNNY%r0;-8yC%3$6$YNbR=eDlq81{GpEQ\#paOkv,liO(#3HTK"9#,1 Ub'^9_C|Fo{xg1N&Fxz*22[b<=# {NxO2aH=Dc{$6q,b2
2021-09-28 23:13:29 UTC	35	IN	Data Raw: be 82 78 62 d5 b9 ff 00 51 a7 95 1d 6b 74 de 58 ac 68 e8 74 28 64 8d 63 a9 d4 c5 55 4f af f5 79 e3 e8 2b 55 59 62 a9 33 6a 15 72 d5 3b cd 8c b0 f4 ed 35 65 49 55 91 4c af 35 85 3d 2c 44 b3 19 1d d0 95 55 01 95 49 3c 6a 9e 16 78 43 27 81 bf 0b bf 0e 5c 89 4d a0 55 e8 a7 95 3c 2f e5 ad 37 5d d2 f5 28 44 15 ba 67 3b 52 d2 cd 49 ce 7a 7e a1 4a 46 4b aa e9 dc de da d5 3d 7c 4d ea 4a c0 cc 7e 65 66 e2 2f 17 bc 50 e5 bf 06 39 40 73 6f 38 c7 2d 6d 75 74 b5 34 1c 9f ca 94 b2 04 d6 f9 bb 5b 11 cb 38 8e 9c b8 2f 1d 2c 01 1a 4d 47 50 2a eb 4b 0a 28 0a d2 b4 2b c7 02 d4 12 d7 5e 6f 12 b6 16 49 2c ce 9d f4 94 d4 f1 b7 73 c0 6b cb 03 1a 32 00 0e c6 e7 0e de d1 71 e0 92 bf 9a 2f 48 fd 55 d4 de bf 7a 48 6a 3b 54 96 9b b5 da f3 1e a0 a9 d3 7a 43 4a 53 b2 67 b2 d7 66 a2 ab Data Ascii: xbQktXht(dcUOy+UYb3jr;5eIUL5=,DUI<jxC'\MU</7](Dg;RIz~JFK=|MJ~ef/P9@so8-mut4[8/,MGP*K(+^o I,sk2q/HUzHj;TzCJSgf

Timestamp	kBytes transferred	Direction	Data
2021-09-28 23:13:29 UTC	36	IN	Data Raw: e4 ea 7a 18 b2 e8 07 93 a6 16 1a da 79 22 e9 b4 d1 15 00 af a0 82 5a f3 02 51 98 2a c6 a6 45 90 b2 05 be d5 a3 db 09 9e 3e 82 ad 3b 43 34 4c 5c 4d 9d 8d a4 52 92 95 0b 2a dd 8a 44 a0 b2 87 f5 2b 62 c3 59 8a b6 42 69 67 0a 0c b4 ff 00 f4 f2 47 7b ad 4c 2c 40 44 93 27 90 06 8f 21 2b 42 4b ba 03 1a bd ee dc 65 40 cf 1e fc 76 f8 63 fa 63 f4 5d 9f 8f c3 8e fc e7 18 04 8c 0c 81 97 60 fc 32 71 ef 3d d6 e9 a6 9d 21 92 39 a5 58 59 ea d0 88 9d a2 56 86 60 88 ef 22 cd 1a c2 d0 89 84 77 7a 79 40 21 65 07 33 60 a3 8d 53 c3 cd 4d a3 8b 53 d1 2b 5a 56 47 9a aa 48 60 0e f3 2b 4f 14 80 f5 2a e3 e9 ad c1 a4 31 92 5e e5 64 8d 5b e5 6d b6 44 ae ee d5 70 10 63 c2 d5 d1 a2 a5 a3 96 22 ff 00 8b 12 a8 88 dc 4a f1 df a0 b8 c6 ac 55 98 15 ef 8f 4b 55 25 17 31 d1 d5 d3 cf 3a d3 ea Data Ascii: zy"ZQ*E>;C4L\MR*D+bYBigG{L,@D'!+BKe@vcc]`2q=!9XYV`"wzy@!e3`SMS+ZVGH`+O*1^d[mDpc"JUKU%1:
2021-09-28 23:13:29 UTC	37	IN	Data Raw: 25 59 18 c6 aa c2 45 40 c7 a2 f9 2b 62 8e 48 c9 92 cf e9 00 1d f8 57 89 1d 3a 79 c8 9e a8 df 28 a5 74 7b c7 20 94 02 c0 df 16 61 8c 97 f9 d4 90 c6 e6 fc 58 f1 f5 02 5c c8 a1 24 59 7d 0e e8 18 ad c0 49 31 20 49 19 bf aa 37 05 49 03 6e 08 81 8c bc 91 37 56 44 11 b3 31 89 59 55 2a 2e 8c aa 92 86 52 4a a3 95 91 71 64 21 d5 6f 92 de d9 1d 27 eb 47 20 9a 55 02 39 51 a9 ee 9d 39 1a 42 19 64 65 c7 31 24 41 48 0c 19 23 c5 ce 57 db 8a 44 41 e4 8a 42 d2 03 0b 16 55 59 19 63 72 f1 bc 76 95 01 c6 50 a1 cb 20 60 71 90 2b ad 98 0e 33 44 2a f3 c7 30 69 01 48 e4 84 46 8e 56 16 12 15 b9 68 97 d0 d2 29 41 83 11 92 dd ad b9 e0 8a c8 a2 7e b9 98 4d 21 4e 9f 4c 53 8c 3a 19 89 1d cc c0 f4 c3 19 31 2b 19 26 56 5c 46 cb 7d c6 64 34 ce b3 4b 29 92 67 49 7a 56 85 82 08 62 68 d5 83 Data Ascii: %YE@+bHW:y(t{ aX\$Y}l1 I7In7VD1YU*.RJqd!o'G U9Q9Bde1$AH#WDABUYcrvP `q+3D*0iHFVh)A~M!NLS: 1+&V\F}d4K)gIzVbh
2021-09-28 23:13:29 UTC	38	IN	Data Raw: 4a 62 f6 63 d3 c8 1e d7 c7 d6 3d 23 2b 2e e4 6d 95 bd b8 ca a7 a7 7a 88 cc 86 3d d5 32 e9 96 0b 94 a1 49 11 2c 8c 30 f5 30 c3 3b 15 5b 07 3b 10 38 34 54 53 ce 03 4b 1a 2e 37 be 2c e5 1d c3 36 31 02 c9 9e e9 89 76 c7 6d f1 56 36 1c 6b a8 b3 2d 38 51 1c 42 75 8c 01 18 32 08 84 b8 6c a1 b0 59 0c 7d 4b 80 cc 81 ca db d2 bd f8 22 ca 82 35 08 ab 80 50 00 b0 fa 1e c0 03 ee 6e 7f 79 3b 6d b7 0b e5 71 80 c6 27 99 a4 0b 22 79 89 0c 6d 32 97 c8 a9 36 45 42 62 67 52 8b 80 be 2a a6 e4 dc e4 a8 18 0f a5 81 36 37 03 61 ee 40 b8 1f 71 f9 8e 28 4a 58 d2 99 a9 92 49 c2 b2 48 82 43 33 3c eb d4 2e 4b 09 9f 26 c9 4b 1c 4d ec 2c 36 d8 70 44 ad 4d 29 a5 30 2d 4b ac fd 1e 98 aa 09 19 71 26 18 f5 42 11 d2 c8 b6 f6 3e 91 73 6f 6e 0d 4d 3c b2 c0 c9 0d 43 41 29 68 c8 9c 47 1c a4 05 Data Ascii: Jbc=#+.mz=2I,00;[;84TSK.7,61vmV6k-8QBu2lY}K"5Pny;mq"'ym26EBbgR*67a@q(JXIHC3<.K&KM,6pDM)0-Kq&B>sonM<CA)hG
2021-09-28 23:13:29 UTC	40	IN	Data Raw: f8 7e 9f 14 5e 68 7c 76 78 33 47 59 a6 8f 10 a8 a9 92 0d 2d 21 ad 6e 67 34 b0 c6 91 d0 4d 49 4f 59 ab cb ae c9 60 88 7c cd 2d 25 52 56 4a c5 4b d5 c5 04 84 e7 51 93 fc 49 78 e5 cd fa 8f 8b 1e 21 6b de 20 6a 32 54 3e 98 5e 6d 2b 92 74 a9 5e 42 9a 1f 2a 53 4f 2c 7a 75 3a d3 b0 54 8e a2 aa 10 6a f5 39 d6 20 f5 15 12 b5 99 a2 54 c7 f4 65 f1 1b 91 f4 df 12 f9 03 9d 3c 3f d6 24 92 0d 37 9c f9 63 5c e5 9a ba 9a 70 be 66 92 2d 67 4e 9e 85 ab 29 f2 16 15 14 9d 6e bc 04 9d 9d 2d d8 9e 3e 04 be 29 be 1f 39 8b c0 be 7e e6 af 0e f5 ea 39 69 f5 1e 4f ad 9b 43 ad 45 62 12 ae 3a 40 be 5a b6 95 8a a9 92 8f 57 d3 9e 9f 55 d3 dd 0b 35 45 05 5a 32 83 91 0b 87 b5 e9 ea 5a 4b dd c2 ef 1f 2e ab f0 dd 1c 4e c6 60 77 f9 ee 61 ff 00 5c c5 ad cb 86 31 97 e7 f1 73 c1 34 ef 41 b4 86 Data Ascii: ~^h|vx3GY-!ng4MIOY`|-%RVJKQlx!k j2T>^m+t^B*SO,zu:Tj9 Te<?$7c\pf-gN)n->)9~9iOCEb:@ZWU5EZ2 ZK.N`wa\1s4A
2021-09-28 23:13:29 UTC	41	IN	Data Raw: ab 65 99 85 3a b9 92 57 9e 36 62 e5 a5 46 90 24 88 be ac 70 17 20 03 b9 69 21 14 ab 1c 60 38 a6 81 64 a7 a4 10 cd d6 a7 f2 cc ed 34 13 b9 d8 c4 66 57 21 23 65 5c 31 0a 40 16 26 b8 79 ce 47 c7 9f a7 eb ef 56 9c d0 0f 7e 3b e0 77 00 10 09 ef db 24 67 e6 38 20 ad 5d 49 20 60 33 d8 0f 4f b1 ed fd 8e fb 70 c9 1b 93 b8 61 6d b7 27 be d6 1b 58 03 f9 ef c7 26 78 63 e1 9e bd cf f5 74 89 43 a3 73 84 fa 5c fc dd c9 1c b4 fa c6 85 ca 95 3a ce 8e 9f f3 66 bc 9a 3d 52 d6 f3 27 52 2d 27 97 75 1d 36 06 6a fa 38 b5 5b 43 ab 32 f9 48 a5 86 42 8c dd ea d3 7f 47 87 31 d1 f3 87 36 f2 2f 3d f3 7d 0f 2b 46 da 12 69 bc 8b e2 0e 83 a9 69 fa 8d 3f 30 78 83 a8 f3 1d 4c 3c b7 a7 4f a0 55 45 4f 53 cb b5 fa ae 89 10 86 5e 53 d5 de 5a fd 42 b1 1e b7 43 ae 9a 39 5d 52 5b 58 4e 30 38 ce Data Ascii: e:W6bF$p i!`8d4fW!#e\1@&yGV~;w$g8 ]I `3Opam'X&xctCs\:f=R'R-'u6j8[C2HBG16/=}+Fii?0xL<OUEO S^SZBC9]R[XN08
2021-09-28 23:13:29 UTC	42	IN	Data Raw: 33 a8 f3 09 1c b1 c6 58 9c 96 39 48 ea 59 2f 63 7c 53 d4 54 95 b0 b1 17 37 a0 f4 96 4a 71 20 8f ab d4 6f 2e 64 03 a9 90 89 fa 82 26 b1 2a c6 10 f9 15 b7 a0 30 3e d6 cf c6 03 24 2c e2 36 a9 68 e5 e9 e7 8f 58 c2 4a 79 81 19 20 c8 50 b2 c6 65 0b b1 6b 16 b9 b0 e0 8a d8 e0 80 d4 19 c0 1e 65 e1 48 d8 86 39 18 43 c8 cb e8 b9 50 bd 53 27 af 1b 96 2c b9 58 00 33 a3 86 05 9e 69 90 01 3c a9 0a cf eb 2c 71 8c 30 8e e8 58 84 b0 2d f2 aa e4 6e 4d c8 da 98 bc b3 55 31 bc 1e 6c 40 b7 c4 20 9c d3 09 18 2e 40 7e 20 88 4a 1c 00 c0 2e 79 5b 70 6d 64 5e 5c d4 d4 98 c4 1e 67 18 45 4f 4f a7 d6 c6 cf e5 c4 d6 26 4b 5b aa 62 ea 5a cb 7c 6e 08 3c 11 48 e0 a6 8e 4a 86 8b 11 24 d3 75 2a 2c f9 13 31 8e 35 bb 29 2c 15 8c 4b 18 00 05 38 00 40 f5 12 65 3c 34 b0 89 3c be 20 3c d3 4d 21 Data Ascii: 3X9HY/c|ST7Jq o.d&*0>$,6hXJy PekeH9CPS',X3i<,q0X-nMU1l@ .@~ J.y[pmd^\gEOO&K[bZ\|n<HJ$u*,1 5),K8@e<4< <M!
2021-09-28 23:13:29 UTC	44	IN	Data Raw: ea 16 4e aa b1 76 6f 58 90 32 90 14 63 8e e4 4c f4 50 c9 46 68 18 49 e5 fa 2b 06 d3 cc 24 28 a0 28 fc 65 75 9f 2d 81 2e 24 0e 48 37 63 73 75 aa a5 82 aa 98 d1 cc d3 24 37 8b d5 15 44 b0 4a 0c 32 24 91 fe 34 6c b2 6e c8 a1 bd 77 91 49 56 27 23 7b e6 a7 8a 6a 73 04 ad 2f 4e d1 82 cb 34 b1 cb f8 4c 8e a7 ac 8e b2 de e8 32 39 5d c5 d5 ae 18 f1 a1 6b 95 74 6f 4c f4 95 4b 0b 42 e5 1a 56 95 f0 89 0a c8 af 18 24 34 78 bf 54 29 50 1e fd 8f ab 70 48 a6 b1 34 2e a9 4e 24 94 49 1c f1 54 07 86 79 60 c2 58 4e 48 ae 62 74 ea ab 1d 9e 27 c9 1c 11 90 2e 03 71 b6 e6 8d 24 31 bb b3 06 8e 46 74 b4 8e b9 3b 07 53 98 0c 04 a2 ce c7 17 0c 03 59 85 8a 8e 0d 64 74 ce b1 8a 9e 9f ff 00 a8 85 a0 ea c9 8d aa 43 9c 31 2c e3 29 03 5c 2a 2d f2 04 92 a7 6e 2a 9d 29 5d e9 5a 60 ad 2c 72 Data Ascii: NvoX2cLPFhI+$((eu-.$H7csu$7DJ2$4lnwIV'#{js/N4L29]ktoLKBV$4xT)PpH4.N$lTy`XNHbt'.q$1Ft;SYdtC1,)\*-n* )]Z`,r
2021-09-28 23:13:29 UTC	45	IN	Data Raw: af 1b 82 37 56 23 8a 9a e2 d7 07 0e fd be 60 e3 23 f4 09 dd 7e 6a 5c d5 c8 3a 8d 6e b3 45 c9 d4 57 a7 ac e7 2d 73 46 e4 98 a4 8a 43 1f 90 a7 e6 0d 51 28 b5 7d 41 b1 0a e4 51 68 83 53 91 9c ba c6 a0 ab b0 6c 52 de 18 fc 6b 78 b9 ff 00 ac bf 12 1e 21 6b 1a 73 2a 72 6f 27 d7 0f 0d 3c 3e a0 a6 bb d1 69 9c 91 c8 a0 68 3a 3a 51 a0 23 a5 1d 52 52 4b 5f 52 f1 aa 67 3d 43 bb 96 63 7e 3e cc ff 00 48 47 c2 94 ff 00 0c 3e 39 ea a7 4d 49 e5 e5 ed 2f 41 f1 37 c4 2e 47 af 99 fa 46 b3 4a a5 f0 d3 9c 67 d1 00 9c a6 13 6a 7a 1e a6 24 d3 ea 5e 46 37 a8 a1 49 ad 69 e2 63 f0 62 bd 59 5d ea ea 0b 75 2b aa 65 95 9a c4 3c 93 55 93 2b 3c ac 46 fd 47 6f 51 39 02 c5 9b 1b b6 d0 25 fe 7d dd f2 38 65 90 50 c2 21 fc 23 0f a8 71 f1 1f 83 c8 25 91 b4 1c 81 9e dc 72 b9 55 b6 87 ef 8e b6 Data Ascii: 7V#`#~j\:nEW-sFCQ{}AQhSlRkx!ks*ro'<>ih::Q#RRK_Rg=Cc~>HG>9MI/A7.GFJgjz$^F7IicbY]u+e<U+<FG oQ9%}8eP!#q%rU
2021-09-28 23:13:29 UTC	46	IN	Data Raw: 49 a1 8d 59 77 2a 31 03 5e f3 75 35 0c 64 90 d5 55 4c 30 62 65 76 79 5b b7 a2 49 0b 57 48 8e 36 c1 5a 48 55 3b 5f b5 b6 3a 4b 74 74 30 88 63 7c 93 73 b9 f2 ca f2 5c f7 10 39 c1 c8 1d bb 6e 5d 57 44 69 8a 6d 01 62 8e c1 41 71 be 5d 9a ea ba 8a ea bb 9e a0 bc 56 5e 2e d7 1a ea c3 13 aa ea ab 2b 2a 89 01 f3 b9 8d 7f 83 4e ca 7a 58 9c 08 8a 06 e7 7a ea 6f 87 1e 18 f8 b3 cb 3c bb f0 fb ff 00 a6 f5 1c a3 ca 1e 1d 6a 3a a7 85 7c e5 e2 b7 87 fc a9 a1 57 4b aa f2 e5 65 0e 85 ac 0e 70 7d 12 bf 50 af a0 83 5d e4 9e 73 f3 1a 64 7c f9 cb 9c e0 b5 1c c1 a2 6a ae 2a f9 55 95 74 f5 44 e4 8e 58 f8 64 e5 1d 2f 98 fc 4d 6e 6a a9 d7 3c 53 f0 f7 9f 79 57 95 39 5b 45 e5 1f 10 b5 da fd 46 b7 93 b4 ee 59 d7 35 6d 6a 9f 40 a1 d4 28 a0 8e b2 a7 4b d1 eb b5 15 9f 94 f9 82 a2 be 1e Data Ascii: IYw*1^u5dUL0bevy[IWH6ZHU;_:Ktt0c|s\9n]WDimbAq]V^.+*NzXzo<j:|WKep}P]sd|j*UtDXd/Mnj<SyW9[E FY5mj@(K

