ID: 492099
Sample Name: FROqdaZTXE
Cookbook: default.jbs
Time: 11:08:05
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

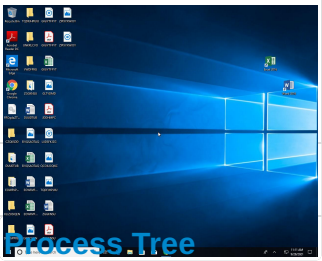
Windows Analysis Report FROqdaZTXE

Overview

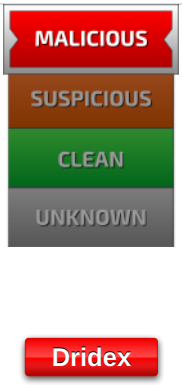
General Information

Sample Name:	FROqdaZTXE (renamed file extension from none to dll)
Analysis ID:	492099
MD5:	24628d042b24cc..
SHA1:	0deb91aa0e4c63..
SHA256:	2c1cbd4e7a27c4...
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

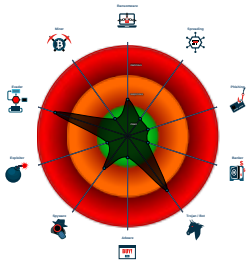


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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...

Classification



- **System is w10x64**
- loaddll64.exe (PID: 6312 cmdline: loaddll64.exe 'C:\Users\user\Desktop\FROqdaZTXE.dll' MD5: A84133CCB118CF35D49A423CD836D0EF)
  - cmd.exe (PID: 6344 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\FROqdaZTXE.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6396 cmdline: rundll32.exe 'C:\Users\user\Desktop\FROqdaZTXE.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - regsvr32.exe (PID: 6380 cmdline: regsvr32.exe /s C:\Users\user\Desktop\FROqdaZTXE.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wlrmdr.exe (PID: 3060 cmdline: C:\Windows\system32\wlrmdr.exe MD5: 4849E997AF1274DD145672A2F9BC0827)
      - wlrmdr.exe (PID: 6320 cmdline: C:\Users\user\AppData\Local\BAz\wlrmdr.exe MD5: 4849E997AF1274DD145672A2F9BC0827)
      - isoburn.exe (PID: 4012 cmdline: C:\Windows\system32\isoburn.exe MD5: 46A0538BD86F949DF1E40802AB6BFFC7)
  - iexplore.exe (PID: 6444 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - iexplore.exe (PID: 6528 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6444 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - rundll32.exe (PID: 6476 cmdline: rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DllCanUnloadNow MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6708 cmdline: rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DllGetClassObject MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6896 cmdline: rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmAttachMilContent MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 7044 cmdline: rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmDefWindowProc MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 7104 cmdline: rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmDetachMilContent MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 804 cmdline: rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmEnableBlurBehindWindow MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6700 cmdline: rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmEnableComposition MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 7124 cmdline: rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmEnableMMCSS MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 7156 cmdline: rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmExtendFrameIntoClientArea MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5212 cmdline: rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmFlush MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 1000 cmdline: rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmGetColorizationColor MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6748 cmdline: rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmGetCompositionTimingInfo MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6764 cmdline: rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmGetGraphicsStreamClient MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 1256 cmdline: rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmGetGraphicsStreamTransformHint MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5340 cmdline: rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmGetTransportAttributes MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5284 cmdline: rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmGetUnmetTabRequirements MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 3952 cmdline: rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmGetWindowAttribute MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 3232 cmdline: rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmInvalidateIconicBitmaps MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 7112 cmdline: rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmIsCompositionEnabled MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6148 cmdline: rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmModifyPreviousDxFrameDuration MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000020.00000002.357565041.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000018.00000002.306023387.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000017.00000002.298078907.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
0000001C.00000002.328825836.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000028.00000002.392891461.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	

Click to see the 19 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

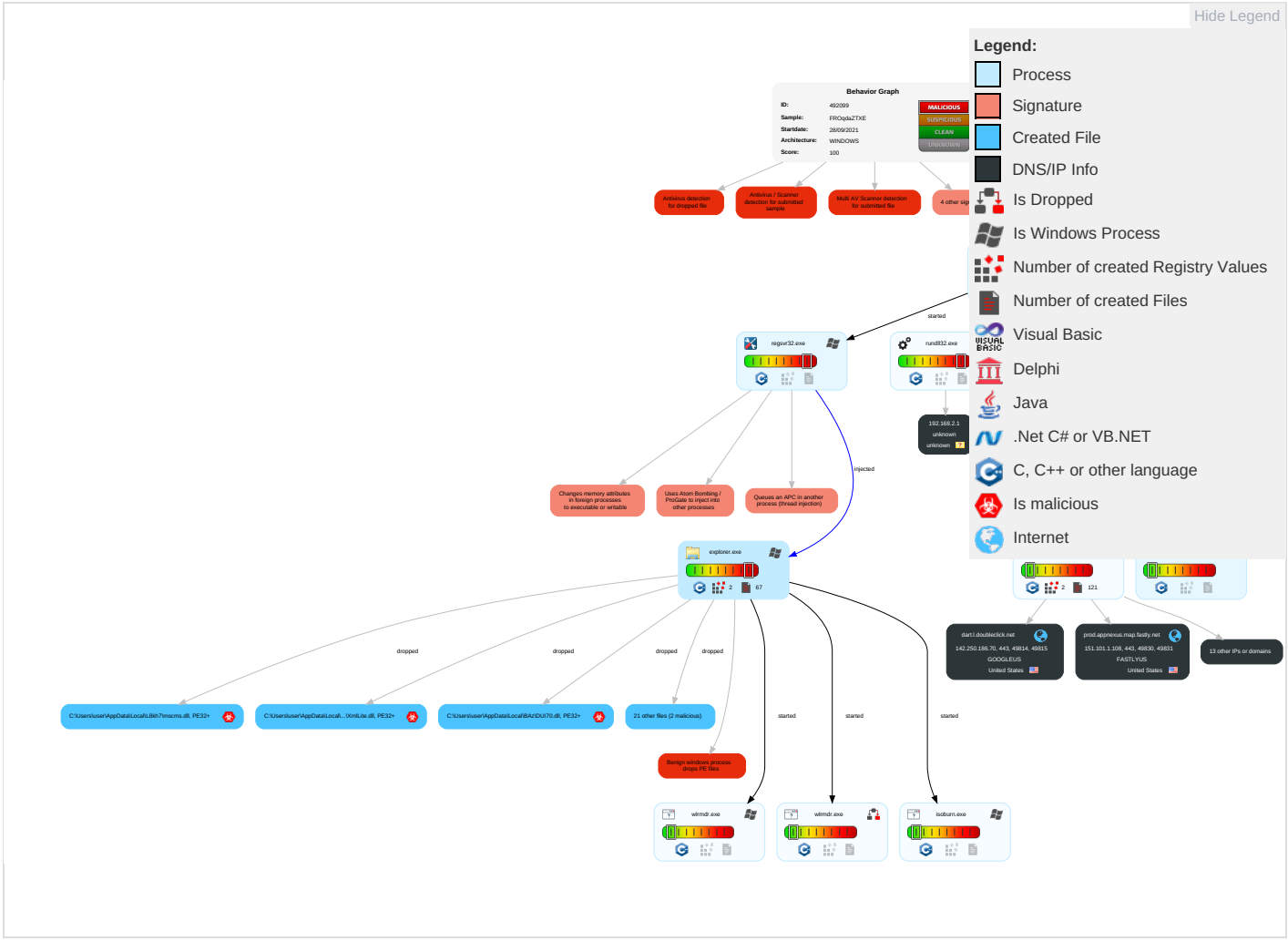
Queues an APC in another process (thread injection)

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	Command and Control	Network Effects
Valid Accounts	Service Execution 2	Windows Service 1	Windows Service 1	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop Insecure Network Communic
Default Accounts	Exploitation for Client Execution 1	DLL Side-Loading 1	Process Injection 3 1 2	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS Redirect P Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Process Injection 3 1 2	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Regsvr32 1	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rundll32 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming c Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Access Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	System Information Discovery 2 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cel Base Stati

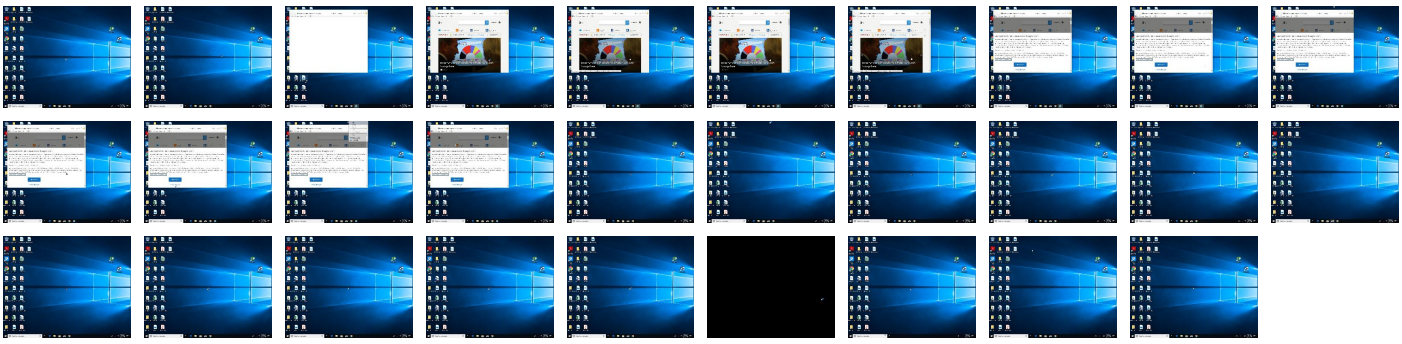
Behavior Graph



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
FROqdaZTXE.dll	69%	Virustotal		Browse
FROqdaZTXE.dll	66%	Metadefender		Browse
FROqdaZTXE.dll	78%	ReversingLabs	Win64.Infostealer.Dridex	
FROqdaZTXE.dll	100%	Avira	HEUR/AGEN.1114452	
FROqdaZTXE.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\BAz\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\37sFQt\WMsgAPI.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\4w8kc\VERSION.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\BmHMcHp\XmlLite.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\L8kh7\mscms.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\BAz\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\BAz\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\37sFQt\WMsgAPI.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\4w8kc\VERSION.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\BmHMcHp\XmlLite.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\L8kh7\mscms.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\BAz\DUI70.dll	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\37sFQt\consent.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\37sFQt\consent.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\4w8kc\psr.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\4w8kc\psr.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\BAz\wlrmdr.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\BAz\wlrmdr.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\BmHMcHp\printfilterpipelinesvc.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\BmHMcHp\printfilterpipelinesvc.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
30.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
31.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
42.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
33.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
29.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.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
27.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.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
20.2.rundll32.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
26.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
23.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
37.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
32.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
34.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.2.wlrmdr.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://crcdn01.adnxs-simple.com/creative/p/11655/2021/9/15/28299829/89a22c36-158b-411c-9c2c-269457db6c00.jpg	0%	Avira URL Cloud	safe	
http://https://ad-delivery.net/px.gif?ch=1&e=0.5327400408745451	0%	Avira URL Cloud	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	23.211.6.95	true	false		high
dart.l.doubleclick.net	142.250.186.70	true	false		high
hblg.media.net	23.211.6.95	true	false		high
lg3.media.net	23.211.6.95	true	false		high
prod.appnexus.map.fastly.net	151.101.1.108	true	false		high
btloader.com	104.26.6.139	true	false		high
geolocation.onetrust.com	104.20.184.68	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ad-delivery.net	104.26.2.70	true	false		high
web.vortex.data.msn.com	unknown	unknown	false		high
www.msn.com	unknown	unknown	false		high
ad.doubleclick.net	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://ad.doubleclick.net/favicon.ico?ad=300x250&ad_box_=1&adnet=1&showad=1&size=250x250	false		high
http://https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location	false		high
http://https://crcdn01.adnxs-simple.com/creative/p/11655/2021/9/15/28299829/89a22c36-158b-411c-9c2c-269457db6c00.jpg	false	• Avira URL Cloud: safe	unknown
http://https://ad-delivery.net/px.gif?ch=1&e=0.5327400408745451	false	• Avira URL Cloud: safe	unknown
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
151.101.1.108	prod.appnexus.map.fastly.net	United States		54113	FASTLYUS	false
104.26.2.70	ad-delivery.net	United States		13335	CLOUDFLARENETUS	false
104.20.184.68	geolocation.onetrust.com	United States		13335	CLOUDFLARENETUS	false
142.250.186.70	dart.l.doubleclick.net	United States		15169	GOOGLEUS	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:	492099
Start date:	28.09.2021
Start time:	11:08:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	FROqdaZTXE (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:	42
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@78/116@12/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 23.3% (good quality ratio 19.8%) • Quality average: 78.8% • Quality standard deviation: 37.2%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
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\37sFQt\WMsgAPI.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2142208
Entropy (8bit):	3.5302448175650736
Encrypted:	false
SSDEEP:	12288:VVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:MfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	A0DFB705E2F217B1D21FB110D877C900

C:\Users\user\AppData\Local\37sFQt\WMsgAPI.dll	
SHA1:	F91A4D053C34DCF499AB61B102A6C2A8D7F7C3A6
SHA-256:	D25C0C43B412568A7D61AF56494413D2C6620A661CF0BD3E8BCBBB2A4140B312
SHA-512:	E3DA8898B1550FAE7522A960F4C96F9C12C1FC83737211EE1326883B0C77EA2ADF7F56C58A3835AE8B42FC4F6E88DC424D53212EB42DDD88D1A00452F0C9793
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\37sFQt\consent.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	157080
Entropy (8bit):	5.924344092826888
Encrypted:	false
SSDEEP:	3072:4eana1Hze2vHL+u5F28BrciRXBis72z5B+o:Aa1TfD+u5F2wrTio2z2o
MD5:	74D31E4F51873160D91B1F80E0C472D0
SHA1:	35DEC0D1A12C6F1F7A460E3AE75E4D74D5BD815A
SHA-256:	113813A699063EBF391D436A4EFE0B6F95F81E12AF773FABE5511B5CA08E189C
SHA-512:	F026CBBDF3792A05091B3CC0A97F825D353BC5FF9AB7248F4544B81BA2F86FD28CEB04468D755715BB3BD220BB72781DC079423D912A56E3793AC1687AEE7E0
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_GE.>)..>)..>)..F..Y>).rZ*..>).rZ-..>).rZ,..>).rZ(..>)..>(.9?).rZ'..>).rZ...>).rZ+..>).Rich.>).....PE..d...i.7.....".....H.....C.....@..... .....PP..\.....h....D...!.....0%..T..... .....(...(...HL.....text..... ..`.rdata...c.....d.....@..@.data...l.....h.....@....pdata..h.....j.....@..@.didat. .....x.....@...consent.b.....z.....@....rsrc.....|.....@..@.reloc.....B.....@..B.....

C:\Users\user\AppData\Local\4w8kc\VERSION.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2142208
Entropy (8bit):	3.5314087045197344
Encrypted:	false
SSDEEP:	12288:AVl0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:lfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	2C9295C58901A934493A7660685F9B71
SHA1:	0C2372FCC3F523C4DF09FFF39A009832C8A8D494
SHA-256:	8432076EBF2DD802D366094CD571F32C751B707D2BCA1D89D88C811DB0F35811
SHA-512:	B28AB1AAF7CFF81167C514C676F87062C50BF3262E7EB03488703B6EFD570B30A4210D1B42496ED4AA333E1B628655AB449E6313C4EBFAE14F21D9A83D677583
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\4w8kc\psr.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	600576
Entropy (8bit):	6.4861677167766665
Encrypted:	false
SSDEEP:	12288:B2mS50ICmAX+ASa8wd9Nkmw6cD8pellpco//EH1:B2mlmeFSa8wd9NStApeCoXEH
MD5:	3B8262EB45E790BF7FA648CEE2CCCB7B

C:\Users\user\AppData\Local\4w8kc\psr.exe	
SHA1:	EDDD81D1B3FD2EE99E42A43B25BD74D39BB850BC
SHA-256:	D1225E9FD2834BD2EF84EADAA4126020D20F4A0F50321440190C3896E69BD5D8
SHA-512:	A3709D39372CDB6D9C9E58932144CE8BA437C2134EFC9BCD2531708C1515CBAEA5929C220DF25D76785F7594BC5F8541E6ED5330EA3CA12E87C4DA5A2171C45
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....$.....}.....x.....x.....x.....x...x.....x.....xR.....x.....Rich..... ....PE..d....S.....".....`.....@.....h.....`..... .....7.....L.....D.....T..... .....X...8....7..@. .....text...5..... ..`.rdata.....@..@.data....m...`.....H.....@....pdata..L.....T.....@..@.didat.....j.....@....rsrc..... .....l.....@..@.reloc..D.....&.....@..B.....

C:\Users\user\AppData\Local\BAz\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2424832
Entropy (8bit):	4.065959472971376
Encrypted:	false
SSDEEP:	12288:yVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1wq:vfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	FD50001CFAB99A0F4FC5234E764688D7
SHA1:	C53C7777677CAA2E55ADE2F6BBE5A99C17B7F72D
SHA-256:	7CBAB28F7489136891D6F53057473F0DC7658629514BB114283E72DC51A4C7B5
SHA-512:	668EFBA621361B52EF214A84284B46BFD4AED4A3FBBAFE9C55E7B0AB06233272BC43314A3E0A456684F7AE311C648115217099D9BCA2735E40CFBAB1B4A45CAD
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....$.....|...|...|....K.#}...'...}.....{}....X.#}....f..|....g..}..*...a|.....}....N..}..*... E}..[.I.E|...'..U}....N.+}..[.K.P|..[.K./}...I.h}..u.Y.k|.....|..W"...|..b.L.t|...|...}.....N|..2%...|..Rich.|.....PE..d., ..DN^....." ....p.....@.....%.....@lx}..b..... .dQ...c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\BAz\wlrmdr.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	65704
Entropy (8bit):	5.834154867756865
Encrypted:	false
SSDEEP:	1536:B14+6gGQ7ubZiQ+KytHIyObsvqr9PxDt8PcPs:QgGlu1iFtHJLu9ZDt8kU
MD5:	4849E997AF1274DD145672A2F9BC0827
SHA1:	D24E9C6079A20D1AED8C1C409C3FC8E1C63628F3
SHA-256:	B43FC043A61BDBCF290929666A62959C8AD2C8C121C7A3F36436D61BBD011C9D
SHA-512:	FB9227F0B758496DE1F1D7CEB3B7A5E847C6846ADD360754CFB900358A71422994C4904333AD51852DC169113ACE4FF3349520C816E7EE796E0FBE6106255AEF
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....$.....j.s... ... ... .s\ ... .o.!... .o.!... .o.!... .o.!... ... t.. .o.!... .o0 ... .o.!... Rich ... .PE..d....2.....".....4.....:.....@.....@.....b.....P.....xg.....$...0.....y..T.....f.....g..x. .....text....3.....4..... ..`.imrsiv.....P.....rdata..J2...`...4...8.....@..@.data...h.....l.....@....pdata.....n.....@..@.rsr c...xg.....h...r.....@..@.reloc.....0.....@..B.....

C:\Users\user\AppData\Local\BmHMcHp\XmlLite.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2142208
Entropy (8bit):	3.530533112491697

C:\Users\user\AppData\Local\BmHMcHp\XmlLite.dll	
Encrypted:	false
SSDEEP:	12288:TVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:CfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	1B21FE07DDE73FEE425060DB465CACE5
SHA1:	571E7FBF8D892A0955FAB7877BD05846E0B71844
SHA-256:	D4CEDF3D8B7706B15109E5F6095369165A1AA007288E9AA5FE59E59A557A2991
SHA-512:	B36B92EA01E7BA24C0A2D33FD92FEF6D4CE537E5928E4312A8ACCEB2A87C076D302577E82863BBBED6CF9C60CA9143DCCE8642A31FB08583C82D3B12E7CDE781
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\BmHMcHp\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:	39969503FDF09107FD3B35F8A29CFB640B96E4A7DD257F9561F8BD34A22DC93B7246A424FC22D06EB1D7A01717CD05DCC3C5B00FB13F222F30D09D7F2EC31B4
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....$.....'...F...F...F...>I..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\IUlxz4RrJ\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2424832
Entropy (8bit):	4.066063391027149
Encrypted:	false
SSDEEP:	12288:HVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1mq:ufP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	68235336EF275078ABF6EDC2C76F7EC1
SHA1:	72CA25ADF54E9407065E3EB5C5B7DAD1D028F419
SHA-256:	077CA1D7B49A000C185E0785654F1E01E3B519A462CF84D1DFB8542B075071E0
SHA-512:	F5A65DCAF4FAB398C10E82FDCD1AA2E5E870D5F35B4C8CFD506A5B8543A98A6AA0EB0DEA4BD44C7854AE9FE0BD641A2F5AC880BD9625DDBA64AABE31F0A84EA0
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d., ..DN^..... ....p.....@.....%.....@lx}..b..... .dQ...c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\IUlxz4RrJ\DmNotificationBroker.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	32256
Entropy (8bit):	5.250876383836324

C:\Users\user\AppData\Local\lUlxz4RrJ\DmNotificationBroker.exe	
Encrypted:	false
SSDEEP:	768:ghunFhykO4aAvnsvpzte5+Ql0/iqmjjn:58kO4asshu+Q+/Ojjn
MD5:	1643D5735213BC89C0012F0E48253765
SHA1:	D076D701929F1F269D34C8FD7BD1BAB4DAF42A9D
SHA-256:	4176FA24D56BB870316D07BD7211BC8A797394F77DCC12B35FFEBAA0326525D2
SHA-512:	F0BD45FE66EDC6F615C0125C1AE81E657CA26544544769651AB0623DD3C724F96D9D78835EF6B1D15083D1BB9D501F6DC48487DDA5C361CAFA96022D5F33A4
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....j.?H..lH..lH..lAs.lT..l'o.mJ..l'o.m[..lH..l...l'o.mC..l'o.mA..l'o.mA..l 'ohll..l'o.ml..lRichH..l.....PE..d.....".....*...V.....&.....@.....n3..... .....x..... .....Po..T... .....]..... .....^..p.....text....(.....*..... ..`.imrsiv.....@.....rdata..P8...P...:.....@..@.data...(.....h.....@. ...pdata.....j.....@..@.rsrc... .....n.....@..@.reloc.....z.....@..B..... .....

C:\Users\user\AppData\Local\L8kh7\dccw.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	657920
Entropy (8bit):	7.269727423438011
Encrypted:	false
SSDEEP:	12288:Nj8lLdFv9GOhS/IzJqrraq/t2qXy6xdRhMA:l8xdFAGS/EEn/tkI
MD5:	341515B9556F37E623777D1C377BCFAC
SHA1:	B0D81F3BCBEAECDFA77DBACE763A07629B9CC2EB
SHA-256:	47DD54A2FDB59C1FB69EA8610CD83E2434F435C56A5FE62E67D0F98B3101A49D
SHA-512:	3639A898B9C636360700325BA3F7F34346AF2A17628C82F23E68074CEB08014D63F42F05D7758B8D0EC0B872EE7098BC10065D338BAF243837937B9648053249
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....D.O.*HO.*HO.*HF..HM.*H .)IL.*H ..I[.*H ./II.*H .+IV.*HO.+H..*H .#Id.*H ..HN.*H .(IN.*HRichO.*H.....PE..d...U.|.....".....0.....@.....P.....$P....`..... .....PV.....x..... .....@.....l..T..... $..... %.....text...Q..... ..`.rdata...`.....b.....@..@.data.....Z.....@....pdata..x.....`..... .....@..@.rsrc.....n.....@..@.reloc.....@.....@..B..... .....

C:\Users\user\AppData\Local\L8kh7\mscms.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2146304
Entropy (8bit):	3.540833977998435
Encrypted:	false
SSDEEP:	12288:1VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:sfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	A26984064E038FBBBF358B0D4BF075BA
SHA1:	3684253C0E8CFA7CD9E43C498FA2D6910EAA51C5
SHA-256:	4193CA795D780EC354CE4790154578CCBE75FFB8259F15D47036E057B2EB2959
SHA-512:	A1D17A4415CFD9AF124A97E9661111282E8B9109A0289EADD667F7AA601F496E3240BE53FDBEDB1F12561A5E5928F73B56C22467EED4CDABA693E1B52E92C79F
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.,, ..DN^....." .....p.....@..... .....@lx}..b..... .g....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\DURNCK2N\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):	152
Entropy (8bit):	5.173076422849107
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsx6wmxvFuqLHIfwEYPJGX7T40AAeQ9qS5wRKb:JFK1rUFkduqswEkIXH40AAeQlvb
MD5:	8A42B7A61684271F7E6594D3CB6FDB9E

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\DURNCK2N\www.msn[2].xml	
SHA1:	04284886B11C51B3580043FCAECD5949B8BAE54D
SHA-256:	2EEF3E731EE7A0BC408376B43B79CB3EFCB98F9366A9F4BB931A031C2AAD75E4
SHA-512:	3F7CFA510567B7F8385BDE44CCFF45EEEF12E6A267CDCC39B1B690C1C170D2F0A13DA61B15A96B90B9FAEFBA1745FA50CC4EC2852D39245B8DB61B96888CE68
Malicious:	false
Reputation:	unknown
Preview:	<root></root><root><item name="BT_AA_DETECTION" value="{"ab":false,"acceptable":true}" ltime="4087958832" htime="30913683" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\QALADACS\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):	2905
Entropy (8bit):	4.897689890157897
Encrypted:	false
SSDEEP:	48:LC+C+C+CY+C+Z+Z+Z+ZE+Z+u+u+ut+k+k+kgj+kgjoM+kgjoM+kgjoM+kgjoM+kE:mhhhYhGGGGEG111t333gj3gj33gj33gP
MD5:	8428A2201DB53CE6AD46B7C5D1C14609
SHA1:	2493B29F999591AC2E73A6CA67DB60A69945B686
SHA-256:	F74C235E1ECBF22D6F496E6D6794E67EF636A50383924B57F20960CAAABD2EA3
SHA-512:	FA0E4E2D3407D02DBFE821E274DCE4C8DB4D52079A17C474B3372F566E64C276D17BE8DB778C2D0789BC5C0582A97AC3E2293707DA784ADE69A14071219FD57
Malicious:	false
Reputation:	unknown
Preview:	<root></root><root><item name="HBCM_BIDS" value="{}" ltime="4043438832" htime="30913683" /></root><root><item name="HBCM_BIDS" value="{}" ltime="4043438832" htime="30913683" /></root><root><item name="HBCM_BIDS" value="{}" ltime="4043438832" htime="30913683" /></root><root><item name="HBCM_BIDS" value="{}" ltime="4043438832" htime="30913683" /><item name="mntest" value="mntest" ltime="4043958832" htime="30913683" /></root><root><item name="HBCM_BIDS" value="{}" ltime="4043438832" htime="30913683" /></root><root><item name="HBCM_BIDS" value="{}" ltime="4043958832" htime="30913683" /></root><root><item name="HBCM_BIDS" value="{}" ltime="4043958832" htime="30913683" /></root><root><item name="HBCM_BIDS" value="{}" ltime="4043958832" htime="30913683" /></root><root><item name="HBCM_BIDS" value="{}" ltime="4043958832" htime="30913683" /><item name="mntest" value="mntest" ltime="4047958832" htime="30913683" /></root><root><item name="HBCM_BIDS" value="{}" ltime="4043958832" htime="30913683"

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{2A92399C-2087-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29784
Entropy (8bit):	1.82861344619002
Encrypted:	false
SSDEEP:	192:rwZ/ZS2QWP3tPFfPPtPVvWPeBPeNfPeEsX:rgBRHPdPdPVPEPwPUPe
MD5:	4874648FDE49F8824E8B74D29955073A
SHA1:	D814694377AEEA404126C2AD8139BD312E5F3202
SHA-256:	98E494594131D5083E5757357C5A51173020B690408BE54206363664354F96D6
SHA-512:	4C92199BABACA01BB4F9DA965B08FA132516203B8CA601803363BDFFFDFD9B1E5DD997D9B5A9B1CC9567CAF81381B8BE8ACAD23B3DC55568EB6F0FA8A743C703
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\{2A92399E-2087-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	365448
Entropy (8bit):	3.630038730642915
Encrypted:	false
SSDEEP:	3072:4Z/2Bfcdmu5kgTzGtcZ/2Bfc+mu5kgTzGtDZ/2Bfcdmu5kgTzGtbZ/2Bfc+mu5kk:x3hYJ
MD5:	8014F4A063143AC15A96AC63E6F410A3
SHA1:	817CE41D6255FEF1F6F089AEFB6234E85D26613F
SHA-256:	687900710605C5AED770B7E5BFA724A036084CF21A3649E58FB1F43D32DAEF99
SHA-512:	AA90C0B98F6DB7EFCBBD15F40BF397B71BC1E5B4801A63E3F67BC90BA17666E7F5D407DD5648CD08C010C68D76DB623698FC24D9122A210CDF2EF32A8498471
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{2A92399E-2087-11EC-90E5-ECF4BB570DC9}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{31495CC7-2087-11EC-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5669606875250521
Encrypted:	false
SSDEEP:	48:IwtGcprYZGwpaVG4pQJGrapbSS9GQpKXnG7HpR2TGIpG:rzZ0QH6pBSSHAWTCA
MD5:	DBE33928EC89E17D62595EDC5BC12C17
SHA1:	9B522E3E0D41E58C640DA9146849F18FF557F079
SHA-256:	C9963B28CF8BD663D055E4DA1B8CE73BB2E7A749A4E306CDA031BD248CF7CE4A
SHA-512:	EF64CC192518817F49F63C210A98B843FD491D119E2CC07EC7361CBCAA765A5329F13EF781D7BEB5E6CA70DB4C1F0D5602AF65119E3C9977EBDE689FC57966
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
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.102965617533081
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEUCnWimI002EtM3MHdNMNxOEUCnWimI00ONVbkEtMb:2d6NxOzCSZHKd6NxOzCSZ7Qb
MD5:	27C6D2331EC7F75388037D3604806385
SHA1:	EF93AEA05D41A168BBEA35A383F36EF4ED32F298
SHA-256:	07BA8FD231E27BD234605CBA8CF9426DB55D017F1F1363092089ED38DAFA0737
SHA-512:	82A9E3D78056F6B40F9B121E003F8B5682F8AEB451B32A854AF24660B87F64CBC6882F5D96B26DC3F0DB1A3681A724EBC2EAAF9C4111F23F2F848186AD12257F
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x022cb1b7,0x01d7b494</date>< accdate>0x022cb1b7,0x01d7b494</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>0x022cb1b7,0x01d7b494</date><accdate>0 x022cb1b7,0x01d7b494</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):	654
Entropy (8bit):	5.16060064038391
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kVtZOKtZOlCnWimI002EtM3MHdNMNxe2kVtZOKtZOlCnWimI00ONkS:2d6NxrI/QCSZHKd6NxrI/QCSZ72a7b
MD5:	EF4EB7F562C832C8A12FCE9182C550FD
SHA1:	55654630DEEFD7A8258244EFE46BDFADD642F374
SHA-256:	FAD843596B1BCBD25AA5424083EAD25EAEF48B482AB030CA31F8E76552234D93
SHA-512:	E48581B2A21DD1C9F82EB8313955DCB45FE5561986690F61312F484326582B6110E8EBCED9B308A10AEFFF2B23E18AC5B3CA7D77A195268E789076321F7BEC72
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x02258b22,0x01d7b494</date><a ccdate>0x02258b22,0x01d7b494</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>0x02258b22,0x01d7b494</date><a ccdate>0x02258b22,0x01d7b494</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Am azon.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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.122961132708952
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLUCnWimI002EtM3MHdNMNxvLUCnWimI00ONmZEtMb:2d6NxvYCSZHKd6NxvYCSZ7Ub
MD5:	D6B65D90C53E334599DF581399C0B443
SHA1:	E5919D68505C01B5F0489422FC0ACD069F0FB12A
SHA-256:	E3F2CAA7CF6907629E821E8DD37BD96259C2EE5D3F960F08BD2C123EA17D3CBB
SHA-512:	0309A9189196D7B0A56AE52B40D6239BF15752F3E5F2B2676E42244A039BDA4D4D6AC628ED8FCEE9C97ECB1149FA63A93D260D54BCFA39EA0EC64A2FF67FF7D
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x022cb1b7,0x01d7b494</date><accdate>0x022cb1b7,0x01d7b494</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>0x022cb1b7,0x01d7b494</date><accdate>0x022cb1b7,0x01d7b494</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):	648
Entropy (8bit):	5.118257565008924
Encrypted:	false
SSDEEP:	12:TMHdNMNxiUCnWimI002EtM3MHdNMNxiUCnWimI00ONd5EtMb:2d6NxVCSZHKd6NxVCSZ7njb
MD5:	54F711E3B90CB750FDF10D3CF38A4E57
SHA1:	2101F67B8D36659DF52FC75651042FC5997CFAFD
SHA-256:	61E9EA24BCC66FDE2C740A4B0B910B5F19B696BB4B550134FCF2CF445C5E10CD
SHA-512:	19F0D468C67A966C26B7F1DE8EBFC3E1DCA2A3D29F6C837AAB67DC3FA1EDEB169995C5CF801C0FB34320EA10ADF3501C163F63A45F6658F152C2147DB0FA99F7
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x022cb1b7,0x01d7b494</date><accdate>0x022cb1b7,0x01d7b494</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>0x022cb1b7,0x01d7b494</date><accdate>0x022cb1b7,0x01d7b494</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):	657
Entropy (8bit):	5.129514498773157
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwUCnWimI002EtM3MHdNMNxhGwUCnWimI00ON8K075EtMb:2d6NxQPCSZHKd6NxQPCSZ7uKajb
MD5:	578F353FCA1DB0DABF3EEAC8849E9F08
SHA1:	CC158CB7D85C8E46D6E042C38C8A09DA3E967DE7
SHA-256:	098BB6D5AF38FA1DF72E11BBB896E0CD4971CA5D030556BD708E7E18709016A5
SHA-512:	0B02BD160A062E3CC03A79AC9946304582EF2CF51228EA9CF34C780AFCA697E93F4BCEBECB21EEEB5802E3BE847AE7DC3E3032D0D31A64D4169D22C9376410A5
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x022cb1b7,0x01d7b494</date><accdate>0x022cb1b7,0x01d7b494</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>0x022cb1b7,0x01d7b494</date><accdate>0x022cb1b7,0x01d7b494</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):	654