Timestamp	kBytes transferred	Direction	Data
2021-09-28 23:13:29 UTC	47	IN	Data Raw: af b1 5e 2d c9 51 94 36 f7 95 52 3f c3 2e 3a a7 2c 4e ca d8 90 01 21 d8 a0 50 1b d7 73 62 09 0a a0 b0 90 d8 c6 bf 86 85 c9 ea 4a 23 06 d7 1b 28 6e ab ee 71 88 16 3b 8b 71 72 bf 49 45 d5 df 39 02 0c 11 9a c4 e5 ea 6b 02 16 35 b7 ad c9 b2 e4 bd ef c1 15 a2 44 ea 44 8c 0e 52 39 58 ec ae 77 54 67 63 9a 8b 25 95 49 25 8a dc 5c 02 7e 56 ce 59 22 13 2c 45 6f 23 23 bc 66 c4 d9 56 44 47 bb 94 21 41 66 5c ae c8 5b ba a3 90 40 c6 8d 80 31 21 12 1c 8b 7a 91 58 aa fa 4b 5e 46 00 aa 29 c7 10 5c a8 67 65 51 b9 e3 32 37 01 fa 78 c8 4b a9 21 c2 de 20 14 a8 60 cf d9 5c 07 c8 06 b6 4a af 63 75 b7 04 59 10 4b 19 95 a2 ed 2f 4d 65 22 ce 7f 0d 9d d1 48 93 11 19 f5 23 5d 45 9a e4 b9 5f 51 e2 c8 e4 8d a6 96 35 bf 52 20 86 40 55 ee 16 42 c6 3f 5b 00 ac a7 17 20 46 58 2e e1 ac 6d Data Ascii: ^-Q6R?.:,N!PsbJ#(nq;qrIE9k5DDR9XwTgc%I%\~VY",Eo##fVDG!Af\[@1!zXK^F)\geQ27xK! `\JcuYK/Me" H#]E_Q5R @UB?[FX.m
2021-09-28 23:13:29 UTC	49	IN	Data Raw: 2e 2a cc c1 1e 24 80 ff 00 dd 12 24 8a 56 43 8f ec 94 24 1d f1 b8 b8 22 a7 56 a9 a1 34 66 89 fa 0f 4e 63 40 f9 b0 e8 2c 6a e8 61 01 83 05 2d 9a c6 53 d7 60 c1 4e fd 8e 83 5c f4 69 4c cf 5e 63 f2 d9 47 99 9d 44 88 5d a4 51 1e 4a 43 64 4c 85 6d 60 4d ed 6e 12 59 69 63 a5 92 59 d3 ab 48 b1 89 19 56 13 35 e3 52 1d 70 85 23 95 da de 92 aa 88 4d c0 b0 e2 ca ca aa 7a 68 3c cc d9 98 01 4d 96 27 95 8f 51 95 50 f4 d1 0b 7c c5 4f ca 31 1b 9b 5b 82 2c 7a b7 a4 1e 5c d5 08 85 e6 87 a1 d5 50 eb e6 98 9e 90 40 03 28 92 f7 0a c1 56 c3 f6 fd b8 49 de 8d 25 a5 5a 83 12 ca f2 14 a4 2e a1 9c 4c 10 99 3a 44 dc e6 63 27 26 52 2e a2 db ef 76 ad 9e 1a 7e 93 d4 06 02 7a 88 a1 86 d1 b4 9f 8b 21 c2 32 6c 2f 18 c8 1b bb 00 a8 08 39 6f b2 4d 34 30 cb 4d 14 81 8c 95 32 b4 50 63 13 38 Data Ascii: .*$$VC$"V4fNc@,ja-S`N\iL^cGD]QJCdLm`MnYicYHV5Rp#Mzh<M'QP\O1[,z\P@(Vl%Z.L:Dc'&R.v~z!2l/9o M40M2Pc8
2021-09-28 23:13:29 UTC	49	IN	Data Raw: 17 e0 89 9e 5a 54 a8 a6 49 3a 7e 69 d6 6f 2d 90 1d 52 8a 2f 31 8c db 25 5b 14 0f bd 88 61 b6 d7 e0 e7 4c d5 58 fe 17 9c 14 e5 ac 00 eb f9 62 f8 9f 55 83 18 fa a5 6e a1 80 24 ee 0f 0b 24 b1 c7 51 05 3b e5 d6 99 25 78 88 8a 46 40 b1 28 32 65 28 4c 23 26 e0 28 66 05 cf 6e 2c 59 a2 eb 9a 70 18 cf d1 32 dc 44 e5 44 7d 40 96 ea 85 28 0e 47 22 a5 81 b0 ca dc 11 45 6a 6f 33 32 a1 8b cc 88 e0 6a 8b 28 ea 74 d8 38 a7 32 12 2e c8 2c e1 14 9b 0b 76 ee 48 43 4e f3 54 2c 06 23 22 48 9e 60 46 00 61 21 41 ff 00 74 da e5 c4 61 08 be 47 12 a2 f6 03 8a d2 78 9e 79 61 5c ba b1 a4 52 49 74 21 70 90 37 4c f5 0f a5 8f a5 97 1b 92 b6 de c3 8b 62 9a 37 69 e3 40 d9 c4 e1 24 62 8c aa 58 c6 ac 31 76 01 65 00 30 05 90 b2 8e d7 db 82 29 01 a7 94 4a 69 da 2f 4c f2 ac dd 20 2d d7 16 ea Data Ascii: ZTI:~io-R/1%[aLXbUn$$Q;%xF@(2e(L#&(fn,Yp2DD}@(G"Ejo32j(t82.,vHCNT,#"H`Fa!AtaGxya\RIt!p7L b7i@$bX1ve0)Ji/L -
2021-09-28 23:13:29 UTC	50	IN	Data Raw: ad 74 6e b8 55 c7 bb 92 e8 de c0 f3 ec 34 0f 89 51 08 85 d8 07 2c 15 cc 64 5c 06 2e 05 d9 85 c3 1c 9d 71 7c 55 48 b1 3e af 7e 30 ea 4b 12 d2 34 af 76 28 8a 0d 83 b4 91 dd 91 9f 1b b7 4d bf c0 40 0f 21 0e 45 d4 0e 37 46 ab 46 b4 ef 50 d0 9b 3b 10 77 66 20 b8 1b 30 8d 86 42 e3 d2 24 9c 09 24 d9 ba 6a 05 c6 cb a8 9c c7 b4 a8 c8 48 c8 c6 c0 5c 01 b8 76 63 66 77 0d 62 81 50 8e e1 7d ad e9 20 77 5b 33 9e d6 b4 b7 00 67 de 3b 67 1d 8f 99 e4 60 64 fb fc 96 1c 92 f4 cc 97 2e 5c 9c 88 2d 82 65 bf cd 18 60 11 ac 2c cc 45 ee 05 c5 f8 ec 17 c3 8f c3 2f 8a 3f 13 7c cc 34 8e 4e a1 fd 5b ca b4 12 a3 73 3f 3d ea e9 34 5c b5 cb 94 f9 03 22 cb 50 aa 5b 51 d5 a7 4b a5 1e 91 40 26 ae aa 66 55 c2 35 62 e3 90 be 11 3e 10 35 6f 89 1d 53 55 e6 8e 67 ac ff 00 93 3c 12 e4 e9 1a 4e Data Ascii: tnU4Q,d\.q|UH>~0K4v(M@!E7FFP;wf 0B$$jH\vcfwbP} w[3g;g`d.\-e`,E/?|4N[s?=4\"P[QK@&fU5b>5oSUg<N
2021-09-28 23:13:29 UTC	51	IN	Data Raw: a1 d6 d3 54 c9 d2 5b ed 77 b2 41 1c 90 39 f3 cf 07 f7 f5 f7 aa 1c dc f2 3b f6 23 f2 5c fb 51 a9 68 fa 6d 42 41 5f ad 69 0d 2c b3 e9 74 86 92 4a dd 3d 65 4a 8d 66 b7 f5 76 90 1e 2a ba 9a b7 8d f5 5d 53 2a 0d 3a a4 51 aa 57 57 87 a3 81 9e 54 91 17 40 7f 10 79 54 c4 b3 d2 3e bd cc 0a 29 ea aa a2 a1 d0 34 6d 4a a2 a6 a8 d0 f3 02 f2 d6 a3 a7 c7 05 64 fa 25 2d 46 a7 41 aa ac e2 af 49 14 2f a8 ad 0d 2d 4e a7 4d 47 53 47 1e 6d d7 f8 12 8d 7c b4 1a 25 2d 30 8e 4a 79 68 39 32 aa 87 47 a8 9e 0a 9a 0d 3e 5a ce 57 d0 74 98 f4 79 d2 3a fd 4b 4d ad e6 3a 8e 6a f1 13 9f fc 1f d5 ea d7 9b f9 1e 1d 2e 3e 6d e4 6a 9a aa 28 51 ce 65 3d 54 2d 34 13 68 f3 69 8f 08 4d 1a 5d 36 aa a3 55 9e 4a 59 a9 4c b3 72 27 85 fa e6 a3 ce 34 c9 5f 33 69 f0 b4 5c c3 cd 5c a7 e2 de 9f 07 eb 2e Data Ascii: T[wA9;#\QhmBA_i,tJ=eJfv*]S*:QWWT@yT>)4mJd%-FAI/-NMGSGm|%-0Jyh92G>ZWty:KM:j.>mj(Qe=T-4hiM]6UJYLr'4_3i\\.
2021-09-28 23:13:29 UTC	53	IN	Data Raw: 38 ec 37 e0 89 c9 21 6e 15 9c 92 a0 2a 00 6f 93 2a 93 72 55 7d 2a 5a 43 bf c9 1c 96 bb 04 57 c8 46 31 aa 80 ac f9 c8 01 2b 88 c1 5b 76 76 c9 81 2a 9b 6c b9 31 c8 59 6c 09 14 3d d0 7d 7d 4a 2c 4e 3b 1d cb 0e f7 b2 87 2a 3f 6a c1 45 8b 0e 1d a4 71 6c 42 ee c0 36 4f 8d 92 c7 26 1b 7a ad 61 e9 ee 6e 48 f9 4f 04 5a 84 72 10 d1 fa 19 81 c8 16 5b 62 97 56 60 5e e4 10 09 50 83 10 c6 ec 0d ac 09 17 89 ae ca 04 6d 8b 67 67 d8 28 28 40 0a 77 cb 26 b9 b6 21 94 62 43 30 da f8 11 86 cc 10 01 4d d5 c9 6b 15 c9 49 56 55 b7 af d4 a0 11 70 54 1c b7 b5 8e 5a b3 5e 21 8a 84 f5 92 d9 8b 86 0e 31 50 96 f5 5d 72 62 6e 02 85 ec 6f b1 16 a8 8e d9 f4 fa 6d 8f 4c 3f 56 eb 86 4c ec bd 3b 65 d4 0e 02 e5 72 98 db f6 af b7 0c b2 33 49 22 18 dd 55 31 c6 42 50 a4 84 df 25 50 18 b8 29 65 Data Ascii: 87!n*o*rU}*ZCWF1+[vv*l1Yl=}}J,N;*?jEqlB6O&zanHOZr[bV`^Pmgg((@w&!bC0MkIVUpTZ^!1P]rbnomL?V L;er3l"U1BP%P)e
2021-09-28 23:13:29 UTC	54	IN	Data Raw: 12 0d ae 38 be aa 7a 88 69 8d 44 34 af 57 27 a3 fe 99 24 55 6b 48 c1 5c e4 c0 ad a3 0c 4b 58 5c 80 40 b5 ef c1 12 54 54 79 75 88 f4 27 98 cb 3a 43 8c 29 93 20 94 9b c9 20 b8 c6 24 b5 a4 63 d8 8b 58 db 81 3d 4f 49 e0 8c 45 3c a2 79 5a 22 f0 a7 51 22 c5 19 cb ca 41 f4 a1 b6 20 d8 dd 8d b8 15 33 cf 02 c6 69 e9 5e a5 9a 68 e3 68 c3 22 18 91 ef d4 95 c9 52 1d 23 3b e2 0a 92 3b 58 db 83 34 d2 c5 2d 32 25 33 cd 1c ac eb 2c aa ca 05 34 61 4b f5 48 37 2e 8c e0 20 45 37 03 23 6b 85 0c 44 1a 60 95 31 41 d2 9a 41 22 ca dd 64 8c b5 3c 62 31 91 59 5e e0 23 b8 37 8c 10 6f db 86 eb de 7f 2c 22 9c 03 0f 57 ac 11 7c bd f3 11 f4 cb de fd 5f 56 58 01 7c 2e c3 df 85 96 59 16 78 22 4a 57 78 65 49 4c d5 21 95 52 9d 92 c6 20 cb 7c 9b ac 7d 22 c0 81 6b ed c4 59 a4 35 22 9c d3 bf Data Ascii: 8ziD4W'$UkH\KX\@TTyu':C) $cX=OIE<yZ"Q"A 3i^hh"R#;;X4-2%3,4aKH7. E7#kD`1AA"d<b1Y^#7o,"W| _VX|.Yx"JWxeIL!R \}"kY5"
2021-09-28 23:13:29 UTC	55	IN	Data Raw: df b6 c0 fd f8 6b d8 8d ed 7e c7 fc bf 7f b7 04 5f 8b 8f 8e 1e 14 f3 37 83 3e 20 78 81 e1 1f 3b d2 f9 2e 75 f0 b7 9e f9 cf c3 4e 6c 89 44 96 8f 99 f9 1f 98 2b f9 6f 58 82 16 70 ae 69 1f 50 d3 26 78 25 42 b1 35 3b 47 29 77 cf 79 f0 cd f0 d1 cd 1f 15 1e 31 68 9e 19 e8 72 3e 99 a3 ac 4d cc 5c f9 cc d1 ac 66 8b 93 f9 1f 4d 2a fa a6 ad 2c 8a 22 81 ea 66 04 50 69 71 cb 20 f3 1a 84 c8 ad 68 96 47 5f 6c ff 00 e2 59 f0 0d bc 0e fd 27 7e 29 f3 1d 3e 9e fa 7f 2d 7c 43 f2 8f 26 f8 eb a4 54 c4 a1 69 e5 d4 ab 34 a1 c9 7c f4 ea aa b8 35 53 f3 57 28 56 ea 95 46 d2 4a d3 eb 4b 21 5c e5 ea 1e 39 f0 2b c3 ee 4f f8 71 f8 56 e5 de 54 e7 7e 6b d2 fc 3f d5 fe 23 79 74 78 f7 f1 35 ce b5 d5 c2 87 5e e5 4f 87 3a 39 5e 83 c3 cf 09 39 78 c5 21 d4 65 e6 bf 19 35 56 14 51 50 50 c6 6b Data Ascii: k~_7> x;.uNlD+oXpiP&x%B5;G)wy1hr>M\fM*,"fPiq hG_lY'~)>-|C&Ti4|5SW(VFJK!\9+OqVT~k?#ytx5^O :9^9x!e5VQPPk
2021-09-28 23:13:29 UTC	56	IN	Data Raw: 4e 58 dc 60 6a 50 e2 0e 9a d4 53 55 51 bb 6a 1a 55 4e 97 5a 64 a4 a1 ae a6 d4 f9 93 49 ac d1 39 3e b5 19 65 1a 35 07 30 53 72 95 27 34 f3 d1 d4 d6 98 f8 6f e2 c0 d4 29 e9 75 fa 3a 1d 72 aa 37 45 58 16 ba 3a 9a 3a 25 a7 d2 95 a8 ea f4 9a 0a 28 69 27 9e 97 46 a3 ad a2 e9 56 e9 31 e8 15 0f 47 5c 34 8e 58 f0 c6 8e a7 56 d6 bc 24 d4 d8 6b 5c 97 af 73 0b 6b 7c 87 57 2c 42 38 8d 55 50 d4 4c d3 47 ac 69 e6 60 f2 73 26 9d 5f 45 43 a5 b8 a8 8e 39 e9 e8 aa f9 e3 4f d2 b9 5e 5a 99 4d 35 72 69 43 43 f0 eb 99 7c 23 94 a4 1a f8 ac d6 b9 af c3 0a d8 eb 32 8d 2c 96 a6 18 8e a5 2d 7c 74 95 90 b4 0f 57 ad 54 26 ad 53 3e 99 a8 50 41 a8 d1 d3 d7 08 75 ea 5a 9a 3a ed 4f 96 75 5e 6a fd 4b e1 7f 85 be 2c 2a ff 00 cc 1c 85 59 a5 d6 72 cf 3b de 86 26 32 65 1a 32 d7 63 f7 8c 71 e5 Data Ascii: NX`jPSUQjUNZdI9>e50Sr'4o)u:r7EX::%(i'FV1G\4XV$k\sk|W,B8UPLGi`s&_EC9O^ZM5riCC|#2,-|tWT&S> PAuZ:Ou^jK,*Yr;&2e2cq

Timestamp	kBytes transferred	Direction	Data
2021-09-28 23:13:29 UTC	58	IN	Data Raw: d6 8c d2 4d 3c 74 d0 41 0e bd a7 d7 69 5e 4b 5c a2 8d a5 58 7f fc ba a1 18 25 5a 03 f3 23 ca 5f ac b4 aa fa 2a ab 4b a7 44 c8 fd 17 81 69 a9 12 b5 60 b0 91 d0 d0 f2 e3 4d 20 8b 25 ca 35 90 a2 90 01 17 37 1f 42 1f a3 a3 99 eb 2b 8e a3 a4 d4 c9 3d 5d 22 e8 75 d5 da 54 b5 12 cf 24 94 7d 4a cd 19 75 88 d1 5a 0a 64 48 b5 0a 88 68 26 68 9e 26 29 2d 21 92 36 8c cf 30 93 d8 ed 95 54 ed 74 d0 dd 6a 2a ad c1 a1 ad a4 a8 91 b3 b5 9b 48 cc ac a8 04 99 24 12 64 61 ce 25 ad 27 8c f0 bb 1f 4b f4 75 66 90 ad a6 16 4d 79 7b d5 9a 4e 56 c5 49 43 43 79 b9 be f8 69 22 8a 23 1d 5b e2 bb 9a 89 df 58 e6 d5 e5 e5 f2 93 23 08 96 27 b8 06 6d 1e aa 92 c5 c8 be d6 16 ef 7b fb 8f ca c1 6c 46 f7 b8 b5 ad c1 0a c6 f9 5a d6 b0 22 e4 9b de f9 76 dc 13 e9 20 ed 73 f5 37 20 1c b2 b8 c7 b5 Data Ascii: M<tAi^K\X%Z#_*KDi`M %57B+=]"uT$}JuZdHh&h&)-!60Ttj*H$da%'KufMy{NVICCyi"#[X#'m{IFZ"v s7
2021-09-28 23:13:29 UTC	59	IN	Data Raw: 56 3d 4a 79 60 68 d1 1d 91 c7 46 44 47 12 12 8d 65 c6 fb 8b 02 58 0e 36 fa 4b 1d 44 49 34 40 98 a5 8d 59 03 29 42 50 e4 42 94 6b 14 37 b2 95 60 0a 96 ed 63 c3 07 77 69 8b c6 ca 55 d4 2c ac 54 f5 ae 15 cc 8a 45 da c1 98 ad de cd 92 df db 8a a1 91 dd 0b 3c 46 19 32 70 16 46 49 2f 84 8c 8a cc d1 96 05 65 51 99 dc b6 2c 14 ee 38 22 74 32 c9 00 94 41 d1 98 c6 ec 20 95 91 70 70 1b 18 d9 a3 c8 0f 52 a0 c9 6e 54 37 bd f6 51 e7 3c 86 7d 28 52 b5 a9 c9 10 19 0b 42 b3 95 36 53 35 94 b2 de c0 b1 03 6e 0d 27 9b f2 b6 aa 6a 6f 39 8b fa e1 59 05 38 25 df a2 71 90 87 6b 29 8c 48 32 01 88 7d 88 60 38 48 d7 54 5d 39 96 69 a9 ce a4 63 91 52 54 8c 8a 61 21 cb a4 5a 30 c2 e1 45 b2 2a aa 3d 8a bf cc 08 aa 91 75 31 40 92 47 0d 29 d4 0a c3 94 2d 21 f2 f9 12 bd 5b 48 08 b8 50 58 Data Ascii: V=Jy`hFDGeX6KDI4@Y)BPBk7`cwiU,TE<F2pFI/eQ,8"t2A ppRnT7Q<}(RB6S5n'jo9Y8%qk)H2}`8HT]9icRTa !Z0E*=u1@G)-![HPX
2021-09-28 23:13:29 UTC	60	IN	Data Raw: bf 0a 3a a4 b6 78 5b 36 08 13 21 f8 76 b2 99 0b 12 7a 80 fa 8e 1e 92 36 b7 b7 0c 33 c4 e4 54 b5 da d8 dc 00 99 1c 14 df 7c 84 78 ab 37 bb 5d 87 7e 08 a2 97 c0 16 55 0f 6d d4 12 57 2f 61 95 af 6f bd b8 ac 87 c2 e1 57 a9 86 c0 b1 c4 35 96 ea 4d b7 04 82 2f 62 40 be c7 22 38 65 ea f4 fd 78 19 6c 7e 5c 84 64 db 6b 5f d4 05 fb fb f7 b7 b7 11 84 85 4d 8a ac 98 90 ad b9 40 d6 1b 95 ee 54 9b 90 0e e2 fc 11 02 ad dc 05 25 98 33 0b db bb 20 6d c0 3d 93 3b 7d ed c3 30 63 8e 36 3b ef 7d ac 3e a3 eb 63 6d bb 77 fb 71 08 7b 5c 10 4f b6 57 b5 b6 bd c2 d8 dc ef 89 ca cb ee 0f 05 b2 db 1b 77 de f7 dc 7d 05 bd ef 63 73 b5 81 1e fc 11 46 04 90 3d b7 c8 fb 8e c4 5b f3 20 03 f6 bf 00 86 ba da d6 dc 9b 9d c3 0f 96 db 5e d7 ef b8 ef f6 e0 b0 6b ad bb 7b ff 00 11 fe fc 46 0d 75 Data Ascii: :x[6!vz63T|x7]~UmW/aoW5M/b@"8exl~\dk_M@T%3 m=;}0c6;}>cmwq{\OWw}csF=[^k{Fu
2021-09-28 23:13:29 UTC	62	IN	Data Raw: 8f 2e d3 d2 f3 17 27 34 13 34 11 8e d9 72 84 c9 ab 7c 38 7c 42 68 8b 59 af 41 51 a6 d1 e9 5c e8 a3 97 e8 a8 75 4d 66 68 74 c0 b0 49 41 4b a6 d6 23 51 57 8d 61 60 6d 2a be 85 e3 49 2a 34 da da 84 49 12 42 ae 3a 87 51 15 2c 94 73 43 24 f4 75 50 ce da 7b 8a 0a 5d 49 e8 f4 59 e1 d6 ab d6 9b 4f d2 34 5d 66 1e 9d 7d 07 2e f3 6e a7 4d 4d ca 9e 05 f3 db 74 b5 8e 43 a5 d0 f5 6e 5d e6 32 34 f9 ba ad 26 c6 f1 14 d7 9a 0c 7f da 5d 64 30 b4 02 1a ca 7a c8 a3 ab 8f 68 c9 01 a3 7b 9a d0 38 01 b8 18 c2 8b d0 b3 3d aa ed d6 dd 0d 2c db a1 d2 3d 5e bc 4f 66 a4 0e 05 b6 cd 3b ab 6d 16 5d 59 6c a0 82 3d 8c 10 51 c5 2d da b1 94 d4 ec 6b 22 82 38 84 70 b4 46 c0 06 a7 01 a2 34 f4 f0 e9 b2 d2 d6 40 69 74 94 d3 e4 d6 2b aa a4 a0 97 4a 13 d5 d6 72 2e ad a9 eb d2 2c fa 8a f2 8b 6a Data Ascii: .'44r|8|BhYAQ\uMfhtIAK#QWa`m*I*4IB:Q,sC$uP{]IYO4]f}.nMMtCn]24&]d0zh{8=,=^Of;m]Yl=Q-k"8pF4@it+Jr.,j
2021-09-28 23:13:29 UTC	63	IN	Data Raw: ba 63 20 11 95 c1 6b 10 0f 1e 0d 3f e3 39 ae af b8 d7 56 42 5c 64 92 8a 67 b5 b4 c2 5e 30 59 b2 38 e4 c0 77 e0 cb f8 18 07 38 59 6a 5f 46 ba db fc 90 4d d5 6e ac 6b fe a2 db 6a db eb 3a 83 41 dc eb e8 62 d0 95 b5 92 c2 5f ea d0 db e9 2d f4 75 ad b6 db eb 9c ca 8b 6c 6f aa 7d 4e ca 58 1b 59 34 84 c8 1f e9 17 23 78 b1 c8 9c f1 a9 a4 9e 2a 72 ce a4 ff 00 a9 e7 12 72 a4 14 34 d4 ba 14 54 72 d4 0e 95 7c 35 90 c9 5c 86 a3 4f 92 18 a9 84 70 cb 19 2a d0 8b e7 97 a7 de 4f 81 7e 5e e5 ba 8a bd 53 9f 79 2c 96 e5 7d 7b 96 8e 14 d6 a6 41 a2 6b 0f aa c1 49 5b a2 2c 14 df 87 0a 47 1e 90 2b 55 86 d3 79 cc b7 ee 7e 5c f9 16 57 7a c8 e2 8a 98 56 67 24 36 30 d1 41 0c a4 35 af 21 92 9f 42 08 19 63 27 25 92 65 c4 de cd db 8f aa 6f d1 c7 cb 95 1a 2f 82 da ae a1 22 4d 05 3e ad Data Ascii: c k?9VB\dg^0Y8w8Yj_FMnkj:Ab_-ulo}NXY4#x*rr4Tr|5\Op*O~^Sy,}{AkI[,G+Uy~\WzVg$60A5!Bc'%eo/"M>
2021-09-28 23:13:29 UTC	64	IN	Data Raw: ef fb fc f8 8e e2 df 41 7e fb ef df ed c6 23 b7 70 4f 7b d8 6f f7 03 82 22 ee bb 58 d8 0e e2 ff 00 9f b0 fd dc 61 cb 20 24 10 d6 fd f6 fa 7f bf f6 78 92 30 00 8e e7 6f b7 f3 ed c6 9f 2b d9 bb db ec 0d ff 00 a7 f1 fd ff 00 7e 08 b9 11 12 55 96 52 f2 06 85 96 21 14 22 30 1a 26 55 3d 52 d2 a9 26 4c d8 ab 0b 81 8d 88 17 bd f8 90 43 2a 87 eb cc 25 25 e4 74 70 98 08 a3 72 bd 28 dd 01 6b 98 d4 6e e4 8c fe 82 fc 64 41 19 50 e1 e5 92 7c a4 79 11 a5 c2 f1 a3 9f 4c 28 11 55 42 46 05 94 ee 4f ed 6e 38 90 c4 e8 ae af 3c b3 96 92 57 0f 26 21 a3 47 61 68 d0 22 20 09 1a 82 b1 fb 9b dc dc 8b 82 2c 7a 78 aa e2 a4 e8 d4 55 2c f5 41 65 1e 69 60 58 96 ec ce 22 6e 90 2c 3f 0e e8 48 cb 72 a3 b9 bf 15 c3 05 6a e9 e6 9e 6a d1 35 67 4e 55 f3 9d 20 a5 64 62 c6 27 11 7c ad 80 21 6c Data Ascii: A~#pO{o"Xa $x0o+~UR!"0&U=R&LC*%%tpr(kndAP|yL(UBFOn8<W&!Gah" ,zxU,Aei`X"n,?Hrjj5gNU db'|!l
2021-09-28 23:13:29 UTC	65	IN	Data Raw: 42 ab aa 15 62 4a 96 5b 82 23 8c 9d 42 d9 8e 99 55 02 3c 00 2a c0 b5 df 3b 92 c1 81 5f 49 0b 89 53 6b 83 b4 0b 20 77 26 4b a3 15 e9 a8 40 3a 60 00 18 16 c8 97 24 86 61 70 b6 b8 5f 60 49 0a fd 46 62 ed 81 55 02 32 13 10 41 6b c8 a4 26 64 b5 c2 b0 67 2a 31 5c 40 66 37 40 19 5d cf 51 98 3d 88 42 13 f0 f1 4b 5a 30 a8 19 83 11 91 2e ce 72 38 82 a9 b0 22 2b d4 52 e5 d8 32 b3 12 a2 d8 98 90 a8 18 5c 5f 33 95 c8 72 01 1b 7a 4f 0c 85 ac 72 60 c7 26 37 c7 10 14 b1 65 5b 5c fc 8a 42 df f6 b1 b9 b5 f8 4c 5c 67 93 b3 86 66 61 70 83 01 89 38 46 55 53 30 a5 09 f5 96 6b b5 8b 30 1b 18 d1 91 08 2e d2 36 4e c1 98 2a 92 19 8b 2a 80 a8 a3 14 04 22 12 a5 99 15 5d cb 39 62 48 9d 43 e1 8b 38 2f 6b 75 02 58 5e df 36 17 3d 8f b6 46 e0 77 df 8a c9 70 b6 bf e2 62 2c 6c 2c 5f 6d ca Data Ascii: BbJ[#BU<*;_ISk w&K@:`$ap_`IFbU2Ak&dg*1\@f7@]Q=BKZ0.r8"+R2_3rzOr`&7e[\BL\gfap8FUS0k0.6N* *"]9bHC8/kuX^6=Fwpb,l,_m
2021-09-28 23:13:29 UTC	67	IN	Data Raw: 68 ed 3d ad 6d 13 53 4f 51 a6 ba 9d d3 0b cd a6 eb 4a ea 69 cc 74 37 5d 57 6a b1 dd 4d 15 49 6c d1 18 ee 56 5b bd 65 14 af 89 c0 4d 45 53 33 3c 4f 0d ee 27 75 fc 35 18 a7 f1 4f 4c e5 ea 83 3c fa 0f 38 50 55 72 d7 31 69 6f ea a4 d5 28 35 0a 79 55 23 97 a8 ad 8c 91 d9 99 5e 12 8d 1c 98 3b 5c 29 b7 52 f5 59 28 b4 ed 4f 99 db a9 46 68 29 b5 4e 6f 95 35 28 29 2a 29 74 da ba 43 cc b5 1c 95 ab 57 9d 10 af e0 72 ed 53 51 d0 f8 69 aa f2 5c 21 6a f9 5f 50 fd 65 e2 8e 8e 91 c1 50 f5 5c 76 c7 e1 e9 61 a7 f1 6f c3 8a 87 e9 c4 64 e6 7d 2a 15 e9 e2 e5 92 ae 59 29 d9 56 ea 19 50 a4 a4 dd 4b 30 21 4d 85 9b 8e b5 73 ea 0a 7e 6d f1 09 24 d5 ab d2 a2 83 9f b9 c5 c6 b9 3d 08 5d 62 9f 51 83 5f d4 74 99 35 35 a6 31 79 74 d7 34 0d 2a a1 39 36 2d 3f a6 94 bc d7 e1 1d 76 ad ce 8e Data Ascii: h=mSOQJit7]WjMIlV[eMES3<O'u5OL<8PUr1io(5yU#^;\)RY(OFh)No5()*)tCWrSQi\!j_PeP\vaod}*Y)VPK0 !Ms~m$=]bQ_t551yt4*96-?v
2021-09-28 23:13:29 UTC	68	IN	Data Raw: 2c 49 e3 d1 dc 7c c2 ca ae c3 f8 51 04 93 6a fa 6c 40 c7 2c 8f 24 6f d5 69 a0 9d 50 5c 83 8f 4e aa b4 b1 16 b9 2d e9 37 3e c7 8f b2 3f 86 0e 5a a8 e5 4f 01 fc 36 d3 aa 17 0a ea 9e 5f 87 58 ae b2 aa 06 9f 5d 79 35 40 71 00 0f 4d 3c f4 d1 e4 ca 18 e0 7e bc 7c a0 7c 25 72 15 77 3c 78 8b c9 9a 05 34 55 32 7e bc d7 74 9d 2e cf 2c 92 8c 6b ab a3 86 47 16 a9 9d 48 8e 29 1e 76 60 96 54 06 fb 76 fb 30 a2 a3 83 4e a3 a3 a1 a3 8c 43 47 a7 d2 53 d0 d2 44 14 28 8a 96 96 24 82 08 82 8d 86 11 c6 8b 6f 60 2d db 8c 75 d8 8d b0 b3 81 c9 71 f2 3c 11 b7 e9 95 97 b5 45 83 2c 84 1c f6 19 1f ea ef 85 97 e9 fd af 9a c0 1e fd af b7 6f eb c4 f4 80 c5 7b fb 9d fe a0 7b f0 0d 88 b9 f9 88 ef ef 88 6d 87 e4 3d 87 d7 7e 08 00 ae dd cf df ef ef f4 ed ef fe 7c 61 d6 65 56 3e df d6 df cf Data Ascii: ,I|Qj|@,$oiP\N-7>?ZO6_X]y5@qM<~\|%rw<x4U2~t.,kGH)v`Tv0NCGSD($o`-uq<E,o{{m=~|aeV>
2021-09-28 23:13:29 UTC	69	IN	Data Raw: 47 f8 2e 2c 4f e5 65 a0 a7 d3 61 a0 7a 6a 39 11 a8 9b cc 75 08 9f aa b9 3e 42 a3 29 8b 12 a4 6e 18 66 02 95 1b 03 72 48 96 4d 3a 99 b4 b6 d3 9e 79 c5 3a 46 a8 f5 12 54 30 9c 22 b6 79 3d 49 52 2c c4 10 58 ad 8a fa 6c 06 c1 ab b4 f8 67 d3 d6 8d ea 27 81 14 40 04 f1 cc 52 6b 44 54 2d e4 fd a2 f6 01 89 b6 65 af dc 8e 29 7a 5d 1c 69 06 9d e4 8f f5 57 48 0c cd 4b 18 ca 67 70 dd 7c f2 36 93 b1 0f b9 f4 ee 2e 0d 95 f4 da 55 46 9c 90 56 3c 69 40 05 38 8d fa fd 25 c5 4a 88 02 cb 90 c8 30 b2 03 91 2c 0d ef 9f ab 82 27 ad a1 8e b1 20 8e 4a 8a 98 3a 13 c3 3a 3c 52 e0 f2 b4 63 d0 8c 6c 0c 8a e4 8c 94 0c 8d af b8 b9 e0 d4 d1 c7 51 35 24 af 2c d1 3d 1c c6 68 a3 82 56 48 a5 62 96 29 22 ae 62 51 8e e5 0b 0b 0e e3 72 38 1a 85 36 9d 34 54 a9 5e e8 b1 45 53 03 d3 65 39 88 19 Data Ascii: G.,Oeazj9u>B)nfrHM:y:FT0"y=IR,Xlg'@RkDT-e)z]iWHKgp|6.UFV<i@8%J0,' J::<RclQ5$,=hVHb)"bQr8 64T^ESe9