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Entropy (8bit):	5.10675343967962
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nUCnWimI002EtM3MHdNMNx0nUCnWimI00ONxEtMb:2d6Nx0UCSZHKd6Nx0UCSZ7Vb
MD5:	CDB5ECD1FCBB94CEDF3D870AF0A62847
SHA1:	A0274BCA54BEAD74E589ECEDE8566443B01DD5DC
SHA-256:	72565410124C053306F59EFCF049B82871502125BE001FE72F9BC2CB2CD8603C
SHA-512:	032F574276F0720BF2D1DB1F107B0C291773BA3393415C6730B5B77A33F9F487774EFBC0DEC392A491BDE694FF1FEFDDDED90ADFC23E843054F6EB923761BC5
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x022cb1b7,0x01d7b494</date><accdate>0x022cb1b7,0x01d7b494</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x022cb1b7,0x01d7b494</date><accdate>0x022cb1b7,0x01d7b494</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\pin20259167780\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):	657
Entropy (8bit):	5.142540569190666
Encrypted:	false
SSDEEP:	12:TMHdNMNxxUCnWimI002EtM3MHdNMNxxUCnWimI00ON6Kq5EtMb:2d6NxSCSZHKd6NxSCSZ7ub
MD5:	539EE359A7E177035C12A4FF7FA839F3
SHA1:	A8E7A62E060F5CF146E2AEF43FF6922C9FA3114F
SHA-256:	E3B47748EAA8180F8C302E97B7D968AD0A052B479C90DA96D5F55B69F16AE85F
SHA-512:	67F43F7027D7C50BE18CC14ABB74E8FAD4C9B0638EC4B4031CE460B221FDB3E44D74F5F7A665DCEDCBB90572505510A9079125E26F1F842FD7165FC2A20CCE2
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x022cb1b7,0x01d7b494</date><accdate>0x022cb1b7,0x01d7b494</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>0x022cb1b7,0x01d7b494</date><accdate>0x022cb1b7,0x01d7b494</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):	660
Entropy (8bit):	5.147808279327627
Encrypted:	false
SSDEEP:	12:TMHdNMNxcVtZOKtZOlCnWimI002EtM3MHdNMNxcVtZOKtZOlCnWimI00ONVEtMb:2d6Nxw/QCSZHKd6Nxw/QCSZ71b
MD5:	FA5E1B26C58E73EC780925D9A6837FF8
SHA1:	2E7BFD10B3F56746F10792E14BEF8C011E456151
SHA-256:	0475AC8A04844B9A11FEBA4B341C41B56D3418890E5425EFAA696416ADC0A714
SHA-512:	8F645CCB46E5A95E2D5355BD17853C0DD08A0F9E8AE63E5E7B0579C42F835C19F8551B801B1C9312740C1B02DF6A5998985CF0F53EF13362BE6466F22655E1CD
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x02258b22,0x01d7b494</date><accdate>0x02258b22,0x01d7b494</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>0x02258b22,0x01d7b494</date><accdate>0x02258b22,0x01d7b494</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):	654
Entropy (8bit):	5.103451860664203
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnUCnWimI002EtM3MHdNMNxfnUCnWimI00ONe5EtMb:2d6NxsCSZHKd6NxsCSZ7Ejb
MD5:	5B6D637C04C48E951A718414051752A7
SHA1:	D17E2C3746620B1CA6D7D7E71745609BF19B29E2

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
SHA-256:	74207C85BFF15751E6957FC78F9A676E689AA3E5F9596F19706597A1FA68BFA7
SHA-512:	2E7074DC98EAC0964B798873ACBA499F3E74D7677B3AF7F6072DF9F1E5D5D73AEA8DD495BDAF94054E60CE91C74E47C7E7DAA7D30135282CB90931D84A172D D
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x022cb1b7,0x01d7b494</date><a ccdate>0x022cb1b7,0x01d7b494</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>0x022cb1b7,0x01d7b494</date><a ccdate>0x022cb1b7,0x01d7b494</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Go ogle.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\dikxvqf\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	934
Entropy (8bit):	7.028247615041727
Encrypted:	false
SSDEEP:	24:u6tWaF/6easyD/iCHLSWWqyCoTTdTc+yhaX4b9upG6:u6tWu/6symC+PTCq5TcBUX4b4
MD5:	30D0A9F6A47A49328AC0AD670C7C29FB
SHA1:	2FC54FE5F8DCE447D21DCA75385D0C7B16B2AC15
SHA-256:	58EA55B81231C1DD2E4B368FC4B5A6A22084D65221F01ABFDE9E00DD581AB4E9
SHA-512:	4DE5720AAD6D1272EACADDD652865E8E2474E7749064F416DD6E5E1192B5E6DA14288DD1B424A289DE6C160644F6DA65DCFD66ACEFF7E7AB02771B70878F5D E0
Malicious:	false
Reputation:	unknown
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`. ... .GZSa....GZSa....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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):	5.324109854583468
Encrypted:	false
SSDEEP:	6144:YXP9M/wSg/jgyYZw44K7hmnidDWPqIjHSjaVCr1BgxO0DkV4FcjtIuNK:CW/VcnidDWPqIjHdQ16tbcjut
MD5:	C906EACCF4FB5B70603D1C1C810478CF
SHA1:	D80452D9411F8AF5611DE5B2B6941A4A44418DF3
SHA-256:	3C9F6E4308C874AF5124CE406E41347CA23F9F0ADE80FA6CA0DC7A79B0AC4F74
SHA-512:	5AD826EEA9C4C10E20C5FA3916D9ACB8169810D2BE6166C5DBD7FFDF64B071728D86E2488A4BC700F46A3E029B741662ADD39A72C093F9B3AE81430C15D01C 9
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\4PB7FJMT\AAOOt8x[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):	2700
Entropy (8bit):	7.82668315500443
Encrypted:	false
SSDEEP:	48:QfAuETAeOjeBSxiqQdKdCE8wQvUbO0mSeUUx7LAh4J/Z3q2QmBn:Qf7E7wLQIMElQvUNmSi8KJvQu
MD5:	4E6C867D40120741CD198C2672103617
SHA1:	45DFF1E5919E7AB66530101C41BDC495D8F98A8E
SHA-256:	6F34DD1D5BDC080B87443915342AFE5393322240966458D788964A0CDA8E9747
SHA-512:	72BC7331EBFD7DA62F5B753FD73CB193B434E72C47E73616A56693894FCD05A424D16902B730F78416A2D306BE2D6EB71CEE851ED979AAFFE9F9D386BB51852
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAOOt8x[1].jpg	
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..:Ih..|.....Gd.)e.9..hd.$.Y&`E-..9..v.\.F..pi.....J....a4..}.....J..v,lg.9x...e.z..w{...N...NJ..i.M.b.>.x.H...#'4;....,l^H}.8;.....t..4lBg.s....Fc[.....K#!....b..Ql.~....dz..>F_...96...3Q.&."..Q.O|. '>.5z..j.....Wk0..iH...."..i.L..0>...j..0[.Nk.1..Q..}*,k..r...U89.....r....(/.....!%s..o....bU.>..7M..lm...J.G.....\ltY...m...;.....=. f..4.].x..?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAOPCyy[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):	27880
Entropy (8bit):	7.8920920440562305
Encrypted:	false
SSDEEP:	768:ItSOxU8zjSGLT46jujuAblABoHPOxpVPGOnk4ygJu:lyc+04S60oHPOVRFyku
MD5:	9869F560621FC400F579BB38E7526EA6
SHA1:	CA8D570D8C6A86DF718DCFFB5B9BC948BCA43E34
SHA-256:	25EE3180EA07313D344E18344CEFB01F8F8A28EA329E798C4FE99CF1A3422F2A
SHA-512:	7BEDA3F2598C1671512312527F52D20F82643B25A2C594EFB1F453BE8E7D191453DD286A8E67B85B7FA11C2F004ACE3A1106666F331A3FD22FAE32A32BB5BAF2
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....Z.(.h.....h.sH...-.%./j.J...8....n..m!.i.i`.g..@Da .U.....2.5.8.....,Lg.4.L|... )..D..h..T.....R.#y.v7..f"...X.I.Z^../s..I....).P..\...ph.H...3)Dj1..L.J..+.TI....L.f.~.B..P...40.qE.U...)..F..d.MCV(.4.I.s.R..i`..Sq...F.....K1.A....).S....(8...K...@....^i.....8....j...@....XLd...,..8.\P...j....@.M.&.(.."......I.`.. .+.3TJ..*.Q^X..)."..F..kA.6...B+.I.5jBeg..8..M1.H.L.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAOQ1gt[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):	11343
Entropy (8bit):	7.9059134105071625
Encrypted:	false
SSDEEP:	192:QtN9sDIRlww5YX1VSCDzfeO8NQ5kNHcIcdeBPq4JlB17h9XnR0tHJB94Aw:+N9yIR15YFVS2feg5kNJlPRJR36HJYAw
MD5:	75EDC68DC0F0929145FEFF9FF048737A
SHA1:	989C5C46190FCBB6A0737472A77BC7664A6B710A
SHA-256:	2BAF3F2176C9377EB292BA964A3C4999573C0DA73C2A4A0F6ABC6887E58AB1ED
SHA-512:	42CE92E7BE14E1EA0EA7CCB71B434FD50D282906219EED3F84A423831F59606B48EDCEFAD3AF32AF4040ECB804D20FAB7AB60D13A817623EC9024D18D32FE6F7
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....,.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..B."..2.3.8;.....L.b3d.}....4.;Y.;."..$.>.n.....@....'.=(....L.>...s..zP..d.....R.wI....:.....Z..f^*@..2..@b2"^c..mC.....1.)....J<..t...=. 1.]?.;.r(`....*..!...3..He..}..jb!....RCg?%.k...5P.....)1..[... $...8..Zh..#..h.Fw.....*M._I.H.d.....+.(....z.....k..M.....E}..h.....U...1..IP"'.L.\.dt.D.....G.....b|.J.....`T.R'.4.[...C...1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAOQeAq[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, 206x250, frames 3
Category:	dropped
Size (bytes):	10487
Entropy (8bit):	7.925141422625732
Encrypted:	false
SSDEEP:	192:Qo8sQCojIrAHlS2JqBUNzDQczpTbwHZr2NUuZNSaAVBQZ:bOpUeIHqBYA8TEHZ5U0XnQZ
MD5:	CA60DC24CD1C10EA3AC66B303BAAEFB9
SHA1:	60035ED163AA784038882C02A9D1DB098D8055E5
SHA-256:	B1E269B22D6088734E559573F9E357BEFECAB46095A2C02DFF81E88B9DE6F6E1
SHA-512:	55EEEC84EA54CBF5D55D6B9356F35C942C1F8EB18A44426216438501EAC7502A73119252B9D1E65F91D12F69E3444D61597E19BD98BDC862BCA55AD87238FFD
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAOQeAq[1].jpg	
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....kb.P...!.Y..T.+..a..1.p....@..69'..b....h...H..SC#....`A.@.#(...GZB...l.E..3.....D.r:P.X.....cv.....Lc0rph..r8..JLB.f c.@IJ. ..8.@M.$... c$*...."+8..\z.G.....<d.....R..G...._.f..8.....!%e..BCW..#9..$..JV...NA.1.A."..#<.zP....@..#....h.":...DNN.....Wm..n.1.C...F.7..M..."...S.B1~.X....V..K&.i<.Q. . ."..+...x.;.Q..O.dq@X.Q....I...pa..i..2.....U&.d.8."....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAOQorx[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):	2189
Entropy (8bit):	7.7749652003743845
Encrypted:	false
SSDEEP:	48:QfAuETA2gEWywOsZdAs+V9cLZjPnxTurNj2N/Xj5:Qf7EpgPOsG90lnxglqF
MD5:	62BFBBA39AF487149CEA4B414AB5CF2B
SHA1:	40CDB5D2A746BCFDC738AB7DF76CE85FD8548383
SHA-256:	614AB0ABD879E2D9FA4A254585796053D4BF6B94CFED23695AE4462AD49A8249
SHA-512:	5CDEAFCD77E356321EF17E11A2151E1F4A7E55A33DC0B631E4FBAE67FC1C0E6B92CEE98ECC3DCCC0617C55801BD1D279FD4DAF4B98980E07E9C2CB8BB5AC 5718
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....".6VS..[.Y...R..z...M?H.Y#W...F..}.*..Q...;.$..@.!.....?:M.F.F..#\.:.7...#.}ER...O6.t...r...dt#.DX.!.h.].X...Q.H....g4.+..... ....E.z...._.$'..H.....:I\...1.1PYD.;.Xc..h.V..d|.....Iot..y..3F.p.,..6.$.....}=G.]0wG$.fs.... ...H.Z.P...3An..../0..(..Td6...W.$H4.5..4+..sY..Z.....l..#f,.=.i^....:(...R*.&.(...C.B...J.....E..N..$l B.~a.G.[S....fq.....!..1Z..c.8.h*.f.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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\4PB7FJMT\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\4PB7FJMT\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\4PB7FJMT\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\4PB7FJMT\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\4PB7FJMT\BBVuddh[2].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:	7E5F09D34EFBFCB331EE1ED201E2DB4E1B00FD11FC43BCB987107C08FA016FD7944341A994AA6918A650CEAFE13644F827C46E403F1F5D83B6820755BF1A4C1 3
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\4PB7FJMT\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BBX2afX[2].png	
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.....*.,I"...)...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$.....X...../.=....f:.....\|c(,.....l.\..<./..6...!...z(.....# "S..f .Q.N=.0VQ._..\|....>@....P.7T.$./)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\4PB7FJMT\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\4PB7FJMT\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\4PB7FJMT\iab2Data[2].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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\iab2Data[2].json	
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\4PB7FJMT\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 I(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\4PB7FJMT\th[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):	49158
Entropy (8bit):	7.966953950119275
Encrypted:	false
SSDEEP:	768:iCxsXGdEjr6mP9zI6ZY/onsq/8j/ApbsbQa9ZjNPRdGvtxLppvI+/vNtU3ERC5lJ:iCAGdir9y67nzAL1Hd8p7Qet8E8J
MD5:	F63557CDF3E015D7C240F74D9FE1F67D
SHA1:	84DA72785D7A42D39D159DEC1D2D0EEF55C4009F
SHA-256:	65448C83646DF3B09E89C479BD4C4E8F41B6AF6B4BF909C319DBCFAFF709262F
SHA-512:	21F243C582039A2C9DFA86B22DA9BF9A4B6368D74E157A9C6367BA611E8B865DC549A49F9A24FB255BFFE582BB3C320303485512B70DF4F70E9B43412A1AF871
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....``.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)===.. ....p.n.."..}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....Q.#..S...o.0..r).`Q.@13HG.8..h..!E*.@.P..i...&h..Sh..g.3M..W...3l@\p..K.aqsKM....d.....;4f.G4..L..H..(..M...I..LS..E-.....P!1F)h.....R..QK .1@.E.(..%.....\Q@..\R..1J))h...0qN...W4.S...%8R.4....sSm..'...;..Dd...v.4.0).....'...bI.W....4.)H..2C8..M8.P.t..:ri.J)z.@.....(.&is@.IN.....%.4...JL..E..}h.%..^...`!4 .b.P.c4R...)h...(...1K.(..)q@.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\37509a60-7d3b-427c-ac74-457c92ddca4d[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):	102504
Entropy (8bit):	7.979655747707165
Encrypted:	false
SSDEEP:	1536:Is5Lq35xCZwigqtqMyayQvdx5nkZu0VSCbEsIj0goZWlTWtGLXCUErhQlj5Fs:X5wQqMsQxXiSxj0ClT8WEOFs
MD5:	8FEE018FE292B797DEEE9FE3B7D94935
SHA1:	2EC97A1B987E724F34BB1FCFC2D02CF0D8D98B34
SHA-256:	38B4E64651EE3A04637CAEED73895B28633160BD2D3BD00138B8C9A583F2C8F4
SHA-512:	21C60DE8B09D7BAF708F56F459B720A7FA0C8DA6F316A6D1A92DB2B634DE6FC51053382BD85A1D493960E6F121674D5B3B52ABA40771EA40BE781CA0D62E13DE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\37509a60-7d3b-427c-ac74-457c92ddca4d[1].jpg	
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....C.....C.....3.....!"# $.1%23B.45AQR.....@.....!1.."A.#2Qaq.$3B...Rr..S..%4C.b.....?.....].k..h...3[L.....r..oK.6Z..7..J.k5...._c%c.(.n.8..=?".....fu.]i..j].V{... {....6.u....jC.so..3...,..1.gcc.X..9....@..y...z.>.Q....r.#E.n..U.cZ'n.k,S.fk?....;#/.@.bu.:.....J.F..F.!.:.....V'c.U:o9D....|.(..\.6)]]6.U2.../.....1..c...!V..!c....=..RVY...l....#L7a..Tl..*... H...AjA,@..)<.H..H4...!.....?QY..m.-:n.a.3.9.Y.E.b.....m.Ud.....$)Y.V. .0..m..yO.f.;.9C.U.....u..!Z.W7.....@....V.....MB.X...%j-.~.}..LE.>+...k.....z..):,{..".....f..m..l.-m...l ..u..Lm...~K3.8aL.'.RiT.){.9..%\.j..'x.....%R.].....C<C...G.^.f.x...2d<7Q.u....Ce..Q.%....a.....jt.e...sYu....Y....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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:	B74308C36987A45BC96E80E7C68AB935A3CC51CD3C9B4D0A8A784342B268715A937445DEB3AEF4CA5723FBC215B1CAD4E7BC7294EECEC04A2F1786EDE73E1 A7
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\B87Z87FM\AAOMcmC[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):	9113
Entropy (8bit):	7.932262057291051
Encrypted:	false
SSDEEP:	192:QnHVSpkf3Gwup6vs4kiGuJ5hksvPV2h7A9g5u3ADfttu3M7m:0HwlweGzJ7ksHV47bMOfttk9
MD5:	105904BC4F757E957DA59BBFFB5A71CA
SHA1:	D7017F7712A01676691DEC10ACCE9D6E249C9717
SHA-256:	136F4D1B4B914A680959F259383CD118BEC75DC376C200976EEDD45F6FEC7ACD
SHA-512:	8BCA9606DB06A5FDD0BC4AEEA4B19ECC35497EFD9FC6E2B6544663CAC3CEBEA1BDF90BF61651B7F1EAE87C1958F0B4803503443894682D2ABFD6AFF016BC0 106
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...V...Z.g..=.y...j....j....$..]q.k..S....P. c.v.o`*).)s=....-....u.p..f.x.:W.y.....1.V%U...O9.\.6m.p6.)C.:..?.....S...[...:...g.. ..@.....-...]L.$.%...4.R$.+.&.@.B.....Gw&..?.....+S!..jX..RE..-..>..m..KM0..;..s.pb1.{.:.P."[...]....5.9;..1.`..S$.q....i.U.....).+.=..B4..;e.q),y..Rr..<.\.A.&.v*....T.G.jD.\.@Ps...] .1.fG-Z=Q`t.A.lCTH..hLR).\R..#.....2&<.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAONDBb[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):	2544
Entropy (8bit):	7.813011384616667
Encrypted:	false
SSDEEP:	48:QfAuETAqwpWfX11ds1RMl1RqRXFApwI/NvIvYQ/vIdSlfBOfw6aYrb2/Lr:Qf7EYW91d9Rq9E/A9gWG+Yrq/Lr
MD5:	F85AC5BDAE345F0B3C81B08B65006C8B
SHA1:	54EB6E9E27D271AFAD5FF469878844DF74B9BD05
SHA-256:	53DD27F6E89D1538A874221FBFDFB7C4EB28065DC50A44E6C267070FF212B36A
SHA-512:	5BD6D61F043DA89C0FA2851DC190128F97945971C25065818B7F7AB7BA30DE973E8F9A2448EBC955572A90651A0816099369F047533A28DB7E682DB38C29FDF8
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAONDBb[1].jpg	
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......K.d...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?.......(.h.;..p>......+.B^f..Wpq.8Z.3..*_d.o......?+.?..'....N.]Y.4.)..d.j.7.....' ..Z..R..E._2...-...T..*Rr..=.....&.O..'.s1..N..U..H.y.....m.. .De..R$(...r.,...M.u$..$T.MJs..........YTz.".%.6..H#..tl].U;G.....O.j..w.p.Z...I3...4.....MD]>.].t.>[..LM..-.r...@..bS.......~.,fa.-8.c..... C..d.J...:.u.)Q.Eb.Ov.....I..*.....Z.e'.....S. .GC..T.U.9.+][.Xe..jVg.....(..o.....P.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAOQkUc[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):	21882
Entropy (8bit):	7.959431825762013
Encrypted:	false
SSDEEP:	384:Nc9fnre+PBlymzg3jObdqc0rS25gj5vz5BbfxHkFLDDWY2dfbn3gK+SFXKv:NofnrDBgbOqcWjs5vzbbfxcLPWYmWSZ+
MD5:	DC986EB829BF80AF75108BD68C409EA7
SHA1:	E0CC1DFA4D33B2449DC6601BC10B5669BA8CFBF0
SHA-256:	D4245AB74E350C560FD0AA240EEE056071317C63B765E4EE3F1E9837A13D2BF3
SHA-512:	4FD1FEFD0BC74CBC5FD8018373B65B6F22F5144D75CC01760A3CC11B9BFC5D281EB7FEC9B5C0AB6FD573AA25FBFD8E8C9EB1A3E56D883DDE5354C1E2FB90 0F4
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......M.7...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?............4.z.#iwq....&>.ky.Wl.....1..,.Sk7.&:....yc5.....)....`F~.4.sC...d.LP..).e.0#.....^L3.....?.......I".,c.rq...6....jy...@r..Qan15.T+. ....x.k.....|.....#...i\....rCm#@.V78t_.#.J...N.OH.cI.M...q..&..-.....^<.zU\...<.h.X.......u...*do...@../......@o..K.h...f[.....6F..3..>.[j.fqxg...6...g.D..Y..ivF...YX....z.-P.)&.(K.2....... v...b.94..<.\.T.5....s.p"y.w.-..s...N.j

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAOQlqb[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):	12824
Entropy (8bit):	7.900002651525535
Encrypted:	false
SSDEEP:	192:Q2lttVIWOdNIVYy5bbJdd7cWUcPKVcigx5FzJbNj7MS14yILuDlCNx4b7BxT3Y:NlttNUJ8bPd5UcPo1yBPILWlax4vBx8
MD5:	01C8A023DF684B5BDF1F1BE3725C36BF
SHA1:	7C0D76BA25FF4D8871F508DF40398A54AAA1360D
SHA-256:	E069A0DF6FC939E32A209940EBC52738D7255D028DFA2DC56A7E86728AB81D26
SHA-512:	95B300E4FBE671780A15295B94DFD58A544E82C1E4C463A01A07774984D9FB5BD5AC7E3551CFA975B338DFE5FB0C7CC4C2063A534D76F1470FB8EA50E0E224D 8
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......M.7...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?.. ....P.....\P ....(......... .`% ..J`..J.(.(..0...1@...B(.1@.@."....C@....@.....b....\P .....(...@.@....P.@..&(........J`.......J.).. h.......A..@....."..".h.j...Z.\.;...ai..&.Xnh...(4.x..@.@....P.@..%...P.P.L..........c.......... ....d. %V...@.h.(.(...-P1(...HL.U..aa...M;..@......$Z.:...-...P.@..%...P.P.L.......(..0#j.W. 4..)...b....b.r{.+..j.N.4......P.M.Z...E1...$.P;..V...1.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAOQlxV[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):	51132
Entropy (8bit):	7.959704897632045
Encrypted:	false
SSDEEP:	768:IVqh+i49S8wsQ/CtCb/cMa2yda89nNPkasJwmCwytknTSCWP1VdseSjJgxI9Q:IQhLplfwMZyasFawOytkaP1V6eSjC
MD5:	3B4A236583736CCF43FB7A8BF8791ED6
SHA1:	FAA69C989E2AA382FF46453E7A6975BA3377F5B7
SHA-256:	3EDEBD740635ADF8D8F5A8822107E050C9E16DB6F3B32E3EF1AFCEEF85740602
SHA-512:	8B6BBAE52ED9408F9065F336DAF5ED33B06102499280857286FB916CF5522A912BE81A4648BBF49D0E07241013EF26AC7DAEF24686FD9A2F8EB5CB1BF0E1BCF 8
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAOQlxV[1].jpg	
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..J.Z.\P...8P..m.....,,=jIJC..!.9>..nYVI.i77,{V.X.,C.99..N....%M...h.6..x.)...JwbCgut...I&;..Db..U.c..mn-."x]..S...N2.....+..3k]..l \|7QZ.s;.....Fg.>R..T..d.^k...a{....J.j.BK6).2a..$..,FP.i.|'.T...m...v.3dt..$J.8lf...6....-.!.....gYc.YG....$#$...c...[R.ON.HZ[a.oU.A.8..f.0.\t5....H[.Fo..K`.b'ur...EE.#..,.q.-p.....J-bn:. .i..bI....R.\..3a&..6.E.Vu!....&...0..2...!....@....L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAOQycW[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):	22335
Entropy (8bit):	7.849848793222804
Encrypted:	false
SSDEEP:	384:IeZWsfe4OCvyqhnVK9eHb9Y/s2RDjAgAxFdHaWGZIWAxSAzKb6qbErMbK8Yp08:IeZhG4Xvy4M9e7UJtgFd52IW30K2qIr1
MD5:	CD1A1080FBDF241E975E8521D27CA42A
SHA1:	C0C7971B58FD34159F2F734FB84E0BCE60CD52CB
SHA-256:	67ECCD5168F33C4ECBF0A78A88983D874F5934CD23DB77297B3D1032C63A130A
SHA-512:	496976442F8B8AD2A518B62AD4310CFFA9601B9094FD3213C852053A32CE5D3013DFBCDE5C15DB410167DA35853DC7976F7FF89AB4EF01B21791B81B79E9F27E
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..@.V..M.F.L...B..a..qL..A..i4.Ph...@...&..p.@.b!P..=A..i.#.....LC.y5.Lf...[t0..D,.4....)... .`..m.9z...|.....B.!_...Qf...>.v...S. ...4.Gbd.o.m.o(zF.Q.Z.....y>{..~.j..r..\..z..&.c.....V...87..')o.Xw..J.(<.d..'.....o.'....t.zZ...}.V...C7Zo.~.+kq.`.?.T..;..'.'.....@.&.....@.4.6..`&.8...N...r.R.t.....n..K.Q.....U|...q ..t.w{..<i.@'....P3B...{?...z...VT.d.;(@