Timestamp	kBytes transferred	Direction	Data
2021-09-28 23:13:29 UTC	70	IN	Data Raw: 6e c1 41 39 5c 80 2e 49 3b 91 3e 00 ed b8 20 ad ec 48 6b ab 02 3e 87 73 60 de cd 7b 1b df 88 ca 1b 1b 96 16 6b 8c 49 17 36 22 cd 6e ea 41 37 07 6e df 6e 15 92 36 5b 30 05 43 29 1e a2 00 21 94 a8 04 11 fb 48 87 72 49 2a 2f 7e 19 82 9b 64 01 c4 86 5b 92 2c c3 60 45 88 bd af d8 dc 7d 47 04 44 8b db be c6 fb 7e 47 bf f5 fc c0 3d f8 42 88 18 31 36 20 11 f3 6c 6f de e0 f7 fd fc 33 2a 92 a4 f7 5c b1 37 b1 17 52 ad 6d ec 6e a4 82 08 3b 12 7e e2 1c 4f 7b 1f df fe 9d f8 22 00 2e 57 04 df 1b 5b 7b 5b ec 0f f5 e3 0b 53 d3 28 35 7d 3f 50 d2 b5 3a 74 ac d3 b5 5a 3a ad 3f 51 a3 9a cd 0d 55 0d 65 3c 94 d5 94 d2 23 7a 5a 39 e9 a4 96 37 53 b1 56 37 f7 e3 38 2a 03 71 de d6 ef 7d bf 2b f1 b3 fc 43 e7 ce 55 f0 b3 90 f9 d3 c4 ce 79 d5 60 d1 39 33 c3 fe 56 d7 79 cf 9b 35 6a a7 Data Ascii: nA9\.I;> Hk>s`{kI6"nA7nn6[0C)!HrI*/~d[,`E}GD~G=B16 lo3*\7Rmn;~O{".W[{[S(5}?P:tZ:?QUe<#zZ97SV78*q}+ CUy`93Vy5j
2021-09-28 23:13:29 UTC	72	IN	Data Raw: 6e 8b aa 5b 95 b9 7f 53 a3 e5 b6 10 c9 a6 bc 6b d4 1e 76 f0 df c6 df 0f 74 cf d6 1c e3 e1 9e a1 aa f2 9d 44 b4 d3 c1 e2 d7 82 d5 30 f8 ab c8 94 7a 6d 46 a2 75 c8 b5 6a 9a 7d 3e 7f f9 9b 4f a2 e5 ce 6b 89 f9 eb 4b a2 ae a0 af f3 88 e7 94 aa ea 53 95 0a 52 1e c3 f8 23 cd 9c 83 ce ff 00 09 be 22 e8 dc af cf 74 3a 8e bb a5 f8 91 a0 73 57 30 72 b3 d4 a0 a9 d2 28 57 50 e8 3e 99 a5 c2 ef 4b ab d6 43 55 ae c9 53 ad cb 53 a9 d3 c1 0d 21 d4 7f 55 c3 0c 34 34 74 91 25 db cd c2 96 be 96 85 d4 93 09 9b 1d ea d7 24 de 13 5c f7 c7 18 9f 6b 9c f8 f7 35 ed 03 6b 77 70 40 27 27 82 ae 75 c7 58 69 2d 77 d3 dd 19 5f a5 2f f6 dd 45 6c 6f 5a 7a 41 3d 65 55 96 68 ae 2e b7 43 16 b3 a1 97 c4 b8 53 b1 ae 9e 80 32 48 d9 04 82 a2 38 26 8e 69 a3 61 31 17 10 3b 01 e0 14 d1 d7 78 cd e1 Data Ascii: n[SkvtD0zmFuj}>OkKSR#"t:sW0r(WP>KCUSS!U44t%$\k5kwp@"uXi-w_/EloZzA=eUh.CS2H8&ia1;x
2021-09-28 23:13:29 UTC	73	IN	Data Raw: f6 bf f8 81 bf b7 df bb 7f 3e 08 88 21 85 c6 e0 ff 00 0e ff 00 eb c3 91 60 71 03 03 f6 16 fe 07 ef c4 18 81 7d cf d8 8b 5b e9 75 3b ed fc 4f 71 7e 0e 7f 51 e9 ff 00 eb 73 f9 85 da f6 3b 81 dc f6 3b df 82 24 26 fb ed ed ec 2d b7 db b7 fb f1 19 b6 f5 1d 8b 01 f5 f5 1e c3 ed fd 07 7e 15 d8 ec 40 36 f7 b2 dc fb 7b 0f a9 e0 dc f7 03 11 70 08 ee 49 20 0c 88 f6 db 62 77 b7 6e 08 8f 14 36 e6 ff 00 c3 b8 da fb 6d fe bc 58 ed 61 ed be df c6 fc 55 c1 14 e2 b6 7b 5b 1d fe bf 6f e6 38 8c f8 9b 5c 76 fe fd f8 a1 9a c3 62 2f fc 78 22 04 af ff 00 6f de 76 fe 3c 23 30 03 fc 20 f7 f7 bf fe 38 46 6c 47 df e9 fe a3 fb ff 00 4a 9d 8! bd 81 17 b0 ed c1 15 6f 23 1d 81 db f2 1d f8 c3 92 4d c8 3f 9f e6 6f ff 00 9f dd f7 b7 0f 29 b7 bd 97 ea 7f bf a7 18 32 49 62 4f 71 6d bf 8e df Data Ascii: >!`q}[u;Oq~Qs;;$&-~@6{pI bwn6mXaU{[o8\vb/x"ov<#0 8FlGJo#M?o)2IbOqm
2021-09-28 23:13:29 UTC	74	IN	Data Raw: 14 31 80 48 31 84 07 a6 12 fe 9b 95 f7 23 82 95 34 8d 42 b5 71 80 68 3c b9 94 5a 2c 54 c0 07 bc 38 86 55 20 91 81 41 7b 8b 0e 24 b3 d2 a5 27 98 94 af 93 e9 c4 de a8 f2 05 19 80 8e f0 e2 c4 83 94 76 0a b7 5c 77 b5 8f 04 56 d5 79 5e 94 7e 6b a0 62 ea c5 d3 eb 01 87 5b 20 60 09 df f1 0b db a4 17 d4 4e cb bf 0d 37 97 3d 0e b9 8b 2e b0 f2 dd 50 b9 1a 8e 9c 80 74 55 ac 7a dd 33 2d 82 fa c2 e7 b5 af c4 a8 9a 08 62 46 9e c5 1e 58 62 50 53 30 65 91 82 c5 b6 0d 8f ab b3 e2 02 fd 57 bf 09 34 91 a7 97 12 db 39 26 e9 c3 74 2c 4c c5 5d c5 8d 8f 4c e0 8e 73 36 00 5d 6f ea dc 88 b7 97 33 c3 d5 e8 f5 bf 17 cb 17 c4 4a 7d 23 ab d1 c8 e6 6d 18 05 f1 b9 0a 01 63 ef c3 9f 2f d7 40 5a 2f 34 22 93 a6 09 4e bf 43 28 c4 98 83 eb e9 07 58 b2 b0 c0 3e 37 b3 31 ba b4 91 89 23 8d ff Data Ascii: 1H1#4Bqh<Z,T8U A{$'v\wVy^~kb[`N7=.PtUz3-bFXbPS0eW49&t,L]Ls6]o3J}#mc/@Z/4"NC(X>71#
2021-09-28 23:13:29 UTC	76	IN	Data Raw: 8d 06 96 a8 4a 99 a9 ff 00 b5 04 a9 24 ad 1e 40 34 ae 14 c2 a6 d3 62 c6 3b 82 d7 2c 77 0b 6b 65 c6 50 9c c5 1d 4c 45 54 ad 92 9c f5 b2 75 79 2f 75 11 a8 78 f1 76 8c a9 b5 ae 43 0b 0c f1 3c 5d 66 09 f7 8c 64 7e 8a 31 2f 71 c9 1c 67 19 f8 7b 87 ef ba d4 ff 00 57 53 a4 90 07 26 57 6a 4f d6 73 24 8e 5a 66 57 05 a2 47 51 f8 62 32 48 36 50 18 5c b6 21 5d d7 8c 1f d5 b0 b5 38 86 4d a4 96 47 a8 78 d4 60 5d ac 4c 70 4b 1b 7a a1 8e 9f d7 d4 4c 5d 33 72 b9 34 2c 8e 5a 0a 97 71 54 ce 4c a2 55 a5 a4 69 64 b0 ab 4a 78 1d 64 78 53 10 cc 22 45 52 87 22 7d 52 03 db 2e 35 2d 43 50 f3 06 ba 76 e9 b4 cd 22 d3 89 11 44 6b 47 0a 36 26 08 00 6c 64 96 48 d4 97 92 e3 d0 6d ee 38 f4 82 d7 76 fa 0e 78 38 ee 0e 7b 83 e7 e6 bc c3 8b 86 d2 31 fe fe ff 00 98 3e 44 71 e6 3c f9 13 c2 bf Data Ascii: J$@4b;,wkePLETuy/uxvC<]fd~1/qg{WS&WjOs$ZfWGQb2H6P\!]8MGx`]LpKzL]3r4,ZqTLUidJxdxS"ER"}R.5-CPv"DkG6&ldHm8vx8{1>Dq<
2021-09-28 23:13:29 UTC	77	IN	Data Raw: 75 b5 13 19 cd bc d3 d4 53 09 a8 cf 8f bc 02 de ec 00 12 06 ef 6b 1b b1 9c ed 8c bd cd ee f0 d6 e0 9c cd 97 aa 9a 57 57 57 51 da b4 45 6b b5 3d e2 76 c3 35 55 0d 15 35 5b 0d 86 9d ee 1b a6 d5 4f 9a 08 ff 00 87 40 69 f6 28 ee 42 2b ad 4b 80 8e 96 df 3b 9c 4c 7f 7a df 08 9c 91 cf 3e 1c 7c 33 f8 2f ca 5e 27 4d 4c fe 24 52 72 36 97 a9 78 83 15 10 0b a7 69 fc ed cc a6 5e 66 e6 8d 0b 4b 00 2d f4 7e 5c d6 75 7a cd 07 46 72 0b be 97 a7 52 bc 87 aa d2 2a f6 25 a4 0b 60 01 3f 5f 7f e9 6f ef f9 29 66 3b 37 7f 7b f7 bf bd f7 ef f5 fb f0 bc 40 2e dc 4b 89 dc 4f 24 fc 4f 3c ae f0 d1 86 81 c7 61 8c 67 18 c0 3c 64 34 fe 6d 04 fb 87 64 73 2c 3e c7 da d6 ff 00 7e 07 13 89 c1 54 a0 ff 00 5f eb c4 e2 70 09 b7 d3 f7 f0 44 7b 1c be 96 fe 5b f1 78 37 00 d8 8f cf fc be dc 60 34 Data Ascii: uSkWWWQEk=v5U5[O@i(B+K;Lz>|3/^'ML$Rr6xi^fK-~\uzFrR*%`?_o)f;7{@.KO$O<ag<d4mds,>~T_pD{[x7`4
2021-09-28 23:13:29 UTC	78	IN	Data Raw: 51 77 76 18 9d a3 27 12 76 04 dc dc 0d cb d5 56 4d 4f 51 45 14 54 52 54 ad 54 c6 29 66 8d 94 25 32 80 b7 96 4b 82 70 00 de e7 15 2a 3d 2c 58 85 24 52 4a c8 e3 af a4 a4 30 ce f2 55 24 ec 92 ac 2c d0 c3 d2 4c c8 79 72 b2 17 50 db 00 01 db 2b de dc 31 ab 8f f5 97 92 30 54 19 0d 2f 5b ae 22 6e 80 5e a6 3d 33 30 23 d4 6e 4d 8d c5 c8 b8 ed c0 96 b2 64 ae a4 a5 4a 29 e4 86 a5 25 79 6b 14 7e 15 39 8d 6e a9 2d c7 76 1b 7c c1 95 99 00 56 0c 48 2d 53 37 9f 14 a2 92 6e 87 40 4b e7 2f 68 3a 86 4c 7a 26 c0 9c ed be e4 6d 6d ad 72 08 82 55 47 25 65 45 22 c1 2a b5 3c 50 ca d3 34 21 60 75 98 dd 62 8a 56 da 47 41 dc 5a eb 66 b1 18 db 81 05 52 54 54 55 42 b0 4a 8d 4b 28 89 a4 92 37 48 e7 2c 81 f3 89 cb 12 e8 00 39 1b d9 7d 36 02 fc 58 95 52 3d 5c f4 ad 49 34 50 c5 1c 4e 95 Data Ascii: Qwv'vVMOQETRTT)f%2Kp*=,X$RJ0U$,LyrP+10T/["n^=30#nMdJ)%yk~9n-v|VH-S7n@K/h:Lz&mmrUG%eE"* <P4!`ubVGAZfRTTUBJK(7H,9}6XR=\l4PN
2021-09-28 23:13:29 UTC	79	IN	Data Raw: e7 69 f5 2a 4e 41 d1 a2 83 5a a4 e6 2a 7d 5b 46 d6 93 4d d0 e9 ea 39 c3 47 a9 4a 9a 24 a6 ad 9a b9 60 89 2a 11 23 95 5b e4 bf 91 39 e3 e1 97 43 e6 27 d6 f9 53 f4 9a f2 0d 5d 65 4e 8d 51 cb 7a 9e 8b e2 77 c3 ed 66 9f a3 f3 06 97 59 26 72 53 6b 8d a4 ea 5a 14 2f 2b 85 92 09 6a a9 e2 a6 95 a0 9e 75 a8 ea 19 5c 8f 42 7f e2 85 f1 45 39 c7 e3 13 c2 af 0a 60 9a 39 28 bc 1a f0 26 83 53 ab 84 be 49 07 33 f8 a5 cd 3a be a9 a9 c3 2c 41 bd 0e fc b5 cb 5c 9b 3a 66 03 3c 75 08 6e 54 03 c7 c9 27 33 e9 e9 2c d2 c7 1a 43 1a 06 72 e9 1a d9 21 f5 85 4e a0 27 d2 a5 5e e4 0f a7 ee 31 6a 6d c6 b2 33 19 a9 a8 8d 92 0d a6 26 96 ba 22 49 04 10 c2 dc 87 03 82 3d a3 8e 3b 72 b8 97 54 3a 25 5b d4 f7 56 c4 fe a7 6b 2d 3f 67 ba 50 d3 d2 55 e9 6a 5b 6e 88 bc e9 97 c9 4d 23 24 6d 68 a0 Data Ascii: i*NAZ*}[FM9GJ$`*#[9C'S]eNQzwfY&rSkZ/+ju\BE9`9(&SI3:,A\:f<unT'3,Cr!N'^1jm3&"I=;rT:%[Vk-?gPUj[nM#$mh
2021-09-28 23:13:29 UTC	81	IN	Data Raw: 85 fb 5d 85 ec 34 86 89 7a 88 d2 82 91 3d 55 a1 11 2e 52 94 0a 0a 80 a8 4a e4 5a e0 b2 b0 75 b9 ba 8f 7f 3d 46 a1 cc 2c 92 e5 54 72 73 ba 2d 90 90 38 e0 10 d3 81 91 cf 1c e4 f6 54 3b a3 dd 40 ba 39 a3 52 7a 45 75 32 a5 b8 02 48 34 c5 a7 41 68 f8 5d 80 37 6d 9a 87 4c d7 dc a3 0f c6 4e cb a1 7b 70 d2 d7 b5 c0 e7 d5 3f fd 6f fd 15 1c 81 1b 45 c8 bf 06 be 32 78 c7 57 4f 21 30 ea 9e 30 f8 9d 43 a2 d2 49 2a ae 4d 3d 4e 9b cb ed 57 38 8c 3b 5f a4 f0 19 24 50 5b 35 56 b0 ae a3 f4 a5 73 07 27 c7 e4 3e 1b be 18 3e 18 fc 02 b4 4d 15 2e b3 a2 72 19 e7 2e 6c 85 00 b2 4a 39 83 9a 5c c5 d7 8d 06 46 58 e8 9d ba 80 15 88 d8 03 e5 c4 2a 55 22 57 53 1c 99 d5 ba b3 10 1a d8 30 5f a1 2e a8 d6 0a 42 b5 db d3 c0 01 8b 46 a9 22 c7 85 3a cb 96 c5 a5 0e 46 6a c6 d7 0c f7 f5 2b 75 Data Ascii:]4z=U.RJZu=F,Trs-8T;@9RzEu2H4Ah]7mLN{p?oE2xWO!00Cl*M=NW8;_$P[5Vs'>>M.r.lJ9\FX*U"WS0_.BF" :Fj+u

Timestamp	kBytes transferred	Direction	Data
2021-09-28 23:13:29 UTC	81	IN	Data Raw: 3f da 66 7c a0 9e f9 c1 3e ff 00 71 c7 c3 b2 93 1f a3 7f 4c a7 91 93 6a a1 ab fa 83 30 7e f7 7f d4 0d 79 ab f5 3d 1c 8e 3b 43 cc 96 7a cb b8 b1 b8 3b 68 71 61 b6 f8 61 c5 c5 ac 6b 4e d1 d8 9f 16 3e 26 fe 22 3e 22 ab fa 9e 35 78 c3 ce fe 20 53 07 8a 78 39 76 b7 56 96 93 95 a9 52 e4 b2 d2 72 e6 97 15 1e 93 04 41 2e 16 29 34 f5 62 41 28 4f 1f 41 3f f0 bd f8 3f 4d cd 7f a4 8f 4d e7 19 68 a1 78 7c 15 f0 17 c5 1e 7b a6 64 17 86 8f 56 e6 34 e5 ef 0a e8 4e 21 5c a9 1a 77 88 3a da c5 9d 40 95 0c 6c 42 8c 48 e3 e6 5f 40 82 33 56 af 9d dd 5b 10 b6 43 09 6f d9 39 2a 9c 4a 5c 98 c4 52 44 01 d8 a9 bf 1f 6d df f0 95 f2 30 ff 00 9d be 32 7c 41 78 ae 74 be 4b f0 73 93 29 ea 24 40 26 29 cc 5a e7 3d eb d5 b1 06 0a 4a c7 27 fc af a5 c8 c3 a8 73 31 c6 58 12 80 ac ed 91 c6 cd Data Ascii: ?f|>qLj0~y=;Cz;hqaakN>&">"5x Sx9vVRrA.)4bA(OA??MMhx|{dV4N!\w:@lBH_@3V[Co9*J\RDm02|AxtKs)$@&)Z=J's1X
2021-09-28 23:13:29 UTC	82	IN	Data Raw: b9 2a db 28 27 22 bb f7 dc db 55 fa cb af 48 69 16 9b ca f5 8f 9d eb 93 d4 10 91 65 e8 ee a1 9b 62 6e 41 60 2d f5 e0 88 c9 35 68 ae a5 8a 3a 55 7a 27 59 4d 4d 49 94 a9 81 d4 7e 14 69 15 c6 45 8e 21 9b 1d f2 b0 b5 bd 4e 65 ac 35 fd 0f 2a a2 87 cb 66 6b 8c 88 48 9c c8 14 45 d2 2a 5b e5 b9 24 7b 6f 71 6e 12 57 af 35 d4 a2 11 4f fa bd a3 97 cd 19 4b 0a 83 2d f3 8b a2 01 b1 17 dd 89 1f 6d b8 63 e7 8d 78 52 29 86 99 e5 cd d8 b3 0a 9f 33 91 b0 c7 75 e9 e3 ee 00 24 dc 5e f6 e0 88 45 2d 63 55 54 43 24 01 29 22 8e 37 82 ab aa 4b 4b 21 20 ba bc 42 c1 70 07 6c 6c 4e 3d c6 5e 96 82 7a a7 96 a5 27 a6 58 a2 49 51 69 a5 eb 75 1a a2 32 80 b4 8c 98 dd 31 3b 00 59 89 dc 5c 5b 71 19 ad f3 55 02 44 a6 f2 58 c6 69 8c 77 6a 93 2d 87 5d 25 46 05 42 ff 00 86 c0 dc 04 dc ee 03 43 Data Ascii: *('"UHiebnA`-5h:Uz'YMMI~iE!Ne5*fkHE*[${oqnW5OK-mcxR)3u$^E-cUTC$)"7KK! BpllN=^z'XIQiu21;Y\[qUDXiwj-]%FBC
2021-09-28 23:13:29 UTC	83	IN	Data Raw: a5 ad a8 e5 0a ad 49 42 fa 5d ab 5e 60 6f 21 3c 78 c3 cc d3 89 ea 25 66 e9 b2 c5 24 ae a6 35 ce cc 62 97 f1 48 52 0c c2 39 19 0e 07 61 61 62 16 f6 ec 37 89 7c e1 ab f3 76 a1 ac f3 4e b9 54 b3 6b dc cf a9 ea 9c cb ad d4 31 25 eb 35 8e 62 d4 6a b5 9d 4a a1 99 86 46 69 aa ab 65 96 59 09 bb 49 23 6d 6b 71 d5 7d 5a a7 a7 54 52 57 96 15 90 90 59 31 69 3a 6e 4b 4a 23 2c c0 02 62 8d ae cd d9 33 3d c0 e2 40 38 20 f7 c2 94 e7 e1 8c 2d ff 00 0b 40 fe 9e f0 ab d3 eb 8d 12 c6 d2 08 d6 28 63 ad 92 45 c0 f5 a4 92 9a 8d 28 e9 f3 7b 1d e7 32 e4 11 4d a3 3b 06 f5 10 34 8d 4d c4 f5 29 22 89 10 ad 49 88 14 65 3d 24 a4 d3 1a 32 80 ba 95 6c 0c 8f 6b 2b f4 ef 70 18 8b f0 91 c9 2b d2 ac 0a a8 af 55 e5 a1 37 5e a0 85 2a ea 7c da b8 6e a1 90 95 54 43 20 44 0d 26 cc 97 40 c7 8c 19 Data Ascii: IB]^`o!<x%f$5bHR9aab7|vNTk1%5bjJFieYI#mkq}ZTRWY1i:nKJ#,b3=@8 -@(cE({2M;4M)"Ie=$2lk+p+U7^*|nTCD&@
2021-09-28 23:13:29 UTC	85	IN	Data Raw: e2 80 ab 1a f4 d1 42 a8 3b 01 db fb 3d fb f7 e1 58 6f 97 d3 db f2 df 82 2b ba 80 77 db f7 8f f6 e1 83 ab 76 3d be e3 fd 78 c7 53 90 ed f6 e1 e2 89 99 b1 5d ef dc fb 28 fa 9e ff 00 5e 08 b2 00 24 d8 71 72 fa 40 51 da d6 23 eb 6e db fb 5a e7 6d ff 00 31 c1 11 2c 4a 15 7e e4 9f 72 7e a7 87 53 60 c7 f2 e0 89 76 de e6 d6 17 e0 12 58 de fb 10 3f 90 b5 ff 00 be dc 4e 27 04 53 8a 9d ff 00 64 1b 1f fc f1 19 af e9 b7 b9 fe 5b 7f 9f 08 36 00 7d 38 22 03 61 b9 bf df 84 67 02 ea 0f ab f7 7e 7f d3 ed c4 67 1b 80 77 1f 97 f7 fc b8 c5 61 63 b9 bd ff 00 77 04 4c c6 c2 d7 b9 3f bb ef fd 38 a9 9e c0 2d fb 6f 6b 77 fb 7d b8 84 d8 5f 8a 19 85 c9 da ff 00 4b fd b8 22 59 9a f6 da dd bf ad bf cf f9 71 86 ce 58 6f ed bd f7 ed c3 cb 20 1d fb 91 6f e3 71 fd ff 00 af 18 12 ca 08 d8 Data Ascii: B;=Xo+wv=xS](^$qr@Q#nZm1,J~r~S`vX?N'Sd[6}8"ag~gwacwL?8-okw}_K"YqXo oq
2021-09-28 23:13:29 UTC	86	IN	Data Raw: 30 de 2b 90 c5 14 a8 7b 91 d4 c4 83 6b f0 d4 90 cb 07 5c 4b 55 25 51 92 a1 e6 8c c8 88 bd 18 a4 b1 4a 75 08 48 65 8f 70 19 89 2d 7d ed db 89 4f 05 44 50 18 e5 ab 79 e6 26 52 2a 5a 34 56 5c d9 ca 01 1a 85 4b 42 19 42 5f 63 87 a8 1b f0 44 ab 15 60 a3 08 d3 c2 6b 84 05 7a e2 10 20 f3 1e d2 88 2f 6c 2f 6f c3 24 8d b8 33 43 54 f4 c1 63 9a 28 ea f0 41 d7 30 e5 10 71 86 6c 21 0c a6 cd f8 a1 57 31 8e 60 dc 91 6e 0c 74 f3 ad 10 a7 6a b9 1e a3 a5 87 9d 28 82 4e a5 8f e3 74 ec 63 24 1b 59 0a 95 fb f0 64 86 67 a6 30 ad 53 c5 37 49 10 55 22 23 3f 51 70 ca 4e 93 de 31 99 46 ba ee 00 90 db e5 17 22 69 d2 a1 a3 45 a7 96 38 9c 49 11 76 92 23 28 68 95 af 22 01 9a 95 76 5d 91 ee 4a 9d f7 3c 49 12 72 f0 f4 a5 48 d0 49 79 c3 23 33 49 19 0f 92 46 43 a9 46 2e 50 86 25 ec 8a ca Data Ascii: 0+{k\KU%QJuHep-}ODPy&R*Z4V\KBB_cD`kz /l/o$3CTc(A0ql!W1`ntj(Ntc$Ydg0S7IU"#?QpN1F"iE8lv#(h"v]J<IrHIy#3lFCF.P%
2021-09-28 23:13:29 UTC	87	IN	Data Raw: 39 6f 6b 71 aa c5 d0 4a 7a 39 25 85 ba c9 a6 ea 15 02 47 20 99 ba b2 82 c1 9c 7c f5 2e 7d 39 58 f4 d3 7b 76 e3 40 a2 96 29 29 15 a4 92 47 b5 2e a1 56 43 2b 04 32 21 c5 19 8d 98 15 b9 24 1f 55 c8 07 14 17 1c 6a 42 48 22 a1 12 ca ae f6 d2 22 8a 59 2a 73 21 63 aa 04 ac d6 0a 70 90 85 3d 00 03 0b 92 c8 77 e0 ae c6 f1 c9 3f 97 9f 91 cf d3 fa ad 7b 14 8d 23 c6 99 52 38 74 b4 00 2d ae 22 a9 7c 8a 42 32 fc 57 c9 8b 33 5f 12 4e e4 03 6e 34 ea 98 de 18 67 6f 30 49 fd 5e 90 ac 8a 43 dd 24 91 4a 46 b8 80 88 e6 dd 36 09 98 53 70 aa 48 37 b6 7a a8 a9 d2 43 d4 75 44 a5 a5 8c 3a c6 72 8c 30 50 ac 99 16 bb 3e cb ea f5 d8 6d 38 ec 34 4a ba f5 63 24 0a b1 f5 a2 91 23 4f 5e 10 5b d2 64 96 4b fa 12 50 ae 1d 96 42 06 c4 f5 4f ca 4a 89 00 3e d6 39 27 fa f2 9a 5a 87 83 a8 92 95 Data Ascii: 9okqJz9%G |.}9X{v@))G.VC+2!$UjBH""Y*s!cp=w?{#R8t-"\|B2W3_Nn4go0I^C$JF6SpH7zCuD:r0P>m84Jc$#O^[dKPBOJ>9'Z
2021-09-28 23:13:29 UTC	88	IN	Data Raw: 05 b6 f5 1f f1 1f f6 ff 00 7e 1d 88 36 b0 b7 ee 03 82 27 c9 48 24 fb 7d 6d fd fb 71 59 37 3b 0b 0e 07 13 82 29 c2 b3 00 0e fb f6 db db 82 4d b7 3c 50 6d 72 40 ee 6f c1 14 e2 a7 93 11 b5 ef 7b 7b 7d ff 00 3f e9 c1 76 f6 07 7e fb 1f cc 71 4b 36 de c4 df df 7f e3 c1 15 45 89 25 bb 13 c2 b3 5a d7 37 3f cf f9 ff 00 7f cf 80 49 0b 7d af fc bb f1 8d 23 ef ff 00 c8 da df 4f f3 f6 07 db 82 26 79 40 27 bd b6 db db b0 f6 df fa 71 8a d2 0d cf bf f7 fd 38 49 24 27 73 db df ea 7f a7 db fb b7 18 72 48 3b dc 81 96 e2 ff 00 4e fb 5f f8 0f 7e 08 8c b3 5c 82 4d ac 6c 76 17 20 1f b7 f7 fc f8 d3 64 90 b1 0a 81 9b 26 00 00 37 24 d8 00 2d 72 49 3d 80 dc fb 7b f0 25 90 b1 55 40 cc cc c0 00 01 24 92 42 85 16 f9 8b 1e c0 6e 78 de 3a 2e 8c 29 82 55 56 28 6a 86 00 a4 46 cc 29 c1 1d Data Ascii: ~6'H$}mqY7;)M<Pmr@o{{}?v~qK6E%Z7?I}#O&y@'q8I$'srH;N_~\Mlv d&7$-rI={%U@$Bnx:.)UV(jF)
2021-09-28 23:13:29 UTC	90	IN	Data Raw: b4 cd 21 3d 67 76 96 d3 b7 ad 4a b3 38 1e a1 80 b8 da dc 11 58 94 f8 d2 0a 43 51 52 47 4b a5 e6 9a 56 35 5d b7 97 af 86 5d 5f 70 f6 b6 d7 3d b8 2f 4e 65 a7 14 bd 7a 85 1d 34 8f af 1c a5 2b 09 42 0e 7d 50 0d 9d b0 19 be 06 e1 9c 1e e0 f1 5a 53 53 ad 17 92 52 fe 59 69 cc 4a de 61 9d fa 44 11 b4 c0 97 bd af f8 83 da e4 13 73 c1 92 9a 17 a3 34 b2 13 d0 31 45 1e 7d 56 47 55 8f a6 c8 4c f1 ba b7 aa cb ea c8 87 06 c7 82 2b e7 84 cc 8a 82 59 62 2a e9 26 70 b9 8d 9b a4 72 e9 97 b1 f4 49 f2 ba 90 43 ad d4 da f7 e0 c9 19 7e 8b 67 2a f4 a4 59 48 8d ca ac 96 46 4c 26 b0 39 42 73 c8 8b a8 2e a8 6f b5 8a d4 43 1c c9 1a 48 1f 15 96 39 14 23 ba 1c e3 39 26 4c ac ac 54 1e ea 49 c8 6d 63 c3 4b 1c 72 74 5a 40 7f 0a 55 96 30 19 94 75 02 3a 0c 82 c8 aa eb 8b b7 a1 cb a1 36 38 Data Ascii: !=gvJ8XCQRGKV5]]_p=/Nez4+B}PZSSRYiJaDs41E}VGUL+Yb*&prIC~g*YHFL&9Bs.oCH9#9&LTIm cKrtZ@U0u:68
2021-09-28 23:13:29 UTC	91	IN	Data Raw: 46 d3 36 8b ea 6e 98 d2 b5 97 ea 77 86 80 f8 58 d7 43 43 35 d2 1d cd f6 aa ed d5 95 11 b9 98 7b cb 5e 76 8e 8e 6a ff 00 a2 d3 e2 32 96 53 4f a5 eb 7e 1b f3 28 85 a8 cc 2d a7 eb 95 9a 54 46 18 9a d3 67 fa e6 96 9d 23 c1 ec 24 52 e4 36 ec ac 09 3c 6c 7a 8f d1 cb f1 61 0d 43 1f f9 47 94 a5 7a 69 2a a4 59 a0 e7 fe 59 c0 06 ce 35 31 e7 58 1c c7 2a 1b 32 b6 ea 0d 8a 8e 3d 7c aa f0 7f 91 39 2f c1 de 45 1a 84 5c c3 4b e2 27 8a d5 35 1e 21 c3 3e 8f e2 0f 3b c2 bc af e1 7c 2f 35 3f 2b 51 42 a9 a9 43 45 43 5b cc e9 3c 35 f5 80 40 16 28 e9 d2 14 a8 7f fb 8f a9 72 5f 84 3a 0a f2 bf 37 f8 b3 cc bc fd e3 15 2f 87 de 19 c5 a5 4d aa e8 d4 bc fd 5b 55 57 cd da b6 bb 5a 34 ad 2b 94 e8 ea ea 29 6b 6a a8 e8 56 aa 68 b5 2d 67 54 69 eb 6a 69 e8 20 71 00 a7 59 24 9d 32 6d af ba Data Ascii: F6nwXCC5{^vj2SO~(-TFg#$R6<lzaCGzi*YY51X*2=|9/E\K'5!>;|/5?+QBCEC[<5@(r_:7/M[UWZ4+)kjVh-gTiji qY$2m