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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\B87Z87FM\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
SHA-256:	10E48837F429E208A5714D7290A44CD704DD08BF4690F1ABA93C318A30C802D9
SHA-512:	5CC1E6F9DACA9CEAB56BD2ECEEB7A523272A664FE8EE4BB0ADA5AF983BA98DBA8ECF3848390DF65DA929A954AC211FF87CE4DBFDC11F5DF0C6E3FEA8A57 40EF7
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\a8a064[1].gif	
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.$.di.h..l.p.'J#.....9..Eq.I:..tJ.... ..E.B...#.....N...!.....,.....dbd.....tvt.....ljl.....dfd.....\|~\|.....D.$.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\B87Z87FM\checksync[2].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):	5.305082513785246
Encrypted:	false
SSDEEP:	384:VZAGcVXlblcqnzleZSweg2f5ng+7naMHF3OZOBQWwY4RXrqt:L86qhbS2RpF3OsBQWwY4RXrqt
MD5:	B5F20E1651F4F1946B488FF06242968A
SHA1:	AEA762A84C24EB4E69086A8FE735F0A86540EA92
SHA-256:	60C18B7845B8A1000103670FEBA257E27DFC731789BC6228A5ACA42CF101B2E8
SHA-512:	37DA7C66E1949934BAF502F133362787FB039C44A7C0E528B9F2F9A382CA782E26CB191127F2863ED4369325252B4E8A7A463C329EF16A50A58CDD66F1641AA0
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\B87Z87FM\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):	5.305082513785246
Encrypted:	false
SSDEEP:	384:VZAGcVXlblcqnzleZSweg2f5ng+7naMHF3OZOBQWwY4RXrqt:L86qhbS2RpF3OsBQWwY4RXrqt
MD5:	B5F20E1651F4F1946B488FF06242968A
SHA1:	AEA762A84C24EB4E69086A8FE735F0A86540EA92
SHA-256:	60C18B7845B8A1000103670FEBA257E27DFC731789BC6228A5ACA42CF101B2E8
SHA-512:	37DA7C66E1949934BAF502F133362787FB039C44A7C0E528B9F2F9A382CA782E26CB191127F2863ED4369325252B4E8A7A463C329EF16A50A58CDD66F1641AA0
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\B87Z87FM\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):	5.305082513785246
Encrypted:	false
SSDEEP:	384:VZAGcVXlblcqnzleZSweg2f5ng+7naMHF3OZOBQWwY4RXrqt:L86qhbS2RpF3OsBQWwY4RXrqt
MD5:	B5F20E1651F4F1946B488FF06242968A
SHA1:	AEA762A84C24EB4E69086A8FE735F0A86540EA92
SHA-256:	60C18B7845B8A1000103670FEBA257E27DFC731789BC6228A5ACA42CF101B2E8
SHA-512:	37DA7C66E1949934BAF502F133362787FB039C44A7C0E528B9F2F9A382CA782E26CB191127F2863ED4369325252B4E8A7A463C329EF16A50A58CDD66F1641AA0
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\checksync[4].htm	
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\B87Z87FM\medianet[3].htm	
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]:{lo gLevel: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 SUPPORTE D":JSON.stringify(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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\B87Z87FM\otBannerSdk[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):	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\B87Z87FM\px[1].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):	3.0950611313667666
Encrypted:	false
SSDEEP:	3:CUMllRPQEsJ9pse:Gl3QEsJLse
MD5:	AD4B0F606E0F8465BC4C4C170B37E1A3
SHA1:	50B30FD5F87C85FE5CBA2635CB83316CA71250D7
SHA-256:	CF4724B2F736ED1A0AE6BC28F1EAD963D9CD2C1FD87B6EF32E7799FC1C5C8BDA
SHA-512:	EBFE0C0DF4BCC167D5CB6EBDD379F9083DF62BEF63A23818E1C6ADF0F64B65467EA58B7CD4D03CF0A1B1A2B07FB7B969BF35F25F1F8538CC65CF3EEBDF8A 910
Malicious:	false
Reputation:	unknown
Preview:	GIF89a.....!.....,.....L..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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\NUEPGTR9\AAOPCoB[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):	1689
Entropy (8bit):	7.675384678812828
Encrypted:	false
SSDEEP:	24:QI/OtlM0XxDuLHeOWXG427DAJuLHenX3au/cHGhvdbLbrhO7b/Qx8hukmJWkhfjD:QfAuETAUxHGXbLb1OQx8hukmJ75Y6
MD5:	BB33C464813AF42B57E10F475894879C
SHA1:	B64A64BEE6B4090E6C9E051DDC96E8ADAFAD9A3D
SHA-256:	F2622C36BA7F1F76D414584219EA573D459BC151D7FF3F626DA09CDFF47CF371
SHA-512:	D06551D78350F802772FD145149C16507B651383804B883058CFE8412AF2C6D249A286B4FEE21F6EECCA0BC2BF606D631D90536BDD954FD2F0DD016966318C32
Malicious:	false
Reputation:	unknown
Preview:	.....JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....J....E.@.h.LCDt..<P...<...p>Z.....8..F@....@4.LD.qHe....=).G...P.T..P..5.4....#+@.....5.....zf.$V ...!....L....F...P.I.16.J .j.#.....s@....x.b.....P....._.@.!..\.L.....]G.....'er...T(.m...j.mc..W.....JN.YJ...<w..~....+.c..s.n.....6...T...\....W.....|.....h.@4.")...F.....y.....n.1.....Q.....i....."..\u...;Kr.*2..*..MH. Dp.S.....Y..."....{..r.\S....[.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAOPLxm[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, 206x250, frames 3
Category:	dropped
Size (bytes):	9185
Entropy (8bit):	7.916314058922854
Encrypted:	false
SSDEEP:	192:QouMCSvWbWPgVE0VHHnNQ6acqPkJlQL+W2pkbtzW5W4:b11WbWPYVnO68P/+Zkx6D
MD5:	B68AF1C5791BEE0CB5F5A3F8C30A9460
SHA1:	ADB1AEED43B31094D7BFC5D6CFB838D7DD51D735
SHA-256:	18480DF05FB36984960E848AA7015F0414E8D6454D33F20B6EFD956400CD8D32
SHA-512:	7DCBB9E90104806389B170C53A3FB29435137F1AF8603F6236A9847A145292C8B1AC50C7F27B461370B8EAAD8F4659C1D4E0F52F9FB021BCEDB4A3A6B56456D4
Malicious:	false
Reputation:	unknown
Preview:	.....JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..^h.y....9.....(..(...@..C;m.....d....;s[..<w..;V...>....Y..)../.Vm....0....F3@..@.....$.....1.....+=M;....\, .4\V-`..s@.4.s@.@.....@..P. {..'..nEM..r..@.[-Y....2.f.y...r..."..L..k.....LP...R....0(...&....@.....#...@.4.s@.@....P...i....7ED.1.U....f.{g.....{..0...dy..u.]n+.p_....Z.y.... W...%.;..)`;Qa.7.E.....P..@..@.E....P. ..@.p;..l.w...@.(.....(...0..I.#..e.D.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAOQ2Ba[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, 206x250, frames 3
Category:	modified
Size (bytes):	7834
Entropy (8bit):	7.7295881600980865
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAOQ2Ba[1].jpg

SSDEEP:	192:Qol0VUcoWk3sMMy3yqb27Zz9K24IqqLzgHqCh7IXTYBRcYDfraCpRw7:bl0VUcVFsyqEZzI27q9BhIj2SYLuCfw7
MD5:	42EE2C935C9BDDEC249ECB9ECD766E4D
SHA1:	8AC5366279F433DBF51F46DBA433F6103EA8856C
SHA-256:	B13142C6716A2D0AC8539FE692E41A7B99F2198BED37F214E894B50DC406467F
SHA-512:	B28E5A7104042DBF46273D13B24BEDC0DA5FA4751BA34BE41F4D1FF45678C643BDFE93F29B9F43915F698486AF8E9DC4493E68541B064A605D1FDA0D175904FI
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?.....P......P.P.@.@..Z..og-.y...8..h....#k..Gr........T.8.I[.0.3.......4..a...C.(....b..._.h...X.. }.@.\..,.)....+@..6......@.....@.,r ..h.kMB..A%....FS.@..jwZ......R.. t.@...(.h......P..kki.G...3.....@.....P.@.@.Ao-.*Y........G....."e:0#........4h,..f.....c..2.(N.\.............b.c....H.ix........$.$.........q.E..m.2...}.3@....v2.c $.Pq@...J8p~.@.ly$P.@..%.-......J..m..-....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAOQ8Nq[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):	28328
Entropy (8bit):	7.967317103692769
Encrypted:	false
SSDEEP:	768:N+46ogSGzyXEDkdv/Hi1kL/QQ2vHNgD7SfWlikmAH:N+UXGzLG/C+L/QQuIOki7S
MD5:	E087E9B93627F2FA5E01C6346C38369E
SHA1:	13A228023A2A22106428D0C9550E747A415B9D3E
SHA-256:	3FBFF3BB58FFBD4EAAFB99732B9BCC6B0E42082D617FF0ED98E155A0B99DA989
SHA-512:	43DA56C335F7A954008C604B7B997E325DE66BCF6A492CF1D030C2A9A763CD53BB7AD5FD73951EB5E8BAA9204C223334948AD535E214702B83F0C2D47F3E5D1
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......M.7..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?.....@5...z@(C.D.Qp$Q..<.C....f.....>..VR9f....Nq.......P.@........n0E ."......ew...;g.P0U.pG_J...U}..(...i"...1.(...`.....N[.{v.\,=!. ..s.........y#.h..KpX..c.XU...L,.h..h..c(.M~....=3..U-.....y.4..S...b6.S.....i..!I.......-...\P"...:...i...}*x..D>...bZ+...VX.I....n.kQ.BGw...n..04..].2......@.0.#.i..hz......lg.ByC.kjfs5kC0...y...&.. u\w..........iY..'....c9?.K..*.......H..W..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAOQeHX[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):	39310
Entropy (8bit):	7.947198785082353
Encrypted:	false
SSDEEP:	768:InZb3aXZ6PmDINnUt0N0xYJxRYqD7cwYmItChYt0Z6scr/d1RgXU:IZb3iRDpqN0xYvEZshYtE6/r/9J
MD5:	9D608A1959FEEA247686002FFE89D30F
SHA1:	41EA8CD638927FA167CD549C3E7FCC9137D22DC4
SHA-256:	F3ACCBE9EE4FB4A95A5E1B77D3A55AFECA3B18068DBD38C23613F17E1CBAA6E6
SHA-512:	7030384239C7331A21487B275EC3CC4E299EABD9A7F3108F992FAE8C41C65D8F8CBF3F0FEEC138F77D08007C179ECC0FC4F631C36235D929EE486E339B98BD2
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......p.n..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?..OC."...ew.P~G..<R...r....Oa........j..X....Y0oc.R..B.I...I., 8."h.07.8K....?._.B.=`....#.H..px&..FG4.Y.....Cg.:.\B2....m4. $(.*.q!.H. .Y..=...ml.U&.L.1'o\zf.....P..aJ.b..QB.1m.1...0...\D....>..D.[...;...R...(..P...P...!....}z.........N.T....G.;....zT.!.T../..Z.uy.o#..}.).=.z..........?.*....Z.s6...w...........A...=2sHc.o.R.AoQ@..> ..n.E....0:.i.!..C.U.9H.&2PA..cx.f..O...q..OA..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAOQjSz[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):	9082
Entropy (8bit):	7.9151179296890115
Encrypted:	false
SSDEEP:	192:Qn2PnbSq1slql0ohC//XfsFPbhDxlB9ab8+/GpEDEZWGid:0PlCw/3sFPdNZk8kSUkWGid
MD5:	6EB835BA36486E7704E09763575E6393

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAOQjSz[1].jpg	
SHA1:	B331A808117702AC2A0D47159D556785EC2E7E50
SHA-256:	FC212AD60FFB17C910A2899F84B4516470303354C9BF92F1D2BE64EB8650E563
SHA-512:	979D9689E7FD0915A4209DA26D845F94C78123B5B501FDD0587EE4F6F5F15A93E4218C037FC06AD35E6C2AF9C075927224E660D792BFFA2AADD78D57D85539D
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..Wi.8P..b.#w...'.....(...l=(.3..@..''..;.@.).9..... ....@...4...<P...H .....@.u.2)...4.*...$.9.0.@....@.-.C..:...3@...Q.... ..''^..&q@..!.9.!M1.0...T.3L.&..f....".Gh..#...,2..P...Sp.}(...8.....(...(...P1.....P...(...=x..Q..=(.m..1.I...0#)..R....4..P.}x.0 ...n..k>h.7P.....P.,K..r.R.'..P...6.1.9.I.p....f.....(..;..... ..M.B(..YO.....2..d.^}i..)..9..C..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAOQsOf[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):	14330
Entropy (8bit):	7.896470907961469
Encrypted:	false
SSDEEP:	384:NdXYrwlJE1WiJnAqeVQFagAtSo8T46VOEoHptcQ/3FCK+:NJgE1ZLe3guSo8cAhoHTcQ/39+
MD5:	F90366295C29ABDF69283CF75C9E4E55
SHA1:	FA32C53A4E80A1890BC2F97945BC5340993B06B4
SHA-256:	355A081B266F8F5B5092A9AAE42FD659121D6C3C0D043BBD0C57667BCDD55267
SHA-512:	53638326821F22D15FC5C0B25509EFE518BA9B9CBE189025C6A59B2E76CC396B1B5B2A5FF685B797AF0A4C5E9D677FCF58A8D93A16593E81E4D2272DD78F500
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....P1....H.....H.j.P.e...'.....Fq.&....[.[d .3.2...b.CD..B.....52... n8$.....F:.....&..r.....w4.R..-..m.C.*|..:.. .B.r.*..r.n.8bHa.@ .....-..L.[h.-.&(.ei.$q.....dI.j.}..I...ouS...{...v{...<...eH\.....qob.....t t=G..W....z...q,.C.I.....k]....A...3.C..=...Rj.kS:K..4`N.....NOG..I\.?b.6n..dGr.c....h.....Ay;.#.f.q@.....Z.>...w .xb...t.>.*....[}Bu...0.{.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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\NUEPGTR9\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1aXBV1[1].png	
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.....&.|?...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\NUEPGTR9\BB1kvzy[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):	1100
Entropy (8bit):	7.749452105424938
Encrypted:	false
SSDEEP:	12:6v/7eZ3IqhrinW+y2UXaxTaJgfcoG7QKJ7OZfhL3cp1pW2krS7BiArfss7P7UIQb:jVT2aCTjG8MOZR372/7iU7UIylHdLN
MD5:	C6E13630360E0B6D880AFDF3CD2A2204
SHA1:	63DCA80F76834F5A3FBE79F661678375239F72A4
SHA-256:	49767874BCF0F0648266F3018B5CCE3CA539B85778E5395D1212ACB114287D65
SHA-512:	CB8F7629DA131226146B12119C06A846A2EC9E9D069711711AC50CD7F31E321144E39270E82EA693E2FE9BFD1634841BF450173807AB6607794E2AF0EBE832C8
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....;0.....pHYs.....+.....IDATx..}H.u....m..rR>..9#--o.....[E1..kWB.#.],\F.8X.....\.&.....x.....y.b..p...z}~y..9....^..|.>....{I.?.;.....:.Uw.|...e.(.....r..Wc7 Zq...F....N.O.}.n...^X..*$.q...&.%.....X....9d{.>...)..8..A...}.x#....K... z~$...4Y...<....)`..p....qr<arhwa.zY.Yq..$.<.....H...~...H|..G...@|./.8G.L..M...U..I...]..r(.s.."f..I...Q..b.x..MYd .D^.mg.G .H.....=Ot.v.D._..6.[o.7*L.....d./B)l....d.....u.....mqB.J.....(R.....".dSj.....{.gB.<...gdT....u~.?`.X.&&&N...|.R..0..O.yV~./..; ..\.X[P....[...1y+++M...J../.+...}>_ mooo...~ohh....`l.....R..."...`.....8...aeP...oL..f~n..m0..tY2.N.rrrT]].JKKk`"...Kw.i.....|.....['<...bHM).....%;..=..D.s.....CN.....Y.,..I.<...s$...v.=5....N..E.YYYjzzZ..A...+]ohIII.. .L?<<|....}&q...].vM..?. ...+....m.....}6....|i.e+..Vf.....V.@...3.d.....cRv.f...E%G..Xvv.....ru...~..j.....\..f.....*.|m,//O..B....D...zUU....Z.kfccc*..."..V__...+**R.B..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BBY7ARN[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):	779
Entropy (8bit):	7.670456272038463
Encrypted:	false
SSDEEP:	24:dYsfeTaIfpVFdpxXMyN2fFIKdko2boYfm:Jf5ILpCyN29lC5boD
MD5:	30801A14BDC1842F543DA129067EA9D8
SHA1:	1900A9E6E1FA79FE3DF5EC8B77A6A24BD9F5FD7F
SHA-256:	70BB586490198437FFE06C1F44700A2171290B4D2F2F5B6F3E5037EAEBC968A4
SHA-512:	8B146404DE0C8E08796C4A6C46DF8315F7335BC896AF11EE30ABFB080E564ED354D0B70AEDE7AF793A2684A319197A472F05A44E2B5C892F117B40F3AF938617
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx.eSMHTQ...7.o.8#3.0....M.BPJDi..*.E..h.A...6..0.Z$..i.A...B....H0*.rl..F.y:?...9O..^.....=.J..h..M]f>.I...d...V.D..@....T..5`. .....@..PK.t6....#,.....o&.U*.lJ @...4S.J$..&.....%v.B.w.Fc.....'B...7...B..0..#z..J..>r.F.Ch..(.U&.\..O.s+...]Z..w..s.>.I_.....U$D..CP.<....].\w..4..~...Q....._...h...L.....X.{i... {.. &.w.:.....$.W.....W..."..S.pu..').=2.C#X..D.....}.$..H.F}.f...8...s..:.....2..S.LL..'&.g.....j.#....oH..EhG'...`.p..Ei...D...T.fP.m3.CwD).q.....x....?..+..2....wPyW...j.....$..1.....!W*u *e"..Q.N#.q..kg...%`w.-.o..z..CO.k.....&..g..@{..k.J._...)X..4)x...ra.#....i._1...f..j...2..&.J.^. .@$.`0N.t.....D.....iL...d/.|Or.L._...;a..Y.]i.._J....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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\NUEPGTR9\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\favicon[1].ico	
File Type:	MS Windows icon resource - 2 icons, 16x16, 16 colors, 32x32, 16 colors
Category:	dropped
Size (bytes):	1078
Entropy (8bit):	1.240940859118772
Encrypted:	false
SSDEEP:	3:etFEh9HYflvlNl/AXlI1pe/WNN00000000000000000000000000000000000001:QNtY6+lKY6
MD5:	4123CE1E1732F202F60292941FF1487D
SHA1:	9F12B11BDE582DAE37CE8C160537D919C561C464
SHA-256:	D961B08E4321250926DE6F79087594975FE20AD1518DE8F91EB711AF5D1A6EF8
SHA-512:	11B24C2E622C408E4774FAE120B719A21A0B2ACFA53230126C35AD6CA57D33D4DE79CBE11D296CFBDE9613CAA03D66B721BD20CF4EE030CF75F5A1FD8A286 A9
Malicious:	false
Reputation:	unknown
Preview:	.....(...&... .....N...(..... ....(... ...@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\location[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	182
Entropy (8bit):	4.685293041881485
Encrypted:	false
SSDEEP:	3:LUfGC48HlHJ2R4OE9HQnpK9fQ8I5CMnRMRU8x4RiiP22/90+apWyRHfHO:nCf4R5ElWpKWjvRMmhLP2saVO
MD5:	C4F67A4EFC37372559CD375AA74454A3
SHA1:	2B7303240D7CBEF2B7B9F3D22D306CC04CBFBE56
SHA-256:	C72856B40493B0C4A9FC25F80A10DFBF268B23B30A07D18AF4783017F54165DE
SHA-512:	1EE4D2C1ED8044128DCDCDB97DC8680886AD0EC06C856F2449B67A6B0B9D7DE0A5EA2BBA54EB405AB129DD0247E605B68DC11CEB6A074E6CF088A73948AF2 481
Malicious:	false
Reputation:	unknown
Preview:	jsonFeed({"country":"CH","state":"ZH","stateName":"Zurich","zipcode":"8152","timezone":"Europe/Zurich","latitude":"47.43000","longitude":"8.57180","city":"Zurich","contin ent":"EU"});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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 D0ib25ldHJ1c3QtZ3JvdXAtY29udGFpbmVyIiBjbGFzcz0ib3Qtc2RrLWVpZ2h0IG90LXNkay1jb2x1bW5zIj48ZGl2IGNsYXNzPSJiYW5uZXJfbG9nbyI+PC9kaXY+PGR pdiBpZD0ib25ldHJ1c3QtcG9saWN5Ij48aDMgaWQ9Im9uZXRydXN0LXBvbGljeS10aXRsZSI+VGl0bGU8L2gzPjxwIGlkPSJvbmV0cnVzdC1wb2xpY3ktdGV4dCI+dGl0b GU8L3A+PGRpdiBjbGFzcz0ib3QtZHBkLWNvbnRhaW5lciI+PGgzIGNsYXNzPSJvdC1kcGQtdGl0bGUiPldlIGNvbGxlY3QgZGF0YSBpbiBvcmRlciB0byBwcm92aWRlOjw vaDM+PGRpdiBjbGFzcz0ib3QtZHBkLWNvbnRlbnQiPjxwIGNsYXNzPSJvdC1kcGQtZGVzYyI+ZGVzY3JpcHRpb248L3A+PC9kaXY+PC9kaXY+PC9kaXY+PC9kaXY+PC9 kaXY+PGRpdiBpZD0ib25ldHJ1c3QtYnV0dG9uLWdyb3VwLXBhcmVudCIgY2xhc3M9Im90LXNkay10aHJlZSBvdC1zZGstY29sdW1ucyI+PGRpdiBpZD0ib25ldHJ1c3QtY nV0dG9uLWdyb3VwIj48YnV0dG9uIGlkPSJvbmV0cnVzdC1wYy1idG4taGFuZGxlciI+Y2h

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\otPcCenter[1].json	
Encrypted:	false
SSDEEP:	768:4zg/3JXE9ZSqN76pW1lzZzic18+JHoQthI:4zCBceUdZzic18+5xI
MD5:	8EC5B25A65A667DB4AC3872793B7ACD2
SHA1:	6B67117F21B0EF4B08FE81EF482B888396BBB805
SHA-256:	F6744A2452B9B3C019786704163C9E6B3C04F3677A7251751AEFD4E6A556B988
SHA-512:	1EDC5702B55E20F5257B23BCFCC5728C4FD0DEB194D4AADA577EE0A6254F3A99B6D1AEDAAAC7064841BDE5EE8164578CC98F63B188C1A284E81594BCC0F2068
Malicious:	false
Reputation:	unknown
Preview:	.. {.. "name": "otPcCenter",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtcGMtc2RrIiBjbGFzcz0ib3RQY0NlbnRlciBvdC1oaWRlIG90LWZhZGUtaW4iIGFyaWEtbW9kYWw9InRydWUiIHJvbGU9ImRpYWxvZyIgYXJpYS1sYWJlbGxlZGJ5PSJvdC1wYy10aXRsZSI+PCEtLSBDbG9zZSBCdXR0b24gLS0+PGRpdiBjbGFzcz0ib3QtcGMtaGVhZGVyIj48IS0tIExvZ28gVGFnIC0tPjxkaXYgY2xhc3M9Im90LWxvZ28tIj48L2Rpdj48IS0tIFRpdGxlIC0tPjxoMyBpZD0ib3QtcGMtdGl0bGUtIj5Zb3VyIFByaXZhY3k8L2gzPjxkaXYgaWQ9Im90LXBjLWRlc2MiPjwvZGl2PjxidXR0b24gaWQ9ImFjY2VwdC1yZWNvbW1lbmRlZC1idG4taGFuZGxlciI+QWxsb3cgYWxsPC9idXR0b24+PHNlY3Rpb24gY2xhc3M9Im90LXNkay1yb3cgb3QtY2F0LWdycCI+PGgzIGlkPSJvdC1jYXRlZ29yeS10aXRsZSI+TWFuYWdlIENvb2tpZSBQcmVmZXJlbmNlczwvaDM+PGRpdiBjbGFzcz0ib3QtcGMtaGxpLWhkciI+PHNwYW4gY2xhc3M9Im90LWxpLXRpdGxlIj5Db25zZW50PC9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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="euputconsent",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\Microsoft\Windows\INetCache\IE\PEJLKQA8\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:HWwAaHZRRIYfOeXPmMHUKq6GGiqIlQCQ6cQflgKioUlnJaqzrQJ:HWwAabuYfO8HTq0xB6XfyNoUiJaD
MD5:	7ADA9104CCDE3FDFB92233C8D389C582
SHA1:	4E5BA29703A7329EC3B63192DE30451272348E0D
SHA-256:	F2945E416DDD2A188D0E64D44332F349B56C49AC13036B0B4FC946A2EBF87D99
SHA-512:	2967FBCE4E1C6A69058FDE4C3DC2E269557F7FAD71146F3CCD6FC9085A439B7D067D5D1F8BD2C7EC9124B7E760FBC7F25F30DF21F9B3F61D1443EC3C214E3F
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.localStorage,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("office")?v("meOffice"):t.hasClass("onenote")&&v("meOneNote")),{setup:function(){s=t.find("[data-module-deferred-hover], [data-module-deferred]").not("[data-sso-dependent]");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\PEJLKQA8\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\2d-0e97d4-185735b[1].css	
Entropy (8bit):	5.2940351809352855
Encrypted:	false
SSDEEP:	3072:FaPMULTAHEkm8OUdvUvJZkrqq7pjD4tQH:Fa0ULTAHLOUdvwZkrqq7pjD4tQH
MD5:	24D71CC2CC17F9E0F7167D724347DBA4
SHA1:	4188B4EE11CFDC8EA05E7DA7F475F6A464951E27
SHA-256:	4EF29E187222C5E2960E1E265C87AA7DA7268408C3383CC3274D97127F389B22
SHA-512:	43CF44624EF76F5B83DE10A2FB1C27608A290BC21BF023A1BFDB77B2EBB4964805C8683F82815045668A3ECCF2F16A4D7948C1C5AC526AC71760F50C82AADE2B
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: Expected semicolon or closing curly-brace, found '@include.multiLineTruncation' */....@charset "UTF-8";div.adcontainer iframe[width='1']{display:none}span.nativead{font-weight: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\PEJLKQA8\4996b9[1].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.....($LKloca...`...f...f....maxp...P... ... .name.....IU..post..... ... .*.....I.A_.<..... .....d.*.....^...q.d.Z.....3.....3.....f.....HL .@...U...f.....\.d.\.d...d.e.d.Z.d.b.d.4.d.=.d.Y.d.c.d.].d.b.d.l.d.b.d.f.d._.d.^.d.(.d.b.d.^.d.b.d.b.d...d...d._.d._.d...d...d.P.d.0.d.b.d.b.d.P.d.u.d.c.d.^.d._.d.q.d._.d.d.d.b.d._.d._.d.b.d.a.d.b.d.a.d.b.d...d...d.^.d.^.d.`.d.[.d...d...d.$.d.p.d...d...d.^.d._.d.T.d...d.b.d.b.d.b.d.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\PEJLKQA8\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:	8FCB3F610856351945CE5A73516DE39F9
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\PEJLKQA8\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\89a22c36-158b-411c-9c2c-269457db6c00[1].jpg	
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\PEJLKQA8\AA3e6zI[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):	382
Entropy (8bit):	7.0628405067840845
Encrypted:	false
SSDEEP:	6:6v/lhPahmpGJgBvZobVFHRvQoGOCTikhlZYL+7UoIt130Yts5Sk/42YoapFQVp:6v/7bHvZoVFHRv9GPxzS5X0sQSa42Yrm
MD5:	D936DF977436E61B66C0058888B9C7F9
SHA1:	0BF93F7EB7CF21128E80DCDFEC692D079B1778BE
SHA-256:	362C8931D87FF99A8F9AF49202A080C9B6AA61F23CBE1FFC704A2B24638CACED
SHA-512:	AD188E306C4B211787531F64D3BD23659492CF601BF82C69AF68420E809F9EDE888EF350E42EBF8AA74EA1B7A369030667E4C7B7BE12254C5CB25FE7C2AB2DC D
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....a....pHYs.....+.....0IDATx.....D@..'...T@.: ....T"%..P.TB..'*P....}.<....&.....fg...4...?... MS..^r]..<i.wqfY...*u...q.).C.....@&.E!}8..m[*.R.8...,"..... ,.U.DQ$.....y.....p.Q>..Kf..*..Kl.+..U...<..u.8.m..$Qe...p.l.F&.:o.h&?[...8.k.....q...C.pw.....P:7..k2MS.o.&^e..y...i.....7.s.Z<'2..h..1..0.X..(.S...Pg\...k.o.....r.`~.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAOQfzJ[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):	27423
Entropy (8bit):	7.970058097383428
Encrypted:	false
SSDEEP:	768:NgmTdYFJRJJNWgt31CowPYUibP3UJ99Jff3d9wHa58dS2b:NgmBAWoIowPo0zEHaadHb
MD5:	D4FBACF766CFAF4E095D781E159BBE97
SHA1:	0D8DDE59952B93487E32FAFD3D455BB3CC80A8CA
SHA-256:	EDF61BE4F10719EAD9D87CFB20C1822B85574C50E6F5ED9D1D39A3C119E30C04
SHA-512:	C10CEA3B28219705F98E1987DC761866FCD1A7125C479C1C046ABA74A6AE0A05AB2A70B9D39991D8741C0C88DF99F4210DF98E1F621482F79DDCE90F859F5A8
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOO......M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.o..p..}+..y.4.^..N)0..!.r..Xz.A...G.\.4+2..2...k.....,.....rs\..S..z....R2.U.*.C....dH..g...Y.ua.m.z.Vg(..Lg...t3!v....c.N.j.!..C.. ...U..F.^.r'...z0..[Ub.p{...c+D..ip.....:.D0).2...0q..._;(I.i.z...7.r=.j5}.b... .k1#$..h....nYA.....=k..K...6....i.+){..W.....C.a.s..s$...B.....w0kSCO..E.pw.B..w...^n+... i..:.....>...)s..G.+.. r.Z3u....9.c}.?..]8Z....I....brO$..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAOQk3w[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):	11707
Entropy (8bit):	7.8965501067778225
Encrypted:	false
SSDEEP:	192:Q2r8alO9ZIqW2Fn80YDVe7boD16e6lECuk4kuBQWAFMBD1uyAF5OK9JROSqA:NgBrx8Je/oz6KCuk4nfSrj3ROE
MD5:	2F09761FBFB646D4F8B444537135E660
SHA1:	6A7634E99CD30E2F2087FAF194BC4D1ACDDA9D4B
SHA-256:	7E670165B8AFAA4F75A3E4CDDC002832C40D66C68846DDCF2EA0C69220545A5C
SHA-512:	BDE5F22A228AAF33D9A258530AC688745A6EB0A354E07735662D264BB69A3CAE31DE7F3A2B8D94310828CF234B151AAC3FAF8E6E4CFE8BBFF710821AC67ECA DB
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAOQk3w[1].jpg

Preview:

......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......M.7...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?..$<W.t..@#p).....3.|K..[.Ks....Z.........[..-#.V+p{..Y#..Z.Q@.@.@.@......-...P.@..-...P.P.L..?...@......f..E#4.1..0.zP#O...........S
.R...B..E..."......Hc_.@C7.h.."?..lc-..B....~...-.z......+....h@.`....(.i.P.@..-...P.@........Z......q...A,...Zo.4Z3h...M.U.L.....Z..h*e.......RBbqLB............@Vi0y..J..h.. 9.5.Oc.neV.(.E.
?...../`=n.T.V1..-h@..)...P...@..-......`..(......(.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAOQkUj[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):	17726
Entropy (8bit):	7.954223149487974
Encrypted:	false
SSDEEP:	384:N5RNYh8Ldp2QuNIksRs1VBkniuunQ7GnzYZVVN5RCWeuT9+OOIIXrXLhUpVaFIm0:NVw8LdpluNUUVaniDQrFFCubO3LhkVaQ
MD5:	02E0EA2C14E343F8BF0C1D0085818AB0
SHA1:	EAECA7CEA9AF6652E9B0093677B80556E9814A36
SHA-256:	965B23A510DF4D20187AF3E47916099383D0A12D45E07496F4158FC1651C0FAB
SHA-512:	973B0D958201B2A268F10D8DF84FA101E8710F8EE531048C328F200F79EB99D6A5BAAA8919EE20A5276A978D4CB57F42F6450A943A4743CBB4AC6B2D38A70372
Malicious:	false
Reputation:	unknown

Preview:

......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......M.7...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?...wFpk....;d......S....(......Z..+....P.8>..hV....`...q...T..M...4.J...Hf...1I.4.R........u...g....hs......4..b..4.$R*...5.M.beUU...`......b.d.
.C....v.....2....4.B.T.A..Bfe...+...#6Y.r.5@Vv,r.....@....t.h..d.8.B...s@......u"...0.)bH#.`Tm6.72...s@.. [..Q.....J.@...*=)..."..y....:F..pE1.k7\...i..0'k..z.6..r(...+....8.h.1..E!.Wd..*..'
.O.A.i.rl,R./..W..vadP.A.c5";q....]A..y..i.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAOQsTp[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):	12670
Entropy (8bit):	7.939270831353812
Encrypted:	false
SSDEEP:	192:QtbtUec0WZt9KBNd9ZOkIR4HikPP5Zrkiukn3V2e8j/y05TrYLIQDnp32gVgB3W+:+btUec01NdWX6PX5Tb3sRjhQDVaB3z
MD5:	6682068B3AAA5194AC97FA5DF5B8B3EE
SHA1:	7EF86F72723688910C9C91F3B3913DF4AA302933
SHA-256:	89C3CC6BD6B6E7F29EA3B66FE431899B40396259D75B615EC0B4C22C0DBD2DC6
SHA-512:	F71A6B56054524169AAB7CA2CBDB8375871D6B3BCD7046DD86F3E2D3FD5E2D2EBB0702F7C328F3B1989B0DEA4FDEC4AF1ECEBC569A5494D21304F1FA657C7ED
Malicious:	false
Reputation:	unknown