Timestamp	kBytes transferred	Direction	Data
2021-09-28 23:13:29 UTC	92	IN	Data Raw: ba 76 93 7a 51 ea 7e 27 d1 73 25 36 9f a8 73 e7 86 6f c9 da df 28 4b 5d e3 67 36 a8 d5 e1 98 eb 74 13 d5 54 45 ca b1 51 47 63 a8 e8 cb c9 bc c3 a5 e9 14 cd ab 0a 69 a9 79 1b 4f d4 2b cc e3 52 d5 a0 59 f4 5a 7d 5f c6 8a d8 39 2e 6e 67 f1 3f c3 9e 55 e6 1f d6 0d a4 f3 66 9d a6 47 ac 4b 5b c9 5e 1c 50 53 2e 9c 93 72 ac 95 35 74 a4 6a 3a fd 76 8f 0b d5 e9 d0 1a ed 3a 86 7a 9d 26 94 c4 d0 d1 4c ab 79 9a 6e 36 6e 35 75 b5 b5 61 c0 67 7b fc 36 77 1c 61 bc 63 8c 7c f2 b1 d3 74 1e 92 f3 91 ad 7a 99 d5 8d 6b 11 d8 24 a1 b8 eb 29 ec d6 a9 03 30 d7 b5 f6 ed 39 4f 6b 88 c7 23 cb 8b 98 ed c5 d1 8d 8f 73 b7 92 b7 64 3e 36 f8 bf cd 3a 37 2d 8e 5c e5 3d 6f 47 e5 fe 6f d1 79 b3 59 d2 34 fe 5a d3 20 f0 d3 47 a4 d0 b9 3a 9e 3f d6 eb 51 59 d4 5d 76 8a 4d 4e bd ce 91 a2 51 cd Data Ascii: vzQ~'s%6so(K]g6tTEQGciyO+RYZ}_9.ng?UfGK[^PS.r5tj:v:z&Lyn6n5uag{6wac|tzk$)09Ok#sd>6:7-\=oGoyY4ZG:?QY]vMNQ
2021-09-28 23:13:29 UTC	94	IN	Data Raw: 9e fd af df f2 e2 39 56 16 ef f4 db b7 18 ec db 01 73 71 df f7 77 df f3 e0 89 99 ad b5 ae 4e fb ff 00 7f df d7 8c 67 36 b0 ec 7b ed c3 33 7d 4e f6 db df 8c 57 63 f5 37 ff 00 2d fd ff 00 3e 08 81 63 6b 12 72 fa ff 00 bf 7e dc 52 58 0e fc 37 14 bf cc 7f 77 f4 e0 8b 72 53 26 9e 95 d5 af 09 87 f5 83 2c 5e 77 16 bc d8 05 c6 13 22 96 38 ae 3b 2e c2 e6 e7 df 85 a5 8e 88 4d 5a d4 9d 13 3b d4 5e bf a4 d9 38 a9 0b 6f c5 50 4e 0f 88 f9 40 51 6b 6d c1 86 5a 27 ad ab 8a 05 8b cf 46 b1 1a c6 58 c0 91 91 81 e8 f5 24 2a 33 01 41 c4 64 6c 37 fa 71 91 45 26 9e d2 57 0a 61 18 9a 19 c2 ea 05 62 08 7c c6 39 5e 46 0a 3a ad 85 af 25 df 6d 8b 70 45 8f 43 15 1a c7 38 a0 e9 74 8d 44 c6 a0 42 e1 87 99 63 f8 f9 fa 8d 9e ff 00 3a ed 8e f7 03 7e 16 82 3d 31 34 f9 62 a3 10 9d 39 fa fd Data Ascii: 9VsqwNg6{3}NWc7->ckr~RX7wrS&,^w"8;.MZ;^8oPN@QkmZ'FX$*3Adl7qE&Wab|9^F:%mpEC8tDBc:~=14b9
2021-09-28 23:13:29 UTC	95	IN	Data Raw: 26 d7 09 91 8f 25 04 02 c0 12 09 5b 82 28 16 0e bb b8 11 f9 8e 9a 2b 91 8f 5b a4 0b 94 cb f6 c4 79 17 b1 3e 92 d7 17 24 58 45 58 04 92 94 11 f5 59 a3 eb 15 c7 a8 58 25 a3 ea 5b d5 7e 98 f4 06 ee a2 e3 61 c4 0f 0f 5d e3 18 f5 c4 68 cf 65 f5 f4 c9 70 97 6b 5c a6 41 ec 2e 40 6b 9b 02 77 2a d0 f5 25 0b 8f 51 4a 75 ac b6 6b e0 0a 64 6d ea f4 30 c4 dc d8 1b 0e f6 e0 88 2a c0 0c b8 04 b9 91 9a 5c 2d 7e a9 50 5c be 3d 9b 1b 13 7b 1f 7e fc 48 d6 10 a4 c4 10 ae 6e c7 02 0a 97 2e c6 4b e3 70 5b a9 96 43 fc 57 04 5f 6e 0a 18 98 c8 13 12 55 d9 65 c4 7e de 36 6c ac 3d 4d 8e d7 dc fe cf 7d b8 31 34 4c 97 88 ae 19 38 f4 8b 0c 95 d9 64 fa 58 e6 1b 23 dc b5 d8 92 4d c9 10 8c 43 d1 0b 18 8c 41 89 00 0c 7a 78 6f 7f fe 38 f7 bf b7 7b f0 18 41 d2 b3 04 e9 08 c0 f6 c3 a7 65 b5 Data Ascii: &%[(+[y>$XEXYX%[~a]hepk\A.@kw*%QJukdm0*\-~P\={~Hn.Kp[CW_nUe~6l=M}14L8dX#MCAzxo8{Ae
2021-09-28 23:13:29 UTC	96	IN	Data Raw: e9 dd 3f 87 04 e7 d6 18 1b 51 0c 52 c7 e3 ae a1 f0 f9 e3 57 26 53 3c 75 7e 14 73 9a a9 9c d5 57 6a 34 cd 0f 31 0a aa d9 11 12 b2 b6 5a 9d 26 bb 50 08 d5 0f 1f 5d a0 48 e9 e9 20 32 34 74 d1 47 17 a1 78 cf 51 5d 43 45 a8 31 ea fa 76 ad a7 c8 91 bb 79 7a cd 32 b6 3a b5 31 a9 60 91 ac 91 06 91 9a e5 2e 86 4c 8d a3 8e 27 23 7f 79 0c 29 57 3c 6c 35 09 a3 a8 66 0c f3 d3 d5 c7 48 8a 83 70 ee 22 82 59 5a 42 48 f9 65 55 ed 63 c5 b3 2e ab 4b 13 21 ad 3a a2 3a 5d 56 b5 60 ad 89 1d 5e e5 a2 5a 89 65 77 66 29 1f af a4 09 b7 ae e4 5f 8e 9b 47 d6 7b e4 71 b5 95 36 bb 7d 44 8d 69 cc ad 7c f0 17 60 7b 1f cb 6b 9d 18 39 c6 5d c8 23 27 6e 71 8f b1 34 ff 00 da 7f d4 ba 18 07 f1 2f 4e f4 7d f3 00 97 d4 5b 6b 6e 96 57 f2 5b b4 3a 07 3e ed 18 c7 62 18 e0 5c de cf 04 02 7e 5c 75 Data Ascii: ?QRW&S<u~sWj41Z&P]H 24tGxQ]CE1vyz2:1`.L'#y)W<l5fHp"YZBHeUc.K!::]V`^Zewf)_G{q6}Di|`{k9]#'nq4/N}[knW[:>b\~\u
2021-09-28 23:13:29 UTC	97	IN	Data Raw: cd f8 19 e1 87 87 9c b5 cc 14 b1 f2 d7 87 bc af cb ce 27 50 93 69 9a 40 ea d3 f5 65 0d 7f 33 57 35 64 c6 47 73 76 09 8b 36 45 98 93 f2 db 7f 52 e8 3d b1 49 6b ad 90 ed 2f 06 59 61 84 12 07 62 d6 87 90 3b f1 9e f8 ed 90 16 9b 72 fb 55 7a 68 fa b8 68 74 cf 4d f5 65 e2 6a c9 e2 a5 a5 7d ca be d9 69 88 ba 42 d6 35 d2 b6 2f bc a5 c6 5e 09 f0 ce fc 0c f0 ee 17 78 7f 44 57 83 1c d3 e1 b7 84 7c db ce bc df 5d cd 15 f5 9c fd 53 a0 43 a5 d6 73 44 30 d0 3d 4e 95 a1 d2 d7 cf 25 46 93 a3 44 8b fa b7 48 93 52 d6 eb 96 95 a5 32 54 55 e0 5e 49 1e 1a 7a 57 3e b4 b4 fb 7c bf 99 07 b8 fc ac 3b ff 00 b7 1b 13 c3 ca 24 d3 79 33 97 e8 c2 08 98 69 d1 49 2a db 02 64 72 ce 6e 3b 06 b3 02 6d bd c8 bf 61 6e 40 a1 a4 6a c7 3d c4 28 6d 23 f6 b9 ff 00 04 6c 43 02 c7 dc d8 84 1b 9d c8 Data Ascii: 'Pi@e3W5dGsv6ER=lk/Yab;rUzhhtMej}iB5/^xDW|]SCsD0=N%FDHR2TU^lzW>|;$y3iI*drn;man@j=(m#lC
2021-09-28 23:13:29 UTC	99	IN	Data Raw: 51 de 38 e2 33 3b 33 b8 03 f0 ac d7 01 8d ce d7 16 be c7 8b 27 ac 68 28 0d 69 a6 a8 72 21 49 5a 96 35 0d 50 4b 85 fc 2c 41 03 25 66 19 f7 00 2b 1b 6d c0 ab ac 7a 7a 35 aa 8e 92 a2 a5 8f 44 8a 78 96 d3 da 52 a0 97 5b 90 a6 30 d9 48 2f b1 04 70 45 5d 6d 6d 3d 22 d3 35 4c 12 4a b3 cf 0c 51 e3 4a f3 18 e4 90 16 8d a4 04 13 10 1d de 42 41 0c 6c 0e e3 8b 6a aa a1 a7 9a 8e 39 62 91 e4 ab 9d e1 a7 74 a7 32 a2 38 01 99 9e 42 2f 0a 11 e9 c8 5f de e4 63 70 b5 95 6f 4c 21 90 53 4f 50 66 9e 28 59 62 0a 5a 05 72 41 96 55 3b 05 5f 4e 44 01 8b 1b ed ec 6a 2a 5e 0a 8a 58 45 3c f3 0a a9 5a 37 92 15 1d 38 00 52 cb 24 ed ec a4 0b 0b db 72 38 22 0f 55 0a 57 52 d3 3c 72 19 6a 23 99 e2 95 61 2e 88 b0 80 19 5a 70 31 8f 21 6b 0b dd 86 e7 87 35 50 f9 ef 27 83 8a 8f 2c 66 12 f4 18 Data Ascii: Q83;3'h(ir!IZ5PK,A%f+mzz5DxR[0H/pE]mm="5LJQJBAlj9bt28B/_cpoL!SOPf(YbZrAU;_NDj*^XE<Z78R$r8"UWR<rj#a.Zp1!k5P',f
2021-09-28 23:13:29 UTC	100	IN	Data Raw: 08 ae 79 02 5b df 2d 87 d2 ea 43 ee 46 e3 e5 b8 fb 80 3b f1 e0 f7 e9 40 fd 02 1f 09 bf a4 66 4d 67 c4 8d 29 47 c3 ef c4 dd 65 33 37 fe b0 72 5e 8b 4f 57 a4 73 a5 4c 31 e3 04 1e 2c 72 52 cf a7 50 f3 66 4a 12 11 cc 74 b5 9a 4f 37 d3 44 b1 af eb 7a ea 48 13 4e 6f 60 7c 45 f1 83 95 bc 31 82 37 e6 5a c5 5a a9 d5 a4 a6 d3 28 91 ab 35 1a 85 8c 83 92 53 45 ea 48 89 04 09 66 e9 c6 cc 02 89 01 ed d2 0e 7a f8 fe d7 28 5e 58 79 23 c2 f7 9d 7d 62 3d 43 98 b5 1e 98 60 41 0b 2f ea fd 3c 3b 02 a4 f5 02 3d 62 dd 94 21 b6 5c 15 4d ce e0 40 e4 7e ff 00 7f bc fe 6c 3f 1f bf a1 5f e3 bb f4 7f ea 7a 96 a9 e2 f7 84 1a 87 33 78 57 4b 3b 25 1f 8f 3e 13 a5 7f 3c 78 53 51 4c 49 58 27 d6 f5 2a 3d 3a 2d 67 90 e7 9f da 87 9f 34 6e 5e 77 90 da 82 5a d8 30 a8 7f 28 a9 21 d5 b4 8a 88 35 Data Ascii: y[-CF;@fMg)Ge37r^OWsL1,rRPfJtO7DzHNo`|E17ZZ(5SEHfz(^Xy#}b=C`A/<;=b!\M@~l?_z3xWK;%><xSQLIX'*=:-g4n^wZ0(!5
2021-09-28 23:13:29 UTC	101	IN	Data Raw: 54 8c 6e 69 97 0d 54 05 a5 6b 9f fa 70 04 3b ee 9e fc 6e da 3f 8a 1f 8b dd 1c 51 c5 a4 fc 45 f8 dd 45 0e 9c e5 a8 63 87 c4 5e 62 64 81 c0 c4 74 92 5a c9 02 8f aa dc a9 da fc 5a ff 00 a6 55 11 1c 36 e9 4e 4e 3c e9 5d cf 6e 0b 9b 27 98 cf 21 ab 9a d7 fd 91 7a db 32 1b 7f 58 34 8c a0 e0 c6 da ad 2b 74 a5 c1 6e 71 bb 6d 7d c4 96 bb 80 e6 ef 20 67 77 b6 5b 87 fd f7 26 9f 25 e6 5a 5d 3e aa 9e 45 5c a3 99 a2 9d 31 00 10 c4 88 a0 19 38 55 25 55 c8 56 b1 39 6d 6e 35 11 a3 d5 54 c5 19 a9 a5 ae 32 c7 19 61 2c 91 47 d0 07 ff 00 de 09 11 5a 34 2b bf 6b db 70 78 f8 11 d4 be 31 be 35 35 3f d6 2b a9 fc 4b f8 e5 32 6b 51 a5 3e a2 c7 9f f5 98 96 64 52 85 63 68 e9 e5 54 8e 33 d3 5b f4 44 64 58 f6 0c d7 e3 4d 7b c7 9f 89 2e 65 89 a1 e6 2f 1c 7c 66 d5 e0 31 08 24 5a ff 00 11 Data Ascii: TniTkp;n?QEEc^bdtZZU6NN<]n'!z2X4+tnqm} gw[&%Z]>E\18U%UV9mn5T2a,GZ4+kpx155?+K2kQ>dRchT3[DdXM{.e/|f1$Z
2021-09-28 23:13:29 UTC	102	IN	Data Raw: e2 86 dd af f4 26 df d3 fa 70 44 0e d7 bf b7 7e 28 27 72 47 63 7f e1 c5 ac 47 a8 9e e4 7f af b7 ef e3 1d cd 87 e7 b7 f2 3c 11 57 23 0b 77 db de db 7d 2d f4 e3 0e 52 49 00 2b 11 fc ff 00 99 fb 9e 2e 63 bd bd 80 bf ef b5 c7 f9 71 88 dd cf e7 c1 16 ff 00 86 6a 89 64 a9 59 e9 8c 09 14 c5 29 dc ca b2 79 88 b1 53 d5 0a 09 31 a9 3b 04 6b 11 d8 a8 20 dd a9 66 99 d2 56 9e 9c d3 c8 b2 c8 91 a1 91 65 12 44 ac 02 49 94 77 0a 64 5b b0 43 f2 90 15 88 c8 10 b1 1a a3 25 48 9e 38 52 25 9a d4 8d 1b b3 3c 90 60 a7 39 94 81 d3 90 be 5e 91 71 8d bd f7 26 9b cd b2 39 aa 8e 14 7e b4 a2 15 85 d9 c3 c0 18 74 5d c9 be 2e e9 91 60 2e 14 81 b7 b7 04 59 14 b3 55 4b 4d d5 9e 90 d3 4c 03 b7 96 ea 24 86 ea cc 23 b4 91 82 87 a8 a1 58 dc 8c 43 90 77 53 c5 42 a2 b5 a8 1a ac e9 ec 2b 84 6c Data Ascii: &pD~('rGcG<W#w}-RI+.cqjdY)yS1;k fVeDIwd[C%H8R%<`9^q&9~t].`.YUKML$#XCwSB+l

Timestamp	kBytes transferred	Direction	Data
2021-09-28 23:13:29 UTC	104	IN	Data Raw: 85 4c 76 8c 2a 95 93 20 72 62 5b 24 c3 ba e2 02 9c 8d c1 ca c3 71 c4 0e e5 dd 5a 32 aa a5 7a 72 5c 38 90 15 bb 1c 54 e4 98 37 a2 cd f3 5f 25 d9 48 32 f2 75 48 c5 3a 58 ad 9b 22 64 2f ea cc 14 c4 2a a8 18 62 43 b1 6f 55 d5 76 e2 29 94 bc 80 aa 60 31 e9 95 62 59 81 52 5b 30 54 05 39 6c b6 2d 71 6b d8 b5 94 8a 2b 39 67 0c 98 80 c4 21 bd f3 4f 67 ff 00 e3 7f f0 9d c7 7e 19 4b 10 72 5c 08 66 00 16 0d 75 0c 42 bf a6 ff 00 3a 59 f1 f9 94 9c 5b 70 78 55 67 bb 66 a0 00 c7 10 a4 93 88 50 7d 79 04 b3 de f6 1d 8f 6b fb f0 54 b1 07 20 a0 86 70 31 2c c3 10 c4 29 b9 54 37 2b 6b d8 58 35 ec 48 e0 8a 2b 31 50 59 42 b9 1f f6 f3 06 c7 fc 39 8f 4e e7 f6 85 c7 f3 1c 02 ce 16 f8 7a f1 53 85 f6 c8 80 4a f5 3e 5b 03 71 9d ad e9 bd bd 43 80 32 2a 19 c2 ac 96 be 21 ce 37 1d 86 45 Data Ascii: Lv* rb[$qZ2zr\8T7_%H2uH:X"d/*bCoUv)`1bYR[0T9l-qk+9g!Og~Kr\fuB:Y[pxUgfP}ykT p1,)T7+kX5H+1 PYB9NzSJ>[qC2*!7E
2021-09-28 23:13:29 UTC	105	IN	Data Raw: 12 be 01 50 cc 3f 5c 49 ce fa d5 21 c4 c9 36 99 ce ba ce 8f 5e a8 6c 09 48 aa 2a 2b b4 f9 1f b9 dd a9 c3 0d 82 8b 5f 8e 6d e5 bf d0 ed fa 3a 79 a4 c1 4f cc de 34 f8 fd e1 75 54 9b 33 6b 1e 57 52 d2 12 4b 11 ff 00 f5 7a 4d 1f 98 19 63 63 65 33 cf 4b 0c 11 dc 3c 92 a8 cd 97 da 4e 67 f8 50 f1 27 42 49 27 a5 a1 a4 d7 a9 fa 8e a8 da 3d 5a 49 31 51 d4 21 8d 1d 42 c2 ea a6 c0 ad 99 ac 5a c6 e4 71 d6 9e 61 e4 7d 7b 45 a8 9a 9b 56 d2 6b b4 d9 e9 db 03 0e a1 49 35 39 4c 88 2c b9 30 08 c4 5c 13 be 36 61 de fb cc 6c cc 97 da 63 da ee dd 9c 3e 1e 59 cf 9a e8 76 ad 4f 61 be 30 3a d3 7a a1 ad dd ed 06 c3 55 19 95 bd b8 74 05 e2 66 9e 40 21 cc 1c 9c 1e 72 17 17 f2 6f fc 33 5f 06 7c ef a7 c7 aa 72 a7 c4 87 89 7c eb a5 48 a2 d5 1c bb e2 07 23 d6 c5 66 17 29 29 a7 e4 6a b9 Data Ascii: P?\I!6^IH*+_m:yO4uT3kWRKzMcce3K<NgP'BI'=ZI1Q!BZqa}{EVkI59L,0\6alc>YvOa0:zUtf@!ro3_|r|H#f))j
2021-09-28 23:13:29 UTC	106	IN	Data Raw: 11 06 16 00 85 16 0f b8 06 ff 00 31 e2 71 38 22 95 15 55 51 e8 cd 56 8f 17 9b 14 89 30 76 89 8c 5d 52 aa 49 e9 75 43 63 72 48 5e b5 c6 de b3 ee ba ad 55 4d 36 99 e6 29 de 34 9e f4 de a7 8b a8 96 92 44 57 02 32 eb 6b ab 10 be a3 8f dc f1 38 9c 11 3e ad 3d 45 22 52 98 1e 31 9d 75 24 12 67 08 70 d1 4c ec 24 0b ea 18 31 da cd 73 6b 5a db f1 2b 6a 67 82 a7 4d 8a 26 40 95 35 13 24 e1 d0 b9 64 58 d9 80 4f 5a 84 6c ae 4b 15 7e fd b8 9c 4e 08 8c 95 13 a6 a1 a6 d3 a1 8c 41 52 95 86 65 28 c6 42 d0 c2 b2 46 51 c4 8a aa 01 3e a0 63 72 7d 98 6c 38 66 a8 9f f5 92 41 78 bc b9 a2 69 f0 e9 b7 53 aa 27 58 ef d5 12 01 86 27 e4 e9 fe 64 f1 38 9c 11 14 9e 6f 3f 59 4e cc 86 18 a1 a7 78 ac 96 91 5a 56 a8 57 c9 cb 10 c3 f0 94 a8 c0 15 fa 93 bf 0f 0c b3 09 ab 63 91 91 d6 1a 88 a3 Data Ascii: 1q8"UQV0v]RIuCcrH^UM6)4DW2k8>=E"R1ugpL1skZ+jgM&@5$dXOZlK~NARe(BFQ>cr}l8fAxiS'X'd8o?YNx ZVWc
2021-09-28 23:13:29 UTC	108	IN	Data Raw: e7 9e 08 c7 23 9f d7 e0 bb df 43 f5 15 ee ea fb 95 15 ca e5 55 5d 4d 49 1b 7d 5d 95 2f 13 3a 2e 5b da 57 83 31 1c e0 07 48 40 1c 01 80 16 d6 a7 a5 11 d6 c1 51 4f 24 b4 b5 94 b3 2c f4 d5 b4 92 49 4d 57 4b 2a 9c a3 92 96 a2 17 49 69 de 36 40 51 91 ee 0e df 29 65 6f 5b 3e 0a 3c 77 f1 03 9e 35 8d 53 c3 ae 74 d4 cf 31 c1 a4 72 d0 d6 b4 bd 7a b1 51 35 98 a3 a7 ab 8a 91 e8 6b 65 89 02 6a 0a eb 32 ba 55 48 23 9e 33 19 0e 67 cf 25 9c 4e 32 38 1b 33 e7 ff 00 da fa 23 00 c2 49 ef b7 bf ca 46 8f e8 57 a3 2a 4b 38 4d 85 da d7 b1 fe 97 ff 00 3e 37 e5 25 2c 54 50 05 8c 02 cf 66 92 42 3d 4e c4 7b 9b f6 16 01 57 b0 1f 5e 27 13 8a 15 85 71 df 7e 19 45 cd b8 9c 4e 08 a3 2d 89 fc af fc ed c2 fd 3e df f9 e2 71 38 22 9c 4e 27 13 82 2a 58 dc 9f b6 df cf 85 3b 02 7e 9c 4e 27 04 Data Ascii: #CU]MI}]/:.[W1H@QO$,IMWK*li6@Q)eo[><w5St1rzQ5kej2UH#3g%N283#IFW*K8M>7%,TPfB=N{W^'q~EN->q8"N'*X;~N'