Preview:

......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO........,...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?..s^....f..pO'............}J....p..&.r...j.a.b...@..%...P.P.@..bP#..}..#.......W>'.4......n-....P...1@....1@....J.(.P2+.x.a1L.....MY.N
.../S....ld.-.....sN....qQ..2.A.........3.e.-..w.@<j6...."....6i/..>nn....k.Y.....&]?F......|....{...C.h1.|.GC....W.c.D.....s.RX..=.*.6..!0.....5.K.&."T..I.A..G.zP..I.......b..R.+.....sLCh.P
.P.P.@.@.0:....0...^...sb~.J_..\G@.....P.@....1@.(........J..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAOy0es[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):	43733
Entropy (8bit):	7.961317703200408
Encrypted:	false
SSDEEP:	768:I/PZxocxbZUQp+/8kxb/780ju8QRCe+rHR8ODaHGTTEIDf:I/P5dZUQpa7ZjJM++W
MD5:	BB33723B2FD3802A0032552CEB3D6CCC
SHA1:	A547B562F5F3D0A815DF37A8242EA902F7F56EE8
SHA-256:	5DF17DA5226805DB1C66276F48B6B96FF5EDDA9DF44A7A249B263E5E16998171
SHA-512:	4D99383F065D1DC2F5B0CDA5294F9D23D22EA7A0E115437993C7C9D833E55E46F667301387ECCAF42776366E024C913ED720E8714E353C53D071862841E60885
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAOy0es[1].jpg	
Preview:	......JFIF.....``.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....X.g....-.nh..G.8..Q...r..*d.....*.\..:"..@.8.....(.{.yi.G.JF...4....(.1....@.@.s.@..'....j.q..J.S....@.3q@..(.1... .....}.D..g..Ls3n '.....p.....v&.h..|...^.t.9;D...y..z...-._....f.%....Z.f..b.3..#..Mlr...)...]...S8.`h.t[.Y.U.do.....Y.].8..#.N..{W.....*A....(4..'...4...X..@..... ...(.b.....1h.h.h.....@..-0...@.....P..'..(.h....H....W..-m...U..P...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\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
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\PEJLKQA8\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):	6131
Entropy (8bit):	5.677610945333539
Encrypted:	false
SSDEEP:	96:8zWTgWLrom9v58GohXa8GmEW/zYPGsQ/nhcJZFwPzQGnZofOSSVzZpH/:50XCYUPGV/hczFw8qofoVF/
MD5:	CD1EEC73170720A028CC764C0BA2623F
SHA1:	7AA621FE61808188A0BA460A6E543A7B8815D5D4
SHA-256:	B1CEB37C17BAF1C688E90C1A1B16B0D6707B87BB7B7AE4140FBCA8FB9BBE1B4E
SHA-512:	E1E03A4941ECCF8E445749DA47A88AD54A4EE8F1CF1A6E4DCAC1A69DEF9617DE0361D21DB5F6F89621326CA0F43AAF03DD7EA7A20A79D364EF345537CAFC6AB0
Malicious:	false
Reputation:	unknown
Preview:	..<script id="sam-metadata" type="text/html" data-json="{"optout":{"msaOptOut":false,"browserOptOut":false},"taboola":{"sessionId":"v2_7c48292231b50f06e9d473f8160757bc_10369ccb-c187-485a-92b8-15667c4d6ad7-tuct84c613d_1632820157_1632820157_CIi3jgYQr4c_GMW75uvQwaT9DCABKAEwKziy0A1A0IgQSN7Y2QNQ_____AVgAYABoopyqvanCqcmOAXAA"},"tbsessionid":"v2_7c48292231b50f06e9d473f8160757bc_10369ccb-c187-485a-92b8-15667c4d6ad7-tuct84c613d_1632820157_1632820157_CIi3jgYQr4c_GMW75uvQwaT9DCABKAEwKziy0A1A0IgQSN7Y2QNQ_____AVgAYABoopyqvanCqcmOAXAA","pageViewId":"0a129fc246bc45a38f1df159edc697c2","RequestLevelBeaconUrls":[]}">..</script>....<li class="single serversidenativead hasimage " data-json="{"tvb":[],"trb":[],"tjb":[],"p":"bing","e":true}" data-provider="bing" data-ad-region="infopane" data-ad-index="9" data-viewability="{&q

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\c2cdec4e-bb8a-4f70-befc-5685d78a3a34[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):	70249
Entropy (8bit):	7.97806731305988
Encrypted:	false
SSDEEP:	1536:qs2ZJjT/qHJlyP5JJynXV/+BjjHmTfUwZ+HkOwThjzSYVZkYrA:L2ZJj2plyP3JynXV/+Y4q+kOwT5hVd8
MD5:	96A5780089597E4C3AB3026C93B1916F
SHA1:	3C0B24A0CBB9E4953DA418AB5C173444DB73B82E
SHA-256:	C3E70ED771BBE36197786CB56FE9158F597A139DA4077976D30F6470486C95E1
SHA-512:	B209B11B620F767E98ABA9E4DCD3CA75035B964F4F87E6A65FD5E1E2C4BC32C5104A7F59DF87CB6BB76454505459D5BAA378EA4C5D842B332743CE55CE5AFF7
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\c2cdec4e-bb8a-4f70-befc-5685d78a3a34[1].jpg	
Preview:	......JFIF.....C.....C.....,..".....M.....!...1AQ.. "aq.#...$2...B....%3R...b&'45STcs.(Dgr.....C.....!..1A."Qa.2q.#.....B...3R....$.Sbr..CD.4Tt.....?....l.....kn~..%1..F...3...;~q.b{r.^.Oo.i..... }.v..c9...".~.o..LO}.....i.$.....|....y..3?H.7.q.....|'2...m.;..D..m..?.C....cx/.....3;...y.#.....b'.....G....O.K..5.[.....o.h..{o.n..>..].dDsm.N..{|G.h.....v.w..b7..;nS....tV..L ...w....|o.....*..k..7..f.....|r.....n.1..r.....?....<.....D...>.....=...||m.....+J.K.....y..v..(....._.._.O._.{o..d.I...%..?.}.=."v.....t....O..i.7..h.....d...1.....b{w..3....j..i...'. x.=.gm.;G.....[....[.}8m..H.... n;w...p.1..>...~....bv..&Yf..DR3;.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\de-ch[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	428786
Entropy (8bit):	5.440748083604423
Encrypted:	false
SSDEEP:	3072:kfoJUWxx+hAkJ8RgeGvZQuTrx7rs2yWCmVDHkWnLkZhns4gANkf48YMWA+JxLf:kfovOhW2rxYHkJnoZhMf1oJh
MD5:	1BC26603A8318076CBFE311B7D1FAAF4
SHA1:	58D1CAAE5578B8BC538E19FCA722EF6EB13F9C6A
SHA-256:	FA71DBCFBF07571FFD0B51A81621FA8C36A0A437A82EF33CEA73B29502E33040
SHA-512:	CA65FA5E3B5B0DB1CF29810DCF93095A6F1A79FBEC3775900BEB596317319A3B74B8AAA4CD55B71BD4A55A117E51F66C854D273462A4003F7B3E83D3CC1A7C1
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:20210921_24422861;a:0a129fc2-46bc-45a3-8f1d-f159edc697c2;cn:0;az:{did:951b20c4cd6d42d29795c846b4755d88, rid: 0, sn: neurope-prod-hp, dt: 2021-09-26T20:02:34.8592887Z, bt: 2021-09-21T00:11:57.7792362Z};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 09:08:54Z;axd:;f:msnallexpusers,muidflt10cf,muidflt18cf,muidflt47cf,muidflt261cf,muidflt312cf,pnehp2cf,platagyhp1cf,bingcollabhp1cf,bingcollabhp3cf,compliancehp1cf,modvenduhrsc,platagyhz2cf,artgly4cf,artgly5cf,gallery3cf,onetrustpoplive,1s-bing-news,vebudumu04302020,bbh20200521msncf,weather3cf,prg-hp-nobkplc,prg-sdonright,prg-adspeek,1s-br30min,btrecrow1,1s-winauthservice,prg-1sw-setcogt,prg-wpo-hpolypc,prg-1sw-halfwea,prg-brandupwhp,prg-corec,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\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\PEJLKQA8\medianet[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	410163
Entropy (8bit):	5.48577153719514
Encrypted:	false
SSDEEP:	6144:zfTkYqP1vG2jnmuynGJ8nKM03VCuPbYEWpJi9Wmn:O1vFjKnGJ8KMGxTpWmn
MD5:	3E5BC33D23ABFA7B028AE4A70A0829B5
SHA1:	96B14E216785F29A20C006D9672853A3A7FD6E4F
SHA-256:	F9802C50AA25596A6A84AADFA53D9343B15F0B8B9F36A0BDF9D1B9B63901E571
SHA-512:	4DB74794B85F09B096419EA6F7672363AD5033C7446C8B0A142021FF69880C64C3CBD6875F7F19E5CD22C6BAD7AB520117BDA9E57E3DF01B4A3F3BA310A48B4
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\medianet[1].htm	
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]:{lo gLevel: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 SUPPORTE D":JSON.stringify(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\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\PEJLKQA8\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
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&&

Static File Info

General

File type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Entropy (8bit):	3.5416544878356326
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:	FROqdaZTXE.dll
File size:	2138112
MD5:	24628d042b24ccca20dfc18374ee15c1

General

SHA1:	0deb91aa0e4c63080d71db61bfed0c7a5fb967ca
SHA256:	2c1cbd4e7a27c47468c2e806e5559c3680f1cd6497c33a65c0a565fe8bab1add
SHA512:	dd3c8457810dc1f17d1ea38be7d8884a89fd668a1b8b3d3d41f221e3997ef434e23a716433e7b214503e10649dba430a1bf648c5a8dd23ff494d49a6d10aa23
SSDEEP:	12288:TVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:CfP7fWsK5z9A+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
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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
.kswemc	0x15c000	0x36d	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kaxfk	0x15d000	0x197d	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pjf	0x15f000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.favk	0x160000	0x1f7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vhtukj	0x161000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hmbyox	0x1a7000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.djv	0x1a8000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hpern	0x1a9000	0x706	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.czzwqg	0x1aa000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bzw	0x1ab000	0x896	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ghju	0x1ac000	0x5a7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.karcim	0x1ad000	0x1cb	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.cnwlmb	0x1ae000	0x1a18	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.epc	0x1b0000	0x543	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.czbkvx	0x1b1000	0x573	0x1000	False	0.00634765625	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
.oyf	0x1b2000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qdkm	0x1b3000	0x6cd0	0x7000	False	0.00177873883929	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.onqsh	0x1ba000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ekjyeh	0x1bb000	0x3ba	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gsm	0x1bc000	0x74a	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xewx	0x1bd000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zfgzs	0x203000	0x128f	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ixtd	0x205000	0x543	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vqf	0x206000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ism	0x207000	0x896	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zto	0x208000	0x1af	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.jfsn	0x209000	0x74a	0x1000	False	0.275146484375	data	3.22828923992	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

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 28, 2021 11:09:07.662230015 CEST	192.168.2.5	8.8.8.8	0x3a45	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:10.588468075 CEST	192.168.2.5	8.8.8.8	0x20a8	Standard query (0)	web.vortex .data.msn.com	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:11.183867931 CEST	192.168.2.5	8.8.8.8	0x6590	Standard query (0)	geolocatio n.onetrust.com	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:11.252336025 CEST	192.168.2.5	8.8.8.8	0xaefb	Standard query (0)	contextual .media.net	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:12.304279089 CEST	192.168.2.5	8.8.8.8	0x46a	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:13.689876080 CEST	192.168.2.5	8.8.8.8	0xb787	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:14.190670967 CEST	192.168.2.5	8.8.8.8	0xbdd	Standard query (0)	btloader.com	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:15.399899006 CEST	192.168.2.5	8.8.8.8	0xca00	Standard query (0)	ad-delivery.net	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:15.400742054 CEST	192.168.2.5	8.8.8.8	0xa31f	Standard query (0)	ad.doublec lick.net	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:15.662914038 CEST	192.168.2.5	8.8.8.8	0x96fa	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:16.607076883 CEST	192.168.2.5	8.8.8.8	0x6e5a	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:18.808243036 CEST	192.168.2.5	8.8.8.8	0x118	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 28, 2021 11:09:07.680926085 CEST	8.8.8.8	192.168.2.5	0x3a45	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 11:09:10.622323036 CEST	8.8.8.8	192.168.2.5	0x20a8	No error (0)	web.vortex .data.msn.com	web.vortex.data.microsoft .com		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 11:09:11.205274105 CEST	8.8.8.8	192.168.2.5	0x6590	No error (0)	geolocatio n.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:11.205274105 CEST	8.8.8.8	192.168.2.5	0x6590	No error (0)	geolocatio n.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:11.272911072 CEST	8.8.8.8	192.168.2.5	0xaefb	No error (0)	contextual .media.net		23.211.6.95	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:12.325813055 CEST	8.8.8.8	192.168.2.5	0x46a	No error (0)	lg3.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:13.710603952 CEST	8.8.8.8	192.168.2.5	0xb787	No error (0)	hblg.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:14.211564064 CEST	8.8.8.8	192.168.2.5	0xbdd	No error (0)	btloader.com		104.26.6.139	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:14.211564064 CEST	8.8.8.8	192.168.2.5	0xbdd	No error (0)	btloader.com		104.26.7.139	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:14.211564064 CEST	8.8.8.8	192.168.2.5	0xbdd	No error (0)	btloader.com		172.67.70.134	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:15.420558929 CEST	8.8.8.8	192.168.2.5	0xa31f	No error (0)	ad.doublec lick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 11:09:15.420558929 CEST	8.8.8.8	192.168.2.5	0xa31f	No error (0)	dart.l.dou bleclick.net		142.250.186.70	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:15.420900106 CEST	8.8.8.8	192.168.2.5	0xca00	No error (0)	ad-delivery.net		104.26.2.70	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:15.420900106 CEST	8.8.8.8	192.168.2.5	0xca00	No error (0)	ad-delivery.net		104.26.3.70	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:15.420900106 CEST	8.8.8.8	192.168.2.5	0xca00	No error (0)	ad-delivery.net		172.67.69.19	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:15.683434963 CEST	8.8.8.8	192.168.2.5	0x96fa	No error (0)	cvision.me dia.net	cvision.media.net.edgeke y.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 28, 2021 11:09:16.624279976 CEST	8.8.8.8	192.168.2.5	0x6e5a	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 11:09:16.624279976 CEST	8.8.8.8	192.168.2.5	0x6e5a	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 11:09:18.827445030 CEST	8.8.8.8	192.168.2.5	0x118	No error (0)	crcdn01.adnxs-simple.com	crcdn01.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 11:09:18.827445030 CEST	8.8.8.8	192.168.2.5	0x118	No error (0)	crcdn01.adnxs.com	prod.appnexus.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 11:09:18.827445030 CEST	8.8.8.8	192.168.2.5	0x118	No error (0)	prod.appnexus.map.fastly.net		151.101.1.108	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:18.827445030 CEST	8.8.8.8	192.168.2.5	0x118	No error (0)	prod.appnexus.map.fastly.net		151.101.65.108	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:18.827445030 CEST	8.8.8.8	192.168.2.5	0x118	No error (0)	prod.appnexus.map.fastly.net		151.101.129.108	A (IP address)	IN (0x0001)
Sep 28, 2021 11:09:18.827445030 CEST	8.8.8.8	192.168.2.5	0x118	No error (0)	prod.appnexus.map.fastly.net		151.101.193.108	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- https:
  - geolocation.onetrust.com
  - btloader.com
  - ad-delivery.net
  - ad.doubleclick.net
  - crcdn01.adnxs-simple.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49774	104.20.184.68	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 09:09:11 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 09:09:11 UTC	0	IN	HTTP/1.1 200 OK Date: Tue, 28 Sep 2021 09:09:11 GMT Content-Type: text/javascript Content-Length: 182 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: 695bd4d9a85842e1-FRA
2021-09-28 09:09:11 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 5a 48 22 2c 22 73 74 61 74 65 4e 61 6d 65 22 3a 22 5a 75 72 69 63 68 22 2c 22 7a 69 70 63 6f 64 65 22 3a 22 38 31 35 32 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 34 33 30 30 30 22 2c 22 6c 6f 6e 67 69 74 75 64 65 22 3a 22 38 2e 35 37 31 38 30 22 2c 22 63 69 74 79 22 3a 22 5a 75 72 69 63 68 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":"ZH","stateName":"Zurich","zipcode":"8152","timezone":"Europe/Zurich","latitude":"47.43000","longitude":"8.57180","city":"Zurich","continent":"EU"});

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49805	104.26.6.139	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-28 09:09:14 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
2021-09-28 09:09:14 UTC	1	IN	HTTP/1.1 200 OK Date: Tue, 28 Sep 2021 09:09:14 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: 1682 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=IeMNrm3UUNrob2Pt00AAJo9Y9H3KEFJs R1PimK297Z%2FOfBx42lrtvgjITmdfKJ9gcZtp8XBIaUDZqzDF2fjmVq%2F3dTLQodxbI3sc4WBnw1czxiVUJYqnlh bDm7yK%2Bw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 695bd4ec6bb8430f-FRA
2021-09-28 09:09:14 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))}cat ch(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 09:09:14 UTC	2	IN	Data Raw: 29 7b 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 2 3d 30 2c 69 26 26 28 74 3d 5b 32 26 74 5b 30 5d 2c 69 2e 76 61 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.va
2021-09-28 09:09:14 UTC	3	IN	Data Raw: 7c 77 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 Data Ascii: |window.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_e nabled":false,"website_id":"5671737388695552"}}
2021-09-28 09:09:14 UTC	5	IN	Data Raw: 65 78 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 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 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 Data Ascii: exOf(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,doma
2021-09-28 09:09:14 UTC	6	IN	Data Raw: 28 65 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 Data Ascii: (e){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(n ull!=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.tru nc(100*(s+u*a)),max:Math.tr

Timestamp	kBytes transferred	Direction	Data
2021-09-28 09:09:14 UTC	7	IN	Data Raw: 64 6f 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 Data Ascii: dow.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":626
2021-09-28 09:09:14 UTC	9	IN	Data Raw: 69 6e 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 Data Ascii: indow.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.m
2021-09-28 09:09:14 UTC	10	IN	Data Raw: 7c 5c 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 Data Ascii: |\/)|klon|kpt |kwc\-|kyo(c|k)|le(no|xi)|lg(g|\/(k|l|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
2021-09-28 09:09:14 UTC	11	IN	Data Raw: 74 3d 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 28 29 3b 0a Data Ascii: t=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	192.168.2.5	49816	104.26.2.70	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 09:09:15 UTC	12	OUT	GET /px.gif?ch=1&e=0.5327400408745451 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: ad-delivery.net Connection: Keep-Alive
2021-09-28 09:09:15 UTC	12	IN	HTTP/1.1 200 OK Date: Tue, 28 Sep 2021 09:09:15 GMT Content-Type: image/gif Content-Length: 43 Connection: close X-GUploader-UploadID: ABg5-UzSZ-Kt1WbGdd88HlCnZf7YcJGLu-DR5tPwPS9bXoxAsvJYwt4jGn6LAHoZbG34sctt0vecv7iFCJZExLBCcbRvF7nEjw Expires: Tue, 28 Sep 2021 09:00:17 GMT Last-Modified: Wed, 05 May 2021 19:25:32 GMT ETag: "ad4b0f606e0f8465bc4c4c170b37e1a3" x-goog-generation: 1620242732037093 x-goog-metageneration: 5 x-goog-stored-content-encoding: identity x-goog-stored-content-length: 43 x-goog-hash: crc32c=cpEfJQ== x-goog-hash: md5=rUsPYG4PhGW8TEwXCzfhow== x-goog-storage-class: MULTI_REGIONAL Access-Control-Allow-Origin: * Access-Control-Expose-Headers: *, Content-Length, Date, Server, Transfer-Encoding, X-GUploader-UploadID, X-Google-Trace Age: 3235 Cache-Control: public, max-age=86400 CF-Cache-Status: HIT 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=%2ByFIvZ%2BL8zbKcRbYGAYfVX3z7Y0hSYG5YnxLpm4QArXxRa3eNnfONuwBBWTkEOvbyyleVlHw9Feq72jWIJaOiexG%2F5MZbncvN9G4rr5W3WCZ2rt8Vf7Wo7zYKFFvkQ5zIw%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 695bd4f48db14aaf-FRA

Timestamp	kBytes transferred	Direction	Data
2021-09-28 09:09:15 UTC	14	IN	Data Raw: 47 49 46 38 39 61 01 00 01 00 80 01 00 00 00 00 ff ff ff 21 f9 04 01 00 00 01 Data Ascii: GIF89a!
2021-09-28 09:09:15 UTC	14	IN	Data Raw: 00 2c 00 00 00 00 01 00 01 00 00 02 02 4c 01 00 3b Data Ascii: ,L;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49814	142.250.186.70	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 09:09:15 UTC	12	OUT	GET /favicon.ico?ad=300x250&ad_box_=1&adnet=1&showad=1&size=250x250 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: ad.doubleclick.net Connection: Keep-Alive Cookie: IDE=AHWqTUkh5fOLAUMX20ZV8xqf__2tu45ymTec8GQqE60qWk9cSV6VA3zk_7PBuUk4
2021-09-28 09:09:15 UTC	14	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Vary: Accept-Encoding Content-Type: image/x-icon Access-Control-Allow-Origin: * Cross-Origin-Resource-Policy: cross-origin Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="ads-doubleclick-media" Report-To: {"group":"ads-doubleclick-media","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/ads-doubleclick-media"}]} Content-Length: 1078 Date: Mon, 27 Sep 2021 10:29:54 GMT Expires: Tue, 28 Sep 2021 10:29:54 GMT Last-Modified: Tue, 08 May 2012 13:08:06 GMT X-Content-Type-Options: nosniff Server: sffe X-XSS-Protection: 0 Age: 81561 Cache-Control: public, max-age=86400 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2021-09-28 09:09:15 UTC	15	IN	Data Raw: 00 00 01 00 02 00 10 10 10 00 00 00 00 00 28 01 00 00 26 00 00 00 20 20 10 00 00 00 00 00 e8 02 00 00 4e 01 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 04 00 00 00 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff 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 00 00 00 11 Data Ascii: (& N(
2021-09-28 09:09:15 UTC	15	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 11 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49830	151.101.1.108	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-28 09:09:19 UTC	16	OUT	GET /creative/p/11655/2021/9/15/28299829/89a22c36-158b-411c-9c2c-269457db6c00.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: crcdn01.adnxs-simple.com Connection: Keep-Alive