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 6680 Parent PID: 6452

General

Start time:	01:13:17
Start date:	29/09/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\vZ1WZMpxTY.dll'
Imagebase:	0x7ff71d180000
File size:	1136128 bytes
MD5 hash:	E0CC9D126C39A9D2FA1CAD5027EBBD18
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000000.00000002.371714871.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 6236 Parent PID: 6680

General

Start time:	01:13:18
Start date:	29/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\vZ1WZMpxTY.dll',#1
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: regsvr32.exe PID: 4292 Parent PID: 6680

General

Start time:	01:13:18
Start date:	29/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\vZ1WZMpxTY.dll
Imagebase:	0x7ff65cec0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000003.00000002.445132804.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 4308 Parent PID: 6236

General

Start time:	01:13:18
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\vZ1WZMpxTY.dll',#1
Imagebase:	0x7ff7747a0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000004.00000002.349426378.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: iexplore.exe PID: 2288 Parent PID: 6680

General

Start time:	01:13:19
Start date:	29/09/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Internet Explorer\iexplore.exe
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 1352 Parent PID: 6680

General

Start time:	01:13:19
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\vZ1WZMpxTY.dll,BeginBufferedAnimation
Imagebase:	0x7ff7747a0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000006.00000002.351510328.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: iexplore.exe PID: 6948 Parent PID: 2288

General

Start time:	01:13:19
Start date:	29/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2288 CREDAT:17410 /prefetch:2
Imagebase:	0xa10000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Registry Activities — Show Windows behavior

Analysis Process: explorer.exe PID: 3440 Parent PID: 4292

General

Start time:	01:13:20
Start date:	29/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Analysis Process: rundll32.exe PID: 4000 Parent PID: 6680

General

Start time:	01:13:22
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\vZ1WZMpxTY.dll,BeginBufferedPaint
Imagebase:	0x7ff7747a0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000009.00000002.358519886.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 3424 Parent PID: 6680

General

Start time:	01:13:26
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\vZ1WZMpxTY.dll,BeginPanningFeedback
Imagebase:	0x7ff7747a0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000000A.00000002.365502864.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: slui.exe PID: 2680 Parent PID: 3440

General

Start time:	01:14:04
Start date:	29/09/2021
Path:	C:\Windows\System32\slui.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\slui.exe
Imagebase:	0x7ff61d6c0000
File size:	445952 bytes
MD5 hash:	96A8EF9387619D17BB30B024DDF52BF3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: slui.exe PID: 6376 Parent PID: 3440

General

Start time:	01:14:07
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\qklwjLaE\slui.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\qklwjLaE\slui.exe
Imagebase:	0x7ff69ed30000
File size:	445952 bytes
MD5 hash:	96A8EF9387619D17BB30B024DDF52BF3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000014.00000002.475371299.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: FileHistory.exe PID: 5972 Parent PID: 3440

General

Start time:	01:14:19
Start date:	29/09/2021
Path:	C:\Windows\System32\FileHistory.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\FileHistory.exe
Imagebase:	0x7ff75fbc0000
File size:	246784 bytes
MD5 hash:	989B5BDB2BEAC9F894BBC236F1B67967
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: FileHistory.exe PID: 5088 Parent PID: 3440

General

Start time:	01:14:20
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\1QHnh\FileHistory.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\1QHnh\FileHistory.exe
Imagebase:	0x7ff7b5960000
File size:	246784 bytes
MD5 hash:	989B5BDB2BEAC9F894BBC236F1B67967
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000017.00000002.484447780.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: PresentationHost.exe PID: 4780 Parent PID: 3440

General

Start time:	01:14:23
Start date:	29/09/2021
Path:	C:\Windows\System32\PresentationHost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\PresentationHost.exe
Imagebase:	0x7ff6aed40000
File size:	259072 bytes
MD5 hash:	E3053C73EA240F4C2F7971B3905A91CF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: PresentationHost.exe PID: 5408 Parent PID: 3440

General

Start time:	01:14:24
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\gKsll\PresentationHost.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\gKsll\PresentationHost.exe
Imagebase:	0x7ff6d6060000
File size:	259072 bytes
MD5 hash:	E3053C73EA240F4C2F7971B3905A91CF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000001A.00000002.511241527.000001B521501000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: SystemPropertiesAdvanced.exe PID: 5876 Parent PID: 3440

General

Start time:	01:14:36
Start date:	29/09/2021
Path:	C:\Windows\System32\SystemPropertiesAdvanced.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SystemPropertiesAdvanced.exe
Imagebase:	0x7ff714cb0000
File size:	83968 bytes
MD5 hash:	82ED6250B9AA030DDC13DC075D2C16E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: SystemPropertiesAdvanced.exe PID: 5952 Parent PID: 3440

General

Start time:	01:14:37
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\rUhH1WSzx\SystemPropertiesAdvanced.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\rUhH1WSzx\SystemPropertiesAdvanced.exe
Imagebase:	0x7ff6683d0000
File size:	83968 bytes
MD5 hash:	82ED6250B9AA030DDC13DC075D2C16E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000001C.00000002.538817965.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: Magnify.exe PID: 6120 Parent PID: 3440

General

Start time:	01:14:49
Start date:	29/09/2021
Path:	C:\Windows\System32\Magnify.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\Magnify.exe
Imagebase:	0x7ff74fc90000
File size:	809472 bytes
MD5 hash:	F97BE20B3744572366666607EE4BA7F7F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Magnify.exe PID: 5428 Parent PID: 3440

General

Start time:	01:14:50
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\N8qUdj\Magnify.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\N8qUdj\Magnify.exe
Imagebase:	0x7ff7a1cf0000
File size:	809472 bytes
MD5 hash:	F97BE20B3744572366666607EE4BA7F7F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000020.00000002.565898043.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Disassembly

Code Analysis