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>2021-09-28 09:09:19 UTC</td><td>16</td><td>IN</td><td>HTTP/1.1 200 OK
Connection: close
Content-Length: 436596
Server: nginx/1.19.0
Content-Type: image/jpeg
X-Clv-Request-Id: c38a3d4b-0c46-4455-bf61-a49c3ab4ae77
X-Clv-S3-Version: 2.5
x-amz-request-id: c38a3d4b-0c46-4455-bf61-a49c3ab4ae77
ETag: "0f8fa892f54b49eb07c2ad015f5f3b6b"
Last-Modified: Wed, 15 Sep 2021 11:15:21 GMT
Expires: Sun, 31 Oct 2021 10:06:41 GMT
Cache-Control: max-age=3888000
Access-Control-Allow-Origin: *
Via: 1.1 varnish, 1.1 varnish
Accept-Ranges: bytes
Date: Tue, 28 Sep 2021 09:09:19 GMT
Age: 1033358
X-Served-By: cache-lga21934-LGA, cache-mxp6962-MXP
X-Cache: HIT, HIT
X-Cache-Hits: 1, 1
X-Timer: S1632820160.516582,VS0,VE1</td></tr>
<tr><td>2021-09-28 09:09:19 UTC</td><td>17</td><td>IN</td><td>Data Raw: ff d8 ff ee 00 21 41 64 6f 62 65 00 64 40 00 00 00 01 03 00 10 03 02 03 06 00 00 00 00 00 00 00 00 00 00 00 ff db 00 84 00 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 02 02 02 02 02 02 02 02 02 02 02 03 03 03 03 03 03 03 03 03 03 01 01 01 01 01 01 01 01 01 01 01 02 02 01 02 02 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 03 ff c2 00 11 08 02 73 04 b0 03 01 11 00 02 11 01 03 11 01 ff c4 01 2f 00 00 00 06 03 01 01 01 00 00 00 00 00 00 00 00 00 00 03 04 05 06 07 02 08 09 01 0a 0b 01 00 01 05 01 01 01 01 00 00 00 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 10 00 02 02 01
Data Ascii: !Adobed@s/</td></tr>
<tr><td>2021-09-28 09:09:19 UTC</td><td>18</td><td>IN</td><td>Data Raw: 00 07 80 03 d0 00 00 01 2e 23 d1 3e 0f 4e e3 4d 81 e2 34 32 3b 0a c3 30 f4 32 06 b0 2c 09 0c 03 00 9a 5b cf 70 92 22 51 d8 8a 9c 0f 10 d1 4a 0c 46 aa b0 c7 25 0e 05 30 a9 8d 1a 60 6a 19 51 c1 1e d9 00 b1 ed 76 9d d8 30 5a 87 8a 24 45 f5 e8 a1 0c 21 76 33 39 ae 38 d4 39 54 b9 ca 5c c2 83 34 77 ac 12 c0 1b 23 0f 9d 7c 45 c6 20 97 87 3c cc 4f 03 d0 00 00 00 00 00 30 70 89 a2 b0 34 00 00 00 00 00 00 00 00 c4 1a 64 21 d9 f6 cd 49 66 36 63 73 92 98 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 01 81 98 00 0a 62 a7 8d 3d 71 93 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 4b 88 d4 32 57 d4 ee b6 d8 57 56 44 64 16 d5 c6 66 d7 7a 01 c3 6c 8a 99 ee 28 8f 11 98 84 ea ee 7b 8b a2 c1 14 81 c4 01 e0 70 84 0b 88
Data Ascii: .#>NM42;02,[p"QJF%0`jQv0Z$E!v3989T\4w#|E <O0p4d!If6csb=q@K2WWVDdfzl({p</td></tr>
<tr><td>2021-09-28 09:09:19 UTC</td><td>19</td><td>IN</td><td>Data Raw: 76 b8 f9 95 be 10 e6 b5 ca 63 d5 4f 03 20 cc 31 02 81 18 38 02 07 0a 5e 9e c4 a6 0a 05 03 40 7a 19 8b 8a 38 b8 c3 25 67 a8 e3 00 85 6e 48 fc 55 80 00 66 18 84 2a ec 34 ae 26 eb aa 5a b8 26 a3 30 b3 99 e0 60 18 87 a1 98 00 c4 0c 0f 40 90 c4 00 00 00 00 00 00 00 00 00 00 00 07 8e 00 62 e3 36 04 ca 99 06 4d 5f 5c 99 31 70 0c 1c 1b 11 e0 7a 00 00 00 01 e8 78 e3 05 32 69 92 1e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 4b 71 55 b5 67 a0 b1 fa 14 36 19 20 ab 5d 66 7e ab bb 03 85 c0 31 42 2f 34 c8 a5 6a 47 c4 58 14 d8 af ee 8b 05 e6 7a 85 40 f4 2d 77 a0 88 0c 55 35 10 48 d7 7b a4 8c 8d 40 3f 41 19 e9 2b 2d 37 a7 88 76 91 73 89 b9 22 1d 3b f0 54 2d 88 75 a6 89 1a 6c 0f 08 16 c3 30 6a 81 ea 88 d4 4a e3 64 3d 54 6e 85 c9 21 57 3b 4c 52 e0 06 01 e0 1a 06 87 80 48
Data Ascii: vcO 18^@z8%gnHUf*4&Z&0`@b6M_\1pzx2iKqUg6]f~1B/4jGXz@-wU5H{@?A+-7vs";T-ul0jJd=Tn!W;LRH</td></tr>
<tr><td>2021-09-28 09:09:19 UTC</td><td>21</td><td>IN</td><td>Data Raw: 40 a5 00 00 f6 44 f1 42 04 00 05 2c 0b 0f 43 20 cc 0b 71 93 4f 1e dc 55 12 b9 31 6b 96 42 86 48 fc 54 c5 82 46 09 21 b0 a2 48 55 3d a4 38 cc 3d 04 8e 45 cc 53 c0 b6 87 86 60 4a 99 a1 9b 80 d0 01 00 5c c1 f1 1e a9 98 79 1a 9a c0 29 e0 34 da 83 5f 33 6f ea 9f 39 d8 a0 bb 56 45 55 af f8 9b 8f f1 c8 a9 88 9d c6 42 c6 ac 0c b2 a3 73 da 48 cc 1e dd b8 ef 38 77 22 89 6d 54 ad 7e 0d 72 26 22 e0 af c5 8c b9 fb 1c d6 ca c6 29 b4 f5 c3 4c 8d cc 38 17 99 dd 0a 68 47 4b 31 c9 35 eb 23 a8 f4 51 48 73 e2 c9 cc f0 95 0c 09 25 b4 31 55 74 c3 46 b8 49 0f 95 9e a3 9b 6a a2 b1 4f 7a 19 31 1b a3 61 fa cd 7c a4 56 fa 6e 47 3c 0f 32 c8 6c 42 c9 44 6e 18 e2 47 39 55 43 8c 98 1c f4 46 82 97 19 a8 96 31 43 cf 54 ce 35 c9 0f 50 c1 4c d8 60 06 80 04 c0 6c e8 42 b6 ac bc 9a 8f c2 75
Data Ascii: @DB,C qOU1kBHTF!HU=8=ES`J\y)4_3o9VEUBsH8w"mT~r&")L8hGK15#QHs%1UtFIjOz1a|VnG<2l<br>BDnG9UCF1CT5PL`lBu</td></tr>
<tr><td>2021-09-28 09:09:19 UTC</td><td>22</td><td>IN</td><td>Data Raw: 34 58 e5 19 12 c2 1d 69 fe d6 46 c8 48 d4 4c 95 d8 86 45 62 c4 7a b3 24 17 22 7a b8 e8 cd 61 ee eb 11 21 0f a8 c9 2c e2 0b 48 dd 21 21 6a 1d 56 77 a1 7d 02 d8 aa 5e 80 13 8e 30 6e 00 40 2d 61 9b 53 07 29 11 2a b9 42 1e dd 77 bb 4f 4b bc fb d0 1d 68 ef 6e 76 c6 75 f3 d4 f9 f0 55 01 e0 7a 00 00 78 c1 33 5d e4 ed cc 12 a8 a9 a1 a8 d0 3b 20 30 31 0f 15 0a 91 3c 89 de bd a4 48 d5 90 c8 10 c5 e9 82 99 c6 a4 bd be b9 4d 6a e0 c0 4a 82 25 30 3c 00 04 ca 87 31 70 69 98 79 22 32 b5 72 7a 9e e6 b9 44 a5 2a 18 04 cc c5 10 48 9a 56 e2 e5 47 2a 67 0a 01 c8 da 38 aa af 80 f0 09 71 83 d0 c8 9c d3 14 f9 c6 38 d9 af 13 b5 16 a5 73 da 7a 49 c9 77 c9 36 69 48 32 1b 3d c2 e8 e5 50 8a 50 c1 af 4a f6 c0 ed cc cb 61 5a 96 32 d2 0c 66 4e 94 fa e7 95 36 d7 ae 4a 2e 0d 5c 5a 20 8a
Data Ascii: 4XiFHLEbz$"za!,H!!jVw}^0n@-aS)*BwOKhnvuUzx3]; 01<HMjJ%0<1piy"2rzD*HVG*g8q8szIw6iH2=PPJaZ
2fN6J.\Z</td></tr>
<tr><td>2021-09-28 09:09:19 UTC</td><td>23</td><td>IN</td><td>Data Raw: ed 73 b2 84 b1 3d 9d ab 21 7e 12 21 60 78 35 55 0f b0 3a 86 2a 78 a7 ad 33 02 d5 b9 0e f5 00 18 b8 49 22 2d 85 4b 03 00 01 32 a1 32 07 c2 a4 c8 20 73 73 6a ab 68 b2 35 6e 95 a7 39 09 7a b8 d4 72 79 10 f6 29 32 a6 71 aa 39 50 95 1a 2c aa d8 91 7b 0c 5e b9 c6 89 27 61 b1 bc d6 98 4a c4 b5 a5 2a 9c de ca c5 8c 57 a9 a2 48 e6 9e c7 10 f4 85 59 ab a2 9c c6 df 3d f8 7f 57 3b 77 21 5e 2a 4e b9 8e b6 64 d6 b9 b5 14 b1 1a 15 f5 e5 fb 0d ae 8d 9d f0 a1 73 5f 35 a0 ea e7 b4 f8 84 76 04 11 06 38 22 27 22 8a 56 b6 0b 64 87 4a eb db df fb 6c bb 59 55 c1 ef 74 57 f8 c7 43 b0 e6 43 94 f8 b5 57 3f d8 82 6f a3 0c 4a c4 67 dd 24 d5 a5 61 89 2b 1c 42 e3 d3 b8 f3 66 9b 9e 8c 75 86 45 c9 d5 da d2 5b b1 c2 b3 09 3d c7 60 d9 54 49 12 b9 4a c3 3e 46 68 68 db fa d6 09 84 72 91 59
Data Ascii: s=!~!`x5U:*x3I"-K22 ssjh5n9zry)2q9P,{^'aJ*WHY=W;w!^*Nds_5v8"""VdJlYUtWCCW?oJg$a+BfuE[=`TIJ>FhhrY</td></tr>
<tr><td>2021-09-28 09:09:19 UTC</td><td>25</td><td>IN</td><td>Data Raw: 72 63 72 ab 51 c7 9c 8e 4e 55 b5 e4 58 d5 ce 46 e7 13 b2 0f 40 06 2e 0b 53 26 86 20 03 c7 1e 3a 22 1c e2 9c ec 00 c6 a2 b8 9c 4b 82 de 86 31 3c 47 17 2a 62 e0 c0 4e 22 97 23 2c f2 2b 8d 32 68 4b c0 a3 b5 30 c6 88 66 4c 95 59 e4 0d 90 cd 0c 55 4f 03 63 44 6f 13 0d 7a 63 82 37 01 5a 44 7f ae a8 e5 0c 78 99 e2 d8 44 ef 15 42 12 f3 05 16 b4 29 12 a7 b3 4b 9e dc 47 47 cd 9e 13 d9 99 7a 4e 77 3e 6f 46 fc e6 7a 7b 02 20 e8 5c a2 24 41 29 4c 5d b0 d4 e5 63 96 b2 27 b5 fb 7a b7 68 7d e7 e7 98 ac 0a 42 0b 5c 85 a8 d1 56 44 30 3e 4c f6 e8 cc 6e de 8b 2f d9 a8 aa 38 3a 77 49 53 1a d2 b3 44 43 79 5b 56 2d f8 29 9e 77 53 9b 6f e1 a4 92 dd 9c e0 f3 7b 69 b5 d2 ec 57 45 6d c6 69 4b 18 44 72 e2 af 39 d0 e2 a8 aa d8 c3 cf 95 76 3d 79 17 41 5a e1 e9 ae 17 5d 6a 6c 9b 2d d1
Data Ascii: rcrQNUXF@.S& :"K1<G*bN"#,+2hK0fLYUOcDozc7ZDxDB)KGGzNw>oFz{ \$A)L]c'zh}B\VD0>Ln/8:wISDCy[V-
)wSo{iWEmiKDr9v=yAZ]jl-</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
2021-09-28 09:09:19 UTC	26	IN	Data Raw: b4 96 53 10 39 3e 59 ae 9b 3d 7a 01 ab 2c b2 3d 04 aa e1 84 ab e1 38 92 bc 59 4c ee 46 e3 20 4c ab 06 82 3d 6b de c7 e5 07 87 7b 9c 4f 13 b6 ea 1e ad 6d f6 f4 ef 9f ca b4 d2 6c c2 ed 21 8e 64 ef 1a 15 fc b4 8d d3 b0 e6 0e 75 a5 45 65 0a 55 5f 4d cd f7 1a e1 5d ca ab 27 8e 0b 78 a6 27 78 a2 19 88 fd 85 70 68 d8 e6 b9 c6 32 ca c5 4b 28 96 23 51 a6 c4 f9 2e 7b c9 91 5b 2d 2a b8 5a 15 58 66 1b 9b 09 89 33 e4 28 8a c3 b1 85 a8 ec 24 aa b8 9a 52 31 13 95 ca e5 ee 8e 1f 51 1c a6 7c f2 bb 23 f7 1c f7 59 d1 6b 22 06 b5 5a 0e 70 2b 14 a9 ec d1 c8 61 91 a9 ea 53 d5 d1 b0 b4 3d a6 ac d2 ca 2b 4e 5a cf e6 27 9f f5 7c d1 f3 ff 00 6b 68 ed 3c b6 93 e4 bd 03 76 f8 9e de ce a5 03 c5 47 1a c1 9a 77 6a ae dd 8c 1f 13 0d 8a c9 1f 1d 89 d6 e4 f7 3b df 3e 75 85 44 a9 9a f7 c9 Data Ascii: S9>Y=z,=8YLF L=k{Oml!duEeU_M]'x'xph2K(#Q.{[-*ZXf3($R1Q|#Yk"Zp+aS=+NZ'|kh<vGwj;>uD
2021-09-28 09:09:19 UTC	27	IN	Data Raw: df 65 cd ed f1 a8 a5 ac f5 ce 45 23 7c 88 5e 8f 46 e9 33 65 82 63 6e a5 ad 4e 7d a4 d4 9d da 6d b3 ac 43 9f d8 bd 49 ef d9 22 dc 6b d4 b6 7e 48 8a a4 e3 15 e5 d8 ae c7 29 37 81 0b 6b a9 65 a3 cb 2f 2e ed 39 05 e7 7e f3 0e de c0 47 cf 6e ef 0f 13 d6 d9 75 1b 2b 86 15 e8 ac 89 36 a3 6f 59 6f 1c cb 3d 78 e5 ba 97 3f 7b cf 77 a7 de fe 68 87 c7 32 30 90 83 7b 5d 5e 56 94 aa d6 e6 13 56 5a f6 af b8 6e 9e c6 5b a4 51 d7 59 7a 1b 11 90 bc 70 f0 ff 00 a1 37 8b b8 f2 9f 9d af 99 39 0f a5 4f a9 17 93 1c 6b ee 19 39 5d 98 97 ae a7 ea d3 3b 3b 3f 65 bd 07 47 9f 7e 3e dd b0 a3 4e 1f 97 76 61 ea 97 74 9b e7 ba 32 2e 9a 86 c8 74 d7 f5 ab 83 ab 3d f4 ba fb df e9 bd 25 04 ba 1b c5 b3 90 e9 a2 8d 31 ce 8e b3 52 42 27 91 b2 2d 86 f1 3f c9 29 74 93 a2 8b 62 fa cd 6c 95 54 ab Data Ascii: eE#|^F3ecnN}mCI"k~H)7ke/.9~Gnu+6oYo=x?{wh20{]^VVZn[QYzp79Ok9];;?eG~>Nvat2.t=%1RB'-?)tblT
2021-09-28 09:09:19 UTC	29	IN	Data Raw: eb 3d 20 d3 87 ea 37 73 99 b5 33 9e 5e 95 5a 62 6c 8e 4e 79 27 6b c5 0f 33 fa 19 b3 b5 e6 9f b9 1d 0d bb f3 9f 45 b5 ab 36 59 00 b5 23 69 8a 5d 34 df 7b 73 9b e8 91 bb 71 6c 9f a8 71 dd d5 fa 17 e6 78 35 59 09 52 4b 61 cd b4 ca ce b4 85 b2 d4 c6 58 9e 1c c3 6d a6 e3 6d 64 4d eb d7 a6 e0 d6 da 5c 36 40 b9 2d 6e 76 79 f7 ae ee e7 61 e2 9f 28 ff 00 3e c3 ba 3e f7 e7 9c e9 f8 a3 d0 eb 8c 08 fe 86 fa 7e 2d eb e9 be b2 d8 ca b1 0b ec 77 2a 9f 04 f2 cb c1 f6 35 8f d3 3d 8a ad f3 7e 23 4a 39 44 db 4d 6e 4e 33 8d d0 6f f7 ba d6 e8 d7 ae 76 50 18 b3 ef 8b d6 8e 72 23 ce 8d be 94 4d 9a 7a df 35 7e 21 cb c6 39 e8 be 8d bd d3 5a 09 97 6e f2 ea 1b e5 ba 6a 20 af ac 5c f5 76 aa 10 cf dd 33 74 b5 b6 5b a2 dc 83 41 16 b2 53 a7 b5 3b 4e 9f e8 5f 6f 7d 3f 33 e7 69 8a e6 68 Data Ascii: = 7s3^ZblNy'k3E6Y#i]4{sqlqx5YRKaXmmdM\6@-nvya(>>~-w*5=~#J9DMnN3ovPr#Mz5~!9Znj \v3t[AS;N_o}? 3ih
2021-09-28 09:09:19 UTC	30	IN	Data Raw: 46 8d 3f 1f 5b 5b 9f 9f c7 0f 13 f4 1e 37 79 67 d3 b5 15 0d db 12 93 77 23 05 6e ca 09 24 89 8f 91 31 a9 5f a5 1d 1e ab 30 d5 2a d8 da c3 b9 9e db e6 dd c1 fa 17 e6 78 15 5b 85 b8 96 4d 0b 35 59 6a 7a 52 fb 5e dc ae 58 25 13 56 8f d9 97 70 b7 32 ed b6 d4 a6 69 e8 ed 0e 6a 7c 42 7e 42 59 fa 5e fb 7e 0a 01 fe ff 00 25 a7 e4 3a 63 9b e7 48 7d 33 3f 8e 5f 27 75 7d 48 cf e6 9f 2c f4 fa 4f d3 72 7d 6c f4 9e 87 53 ea 71 92 6f 18 d8 a2 ea 5d a5 7b fe d3 58 a0 a3 d6 5a 74 6c 2e de af 5a 3d ce 65 c4 90 de 8e 59 f4 1a 57 fc 4f 4f 4a 5d 2a af 89 c2 6f 38 e5 91 7c ea d7 1c 79 fe 88 fe e4 ea 6c 1b da 73 87 b0 c5 8d be 79 6a ac 96 48 6e ba 9e c7 ca ac e2 ad ba bb 7d 2e a7 50 66 f4 ec e6 43 a8 1a c4 fb 73 1a 0c b6 e7 72 56 e8 c3 a9 55 8d 57 8e fa e8 16 4d 24 fa 81 ce f3 Data Ascii: F?[[7ygw#n$1_0*x[M5YjzR^X%Vp2ij\|B~BY^~%:cH}3?_'u}H,Or}!Sqo]{XZtl.Z=eYWOOJ]*o8\|ylsyjHn}.P fCsrVUWM$
2021-09-28 09:09:19 UTC	31	IN	Data Raw: b2 f1 87 d2 3c 81 aa 69 db 52 de 4f 82 67 33 24 70 cf 2e af 66 3f 35 3b d6 2b 55 95 bc 88 9c b4 be b3 7a 36 77 7f 47 93 95 cb 1a 29 0d 59 66 77 13 bc 53 bb e2 8f 8f fd 59 4d b7 5a cb cb 5d eb e7 1d 76 d3 6b f3 a9 d8 7d bf 28 ed e8 9c 4e b8 db bf 15 af 79 9f 37 4e 17 09 bd 3e c1 c3 f5 43 d6 bc 2e 0f 5e da 21 5d 1d 1b 15 25 aa e8 5e 67 a1 72 c6 bb 52 cc bd 5e b8 92 4d bc e9 f3 76 1e 5c 8a 47 27 53 66 22 8f e1 53 f2 23 ae d5 3b d1 32 e9 6a 75 d3 ab ea ed 2c bf 2f a5 b8 3e 3b 6c fd 0b bb e5 1f 99 51 f2 6e 47 a2 9e 99 0f 16 ba 79 7a e5 c0 4d c8 df 60 d1 33 95 7e c3 5a 99 06 45 0e 82 58 d6 ec 17 de be 60 db f3 1f 53 b2 1d a7 47 b2 bd a4 ae ad b3 f3 67 f2 36 6d 75 d9 e1 73 7f 99 dd de dc 1c be 99 75 16 7b 4f f4 af 4a 9e 41 eb 4a 34 51 3a 8e cc 99 36 74 72 6a d2 Data Ascii: <iROg3$p.f?5;+Uz6wG)YfwSYMZ]vk}(Ny7N>C.^!]%^grR^Mv\G'Sf"S#;2ju,/>;|QnGyzM`3~ZEX`SGg6musu {OJAJ4Q:6trj
2021-09-28 09:09:19 UTC	33	IN	Data Raw: 63 31 9b 48 8e 45 da 87 13 4d 23 d9 15 60 dd 6a 9c e7 42 07 4b f1 7b 14 f6 25 98 64 ec 4a 9f 3e 79 95 f8 67 f3 d7 68 15 e9 cc e4 1f 98 fa 77 ce a7 97 7d 07 4f 5b cf 7c 8b 56 bf cb f4 9d e4 aa 95 ed 7c fd 00 ef bc 57 54 ba 6e 21 f9 5d 84 f5 2a fd ae 7b a0 f8 dd 37 df 7f aa 79 55 f1 06 79 0a 85 c8 69 5c b8 9c 24 f1 2e eb e7 af cd 7e 99 a3 6c 68 5f 99 36 ba 25 c0 ed 5e 39 91 f4 73 eb bf 9a 6a 39 32 f5 e7 9b ec 2b 5c ad 58 fb 24 c6 66 46 91 cd ec 6f 83 de 92 45 16 21 2e 48 d4 d8 1e 5a e5 8e 89 fa c2 3f d8 83 61 bb de 47 aa fe c5 e7 bb 7f 73 06 81 c8 d0 d9 69 ab fe 7e df 97 7d b5 75 66 b5 77 c2 51 b2 79 0d 26 3d ed 3f ae cf a9 7c 8f 5f 75 3d 0f 8b 1f 3a 72 95 97 39 6e b6 f4 6c dd b1 e0 73 79 dd e9 bb 5c f5 f5 eb 1b f3 e7 54 2c 7b 8e 44 b5 fb 79 c7 eb f3 c2 ab Data Ascii: c1HEM#`jBK{%dJ>yghw}O[|V|WTn!]*{7yUyi\$.~lh_6%^9sj92+\X$fFoE!.HZ?aGsi~}ufwQy&=?|_u=:r9nlsy\T,{Dy
2021-09-28 09:09:19 UTC	34	IN	Data Raw: d5 6f a1 7c ca ea eb 33 7a 6f f9 ed f7 ef 15 f5 79 ea ab ea 7f 9d f6 7f b6 f3 1d 59 f9 97 da 8b 57 46 1b 1c aa 27 be 04 96 37 49 eb b7 f4 9b 45 d8 bb 2c 8e 23 a3 94 e5 b1 6c 40 a9 a5 67 95 66 08 e7 db 3b 14 e7 74 dc 6a 0c 03 23 12 be 6c 31 c6 32 95 af 66 73 b7 59 20 57 f0 c0 e5 7a 3a fb 94 dc f8 d2 f9 ff 00 ea bd 77 65 b4 69 66 43 8d b7 30 cc da a3 fb 6f 32 e6 5f ba fc d9 13 d8 c6 96 2d 99 a2 16 1c 4f b2 11 bf 59 af 7f 76 21 ca 4c 89 a2 75 a8 f1 57 ca bb 1f 97 2e 3f dc b5 5b 55 36 cf 0f a0 e9 87 9e 75 db 57 bb ca c0 f5 ea de de 8f cd 5a 9e a1 e7 74 0f 8a 77 e8 72 ad 60 a3 4c 81 16 e3 6b 95 8c d9 f6 97 c2 af f2 a6 72 1e aa 18 aa a2 48 de 67 64 e6 78 be 70 ec d1 da cc 5f 5d df 0d ba 7d 3b ea b9 a9 37 8c 7c 8b b8 97 76 b9 f7 85 d7 7c b2 60 72 d3 da b2 5d d1 Data Ascii: o|3zoyYWF'7IE,#|@gf;tj#|12fsY Wz:weifC0o2_-OYv!LuW.?[U6uWZtwr`LkrHgdxp_]};7|v|`r]
2021-09-28 09:09:19 UTC	35	IN	Data Raw: f3 e1 eb a4 f9 f7 6c d1 4b 70 cc 1c 8c af 5d 80 9e dc ed 8f 6b 68 90 8f d6 ba 34 91 4a e5 99 2b 6b 6f 07 61 cc f4 87 ef 9f 99 7a d9 e6 7d 6e 9f 52 bf af 1e 9d c4 fc b7 7c 19 f5 16 ce f2 7b ed a3 d5 35 aa 51 49 6a 1c d5 35 59 6e 45 37 de 44 0b db 84 81 14 85 7d 4a 65 8f 35 6b 93 d3 b2 f6 29 cd a4 58 eb d2 c3 bb 56 73 34 7e 0b 1d 94 73 44 ab 6b 3e 79 61 53 cd 05 57 c8 ec cd 50 8e d8 89 6b 60 2a 0b 7f 1a 0c c9 f9 2c e9 ca fe 4b 1b 46 97 2e a6 a4 7d 18 6b a5 96 3a 48 2b 12 42 e8 a4 24 d3 91 2c bd 0c ec 9c 32 d1 be a3 81 ec 74 53 cc fd 4a cf 8e 4b d3 26 ed 87 4f 4b b6 de e7 e3 1c d9 f3 eb df 3e b7 fa be d3 73 da b3 fa 97 ed e7 45 b2 7f 41 f9 06 b4 78 ff 00 61 7e 72 3b 2d f3 23 7c 86 0e 47 15 00 37 46 10 f1 c9 5c d1 b5 9f b0 9e b1 e4 ff 00 2d be 1b f4 3f 65 3d Data Ascii: lKp]kh4J+koaz}nR|{5Qlj5YnE7D}Je5k)XVs4~sDk>yaSWPk`*,KF.}k:H+B$,2tSJK&OK>sEAxa~r;-#|G7F\-?e=
2021-09-28 09:09:19 UTC	37	IN	Data Raw: ce 08 ed 27 d8 41 25 8a 26 b4 1b 93 66 c3 00 47 1a f7 08 c8 73 9b 75 4c f6 5a ed eb b7 dd 5f 2e fd 0b 72 1d 25 ad b7 95 c0 9e f3 99 f9 c6 f8 9b e9 6b 77 8d df 24 93 c1 b9 21 95 77 46 a5 ad 49 b1 fb 1e 92 5c 89 27 73 a7 af f4 1f cd df af b3 b5 68 9c ad ea 82 a6 a5 47 ce ec d1 f8 db d5 6e 4e ba 1b d3 4b fa 0c d9 b7 59 cf 4f ba 7e 72 ce e9 79 cb 87 a4 e6 ae 6e 8f 9f bb 7a 0e 76 ea d5 c6 b0 d6 84 fa 06 ce b2 63 f8 06 e0 22 e1 d7 19 ed 68 56 cb 80 db f1 d6 7c 05 49 23 63 58 b8 94 c4 8a 58 93 62 91 af 59 2c 40 40 d7 38 0c 87 bd ae 2d 9b a6 be 33 eb 31 6e 0f b1 a3 35 72 6d ff 00 49 e6 34 df 88 d7 e9 d7 75 4f e8 4f d1 fc 58 9b 11 fa e6 e0 e8 be 50 fc 47 d8 35 52 df 53 f5 a3 e8 3e 65 2a e5 ad 6b 77 1d d7 22 82 c2 47 b4 87 a1 d2 d7 3e 68 9b 9b 32 b8 a6 6d aa ef 26 Data Ascii: 'A%&fGsuLZ_.r%kw$!wFl\'shGnNKYO~rynzvc"hV|#cXXbY,@@8-31n5rml4uOOXPG5RS>e*kw"G>h2m&
2021-09-28 09:09:19 UTC	38	IN	Data Raw: d2 0e 9f 0f 9f 9c f6 ff 00 cc e7 c7 3f 42 4a b0 b4 12 b2 35 cb 2a 69 a1 6c b1 16 b4 36 aa 38 a7 9e c0 fb 61 b7 6c c9 1f 3d 92 0f a2 6e a3 90 fa 50 a7 37 cb af c5 7f a8 ff 00 46 3f 45 fc 4d be df 4a fc af 92 37 36 b8 d2 54 6c cb 80 63 4d 49 72 fd 4d 2f c7 f5 d4 d7 2b d8 54 bc bf 53 51 f3 3d 55 3d c6 f6 7a 7f eb 9e 29 f3 69 eb 1c 03 15 4b 6d e3 9f 59 79 dd 90 c7 d5 d1 e7 25 b2 b6 dc d6 05 8a ad eb 2c d6 16 ba 4b 6d fd 91 37 a3 67 c8 af b1 c8 5b dc 62 31 d1 87 33 31 6b eb 6d 6d 1b 82 87 51 b6 7e 63 ee 1a a7 db 79 d3 92 db dd be 3b b3 9f c9 49 b2 c6 6a 19 69 df b1 74 7a 57 73 9c da da 2a b6 bb d0 8e 21 ec ca 6a be b0 8a ca ca e6 68 62 96 1a d9 2b 19 61 96 4b 4f 53 ee 8f 7b e4 0e 98 d1 df 90 58 d5 d5 9d 3a fc ee f6 47 e8 6f 23 ac 57 9d fa 37 2b a2 a3 4d d0 db Data Ascii: ?BJ5*il68al=nP7F?EMJ76TlcMIrM/+TSQ=U=z)iKmYy%,Km7g[b131kmmQ~cy;IjitzWs*!jhb+aKOS{X:Go#W7+M

Timestamp	kBytes transferred	Direction	Data
2021-09-28 09:09:19 UTC	39	IN	Data Raw: b8 b9 ee 8e 1e c6 4f 63 87 60 f3 5e c9 57 43 69 35 32 b9 71 f4 47 c9 55 85 2a b3 d8 d2 5a d9 2e b9 eb ed f6 85 79 bb 91 b6 26 57 50 cd 09 a7 2a 4b 74 78 5d ec 1e 1d cd 4e 6f b8 47 1d 84 8e 63 c3 e4 75 4b 2d 0a c7 38 dc c6 d4 35 a3 34 b2 2d 47 3c 2b 5f 98 af 43 17 2c 8e ca ae 30 ca 95 c4 cc 85 f9 23 71 69 2b ae ee 05 55 65 f7 cd 7a 3d c7 c6 7a 26 91 fa d7 ce 8f 70 6a 4d b1 7b 2c 14 6c b3 4f d8 53 a9 f9 dd ce e1 37 a0 e9 f7 d9 9f 24 c6 79 e7 ea df 09 d8 4c a6 6a bc b9 ab bc b6 9f 04 9c bf f3 fd cd 2f b9 bd da bf 41 e1 59 f3 59 d4 3e cc ef b7 ce 9c 86 e2 55 9a c9 9a 33 ad e9 fc 66 74 3d 07 17 b4 21 83 d7 b4 c9 0b 88 8a fb 54 2a 64 53 e2 e7 cc 85 76 70 fa d9 64 ab 2d 62 b5 5e 06 b8 bd 93 d6 4b 4b cf 10 7c 1b aa ca 5f 72 7e 81 c4 93 53 62 9b cd bb 42 e2 ef eb Data Ascii: Oc`^WCi52qGU*Z.y&WP*Ktx]NoGcuK-854-G<+_C,0#qi+Uez=z&pjM{,lOS7$yLj/AYY>U3ft=!T*dSvpd-b^KK |_r~SbB
2021-09-28 09:09:19 UTC	41	IN	Data Raw: 99 d1 d5 14 36 2b 69 a3 c2 29 e4 8e 72 95 91 f4 72 16 c6 8d c8 5b 15 ac 8f 14 47 26 d9 77 16 5c 2b 13 e3 7d 6b e4 4e 73 83 1c ee f6 bb ba 4b 56 37 d8 62 9f 24 df 6f 1d 04 1b 63 9b 94 d5 5e c6 97 d5 9f 46 ab bf 45 ea cf a1 cd b3 a3 51 1a 20 e2 4f 9b d1 ef 47 94 fb 6d 0b ef 9f 37 da f2 d7 b1 61 9e 40 b5 ea 59 32 9a f7 aa 3f e4 1c e4 f1 ef 74 e8 37 b0 f9 e5 a1 6f 0a cb a2 f8 9e e3 3b 99 ca 52 d4 bc 0d 8d 60 ca d7 a0 b9 ed fd 4d cc d3 a2 e7 92 ec e9 39 38 4e 9e 7c 46 a5 d4 90 ce 58 f0 f6 3c 09 2d 6c 8a c9 a3 65 32 dc d7 f9 eb db 2b 61 86 5a 9f 43 fe bb e5 1f 55 7e a5 cb a3 8e 54 ed 4f 05 26 16 f9 1a 60 a7 8d 79 63 4a 53 d5 4c 50 f0 0f 0c 80 d7 22 c9 18 6a a2 95 16 08 12 85 77 cf 5a a7 38 fe c6 9f e4 fa ca 67 93 eb 6a 0e 37 b3 ac 78 8e cf e5 43 e9 7f 9e 34 5b Data Ascii: 6+i)rr[G&w\+}kNsKV7b$oc^FEQ OGm7a@Y2?t7o;R`M98N|FX<-le2+aZCU~TO&`ycJSLP"jwZ8gj7xC4[
2021-09-28 09:09:19 UTC	42	IN	Data Raw: c9 d8 fa 1c ea 74 bb 97 1f 22 e8 d7 3d ab 9f de 3d b5 c6 2b 04 35 fe 06 28 52 e4 c7 55 d4 c8 74 a0 da 4f 40 c9 fb e4 e8 bc 8b 05 33 13 d1 8b 48 56 b1 c6 42 30 d1 b9 ab 7e 57 dc f2 4b c9 bd 23 e7 63 9d eb 74 02 fd 36 a8 90 31 ce 91 dc 9d e6 e9 cf 28 e8 6e 3d 2a 9d 70 c9 83 a4 1d 77 1f b1 9e ab c5 0d 27 d5 dc d7 51 49 f1 fd 75 17 c7 f6 14 af 15 da d4 fc bf 64 c7 5b 5e 21 7f 12 9e e8 79 ca 67 73 9b a9 7a 1c 0a 7b 7f 99 ab 7a 2e 5a a0 dc c2 80 ec 66 46 b5 a8 5e 74 ee 5e 99 9a 56 25 77 4f a2 b7 3d 86 4b 02 29 25 68 d7 74 2c 98 a0 a7 fb af 2f e8 65 dc 4b 2d 97 f4 3f 72 2b 69 ce b4 ab 24 17 5b 5a 09 65 4b cb 9f 67 6e e7 ec de 95 1d ae bd 5f 67 f5 73 f6 b2 5a b6 3d 57 f3 9b c1 fd 7b 0c dd 05 4d 99 63 26 85 91 e8 cc b1 e8 45 f8 74 72 c4 5a 33 6e 9e a7 49 0e ef 41 Data Ascii: t"==+5(RUtO@3HVB0~WK#ct61(n=*pw'QIud[^!ygsz{z.ZfF^t^V%wO=K)%ht,/eK-?r+i$[ZeKgn_gsZ=W{Mc& EtrZ3nIA
2021-09-28 09:09:19 UTC	43	IN	Data Raw: a4 e0 d4 83 dd c4 aa b7 79 da 93 7b 9d a8 ba 0e 7e 9b dc e6 69 0e 8f 95 ae f6 72 a4 53 36 5d 1b e6 15 e7 b1 9b 66 d8 ad 3c d2 21 fa 16 bd b5 ef 0d 95 de 77 49 63 64 b9 6d bf 32 aa 88 86 59 d9 53 58 8b dd 48 b6 f3 42 2d bf bf 47 6c 37 33 36 17 57 2a f9 d6 cf b4 b7 b1 b7 06 6a 72 29 33 d1 ce a5 00 7a 67 22 64 f6 94 f8 0c 00 1e 24 5e a3 4a 04 0b 23 68 d6 87 35 24 a8 a9 a3 ec 4d 94 a3 de 9a be 43 24 02 9d fe 7d 79 af aa f2 e7 94 d4 e2 75 ec ce 5e e8 d2 d6 82 5f 51 e6 35 31 24 6c 54 75 59 67 8d 59 b9 34 e1 8f b0 ed c3 b1 10 6b a0 e0 3b 4b 8a 64 ee a1 81 d4 b6 bd 95 93 b4 d5 94 8b d9 76 1f 51 c8 6d 2f 75 c1 53 70 5e d7 4e 53 ad a8 b9 bd 66 f8 2d 37 50 da 49 47 44 f5 99 45 fa 5b 01 ef 1e 3f be de 91 e5 7b 19 90 df 80 ff 00 3c f4 4e 41 f2 1d 34 19 8e ab 9b 6d 3b Data Ascii: y{~irS6]f<!wIcdm2YSXHB-Gl736W*jr)3zg"d$^J#h5$MC$}yu^_Q51$lTuYgY4k;KdvQm/uSp^NSf-7PIGDE[? {<NA4m;
2021-09-28 09:09:19 UTC	45	IN	Data Raw: de f7 a9 4f ba 3c 47 ad cc 97 cd 9c 77 ab 30 a4 7b d1 a2 24 86 68 8c 16 e3 8f 6d e3 af 85 7a 19 cf 55 9b cb aa d6 be 5b 7e 60 f7 ee 09 f5 19 34 f6 8c 11 67 b4 f5 7b da 39 ec 27 f3 5a de 7c 7d cf 7a 9c 3d a4 ee 39 4e 80 f4 9c d7 c7 ff 00 8f f5 4d b9 9d 23 90 da 6d 22 cd b2 5e c5 aa d2 1a d2 a9 65 2d 92 c5 96 07 26 b9 d5 16 44 8e 76 6c 89 54 5e 3c b8 62 5a 4f b0 ee d4 d9 bc 8a da 39 6d b6 5c 2f 9e 57 b0 e5 1c 9a 8b 6b 1a bd af b3 be 7a 5d 66 e1 f7 5e 29 55 d2 ee ab 1e 47 a1 ae 34 33 5a 5d 0c 62 38 53 55 77 91 5f fb 3c a3 b9 60 4f 5b e8 8b 67 ce fe 3a 79 a6 fc d5 5c ef a4 bb 15 a6 5a cf 95 79 b9 c7 8e 87 83 da 6c 17 f5 2f 23 b3 b8 2a 54 a5 0c f7 eb 7a fb 1f 1c b5 54 3c c4 0a e6 9e ca 9a 6f 94 73 6a 36 56 7a b1 a7 3c 8a dd 96 d7 30 c5 97 ac 4c b6 9e 86 e3 55 Data Ascii: O<Gw0{$hmzU[~`4g{9'Z|}z=9NM#m"^e-&DvlT^<bZO9m\/Wkz]f^)UG43Z]b8SUw_<`O[g:y\Zyl/#*TzT<osj6 Vz<0LU
2021-09-28 09:09:19 UTC	46	IN	Data Raw: a9 6d 11 b1 46 0a 34 ce 14 a2 15 25 c0 3e a2 e8 b0 0a ac 1b 4a 7c 5b 7f 21 e9 9d 79 05 d2 b7 97 e0 67 00 b0 df 48 87 e0 c3 71 e9 b6 83 86 3f e1 05 27 fc 77 fa 4b fd c4 d2 b0 ff 00 c0 02 96 d1 42 06 8a 91 ff 00 1e 9f aa 73 f9 c6 a2 fd 52 7e bf 50 6e ec 09 df 5b e9 58 02 24 52 7f 04 2b bc 5f 87 6f 80 d0 fa 7c 19 49 25 48 f8 1f 98 d7 8a 9d 14 5d 29 6f 27 04 b2 b1 f2 7f d4 37 3a 20 fa 71 82 01 55 1a 27 63 e6 da 24 93 17 c0 90 3e 05 54 97 55 01 58 82 ee 46 87 d3 41 40 d6 c7 f0 6e 0f c1 0b 6f f1 0c c3 fc 72 37 56 24 b2 69 3f 57 fc 6e c7 5b 1d 20 23 4d fa 76 db 5b b3 7e 12 17 6f f8 94 fd 56 02 f8 8d 44 7f a9 2f eb 6f d5 ad c6 b7 1a dc 1d 7d 35 e6 da 0c 36 dc 1f 84 25 bd 2f c6 34 3e 9f 17 04 86 5d 87 c5 57 cb 5e 9e bd 3d 3a 79 31 8f 61 08 db e3 27 e9 f8 c6 76 77 Data Ascii: mF4%>J|[!ygHq?'wKBsR~Pn[X$R+_o\|l%H])o'7: qU'c$>TUXFA@nor7V$i?Wn[#Mv[~oVD/o}56%/4>]W^=:y 1a'vw
2021-09-28 09:09:19 UTC	47	IN	Data Raw: 10 1b 96 5f 1d 01 b9 f0 1a f0 1a f0 1a 55 f1 d1 4d cf 80 d3 26 c3 49 f5 3f 30 ab e3 a2 9b 9f 01 f0 0d b0 31 b6 86 ea 7f 5e 80 fc cc 36 2a 37 24 6c 75 ff 00 92 3d 1f af f8 2b fa 99 7c b4 3e 41 fe aa 37 3e 03 e0 0e c7 d4 d3 7e 8d 28 dc 91 b1 56 f1 d7 a9 a6 6f 2d 56 fe de 47 4c de 22 87 e6 9a cf f7 8e b6 d3 1d 87 9e ff 00 05 6f 87 97 c9 7e 93 7f 6a 2f f4 3a 6f d3 f8 13 f4 9d 20 de 35 5f 1d 47 fa ec 7f 73 5e 2a ba 46 f9 cd 1a 3a a8 28 bb 8d 1f 98 d6 fa 8d d4 6a 40 fe 71 b3 09 22 fd 26 40 84 39 74 85 dd 94 c6 09 04 80 cf e9 8f 32 da 62 c0 c5 1a f9 9f d3 11 91 74 7f 2e be ba 31 2b 18 82 aa 4b 26 ed 12 b2 fc 24 08 52 2d 82 d7 0c 0e bc d0 05 42 03 01 e3 a2 ac 3e 04 93 f1 d8 6f f1 00 0f c2 df a2 5f d5 1b ed a8 db e4 a4 15 ff 00 0 8 15 03 f2 b6 be 43 40 83 f8 8e b6 Data Ascii: _UM&I?01^6*7$lu=+\|>A7>~(Vo-VGL"o~j/:o 5_Gs^*F:(j@q"&@9t2bt.1+K&$R-B>o_C@
2021-09-28 09:09:19 UTC	49	IN	Data Raw: 7f 08 1e 3a 53 b8 d3 fe a5 6f 1d 03 bb b8 43 a6 1b 81 e4 ba 8e 45 91 8e df 82 b0 dd 32 bf 28 ff 00 cb 16 de 53 e4 7f bc 4f c0 9d 87 98 d0 3b 7e 08 fe 9b ed ad bc 53 4d fa 95 7c b5 fe 72 7e a3 a7 fd 51 7e 28 ac 82 1e 0f 24 ab e0 8a 62 53 2a 12 0c a6 c7 94 36 7f 34 d5 00 77 41 b1 1e 9e 9e 2d f5 4d 82 35 da c4 84 95 8c b5 e4 49 e3 58 e2 40 e9 b2 8f 13 24 53 32 49 6a ab 58 3e 25 34 66 61 a1 6a 4d c3 49 b1 07 4a c4 08 bc 8b 98 f7 72 a4 17 8c 14 30 be c2 26 87 50 d8 3e 3b 45 32 c8 aa ae 7f 20 59 63 63 f5 fc 5b 0d 2a aa 92 a3 64 69 15 54 13 a6 55 2a be 3b 0f 03 a8 87 f5 67 db d2 9c ed 34 64 07 88 2e c9 fd af f0 48 23 44 10 15 b7 ff 00 05 37 f1 27 6d 6e 87 5b a8 d7 d5 94 f8 e9 5b e6 02 9d 7e 55 d7 92 eb f2 69 bf 4a f8 ec ad f3 f2 5d 79 2e a7 0c 42 85 2b f9 35 ba Data Ascii: :SoCE2(SO;~SM|r~Q~($bS*64wA-M5IX@$S2IjX>%4fajMIJr0&P>;E2 Ycc[*diTU*;g4d.H#D7'mn[[~UiJ]y.B+5
2021-09-28 09:09:19 UTC	50	IN	Data Raw: a8 d3 4a 8a 16 71 26 a1 3e 46 6a 80 cc 9e 9c 63 e2 5c 15 f8 0f 9e 95 4a e8 fd 75 e9 a2 89 3f 56 81 20 c7 29 3a 77 1e 2c 77 3f 05 20 69 40 78 e5 45 42 87 c8 ca 0a b6 9b e6 c3 f2 68 fc ce 93 c5 cf a5 b6 99 83 0d 05 2d a2 84 0d 2a 90 74 8a 54 95 3e 4e c1 b4 58 15 d3 57 8c 86 a6 a7 52 63 ed 6d 14 99 18 16 0b b2 3b 19 11 97 51 c6 bb c8 14 3f c6 af e8 cf 7c e3 d6 0b fd 5d df ee b9 d8 b1 dc ed f0 43 f3 db c4 02 0e 84 80 04 90 6d 8e 6f 2c 8c c3 69 25 fa 78 1d a3 fd 27 ea ff 00 ab 4c a4 ac 1f dc 91 4f 90 52 74 ac 3e 0f f4 be d3 19 eb 4e c5 ad 16 37 6d 25 65 86 bd 7b 02 55 a7 1d 75 b3 0b 49 1d 8a df 6e be 4b 22 53 8f d7 b1 ea c8 20 ab 69 2d 41 58 2f ad 68 c6 ba 61 32 d8 ba 24 96 2a 6a cb 12 78 69 da 45 49 04 92 c7 2d 00 56 18 e2 ae 13 c7 d7 31 27 93 2a 29 49 09 58 Data Ascii: Jq&>Fjc\Ju?V):w,w? i@xEBh-*tT>NXWRcm;Q?|]Cmo,i%x'LORt>N7m%e{UuInK"S i-AX/ha2$*jxiEI-V1'*)IX

Timestamp	kBytes transferred	Direction	Data
2021-09-28 09:09:19 UTC	51	IN	Data Raw: 9d 01 b9 48 db 52 c6 f1 b2 a8 3a 9b e9 6f fd 57 ff 00 c8 a9 f9 b4 aa 1d 44 2a 0f a4 e7 46 10 a0 45 20 3a f5 50 ab c9 b1 90 a9 5d 80 d0 62 ba dc ef e6 74 0e c7 d4 3a db e2 1b 7d 2a f8 e8 3e e5 50 30 01 23 d4 a4 19 23 fc 05 41 21 40 d2 fe ad 13 b3 23 79 0d 32 06 2e a1 74 37 0d ea 1d 03 bb fc 08 dc 7a 43 4a 3c 47 91 32 37 e6 0c 0a b1 1e 9e 99 8f a6 ac 5b 40 ec 44 a4 6b 7d f5 24 a5 59 9b c7 4a db b7 a4 34 cb be 80 d8 3a 05 01 c8 58 c0 3a 6a b1 96 f4 5d 35 45 89 93 91 ff 00 69 98 b0 e3 bb 35 ab ec bb 1f 99 db 5b 69 ff 00 50 24 36 fb fc 07 d0 31 03 8f 7f ef b2 ff 00 77 e0 bf 09 3e a0 ed ad f7 48 86 f2 3f ea f8 c8 76 11 57 b4 75 67 17 05 44 8d 2f c6 86 e5 a8 1a 0b 76 d2 c5 c7 92 b5 cb 59 16 b3 1e 0a 67 b9 8c aa 6b d7 31 4a 64 02 c9 59 6c da 9a 49 63 80 bb 35 54 Data Ascii: HR:oWD*FE :P]bt:}*>P0##A!@#y2.t7zCJ<G27[@Dk}$YJ4:X:j]5Ei5[iP$61w>H?vWugD/vYgk1JdYIlc5T
2021-09-28 09:09:19 UTC	53	IN	Data Raw: a3 e6 ce 0d dc bc cc 38 bf 57 3b 3e 31 66 76 69 1e 61 5d 68 d5 b2 2a 54 8e 9b cd 8a 8a 69 21 a6 88 2f 79 a4 02 13 30 5a 81 00 89 c4 b4 0b 24 97 87 cd 90 16 8d d8 17 b3 33 88 6b 06 d5 c5 5f 18 dd 94 c9 71 bc 23 b8 65 05 16 ea d8 ab 04 69 06 f0 48 59 da 1a f1 2b 24 70 af ab 34 31 53 77 b9 1e f1 bf aa 2d 2b 8a d4 1c bd 43 3c 90 05 9d a5 12 fe 9b 8c 3e e6 56 6f b8 8c ec b5 19 8d 59 a7 22 56 44 62 80 12 36 1a f4 84 9a 30 78 b3 21 de 38 ca 33 36 da 8d 55 95 b6 06 73 e2 d5 37 da d3 78 80 48 d0 76 de 56 8c c2 8c 46 98 9d eb c8 e4 79 b6 8e a5 0c 08 66 3a 54 05 40 f1 d0 dc e8 c6 84 bc 41 17 73 a8 48 24 2a 8d 37 89 08 01 2e a4 18 48 24 8d 4b f5 08 bb 15 41 a4 f3 de 46 60 51 a5 6d 0f 11 a7 05 8b 6e 15 77 f1 d7 8b 1d 46 08 d3 4f f3 51 e4 24 04 af cd 4a 3e fa d9 4e 8f Data Ascii: 8W;>1fvia]h*Ti!/y0Z$3k_q#eiHY+$p41Sw-+C<>VoY"VDb60x!836Us7xHvVFyf:T@AsH$*7.H$KAF`QmnwFOQ $J>N
2021-09-28 09:09:19 UTC	54	IN	Data Raw: f2 0a 14 ec c1 1e 39 9a c1 79 a0 d7 ae 02 2c 68 43 48 9e 9b 6f ac 5b 88 c2 c4 b6 a6 9e 9b c7 08 a1 71 a3 54 92 25 96 68 2a 47 95 e4 b6 a4 d4 97 65 97 46 42 ab 1e 72 d5 43 53 9d 64 22 18 fe 51 89 bb 20 3b 9b 0a e7 48 36 4f 1f cd 23 15 46 24 a8 5d c0 8d 86 88 d8 85 07 41 40 f8 32 8d 81 d8 92 01 94 79 04 05 49 1e 72 45 fd 47 f0 32 01 1e e0 7c 86 9b e6 be 20 69 d0 3e 9d ca be fe 4c 54 36 b6 3b 7a 53 69 60 98 17 82 57 51 0c b1 28 dc 0f 2f cf 6f e5 a0 e8 91 97 63 a4 90 e9 2d a3 31 f9 e9 d1 d8 45 f9 75 cb 09 30 46 a1 97 04 7c 6c e4 7e ac c4 96 62 a7 fc fe ba 8c ed 31 fa ef a5 3b 6a 39 0f 8f 5d 2f 97 28 6f 87 fe 7d 48 03 69 d0 6f a5 50 42 6a 1f d7 38 fe ba fe a5 1f f2 1a 0d b6 a6 c9 d7 87 17 87 c9 e1 f2 94 96 da 1d 36 66 04 c8 c7 8c f0 b1 36 3e ca c9 ca 91 b0 f5 Data Ascii: 9y,hCHo[qT%h*GeFBrCSd"Q ;H6O#F$]A@2yIrEG2| i>LT6;zSi`WQ(/oc-1Eu0F|~b1;j9]/(o}HioPBj86f6>
2021-09-28 09:09:19 UTC	55	IN	Data Raw: c7 d4 1a 43 f3 8f f4 cf 19 5d 61 6f 35 2b 51 07 96 21 0b e9 e2 50 62 80 fa 55 9a 06 8d 56 3f 18 aa c3 26 a7 44 5d 20 f2 43 b9 d3 7c c2 81 e3 a8 ff 00 32 32 f8 9f 98 d2 b1 68 ce 93 f2 90 c0 95 1e 46 34 f1 98 83 a0 5b 69 a5 93 d3 2a 5e 4f 4c e8 3e da b0 de 61 ff 00 4b a6 e4 9d b4 df 3d 7d b1 49 51 54 6b 61 a0 a2 36 a5 61 a6 d4 91 98 87 87 ca 49 de 79 b1 f0 18 a5 e5 df 9e 08 db ca 2e 2b 0c 73 4d 97 41 1b c8 db 96 fa bb ee 34 ae 3d 5d fe 4a de 5a 0d f3 4f d3 d5 83 cf 9a b7 cc 7c 22 fa 49 a6 fa a7 d4 2e e1 46 da a8 37 d4 a9 b0 23 fa b5 d7 7a 83 59 fc 52 cb 1c 41 66 af cf b8 c5 fc c7 18 e0 f8 d5 ca 66 7b 1a 7b ef c5 e5 b7 7a ac fc 27 b0 6f f1 ac cf 18 ff 00 6e 49 c8 fb d2 94 98 7c be 37 21 fb 95 2e e6 e3 c7 31 c2 39 2c 9e 79 3e 14 7d 0b b6 65 31 71 76 82 3c be Data Ascii: C]ao5+Q!PbUV?&D] C|22hF4[i*^OL>aK=}IQTka6aIy.+sMA4=]JZO|"I.F7#zYRAff{{z'onI|7!.19,y>}e1qv<
2021-09-28 09:09:19 UTC	57	IN	Data Raw: a7 a7 19 f4 e3 6a d1 99 1b 8b c9 f6 95 eb cb 0d 85 f3 75 d3 58 91 55 64 86 68 9a 50 11 65 97 4b 60 b4 6c 59 c0 dd c7 89 3a 00 8d 2b 02 58 22 e8 af a6 11 5d 95 2c ff 00 5a 75 21 ec cf b3 0d dc fa 92 0d 16 fe 8c 03 78 da 37 66 96 2f 18 a9 ce f6 0b ca 8d a6 99 76 91 86 89 f1 0c e0 b3 86 0f 3e eb 24 53 3a 3d 57 dd 5c 16 2e a4 2d 14 63 2c b1 0a 2a b2 a3 12 3c 9e b2 b0 97 97 ff 00 66 56 02 2a 76 e5 4d 64 2c 34 80 80 75 64 85 72 40 0e 41 31 1f 19 4f cc ee 74 9f ab 72 35 d3 bb 9e 4f 20 21 9c 31 0a 0e ca 08 d5 8d 98 bf d7 4b fa 53 55 81 6d 39 12 55 d6 34 03 05 a5 da c7 4b f6 25 83 0e 42 03 36 33 08 f1 34 9d a5 6e df 0f e6 a2 05 bb 1f 66 e1 22 c3 f2 2b 10 c2 ad 0c 8b fb 1d aa a6 f7 15 c0 c5 2c b5 71 a9 96 a1 82 39 3f 53 0b c7 e7 85 9a c5 96 c9 66 a9 7f 4a 59 37 f1 Data Ascii: juXUdhPeK`lY:+X"],Zu!x7f/v>$S:=W\.-c,*<fV*vMd,4udr@A1Otr5O !1KSUm9U4K%B634nf"+,q9?SfJY7
2021-09-28 09:09:19 UTC	58	IN	Data Raw: 8a 9d 8c ad 9e 55 c6 d3 f6 24 b8 aa 94 94 ad 29 06 fa b9 0a 16 8e 44 8d a2 ac cc d6 5c 48 fb b2 e9 54 88 f8 29 f5 28 03 b1 96 11 23 59 a9 20 69 ea 94 d0 79 6b 6a 8e 4a 51 14 16 d6 ca c5 3f 8b a9 49 44 c6 3f 0a f0 96 93 c1 37 f1 0c 93 22 a1 50 41 60 c2 59 23 8c 84 85 62 8d 1f d5 64 00 6b c7 73 11 1e a2 5d 51 3f 3a 79 24 c9 e0 32 ef ea ee 0e b7 db 5b ef af 93 02 8a 40 f9 09 58 9d 40 49 d0 99 01 8c ef af 91 d5 2a e4 d2 a1 5d 92 b0 74 a9 11 0a da a1 22 bc fc d0 95 af 3b 1f 42 b1 25 ee 91 bd 86 f9 b9 1b fc b4 e0 ee 8c a2 45 fc ca 9a 1f a8 eb a2 53 6c 83 fd 46 97 eb a9 c7 92 95 1a 5d b7 50 bb 6a 0f ee c3 f9 ab c2 01 8e 80 fe 86 52 30 67 a9 f6 75 a6 b3 15 9b d1 70 2e 4b 94 e2 d7 b8 c6 50 63 b2 9c ea 0a 78 de 69 d4 5d 8b 6f 1b 6f b8 e1 6a fc ef 1b 29 ce 3d cc 85 Data Ascii: U$)D\HT)(#Y iykjJQ?ID??"PA`Y#bdks]Q?:y$2[@X@I*]t";B%ESlF]PjR0gup.KPcxi]ooj)=
2021-09-28 09:09:19 UTC	60	IN	Data Raw: c9 03 b7 a9 3d 67 5b ab 5c e3 a4 96 7c 8e 22 ea 58 a1 5e 74 2a 81 da de 26 29 eb d2 c7 01 ab 31 cd 5e ed 59 c4 3a 39 8a eb 3c b7 63 9d 23 0d 16 83 cd 24 55 5e 48 a5 9e 00 67 bf 45 12 88 67 aa f5 99 1e 4c 62 45 62 3b 1e 54 4f 1b bb 62 e6 72 d1 ff 00 d3 72 72 1f bd b0 e4 49 5c b1 d4 7e 85 6a f2 78 78 2f a6 d1 44 3d 25 b0 ae ca 20 33 6a 5f 38 db 07 c0 f9 26 60 62 78 6f 18 e3 a7 39 c9 56 cc 2d 23 c9 f8 30 f7 7f 6e c9 f7 bf 0b 35 73 35 e5 f5 4c d0 6e 2e 41 22 ad ca ae 75 0d a9 a9 4f 0f 20 c8 4d aa f7 44 70 f0 ea 83 2b 93 7a 96 9a 38 e4 b0 34 24 1a 53 1b b7 d0 3b 92 19 12 50 f4 60 6d 58 a5 e9 bd b4 5f 04 df ca a6 4e 64 68 2f 43 30 b1 14 6a d2 d2 90 48 3d 4d ec ce d0 88 e0 b2 f3 5a 89 14 c2 a6 29 68 3f 94 6d 4e 01 29 8a 3d be dd 35 cf e4 02 fc 12 17 6a 97 fc 45 Data Ascii: =g[|"X^t*&)1^Y:9<c#$U^HgEgLbEb;TObrrrl\~jxx/D=% 3j_8&`bxo9V-#0n5s5Ln.A"uO MDp+z84$S;P`m X_Ndh/C0jH=MZ)h?mN)=5jE
2021-09-28 09:09:19 UTC	61	IN	Data Raw: f2 01 6f 05 9e 5c 65 fa f7 38 d5 fc 7e a3 59 4c 77 1a c3 66 20 a8 f3 c1 8e b5 15 be 19 c3 31 d8 5c df 24 99 56 84 59 fb ea c1 2d 58 96 3c 15 61 06 37 a6 4a 47 6a 4c 89 ad af 71 1c 81 e6 c6 e0 a1 49 2d f6 04 71 e2 ed 59 39 5a 5a e2 9c 7e 2f 47 05 0a c3 6e 68 22 26 46 74 d1 8d 4d a9 61 54 78 a8 48 fa b1 ea d6 79 ac 44 b1 24 57 06 a6 92 cb 0b 12 00 b0 48 21 56 11 c9 5a bc 91 b3 de 31 4d 5b 1d 18 59 6e 49 1c 96 91 91 65 86 38 64 53 6c 02 b1 ac a9 46 ea 62 62 31 04 d2 21 20 c0 11 8d 75 7d 50 a8 23 bb 3c 64 e3 6f 21 37 ae 0d ac d0 4d f5 55 08 c7 aa ee c8 7c 53 07 50 b5 a2 19 c4 47 f2 81 b9 61 e2 4f c7 ff 00 b7 a4 60 ea ff 00 5c 2d a7 a3 94 82 48 f2 58 ee cf e2 8f c4 33 49 99 c7 cc 13 c2 c3 f0 9c 02 cd 62 9f 1c 96 a7 18 7f d2 a8 75 27 c1 93 72 7e 81 0a a4 6e 37 Data Ascii: o\e8~YLwf 1\$VY-X<a7JGjLqI-qY9ZZ~/Gnh"&FtMaTxHyD$WH!VZ1M[YnIe8dSlFbb1! u}P#<do!7MU|SPGaO`\-HX3Ibu'r~n7
2021-09-28 09:09:19 UTC	62	IN	Data Raw: 10 1d 05 df 55 61 01 ed e0 66 a9 82 67 1b 79 c7 a8 2d 78 b6 41 af 63 e6 c2 f3 1c be 3a c7 00 e7 18 0c 9e b2 3c 6e ed 49 79 0e 0a 8e 3e 6c 73 c1 90 c1 5d c2 fe de 99 ec 30 bb 7d 1b ec 6e 66 a8 57 91 72 53 43 0c 7c 33 08 d6 f2 d9 95 a7 63 9b 70 49 0e 3f 9b e6 64 13 67 f9 9c ef 6e cf 54 4c d1 65 73 39 24 ab c6 fd ab 53 c7 59 c5 f7 46 6e 1c 1f 08 af 50 5b b7 cd 24 8e b3 66 32 33 4d 17 5e e1 97 8a 70 5c 6c 5f 6f 15 7b 6e d2 d4 9c cb 2d 7a a4 18 52 18 5b 21 5e bd 81 20 9e 1d 24 92 78 33 ca 23 97 23 8f 2d 92 f4 c5 08 6a 49 6f 43 1c d5 94 bc 9f 77 51 91 17 35 3c d4 e4 a7 95 fb c8 6e 54 7b 4c 08 2a bf 48 3c d0 bf a6 34 19 06 8a 33 08 c3 78 42 54 14 a9 09 13 08 85 89 9d 7e db 28 0b 5e b7 b7 dd c4 c3 ce b3 01 5d a4 f1 22 67 65 a5 f2 c7 56 65 2b a0 37 d2 02 07 86 da Data Ascii: Uafgy-xAc:<nIy>ls]0}nfWrSC|3cpI?dgnTLes9$SYFnP[$f23M^p\l_o{n-zR[!^ $x3##-jIoCwQ5<nT{L*H<43xBT~(^]" geVe+7

Timestamp	kBytes transferred	Direction	Data
2021-09-28 09:09:19 UTC	64	IN	Data Raw: cc 06 e3 47 e0 b3 78 37 3e e3 49 86 b8 ec 1b 5e 7b 1f 53 5d 3d 90 69 f1 59 20 7f 75 c1 9d e6 b1 52 73 a5 a1 68 86 c5 ce cc b0 ac 9a d9 6a c3 62 a3 47 3f da cd af b4 94 05 ac cd a4 a9 3f 93 52 b0 48 a9 30 d4 54 fc c2 d3 8c 18 69 28 78 e7 11 e3 9f 06 1a 2e 95 8e 8e 23 09 3b c6 56 c7 4a 71 a5 90 f5 1e 1f c9 3a e7 27 52 5a 7c fe de 3a b8 e5 78 fb 52 e1 33 af 92 05 24 58 79 96 16 5e 57 86 e2 57 63 4a 59 24 33 c1 93 9a 0a 12 6e 8f 99 cf f9 e2 f9 9f 1c 8d a6 cc f2 bf 56 9e 23 35 5a 59 b3 5e 31 d2 c3 59 c7 d6 93 98 f4 8d 88 60 c3 72 7b 52 e6 f9 1f 2a b4 ac b8 78 4a 27 19 c7 4c b8 fa 4c b5 aa c9 13 59 9e 69 66 b1 4d 56 39 85 49 31 17 78 e4 2d 66 1b 65 3d 7b 36 31 d3 49 65 e8 c8 8a 98 bf 09 12 89 56 b5 8c 91 db f6 c3 19 aa be 94 2b 1f af 3b 51 60 8d 49 63 d2 44 1f Data Ascii: Gx7>I^{S]=iY uRshjbG??RH0Ti(x.#;VJq:'RZ|:xR3Xy^WWcJY3nV#5ZY^1Y`r{R*xJ'LLYifMV9l1x-fe={ 61IeV+;Q`IcD
2021-09-28 09:09:19 UTC	65	IN	Data Raw: 91 c8 04 a9 d0 0a 74 ce 00 65 de 35 db 72 a7 c9 15 81 e4 dd 61 92 e4 f9 5a 9e dd 79 7b ea 1f 6d a9 1e b9 3d 6c 3e 2a d7 4a 71 6c 27 2d 6a 9c 1b 82 d1 d4 38 ec 35 72 26 8a 30 6f c9 13 3d c7 3a 36 8b 2b 4e 1b 4d 21 f1 f3 7d 79 b6 9a 52 0b ca 48 91 bf 34 6a 66 9b 29 1c 9e a9 8d 52 38 8b 78 12 77 94 31 2c 00 81 49 f1 23 c8 ba 8f 07 f3 65 53 e2 00 5d 15 24 93 be 88 07 5f 3d 07 66 d6 e3 7c ce 36 3c b5 18 38 e5 68 d5 71 55 e3 0a 91 52 d5 e6 da 1e 2d 22 c3 c7 24 bd 22 6a 3c 94 9e 11 de 0c 05 c4 3a e4 64 45 c8 26 91 ab 64 ad 33 7a 79 00 ac c1 42 e8 7c 89 24 e8 92 da df 65 52 06 bf 31 78 dd 54 12 ac 63 dd 86 db e9 6e 33 34 76 dd 5a e4 0e ec f2 bf a5 02 cb 30 80 13 3d 44 82 b4 b3 c0 e9 77 8f 61 69 ef 2b 0a c7 3f 2a de 81 f9 0d 9c 3e 5f 95 3b 3d 4e 41 85 93 13 92 c0 Data Ascii: te5raZy{m=l>*Jql'-j85r&0o=:6+NM!}yRH4jf)R8xw1,l#eS]$_=f\|6<8hqUR-"$"j<:dE&d3zyB|$eR1xTcn3 4vZ0=Dwai+?*>_;=NA
2021-09-28 09:09:19 UTC	66	IN	Data Raw: 72 f9 cc 78 19 65 f5 fe 0a a0 8d 27 eb 8e 26 f4 62 a1 f3 95 88 97 4d fa a3 3a 33 47 ac 54 72 ce dd a4 fe b6 66 6b 2b e3 d7 1c d3 1f c1 ad 58 f7 39 10 19 0f 72 3c a2 c2 d8 ef ae c9 b6 6e f6 17 60 e5 15 e3 e5 f9 09 2b f0 5e 59 64 d5 ea 9e 57 23 57 e9 ac 9c af 17 4d d6 46 af d5 bc 4a b3 57 e1 bc 46 98 a9 8e c0 43 24 57 13 05 4c cf 34 8e 5c 90 ac 54 03 b1 f3 23 5f e4 18 fa 6c 36 8c b1 08 46 c5 dc ed 19 2c c5 8b e8 8d b4 14 0d 01 f3 df c7 f0 5d fc d2 eb 2a 02 c1 91 4f 56 ce 33 17 e5 5b 31 83 92 52 f8 3b 49 a9 71 b7 21 3e 84 9a 23 7d 48 c5 f0 d4 49 68 67 b1 18 1e 89 02 23 0a 69 95 23 09 1b 3e a2 0c 74 1d 86 bd 46 d4 85 96 38 19 9a 36 07 76 46 33 02 3d 26 c5 ba 2d 4c 8d 9a 62 9e 42 76 cf 52 ca d8 48 46 55 5b 5e bc 7b 4d 22 3a b4 b1 95 96 4d 92 47 dd 7c 7d 5d 0a Data Ascii: rxe'&bM:3GTrfk+X9r<n`+^YdW#WMFJWFC$WL4\T#_l6F,]*OV3[1R;Iq!>#}HIhg#i#>tF86vF3=&-LbBvRHFU[^{M":MG|}]
2021-09-28 09:09:19 UTC	68	IN	Data Raw: 51 86 7a 72 6e 1e 3d 1f aa b7 88 61 e4 12 28 f5 2c 0a d2 a0 65 67 fa 81 e5 a2 be 25 9b c8 3f cc 74 62 a4 99 da 78 6e c0 8f b5 32 1b 36 b9 56 49 f2 b9 9d 28 dc a8 d8 47 ac a5 d8 69 53 7c 9a 02 d9 0d 87 ee f2 07 9b 88 c5 9a 4c 85 19 6b 48 71 d2 c9 a9 71 36 4a 5a c3 64 50 36 2e c0 d4 55 25 85 b5 c1 70 56 a1 eb 08 ff 00 a8 87 f2 ea b5 5c 64 55 96 16 15 1e 97 aa f3 70 d5 b6 f0 70 e8 23 5a 98 4c 65 71 8e c5 53 c8 9a d8 9a f8 d4 9b 68 67 72 ed a4 93 65 07 cb 4a 9e 40 a6 c0 e8 9f 2d 6d f9 80 db 5b ff 00 52 43 e6 a4 79 0d fc 75 f5 d0 fc a3 44 ee 34 1b 44 ee 74 c3 f2 a7 c8 f2 27 02 4e 31 17 af 9c 0b b1 9a 38 e4 56 ad 1b 68 d4 55 d7 a2 74 f0 39 d7 20 8c 98 ba e6 71 4f 9a c3 7d 63 5c dc de bc 83 7d a3 b5 f3 99 08 8d 87 8b 2c 13 4c b7 e4 06 cf 14 1f 35 93 cb 53 cc 16 Data Ascii: Qzrn=a(,eg%?tbxn26VI(GiS|LkHqq6JZdP6.U%pV\dUpp#ZLeqShgreJ@-m[RCyuD4Dt'N18VhUt9 qO}c\},L5S
2021-09-28 09:09:19 UTC	69	IN	Data Raw: 3a 0c be 3a f1 6d bf 0f 0c c2 2f 22 e4 de e8 b2 f2 0c cc 9e 48 ea 3c 35 29 44 d4 ee 8e c1 bc 5a 08 a1 9d 21 96 4a 53 f1 2e d0 c6 bd 4c 26 4f 17 98 a8 36 dc b8 dd c6 e2 fc 69 22 cd 74 7a fe b2 ab 55 e5 5f f2 54 69 71 0b 3a 97 3d 8e c3 62 eb c6 f2 4f e4 a3 46 44 f1 b6 23 95 6d af 1b cd 5b ce e5 31 98 b8 96 49 6c 59 a9 49 2c af 08 eb bc 65 b9 39 26 4e 0b d2 a7 d0 81 a2 37 0c a4 2a c6 c4 69 4f f4 eb 86 42 19 5b 44 83 a1 af f3 20 9d 1f 98 20 e8 8d d0 b2 a2 9d ce 98 0d 81 1b 6f a3 08 65 24 6b 60 c2 b2 f9 e2 e5 fa 10 3c 74 df ab 60 75 f5 1e 2b af 37 1a 32 f9 ea 6c 46 12 c4 e8 d5 04 6d 1d 37 d0 81 98 b5 69 06 a3 82 48 d3 ed d5 92 ed 68 16 bf ed 91 4e 51 e6 48 a3 7b 2a 7e e6 65 68 b9 13 d7 4f 46 c1 61 5a 32 56 83 9d 26 16 ee d5 78 7f 22 b3 aa bd 53 cc 2d 88 3a 37 Data Ascii: ::m/"H<5)DZ!JS.L&O6i"tzU_Tiq:=bOFD#m[1IlYI,e9&N7*iOB[D oe$k`<t`u+72lFm7iHhNQH{*~ehOFaZ2V&x"S- :7
2021-09-28 09:09:19 UTC	70	IN	Data Raw: d9 d6 30 11 76 e6 43 1d d9 09 93 e3 b9 3a 4f 24 72 44 1f c5 8a a2 c8 d5 6a 4d 90 7c 5f 04 b5 62 f7 12 e2 5c 73 13 21 48 d1 fc f6 d4 d2 02 f6 e6 45 5c c4 fe 4e d1 49 29 fb 1b 20 b8 68 8a b3 6f 4e 64 8e 5c 0d bf 28 20 66 6d 29 0b ab d9 37 a9 24 6f 36 42 fc 38 7a 55 96 be 2b 8d db 61 9f c6 e0 2d f2 2c ec fc 83 2a bf 20 47 90 4f ca 1f 63 a2 36 00 93 f0 40 a4 0f af 99 1a 67 df 4a 14 99 36 07 fc b7 db 4a ec 09 6d f5 f2 dd 8e fa d8 e8 9d 7d 42 8f 12 76 d7 cc 6b 6f 96 20 93 7d f7 f0 24 6c c0 01 a9 23 6d a8 61 61 78 32 7c ab c2 b4 92 33 9a d0 3c ec b8 b8 2b 09 e4 9a 69 64 bf 56 12 d9 9a 21 bf 77 76 d4 99 1c d3 03 26 46 51 88 31 7a cf 4f 11 28 53 e9 64 2a ee cb 87 8d c5 88 94 b4 4b fa 74 46 ff 00 06 6f 1d 59 bf 5e b6 b9 67 64 d2 c5 41 ca 7b 0f 25 9e 92 20 d2 81 6f Data Ascii: 0vC:O$rDjM\|_b\s!HE\NI) hoNd\(fm)7$o6B8zU+a-,* GOc6@gJ6Jm}Bvko }$l#maax2|3<+idV!wv&FQ1zO (Sd*KtFoY^gdA{% o
2021-09-28 09:09:19 UTC	72	IN	Data Raw: 7f 87 99 4d 27 ea 3a 67 2d a5 59 59 ad 4d 16 32 0c 16 66 ce 56 c4 72 1f 39 06 eb e2 06 8b 97 d7 91 07 f5 6b 6f 1d 13 b9 f2 3a 1f 3d 37 cb 5b 6e 36 db 47 e9 b9 1a 23 70 aa 15 76 db 5e 24 3d 85 92 41 36 32 d5 4d 58 47 86 54 05 89 88 6b d3 1a ac 10 c9 1c b6 a2 c4 71 1a 7e 14 65 45 29 c9 ab c7 36 4f 8e e3 44 74 2c 55 64 5b 27 c5 1e 62 5a 3b 0d 24 d3 b9 36 b1 1f eb c9 d8 e6 49 5e 43 52 ed 7f 4f 1b 95 88 4f 1e 43 f2 c3 c7 39 35 cd 56 eb be 57 2b 43 d5 56 e5 d4 5d 55 87 06 b7 5d 71 2a ab 57 8f 71 aa 5a 8f c2 1d 7d cb f8 cb 28 56 6b 32 17 17 59 01 bb 21 8a c4 ed b7 dc 3f 8a c8 d3 c7 34 81 a1 90 8f 34 61 ea c3 22 8d 43 ad cb c7 33 2f 84 ca 43 37 f7 fe 7b c4 c0 44 37 d2 1f 4c e2 32 94 69 c7 8b e4 fc 7e 45 82 c6 3e e2 ac 60 0f 04 1a fa 7c 3e bf 04 1f 2f 80 04 eb d3 Data Ascii: M':g-YYM2fVr9ko:=7[n6G#pv^$=A62MXGTkq~eE)6ODt,Ud['bZ;$6l^CROOC95VW+CV]U]q*WqZ}(Vk2Y!?44a "C3/C7{D7L2i~E>`|>/
2021-09-28 09:09:19 UTC	73	IN	Data Raw: e5 21 05 51 94 2f 92 e9 98 78 a7 e7 fc 27 e1 b8 1a 3f 57 fd 56 c0 31 64 63 26 43 1b 69 eb b1 d3 c2 54 98 58 68 a0 1a 50 0e 8a ae de 2d af 13 ad 8f c1 41 de 30 0e 82 90 00 27 52 46 3c 44 3b e9 68 b1 d4 38 f0 15 6b 04 d4 30 87 68 aa 79 34 28 be 31 aa ed f3 d0 3b 69 1f 70 ce c4 ca d1 a0 b1 98 c6 c3 1c 9c d7 19 12 d8 e7 ac da 7e 6b 93 93 53 72 1c d4 cd 66 7b 53 b4 1b 49 aa f2 b4 0b 0a bc 95 c4 52 ae bd 3f 92 c6 84 60 f8 c6 5f 90 cb c6 38 36 27 8e c3 e8 aa ab c4 80 49 0f 9e ac 26 f1 f2 c8 e4 4c f0 d7 f9 32 30 1f e6 77 d7 82 90 09 1a 4d 81 60 08 d0 04 97 53 a3 be c3 6d 87 cb 4c 01 69 cb 6d 6a 51 47 10 b3 25 b9 03 29 47 3b 9d 9c eb f3 2e a9 96 2b 8e e3 36 ee c3 93 fb 5a 10 d2 a6 af 0c bf d5 ac ca e2 74 8d 46 88 8f 52 49 0c 69 3d e5 1a 86 59 9e 5b ff 00 fb 96 24 Data Ascii: !Q/x'?WV1dc&CiTXhP-A0'RF<D;h8k0hy4(1;ip~kSrf{SIR?`_86'I&L20wM`SmLimjQG%)G;.+6ZtFRIi=Y[$
2021-09-28 09:09:19 UTC	74	IN	Data Raw: 76 6a 40 8f 85 9f d1 ff 00 80 8f fc 01 ff 00 4d 6f d5 a3 fa 71 bf e9 80 3b 6c 75 e2 74 07 c8 0d be 0c a4 eb e9 f0 65 24 5d dc 59 d0 fa 7e 16 d1 53 b7 c1 be ba 2a 00 5d 80 20 1d 10 a0 12 4e b7 3b 68 fc 08 04 01 b0 f8 00 36 f8 ed a5 f9 69 be 8b fa 43 1f f1 46 8e df 80 1d 1f a6 c3 6d 6c 36 03 e0 3e 9f 80 fd 07 ea a8 a3 e1 64 1f 0f f8 dd ff 00 00 ff 00 c0 0b 13 aa c7 f3 a0 0d 1b 8d 97 19 bf db 00 40 d6 c7 5b 6b 6d f4 a8 0a b8 03 5e 23 5e 0b f0 bd fe a7 40 9f c4 da 3f a3 e0 df 5d 1f cd a2 9e 20 fe 7d 78 1d 11 b6 b6 fc a1 77 d1 53 b1 f9 68 36 ff 00 1d f5 be da 71 ba 69 47 97 c5 8e e0 7e 90 77 ff 00 1f 6f 96 80 df 44 6d a0 37 d6 fb 0d 0f 96 89 df fc 0f fc d5 3e 63 c7 6d 4a 37 8c fd 48 db fe 23 6f 89 6d b4 ab b7 e3 1f 0d ff 00 c0 db e0 5b 6d 03 b8 ff 00 1c fd 6a Data Ascii: vj@Moq;lute$]Y~S*] N;h6iCFml6>d@[km^#^@?] }xwSh6qiG~woDm7>cmJ7H#om[mj

Timestamp	kBytes transferred	Direction	Data
2021-09-28 09:09:19 UTC	76	IN	Data Raw: 81 6f 25 df f2 fa 2b e0 b1 80 eb 10 65 9d 46 95 7c b4 3e 7a 41 b4 8f 26 ec 1b 6d 22 6e 64 5f 05 db f0 0d 0d 78 fc b4 3e a4 fc c9 db 5e 63 5e 49 a1 f3 0a 76 d3 7e 6d 01 b7 e0 07 62 c7 7d 0f 91 6f cc 7e 1f 5d 6d f2 1f 03 aa df dc c3 7c c1 1b 6a 41 b8 92 4f 29 3f c7 3f 30 ab e3 f8 09 d8 ef f8 09 db e1 b7 c3 7f 9f e0 3f 3d 78 e8 2f e1 3f 40 76 d6 ff 00 20 77 ff 00 13 f3 68 1d b5 e7 a7 85 94 10 74 ab b7 c1 9b 62 75 8a 4d ee 56 fd 19 1f 94 18 25 de 99 1b 1f 86 df 01 1e e3 d2 3a 23 62 57 7d 0f d5 77 fd 5f c5 3f 51 fa bf d0 68 6a 5f 80 3b 16 3b 9d 7c 86 bd 6d 91 22 6d e3 2c ad 6b f3 69 00 8d a5 fc ad 04 a4 a9 ac 52 b2 88 fd 38 24 f9 d9 40 0f dc 3b 2b f9 b4 9f 99 48 f9 6a 23 f9 d9 76 98 8d ca b6 89 f2 d3 3a a8 f9 9d 05 db 4c a3 62 0a 84 24 97 27 c3 5b ec de 4b a7 Data Ascii: o%+eF|>zA&m"nd_x>^c^Iv~mb}o~]m|jAO)??0?=x/?@v whtbuMV%:#bW}w_?Qhj_;;|m"m,kiR8$@;+Hj#v:Lb$'[K
2021-09-28 09:09:19 UTC	77	IN	Data Raw: 15 02 4c 5f 4b f5 dc 6d 11 1e a6 14 29 8d 97 fe 5a 50 3d 3f f3 f9 eb 63 bb 00 07 9a 85 f2 3a f2 27 e0 aa db fc ff 00 0f d7 f1 78 8d 01 b7 e0 d8 6f f8 0a 83 a0 00 f8 ee 3e 03 e0 49 d1 dc 85 dc 0d 6f f3 fc 24 03 f8 54 fc f7 1f 0d 8f 92 bb 26 8c ca cb ba 36 9a 07 55 d2 93 f0 27 4e 13 6e 37 f3 b5 59 14 c5 99 00 56 e3 03 6c 69 03 6d 8e 8e e3 5b 9d 2a b1 d0 41 e2 cb a2 a7 72 ba b6 00 aa 7f 56 8e 86 94 9d fe 12 6e 4c 60 78 d8 fa 68 79 36 80 03 43 52 4e d2 33 96 b0 41 08 23 8c a6 98 17 2f 53 68 a5 1e 94 31 b3 b2 ba 49 23 5b 42 67 40 4c 72 57 62 df a9 ec b2 08 fc 81 8d 36 53 24 66 3b 5b 79 32 84 00 ae c0 27 90 72 44 4b 19 1a 50 cf f0 3a 07 6d 79 e9 9b 7d 6f f8 09 db 46 60 1b cd 74 0e 99 b6 d2 fe 64 df e7 a6 45 20 b3 c0 c1 d1 be 3b fc 0c 61 a4 f0 54 d1 5f 96 a0 1b Data Ascii: L_Km)ZP=?c:'xo>lo$T&6U'Nn7YVlim[*ArVnL`xhy6CRN3A#/Sh1I#[Bg@LrWb6S$f;[y2'rDKP:my}oF`tdE ;aT_
2021-09-28 09:09:19 UTC	78	IN	Data Raw: 4f c3 c4 6f f1 20 1d 7d 00 d3 6e 00 fc df 10 4e bc 8f 91 1b e8 00 09 d1 d6 e7 cb e2 74 34 3e 7f 84 e8 68 fc 0e bf c9 46 fa f9 eb 6f 81 fa 26 bf cf 5f 21 f0 f9 68 1f cc e4 82 c4 8d 71 32 4d ec 77 fa 6e 4c 01 5e 32 4b 50 f4 c1 3e 9a e8 a8 60 14 00 10 2e 80 d3 68 a8 21 d4 29 c9 1d b1 a7 eb f0 3f 05 fa 68 fd 20 50 5a ce e4 7c 62 fa d7 3b c6 66 96 4d 3a f8 b2 59 35 e0 b9 4e 1a ed e8 b5 a6 a1 5e 39 29 2c 2b 09 f9 f9 c9 19 1a 08 42 8a 73 30 0a 4e be d8 48 92 46 42 c0 59 23 c9 b7 85 2c 70 8e 2c 7e 2e 56 16 80 f2 d4 31 c6 cc e7 d3 67 71 e5 e3 b2 8f 96 bc c6 a3 af 13 33 c7 12 b8 b0 d1 cc e3 72 a3 6d 30 dc 11 b6 80 f1 3b ee b0 69 8e d2 31 f2 d6 fe 40 21 d3 42 57 4d f2 08 77 25 09 95 46 df 03 f4 4d 46 47 a9 62 08 e4 d4 52 4d 02 fa ea e3 7d a5 c0 46 7e d6 01 b2 4a 36 Data Ascii: Oo }nNt4>hFo&_!hq2MwnL^2KP>`.h!)?h PZ|b;fM:Y5N^9),+Bs0NHFBY#,p,~.V1gq3rm0;i1@!BWMw%FMFGb RM}F~J6
2021-09-28 09:09:19 UTC	80	IN	Data Raw: 55 1a f5 93 5e aa 34 bc 31 83 5b a3 f2 ad c8 e2 54 a3 c7 46 f5 1c 82 fe 2b a2 a4 68 29 3a d8 0d 04 25 0a 13 a9 15 7c 36 1a ce 29 18 7f c0 bf 53 f0 76 50 06 8f d2 6f ee 38 1e 97 e6 6a 9a e4 94 eb c1 81 47 59 a4 68 99 63 c9 29 94 62 ef 55 bb 4e 49 80 48 66 88 3c 1e a5 0b b6 d1 4c 70 23 09 79 05 63 0f 25 65 59 16 eb ad 8b 13 80 98 dc 9c 4d 63 0d 16 f6 31 39 50 ae 71 ff 00 92 0c 73 93 98 99 18 cf 21 74 96 46 2c b1 b1 d9 9b c8 e9 c7 cc c8 48 8e 35 2a d1 2a 24 b2 8a b5 24 80 c1 0c 67 f3 48 7c 63 f0 90 ac d2 08 74 3f 36 81 dc ac ee 9a 79 0c 8c 64 27 42 43 36 99 7e 7e 23 5b 82 ae a3 72 3c 75 39 3b 2c 61 9d 63 50 19 e1 44 0c 59 53 fb 8d fd de 36 7f e5 61 8c 7a 25 00 19 18 56 cd a6 c6 d6 de 38 2f 04 92 e5 88 8a e4 a3 89 03 d6 9c c7 5d 74 c1 e3 6f 0f ce bf 21 6f 76 Data Ascii: U^41[TF+h):%|6)SvPo8jGYhc)bUNIHf<Lp#yc%eYMc19Pqs!tF,H5**$$gH|ct?6yd'BC6~~#[r<u9;,acPDYS6 az%V8/]to!ov
2021-09-28 09:09:19 UTC	81	IN	Data Raw: 03 4b 20 07 f5 bc 5f 91 b7 f2 43 e4 af e8 80 aa 54 2f 9a 05 11 90 51 3c d9 3e 7a 0d e3 2f 10 3b c1 17 f6 cf cd ae 1f b7 cc 01 f9 8b 6c 74 54 93 12 95 97 fb 6c f2 02 5a 04 75 48 22 55 30 93 a6 c4 c3 74 0a 31 d7 7c 6e 32 bc b6 15 45 68 91 fd 46 c3 55 65 92 ac 5b 24 51 90 64 81 bc 89 f1 d4 ad bb c7 29 73 9d a1 16 47 19 62 26 ad 66 49 63 71 f2 7d 03 b1 91 64 66 61 32 87 96 68 d4 3b 3a 0f 91 63 b9 d0 fd 3a 91 7e 63 e6 15 81 d0 91 52 4f 54 6a 56 f3 0a 7c 75 bf cb 7d d4 9d b4 bf 9b 53 cc b1 cd 56 bb 45 0f 81 d0 3f 38 be 4a 21 3e 40 f9 0d 44 de 9a 7a ec d0 4d 33 cb a9 7f 57 cc 6a 68 ab bb c8 a5 26 f9 88 e0 ae 91 46 d2 09 17 84 9f f9 8a 6b e3 5f 94 b1 15 78 8c f2 58 a2 c3 7d 78 ed a6 5d 80 fa fc 47 cb 4e 3c 17 98 b7 87 1a 8b fb 5f 01 af f3 5f a1 d3 8f cc 06 da ff Data Ascii: K _CT/Q<>z/;ltTlZuH"U0t1|n2EhFUe[$Qd)sGb&flcq}dfa2h;:c:~cROTjV|u}SVE?8J!>@DzM3Wjh&Fk_xX} x]GN<__
2021-09-28 09:09:19 UTC	97	IN	Data Raw: 79 4d 26 bc ef 2b 05 dc 00 07 88 d8 7c b5 be da 27 47 4a 76 24 ee 74 5c 02 ed b9 df f1 91 b8 50 40 2a 47 e2 1f 5a e3 79 71 ca c9 12 fc f5 5b 21 3d 45 15 30 99 12 31 af 08 15 24 0b f6 b6 23 66 16 37 13 2c 7a 69 d3 5f 71 10 d2 da 89 4b dc 4f 23 7e 71 a1 90 ba 0b e4 af c8 44 92 39 80 95 28 c1 4a b8 28 0e da bc e0 8b 4a 5b 57 20 45 6a c0 21 8a 78 d1 05 d5 1a fb a2 75 1d c9 41 ab 6a 52 7e ee 25 19 2b 9e 9a f2 19 9a 49 80 3e a1 3e 21 33 f3 62 32 62 44 2a 77 2e 91 2b 28 75 53 be fa 5f 4c e9 58 ab 36 ee 5c f8 8c 7e 22 b4 d0 db cc 63 83 73 4c b6 2e d6 28 36 eb 33 a9 4d fe 48 c0 05 85 fc 08 df 5b 6c 47 cf 4b f5 58 fc 83 42 03 06 09 a6 20 92 de 21 01 71 e9 b6 80 d9 5c 1f 35 52 c6 bd 94 a9 6b 92 dd c4 63 31 98 61 6b c4 87 d2 46 17 47 f2 8a 71 9b 37 b1 d6 52 c0 8a ec Data Ascii: yM&+|'GJv$t\P@*GZyq[!=E01$#f7,zi_qKO#~qD9(J(J[W Ej!xuAjR~%+I>>!3b2bD*w.+(uS_LX6\~"csL.(6 3MH[lGKXB !q\5Rkc1akFGq7R
2021-09-28 09:09:19 UTC	113	IN	Data Raw: ca 51 fb e8 3a f7 09 c2 e4 c1 76 47 53 d9 c1 70 44 fe 40 7a c6 4e 35 de 3f c5 37 ba 5c 86 57 15 fc 8c a5 4e 33 8f a1 ce 33 1d 61 d9 9c 63 b0 3a e7 dc ff 00 49 74 cf 3d c7 cd 81 f6 df c8 a9 d0 f7 13 85 b8 c4 ff 00 21 5f 71 80 ec 6e c2 e7 51 f3 29 ec d6 c7 5f eb ce 35 96 e4 97 3d bb 7b 94 c1 27 2a e3 5e d6 b3 18 ee 1b d8 dd ad c9 ef f3 7e 49 db b6 2f 52 e9 df e3 65 03 a4 72 f2 cc 55 bb d8 9b f3 cb 27 32 e2 18 0b 98 ec d4 79 3d 48 f5 97 1b 10 a5 53 1b 89 92 dc b4 f0 58 77 a7 77 dd 9f 79 57 cb f2 5e 1f c7 72 bd 85 cd 70 38 b8 b1 18 4e 6d ca a3 e3 1c 57 ac f2 1c a7 93 e4 6f f2 d3 98 bb ee 0b 86 5b cc 2f b4 9e 18 f7 e0 91 bf 36 4b 90 08 c6 56 cd ab f8 8e 27 9f bd 8d cc cb 91 95 ae d7 b3 62 ea df 5c 9a 57 c5 d6 6c 14 7c a2 f4 c6 0c 5f a9 c8 6b 9b 36 29 72 1e 61 Data Ascii: Q:vGSpD@zN5?7\WN33ac:It=!_qnQ)_5={'*^~I/RerU'2y=HSXwwyW^rp8NmWo[/6KV'b\Wl|_k6)ra
2021-09-28 09:09:19 UTC	129	IN	Data Raw: d7 1e f1 7b 5f db 9b f0 4f e5 67 b6 2f 64 38 27 f2 a8 29 63 b8 cf f2 dd d4 16 c6 33 df f7 b6 fc d5 0f 72 7d a9 d5 fd ff 00 d2 f9 4c 5b 67 ba f3 f8 ab f7 03 e1 81 e4 d9 3a d1 cd 99 cf 59 a4 f0 e4 24 2c 33 43 d1 9e fd eb 57 06 4d a2 ae f9 6b 33 48 f7 bd 31 3e 6e 11 5a 6e 4f bd 99 79 2d 6b 14 f1 39 9a 29 63 85 f6 6f 1f e5 b9 4e 59 ed a7 87 61 70 b7 fd be 67 70 19 6e ae eb 3e 95 bd 63 92 b7 58 52 67 f7 6f d1 fd 77 ca 7d db 73 fe c9 ec 8a fc 13 1f 93 cd 76 95 2e ae e9 be 35 c9 bb 33 db b7 4d 62 31 c9 c6 78 2f 1a cc 74 a7 2b e4 bc af 37 57 ac a2 c3 f6 4f 54 75 4d 1e ac e4 39 ae f6 f5 f9 0d fe 29 d4 bd 81 9e ca d8 e3 a9 d5 bc c7 19 cb 25 97 95 f5 6d 5e 4f d9 90 fb 38 6e b4 eb 7c 17 ef b9 1c 17 45 fb b0 e7 1c 23 8f fb 29 f7 11 6 3 9d 3c 1d 80 72 96 fb 0b 94 e7 79 Data Ascii: {_Og/d8')c3r}L[g:Y$,3CWMk3H1>nZnOy-k9)coNYapgpn>cXRgow}sv.53Mb1x/t+7WOTuM9)%m^O8n|E#)c<ry
2021-09-28 09:09:19 UTC	145	IN	Data Raw: 48 57 b6 85 59 89 a8 32 0a 00 ec 84 47 ab b0 96 af 6f 72 f1 60 8a 93 22 f8 f6 bb 76 67 40 51 97 e1 d4 8c 54 a4 23 e1 0a 64 9a 92 88 1e 23 c5 7e 24 72 13 b0 6e d8 51 0f 8a cd 66 a7 6f 05 e2 24 32 80 24 b8 8a 95 30 28 46 51 19 53 89 78 8f 05 7a dc a6 64 09 7a d1 66 7a a1 54 f1 0f 22 b3 48 55 64 c3 6a 24 aa 6d 44 02 c4 a6 9e c5 99 d7 86 2e 11 3c 14 88 c5 90 31 35 8a 00 8a b2 9c 66 1a ab f0 eb 6b 7a 79 0a ee 46 51 f8 48 c1 7c 21 ca 31 01 d3 b7 88 76 b7 d3 66 58 27 ec 05 d6 75 74 ee 0a ec b9 a0 19 01 f6 59 5a e5 f4 d9 96 08 4b 6a c1 31 14 54 8b 7d 20 16 3d 8c cb 14 47 60 93 a7 ec 66 41 3b fd 3e e5 87 6e 0a 52 6c 02 12 8a 25 60 9d d3 37 63 23 54 02 c7 b7 14 38 f6 b3 2e f5 97 7a 32 b7 22 4a 8c 0c 43 f6 03 c1 7a d6 0a 3c 64 3d cb 54 37 5c 2a 5c d0 e4 99 bb 0a 8c Data Ascii: HWY2Gor`"vg@QT#d#~$rnQfo$2$0(FQSxzdzfzT"HUdj$mD.<15fkzyFQH|!1vfX'utYZKj1T} =G`fA;>nRl%`7 c#T8.z2"JCz<d=T7*\

Timestamp	kBytes transferred	Direction	Data
2021-09-28 09:09:19 UTC	161	IN	Data Raw: c8 46 42 88 fd 84 c0 34 50 02 54 5e 6c 30 35 3d e8 48 93 2b 3b 9e 8e b2 66 11 9f b5 0c d5 08 5d b3 7a 42 5f 64 15 5b 92 13 03 d6 88 37 4c 88 e2 81 fc c4 b9 3a 71 39 1e f4 2f 0b a7 38 2e ce a2 2f 02 0c 2a 1f 85 51 8e 38 7b d1 31 89 88 81 c3 7a 10 cc 48 42 59 48 87 bd 68 f5 72 b4 f1 84 8b f2 3b 59 f6 0a a8 5d d2 6b 27 7a fd f9 30 12 88 8f 85 89 12 0c 4e 2c 31 66 76 c4 15 07 8b c8 10 c7 8a 25 bf 10 07 7d a3 7a 89 99 32 b3 99 c8 de 01 e3 bf 6a d3 6a ba 73 da b5 78 0c cd 4f 2c 39 ad 36 72 5f 93 eb 1e 20 0d 48 3e 21 ba bb 9b 15 19 e9 6e 48 d9 31 04 39 de 1d 48 31 6d 8a 42 4f 9f 67 35 11 2f 89 97 87 14 32 a2 c3 62 b3 18 cc 8b a6 44 0e f9 7f 5f ea 54 72 4f 34 c4 05 38 ed 44 9b 6d 21 88 dc 88 10 65 d4 1c e1 0f 72 bc c7 eb 95 6f 9f b9 4b 72 93 2a 1a 84 1c d5 4e 5a Data Ascii: FB4PT^l05=H+;f]zB_d[7L:q9/8./*Q8{1zHBYHhr;Y]k'z0N,1fv%}z2jjsxO,96r_ H>!nH19H1mBOg5/2bD_T rO48Dm!eroKr*NZ
2021-09-28 09:09:19 UTC	177	IN	Data Raw: 0e fa a9 c6 52 d3 e4 73 fe a6 3d d8 92 14 ad 6a ba c5 f9 59 27 e0 b6 d6 61 e8 80 a9 e3 89 0c 36 2c b2 12 7f 4a 66 2c 56 9b a7 5d bc 2d 5a bf 21 13 33 84 5f 07 3c 70 0a 56 35 da 9b a6 eb d4 10 3c 5c 71 c0 ef 43 3e 8a 37 78 ca 84 72 e0 b2 d9 e8 f6 72 8d e7 72 02 c6 82 d4 25 b8 60 de 8c 56 50 4e 6e ef da 8d 4f eb de bc 04 f7 ff 00 5a 93 62 9e 45 78 88 ca 9c e1 ee da ae f5 8b d6 5e e6 73 1b 6f 88 1b d9 4a 46 66 44 92 5c e3 55 5e d6 18 a7 54 4d d8 fd ae 8b 22 76 2c 0f 63 c8 17 ed 0c a3 38 fc 48 1a 55 30 c5 d7 4f 23 ed 7b d5 15 b1 b6 28 32 11 59 ae 58 8c a5 85 54 04 81 c8 f5 e5 c3 8a fc 8e 88 1f 22 f6 94 5d 3e 86 f4 e6 f5 2b 9a 0e 95 a5 f3 2f c6 12 91 72 22 00 8e 2e 4e fd 8d de c8 42 5a 6b 30 9c 45 0f 98 1c 7a 96 7d 4e a7 4d 11 fc 5f 89 e8 20 53 92 31 9f 54 d3 Data Ascii: Rs=jY'a6,Jf,V]-Z!3_<pV5<\qC>7xrrr%`VPNnOZbEx^soJFfD\U^TM"v,c8HU0O#{(2YXT"]>+/r".NBZk0Ez}NM_ S1T
2021-09-28 09:09:19 UTC	193	IN	Data Raw: ae c7 64 a2 01 ee dd d9 7a 5f c2 7d 8a d3 fd b3 ed 44 6c 54 5b 53 0e c7 41 15 b5 6a 7e e1 57 07 f1 1f 6f 60 0a 9f 4a d7 2e c7 1d a7 92 98 b7 fc cb 92 0f c8 7e e5 94 c4 85 28 1c 48 53 22 b9 62 e7 f5 de 89 91 f0 14 32 c8 7c 23 de 84 28 64 ad ed 9e de 15 59 0e 25 1b b8 88 8c 14 35 26 43 2c b6 6d fd 9e b5 2f 26 dc 85 b2 76 b6 3e 94 65 72 2e 4b e0 bc 21 9b 7a be 40 a8 89 44 9d aa 24 9f 0f 6b 03 e1 fa 04 94 ec a3 93 17 44 c8 d5 04 dd ae 0d 17 87 14 07 d0 60 42 c8 03 84 40 07 f4 4d d9 0e 68 f2 54 dc ae 3f d9 3e c4 78 93 ed fa 38 a7 ec f0 62 9e 58 fd 07 fa 6c c7 e8 0f a7 4f d0 39 4e 3f 41 54 fb 3b 1f b3 14 09 28 e7 8c 8f a1 40 c5 c7 34 3c b2 19 17 1f 4e 4a ec f6 46 21 fb d3 ad 51 7f a8 7d 8a c3 7d a9 7b 93 7d 17 41 fb 75 3f 70 ab 87 f8 8f b7 b0 1e c7 ed 04 ed 52 Data Ascii: dz_}DlT[SAj~Wo`J.~(HS"b2|#(dY%5&C,m/&v>er.K!z@D$kD`B@MhT?>x8bXlO9N?AT;(@4<NJF!Q}}{}Au?pR
2021-09-28 09:09:19 UTC	209	IN	Data Raw: 6e c2 db 96 79 c8 15 07 b6 f0 26 af 88 dc 47 17 57 ba 46 aa f9 96 a6 cb 64 27 eb 40 c8 b8 1b 5e 20 d7 63 76 40 3a 88 cd 50 b0 28 44 21 99 4f 5b d4 b5 76 f4 fa 37 f8 a6 5a 9b c0 c6 43 ee 82 ae e9 ba 2e 90 6a 2e 07 fc 49 36 4e 0d 5c cc 79 22 27 d5 e7 6a c9 c6 16 a2 2d f7 67 8f 8a 9f e9 0c 51 b9 70 ca 57 0e 26 52 33 27 bc d7 bb b2 33 1f 01 23 37 11 b4 7a 15 db 31 3e 0c d9 81 d8 41 fd 6a 99 ea a2 37 05 78 5c f8 1e 3f b9 75 5c a4 00 a3 1d a1 5b 8b 6d 0b bd 49 b6 ad 06 83 55 62 13 b1 3d 4f 89 dd cc 58 50 2f f3 6f 95 09 98 8c 1e e5 b2 ef 21 b5 a8 d4 e2 55 cd 25 fb 63 4f af 85 0c 08 ca 09 d8 dc 77 f1 4d 71 84 db 07 74 e8 a3 d8 ce 80 47 b5 93 26 05 33 d5 05 6a 4f 84 87 b5 6a ec ca dc 67 19 6a ee 9c b2 c3 e2 6a ab d2 d4 e8 46 96 f1 05 a7 64 7b 5d 8b 1d ab 47 a4 e8 Data Ascii: ny&GWFd'@^ cv@:P(D!O[v7ZC.j.I6N\y"'j-gQpW&R3'3#7z1>Aj7x\?u\[mIUb=OXP/o!U%cOwMqtG&3jOjgjjFd{]G
2021-09-28 09:09:19 UTC	225	IN	Data Raw: 43 54 77 af cb 7e 67 f3 dd 3e 4c f6 ef 97 90 ff 00 87 76 5e 28 37 d9 72 08 f0 b0 75 66 f5 df 96 f5 e7 51 97 c4 07 95 95 f6 b5 5c 8e 25 79 9d 2f a2 5b 85 a6 69 79 b2 13 ca 77 08 8f 6e ce f5 18 e8 35 16 ec 48 cb 18 c4 10 5c e1 94 d1 b6 71 57 fa 8f 5a d7 9b da b2 c1 e4 6a 6b 84 77 01 b2 22 81 13 1b 44 68 f4 f1 32 94 8e 22 79 43 b8 dc c7 2b fd a9 91 f5 4a 94 e5 16 99 94 89 1c cd 14 84 71 21 b9 3e de e5 67 49 68 b6 a6 31 ac c0 a9 e6 30 42 37 5a 44 17 76 6a f7 28 06 da ae ea ba 3f 44 bd 7f 4f 12 d9 86 56 7a e0 65 28 fa 9f 8a 9d 8b bf 2f ea 7f 32 0b 65 11 35 23 10 f9 72 7f a6 db 89 44 ea 7a 1d fb 03 17 b9 19 08 73 33 88 94 07 29 18 ef 76 5a 3f 94 7e 56 16 65 f3 8e b6 12 95 db f6 cf 9b 6b 43 a6 c2 57 26 4b 44 5f b8 1e 3a 78 cb fd 67 8b ea 82 74 7d 2b a7 c1 b4 96 Data Ascii: CTw~g>Lv^(7rufQ\%y/[iywn5H\qWZjkw"Dh2"yC+Jq!>gIh10B7ZDvj(?DOVze(/2e5#rDzs3)vZ?~VekCW&KD_ :xgt}+
2021-09-28 09:09:19 UTC	230	IN	Data Raw: 12 da f3 38 6c de 81 da 8b 87 9a 61 f0 a3 d8 68 b3 3e 2b 20 0e 0a 00 43 6a 8f e6 6c fe 19 da df bd 44 9b 31 9e a3 0a c7 f7 94 62 6c 8a 6e a0 f4 23 2d fc 3f 7a 00 d7 82 10 95 99 57 70 74 df 97 91 1f 74 a6 86 88 b7 1a 7a bd e8 c4 d9 84 38 bb fe c5 f8 ba c1 13 b4 08 fb 0e 64 23 23 23 2d a5 f1 40 c7 4c 0c a3 be bc 17 83 49 6c 4f 7e 50 8c 25 62 06 40 3b 44 87 e7 b2 88 ce f4 e3 6e d8 7c 65 1a 36 27 e2 d9 8a cf a8 eb da 58 c3 8c f1 e4 03 ba 22 d7 51 95 f9 0d 90 8b bf dd ad 7d 4a 63 49 d1 75 13 6f b5 21 02 79 78 64 8f e4 be 5a d2 5b 3b 33 13 22 db cd 03 96 c7 8a 32 b0 74 f6 0e 0d 08 16 1e 92 ef de 89 d5 f5 fd 44 b8 02 23 1e e0 00 af 7a 94 b5 7a ab d7 64 7f 8e 6e 76 6c 3e e4 6d d8 72 e0 54 89 39 3b 41 26 45 db 82 89 b8 1b c5 94 9f e2 18 85 6c e7 68 19 65 25 b0 f5 Data Ascii: 8lah>+ CjlD1bln#-?zWpttz8d###-@LIlO~P%b@;Dn|e6'X"Q}JcIuo!yxdZ[;3"2tD#zzdnvl>mrT9;A&Elhe%
2021-09-28 09:09:19 UTC	246	IN	Data Raw: 50 91 5d e9 e1 ad fe f3 f1 a6 ff 00 1e ba db 7f d5 fd 7a af 8f 95 35 35 45 36 a6 ae cf 4e 36 b2 78 f5 fc a2 35 8e 6a d7 92 c3 f0 a6 ff 00 0e ba 88 ab 71 35 5a 30 f0 1b d4 01 b7 5a 68 57 ad 53 7e b5 f9 ba fe ad 26 ff 00 ba 3c 3f d7 fd 1b 0d 53 a6 a8 47 2a 74 3e 47 ad 47 ff 00 12 dc 8d 75 1f a4 6b a8 fd 23 fa 77 23 5e 3f 7d 3f b7 5b 6b af e8 a1 3f b7 5c 94 96 04 f8 d3 c2 9f 6e 89 3b 1a 1a 8f 2d b4 36 da 9a 1b 9e 34 00 8f 89 26 87 af 86 a9 b7 da 69 a2 ca 05 7c c7 e8 d7 cc c0 0f 8e be 53 ca 9d 69 b0 fd 3a 3c 45 6a 49 3e 1d 75 bf 4d fc b5 d4 7f 4e c6 ba 2d b9 07 7a 7d bf d5 a5 65 ea 58 2d 7c ab 4d eb 5d fa 6a 87 72 36 27 cc ff 00 f1 21 b5 7e 1e 7f 0d 30 e8 0e e0 79 50 ff 00 af 5b 9f bf a6 b6 d6 e6 9f f4 09 3b d6 9a a7 5a d7 e1 f1 fe 83 53 4d ab a1 4f 13 4f d7 Data Ascii: P]z55E6N6x5jq5Z0ZhWS~&<?SG*t>GGuk#w#^?}?[k?\n;-64&i|Si:<EjI>uMN-z}eX-|M]jr6'!~0yP[;ZSMOO
2021-09-28 09:09:19 UTC	262	IN	Data Raw: bf 52 65 16 ca 05 90 a3 98 d2 40 25 b6 b7 77 14 9a 78 6d a4 e4 b1 4d 20 14 24 78 6e 37 d3 5c e1 b1 b8 99 30 cf 2b 11 6e f7 31 fe 6d a1 e2 3d 24 05 63 e1 2d 2a 41 de 9e 5a fa 7b 9b 39 ed 6f 91 3f 36 19 d0 90 a6 9f 37 1b b8 08 47 df a1 3c 75 ca 8b 12 4a c4 48 65 90 54 12 37 1e ac 86 ba bf be b3 8a 21 34 e9 ea 3d c4 55 22 52 a3 e5 76 60 48 28 80 ef 41 ab 5b cc 9b ad e5 c3 f3 36 aa 21 5b 97 2e c0 89 4c 08 4d 28 4e df 37 4d 73 5b 53 68 c8 ea d1 a4 a2 34 70 87 74 61 c1 8f 2a af 51 e0 74 be b3 11 5e 21 0a 91 c9 88 ea 16 a0 8a a8 a6 b3 d0 67 ad e3 82 36 c8 dc b6 34 43 fe 0a d8 bd 4c 43 a5 4b 9a 55 8d 77 3a 78 ca f0 e5 34 8c 4d 7a d5 89 a8 a8 f8 e8 c3 62 a0 84 00 cd 23 95 2a 16 a7 a2 d3 73 f0 ae 96 1b 85 00 96 06 a0 79 0a 6b e4 0a cc 8d 55 5e 54 26 9f 71 f1 d5 bd Data Ascii: Re@%wxmM $xn7\0+n1m=$c-*AZ{9o?67G<uJHeT7!4=U"Rv`H(A[6![.LM(N7Ms[Sh4pta*Qt^!g64CLCKUw:x4M zb#*sykU^T&q
2021-09-28 09:09:19 UTC	278	IN	Data Raw: a2 54 f0 28 5a 84 28 3a 75 b8 2a cc 3f 03 b1 07 81 a5 08 04 fe 13 a5 06 67 93 1b 7e d1 a1 8e 52 d2 2c 37 4c bc 79 2b 7c c8 91 48 2b b6 c2 ba 63 65 38 b7 45 25 89 1f 37 37 1d 10 f4 e0 09 14 a8 d4 b6 ec 97 12 5c 40 a1 24 e2 a7 89 a5 77 ac a0 2f 87 81 d1 b9 78 ca 55 8a 2a 36 e5 59 4d 19 98 02 41 e4 3a 53 a6 aa e8 0d 0d 3c b6 fb 0d 3c 4e 8a 71 52 1b a8 25 58 91 e4 54 d4 f8 69 d6 da 56 b5 62 6a 86 23 40 4d 6a 41 4d 90 2d 7a f9 e8 5a 99 e3 92 2f 51 14 4c 14 f3 55 32 22 1e 4a 2a 00 25 c0 db a7 8e 96 58 42 89 7d 30 4b 30 56 6a f1 04 d1 bc 35 70 b3 4a a1 44 44 03 f8 7c 37 ad 69 53 5d 48 d2 3b 33 06 35 25 aa 2b 5d ca f9 0d f5 23 ab 72 3c 68 38 bd 48 61 d7 a1 eb d3 4f 25 c9 aa 30 aa 01 51 41 51 f3 13 4a 28 1d 37 d3 ca 0a ac 2a bc 9e 59 0a ac 68 b5 e2 49 99 f8 c7 e1 Data Ascii: T(Z(:u*?g~R,7Ly+|H+ce8E%77\@$w/xU*6YMA:S<<NqR%XTiVbj#@MjAM-zZ/QLU2"J*%XB}0K0Vj5pJDD|7iS] H;35%+]#r<h8HaO%0QAQJ(7*YhI

Timestamp	kBytes transferred	Direction	Data
2021-09-28 09:09:19 UTC	294	IN	Data Raw: e5 5e 5d d5 02 fa 0b 41 d4 b3 80 37 3a cf f7 75 d5 d4 12 49 7d 72 98 ec 55 b1 42 cd 8d c7 b1 69 6d e1 81 65 76 2a ab 1b f2 7e 1c 57 d5 76 a8 e9 ac 46 13 1c c8 33 3d c9 f4 56 10 a2 c0 f2 bb bd cd dc 36 70 22 a4 7c a4 69 24 ba 9c 1d 87 e1 07 cb 5d 8b ed a6 0d 7d 5b 1c 56 26 de 0b c4 12 07 6b 9c a4 91 ac d9 3b d5 72 28 cf 73 76 ce fc 49 1c 41 1b ea fb f9 7b f6 d6 40 f6 b2 e3 e3 93 dd fe f3 b1 94 98 7b 5f 09 73 20 65 ec eb 09 a0 70 5f b9 7b 9a 0a 89 c2 12 6d ed 58 83 f3 36 d6 d8 6c 7e 35 70 d6 3d bf 6a 98 db 1c 72 c1 1d b0 b6 8a c5 16 08 4c 50 44 04 4a 8c 88 0d 00 1f 1d ea 74 17 27 04 e2 0a 93 1d cc 61 44 0c 0d 69 ea 0a 9a 13 fb 75 2b 59 aa 41 0a 1f cb 9e 52 e4 38 5f 82 32 90 bb f5 a6 fa 12 59 5a e3 27 c4 d9 33 c9 5b 6b 99 85 d4 d1 8a b3 7e 44 fb 36 c3 a2 ef Data Ascii: ^]A7:uI}rUBimev*~WvF3=V6p"|i$]}[V&k;r(svIA{@{_s ep_{mX6l~5p=jrLPDJt'aDiu+YAR8_2YZ'3[k~D6
2021-09-28 09:09:19 UTC	310	IN	Data Raw: 75 de 9b 6b 2c a4 83 f9 aa c0 54 0d c8 52 4e df 1d 42 41 a7 24 96 a7 6a 57 83 53 72 28 36 d7 b8 29 b0 31 65 c2 39 e9 c9 8d bd a5 07 db a9 50 9f c3 71 37 d9 42 d5 1b 9e b5 d5 e4 58 e9 21 9e 38 2e ae ef 32 06 d2 dc 4a 6f d1 a6 96 29 6c c8 62 38 48 2a 0d 7a ed ab fc 86 6e fa 57 8f 1f 32 5d f2 82 33 1c b7 06 68 92 2b 6b 09 22 54 93 ea 1a ca 43 50 8a 03 17 14 35 d2 7b 5f 7d 9a 09 ed d7 79 5f da e4 2e ce 51 20 96 cb 15 9e 5b 79 6d f1 97 d7 05 fd 3b bb 13 35 42 5c 50 05 e9 b6 ad fb 73 bf 72 76 eb 8d bb 87 e9 65 be b7 0b 2e 16 7c 16 72 18 96 c7 23 7d 2b 10 bf 48 67 68 b9 35 19 55 18 d7 6a 9d 7b bf d9 5d b7 73 6f 95 c1 f6 c7 76 bc dd af 73 64 52 f2 de 3c 27 73 da db f7 06 3b 1c b7 50 bb c7 7a d8 d5 c9 9b 60 c8 4a aa c2 37 ea 35 da fe c7 e5 d8 e5 ff 00 88 65 a4 cb Data Ascii: uk,TRNBA$jWSr(6)1e9Pq7BX!8.2Jo)lb8H*znW2]3h+k"TCP5{_}y_.Q [ym;5B\Psrve.|r#}+Hgh5Uj{]sovs dR<'s;Pz`J75e
2021-09-28 09:09:19 UTC	326	IN	Data Raw: 8a f2 e4 08 3b 81 e2 4f 86 ae 33 fd ae f3 cb c6 ca 53 75 69 32 fe 21 0b 55 eb 18 a2 95 68 c8 e3 4d 59 5d 5d db 0b 6c fd c1 25 67 5a fa b1 5b b8 01 a2 66 03 97 cd c4 82 09 e9 a7 c6 b4 b0 47 71 6d 62 d3 08 e4 9b 8e f0 c3 40 1a a3 f0 d0 57 50 60 6e 60 82 08 20 6b a8 cb ad d1 63 2c 61 8c 22 50 a4 1e 22 4e a1 4f 96 b2 02 e2 60 c0 88 78 d7 70 22 48 98 a8 5a 6d 4a 36 af ed cb fe 44 6d 22 f2 24 06 68 dc 92 54 93 5e 84 ec 45 35 71 65 7a b1 48 6c 24 ac 72 14 e7 24 8a 63 22 16 f5 4d 5b e4 09 fa 4e b2 19 96 54 68 e2 f4 e2 8c 95 05 94 1b 63 3c 89 c8 54 f1 62 ca 69 e0 da c5 d9 5c da 48 f7 16 b7 4f 33 ba a0 68 e3 0a ec b2 33 72 dc 29 52 40 fb 4e b3 0f 87 4b 9b 7c 2d a3 05 9e ea da 25 16 a3 d2 b7 a8 84 0a 9f 52 79 16 9b 78 0f bb 4d 96 ed 5b d8 e6 ba 28 bc ec a7 8a 45 4b Data Ascii: ;O3Sui2!UhMY]]l%gZ[fGqmb@WP`n` kc,a"P"NO`xp"HZmJ6Dm"$hT^E5qezHl$r$c"M[NThc<Tbi\HO3h3r)R@ NK|-%RyxM[(EK
2021-09-28 09:09:19 UTC	342	IN	Data Raw: 46 31 c8 39 3c 4a 48 0f ef 28 a7 51 5d 55 cf ab 1a 31 49 63 60 68 42 9e 2a 78 b7 5d d4 7c 46 a2 9a de 78 d2 41 34 5c e2 25 91 43 86 56 2b c9 80 55 51 40 7a eb f1 00 d2 2a 4e 94 20 93 1d ca 09 48 5e 24 fc d1 cc cc ac 7c 49 d3 2c 9e a4 67 e4 e2 4d 50 30 70 39 7e 2a 54 01 fa 75 ea 33 ba 7f 74 28 56 e3 c0 71 1d 49 00 95 1a 01 99 98 9a 7e 71 d9 57 ca 2a 8f 94 31 3b 6d b6 a7 b5 b6 77 83 25 1c 90 df e1 ee 40 1c 71 f9 cb 16 13 63 ae aa 08 67 48 ae 00 57 0b f2 98 99 c7 8d 35 63 92 8a 34 85 ae 60 11 de 5b 32 71 6b 0c 8d b4 f3 5a e4 71 c7 d3 04 d7 1f 7f 1b c5 c8 7e 30 16 a6 84 1d 3b 19 1c 4b 52 51 d5 bd 35 8c 9a 57 92 83 5a 6d d4 f5 d7 d4 19 18 89 be 63 ea aa 27 5d 81 08 b5 0c 2b e5 5d 7f 30 9e d9 de 7f c4 dd bf b6 76 9d ff 00 8c b2 0b c7 ea 7f c9 fd c5 1e 2f 3f 69 Data Ascii: F19<JH(Q]U1Ic`hB*x]|FxA4\%CV+UQ@z*N H^$|I,gMP0p9~*Tu3t(VqI~qW*1;mw%@qcgHW5c4`[2qkZq~0;KR Q5WZmc']+]0v/?i
2021-09-28 09:09:19 UTC	358	IN	Data Raw: 91 ff 00 c6 53 c6 a4 1d c6 bb 97 b6 f2 df 46 66 86 ee e3 d0 66 1e 9f 08 ae d4 ca 14 29 14 f5 23 f5 00 71 d5 4f db ab 8e da 82 49 2e 72 3e bc 8d 6a 44 2f 24 1f 4c c7 d4 34 92 9c 7e 58 da 94 d5 fd be 4d c9 55 1e bc 11 12 21 4f 4e e1 1d ca a0 5f c5 24 74 a9 1a be 93 1f ea cf 87 b7 99 92 26 65 72 e9 25 49 94 10 77 24 53 52 59 59 a4 c5 65 80 08 c5 ba 97 08 ec 38 95 78 d7 e6 a0 3f 30 f8 e8 64 2e 3e aa e2 f2 78 5e e2 e1 ee 99 ab 53 50 d1 f1 7f c2 d5 1f 66 bb 97 1f 7b 34 31 de cd 6b 7d 1d b5 bc ec a1 dd d9 24 87 8a af 52 54 10 7e 3a ef 88 39 16 b5 5c 3e 05 57 6a 03 20 b6 b2 43 42 6b 52 a0 eb d8 f8 62 7a cd 05 e5 80 14 56 04 83 8f 74 21 8f 90 3a 47 a9 01 63 89 49 fe eb 80 2b f6 92 7f 46 ad 67 94 57 8b 5a ab 6e 1a aa d3 40 c2 80 54 9a 0d 76 dd c5 a2 ca 15 31 18 f6 Data Ascii: SFff)#qOI.r>jD/$L4~XMU!ON_$t&er%Iw$SRYYe8x?0d.>x^SPf{41k}$RT~:9\>Wj CBkRbzVt!:GcI+FgWZn@Tv1
2021-09-28 09:09:19 UTC	374	IN	Data Raw: 26 09 7b bf fc b3 8f 9b 15 98 83 3f 7c d6 e9 71 7d 92 7c 9d f4 70 db d9 da c9 25 d0 b6 be b5 8a ca 3e 2e a6 32 e6 bc 8b 54 6a 6b 95 f7 13 3b b5 94 d0 5d 59 59 cb 69 67 8b 29 28 78 65 8e 19 b8 cb 2c 0b 25 b4 9c 0a 23 f1 6a 0a 00 75 8a fa 16 9b 2e b6 09 3d bc 37 97 52 ae 46 e6 cd 58 8f 5b d2 8e f0 1b 79 7a 82 55 c5 07 80 ae ac 62 c5 8b 6b fb 48 64 86 de ce 7b 57 fa 18 e3 79 e5 e5 00 93 10 f1 47 04 2c ac 37 65 ae f5 f0 d6 33 03 f4 53 c9 1d ee 4a 1b d8 ad f1 d7 cb f4 69 91 86 77 5b 89 e3 11 90 9e 94 d6 e0 ac 91 10 52 bb 80 0e fa ee 0b 2e e2 c6 b2 5b cf 24 97 71 c1 79 1c c2 28 2e e2 75 46 55 57 01 24 fa 8b 76 26 32 0f 45 fb 35 97 b5 c6 ad d4 51 5d dc ba 7a 0d 1b d0 c5 73 23 3b 5c 1a 9a 98 61 26 82 94 d4 58 56 a4 77 31 da c0 60 98 b2 2b b9 8c 89 04 f1 46 1e 4e Data Ascii: &{?|q}|p%>.2Tjk;]YYig)(xe,%#ju.=7RFX[yzUbkHd{WyG,7e3SJiw[R.[$qy(.uFUW$v&2E5Q]zs#;\a&XVw1`+FN
2021-09-28 09:09:19 UTC	390	IN	Data Raw: d6 f6 b3 46 f9 2c 7d ad bd ba 09 60 58 2c ae 2e 21 7b 79 ee d6 23 90 84 19 62 5b 3f 56 36 8a 36 32 33 33 14 66 3a e3 1d ec 37 d6 36 f8 e4 8a 28 67 9d 22 b8 94 d9 5d 42 5e 7b 18 6c ad d5 ad af 2d ee 99 a5 78 18 b5 14 f8 83 4d 7b b6 d8 cb ab 4b fc 79 f7 03 b9 1e d6 eb 1e e1 ec e5 8e 5c 84 92 b3 5b 3a 45 0c 6f 11 96 46 a1 0a 01 35 d4 44 a9 58 e6 9c b3 83 5a 9e 1c fe 52 3c 41 1a 8a d9 76 17 19 28 22 48 87 5a 16 60 0d 7c 69 4d 05 61 f3 75 a7 95 3c ff 00 46 a4 30 56 22 a2 80 ad 2a 4e db 9a 0e 95 d7 cd 2c 8e 00 00 29 3b 6c 3f af 44 c9 02 71 ad 49 24 9d cf 9a ee 37 3a e5 24 47 90 47 8c 04 d8 51 86 c7 a7 50 6b ae 65 96 94 22 9e 9b 29 04 82 2a 2b e5 ac 9e 16 49 cc f2 e3 b2 11 5c c4 84 d0 ac 4e 4b 49 4a d4 d5 cd 3f 46 bd 8c cf ab 54 14 b3 8e 59 06 c0 b3 45 2c 61 18 Data Ascii: F,}`X,.!{y#b[?V66233f:76(g"]B^{l-xM{Ky\[:EoF5DXZR<Av("HZ`|iMau<F0V'"*N,);l?DqI$7:$GGQPke")*+I\NKIJ? FTYE,a
2021-09-28 09:09:19 UTC	406	IN	Data Raw: 44 d6 ab f4 d8 d9 6d ee 4b 5e df dc 43 34 6d 19 a3 10 ad 22 86 91 4b 20 c4 62 6c ae 05 d6 27 29 32 ba e2 ee a2 55 b8 7f a5 b4 7f 5e 6c f4 56 86 28 20 62 d6 8c 79 2b 7a 80 3c 80 80 05 34 97 b1 42 af 65 7b 90 be bf b7 36 9e 95 c3 5a 63 f0 51 cb 14 30 42 97 75 87 21 8f 9a e2 22 e9 04 fc b9 f1 70 1b e6 14 ba b8 9e 29 ed e4 ee 5c db e4 71 59 7c 6f d1 bd c6 23 35 34 45 52 d2 3b 29 8b 46 96 97 42 25 0b 0c a7 d2 ba 8c bc 0c 56 40 ac 64 bb 91 04 79 8c 55 bc f1 f7 05 b4 51 fc f9 0c 24 d1 ac d1 5d d8 c9 3d 4d d1 b1 59 5c c0 b2 d5 e4 c7 cd 2d bb 1e 71 50 7d 3e 2e f2 ee e2 6c 5c f7 97 7d bb 97 79 38 b4 98 89 da dd 24 c7 65 62 99 83 bc 12 47 e9 c0 79 72 e5 12 44 ea 43 2d 4d c0 96 76 83 1f f5 f0 e6 b1 98 ac 78 fa 7b 8c 76 68 c3 23 5d cf 8c b9 ff 00 c4 da 40 a9 cd bd 26 Data Ascii: DmK^C4m"K bl')2U^lV(by+z<4Be{6ZcQ0Bu!"p)\qY|o#54ER;)FB%V@dyUQ$]=MY\-qP}>.l\}y8$ebGyrDC-Mvx{vh#]@&
2021-09-28 09:09:19 UTC	422	IN	Data Raw: 96 50 e0 ae 70 9e 84 07 f0 b4 96 92 e6 73 56 86 f6 3f 9a b2 45 24 2b c4 81 c7 47 93 74 04 28 a9 a6 c6 82 82 9a 3b 9d b9 78 fe 8e bf 01 a7 6a 36 e0 28 0a 48 2c 08 e1 d4 7d be 3a c8 c1 72 ad c2 ef 9c 40 16 1c 54 06 e4 a2 84 f5 5a ed a6 29 46 25 4d 29 5d f6 3b f4 d3 b9 15 a8 00 8a d7 70 0e fd 7a ea 72 40 72 4a 82 a4 56 aa bb 9a 8f 10 46 98 c6 04 63 9b 01 c7 90 6e 15 3b 0e 3b f4 d2 b3 99 87 1d 81 2d 21 ae de 55 27 ae bd 0b 76 67 95 d4 a8 52 ef b1 22 84 b0 3d 00 1f b3 4d 73 77 21 79 64 2e 5b 72 54 72 26 a1 41 3b 03 ad eb e1 e3 e3 4d fa 57 42 95 24 d4 81 e7 4f 89 a6 a0 58 c8 56 69 10 11 51 d7 91 ae fa 87 95 58 05 3c cd 76 01 a9 4a 50 f8 ea 49 ac d5 8d dc 36 77 53 59 a1 35 67 bd 86 d2 59 ad 02 8e bf e3 c4 bf a8 75 d7 78 47 77 90 9e cb bb 3d c3 ee 7c e9 ef 7c ed Data Ascii: PpsV?E$+Gt(;xj6(H,}:r@TZ)F%M)];pzr@rJVFcn;;-!U'vgR"=Msw!yd.[rTr&A;MWB$OXViQX<vJPI6wSY5gY uxGw=|

Timestamp	kBytes transferred	Direction	Data
2021-09-28 09:09:19 UTC	438	IN	Data Raw: e0 b8 59 14 d3 e7 91 7e 6f 1d 33 63 f3 77 3e f3 f6 9e 3d 64 e2 b9 ab 5c 27 b9 d6 a6 da db e5 50 d9 2b 59 6d 7b aa 08 f8 0d 8b cb c8 57 72 4e 97 07 ef ff 00 b0 5d c5 da 77 b1 08 63 bb ce 7b 7d 79 f5 d6 a1 81 02 69 ee 3b 5b ba 4d a6 5e dd b9 57 94 70 5c ca b4 1b 75 a0 8a d7 b5 7d e0 ed bb 3c cd d3 20 8b b7 fb bd 2e bb 2b 32 8d 2e c2 03 0f 71 c1 6d 6d 34 bc d4 80 61 b8 60 c7 a5 6a 34 97 56 e6 39 e0 bb 4e 51 5c c2 c2 e2 da e2 3a 83 58 6e 15 9e 19 d6 a4 6e 09 d0 be c4 dd dd e3 ae e3 25 e3 ba c7 5c 4f 67 3c 6c a7 e6 65 9a de 58 d9 4a d3 7d f6 d4 70 db 77 a3 f7 0d 84 24 11 8f ee 9b 38 f3 28 e0 d3 f2 fe ad d2 3b ee 34 f1 0d 51 e7 a8 ad 7d c4 f6 f6 6b 53 cd 56 6c bf 6a df 19 a2 65 a7 cc ff 00 c2 ef ca 3f 0d fa 2b d6 be 5a 86 1c 47 7e e3 b1 f7 f3 10 06 2b b8 92 7c Data Ascii: Y~o3cw>=d\'P+Ym{WrN]wc{}yi;[M^Wp\u}< .+2.qmm4a`j4V9NQ\:Xnn%\Og<leXJ}pw$8(;4Q}kSVlje?+ZG~+|

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 6312 Parent PID: 3568

General

Start time:	11:09:04
Start date:	28/09/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\FROqdaZTXE.dll'
Imagebase:	0x7ff61d1b0000
File size:	140288 bytes
MD5 hash:	A84133CCB118CF35D49A423CD836D0EF
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: 00000000.00000002.406765007.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6344 Parent PID: 6312

General

Start time:	11:09:04
Start date:	28/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\FROqdaZTXE.dll',#1
Imagebase:	0x7ff7eef80000

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: 6380 Parent PID: 6312

General

Start time:	11:09:05
Start date:	28/09/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\FROqdaZTXE.dll
Imagebase:	0x7ff6b14d0000
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: 00000003.00000002.369118065.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 6396 Parent PID: 6344

General

Start time:	11:09:05
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\FROqdaZTXE.dll',#1
Imagebase:	0x7ff767900000
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: 00000004.00000002.247188597.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: iexplore.exe PID: 6444 Parent PID: 6312

General

Start time:	11:09:05
Start date:	28/09/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Internet Explorer\iexplore.exe
Imagebase:	0x7ff788920000
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: 6476 Parent PID: 6312

General

Start time:	11:09:05
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DllCanUnloadNow
Imagebase:	0x7ff767900000
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: 00000007.00000002.250016607.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: iexplore.exe PID: 6528 Parent PID: 6444

General

Start time:	11:09:06
Start date:	28/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6444 CREDAT:17410 /prefetch:2
Imagebase:	0x7ff797770000
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: 3472 Parent PID: 6380

General

Start time:	11:09:07
Start date:	28/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: 6708 Parent PID: 6312

General

Start time:	11:09:09
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DllGetClassObject
Imagebase:	0x7ff767900000
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.00000002.258163972.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6896 Parent PID: 6312

General

Start time:	11:09:13
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmAttachMilContent
Imagebase:	0x7ff767900000
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: 0000000C.00000002.269372359.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 7044 Parent PID: 6312

General

Start time:	11:09:16
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmDefWindowProc
Imagebase:	0x7ff767900000
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: 0000000D.00000002.280311070.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 7104 Parent PID: 6312

General

Start time:	11:09:21
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmDetachMilContent
Imagebase:	0x7ff767900000
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: 0000000E.00000002.282558272.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 804 Parent PID: 6312

General

Start time:	11:09:25
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmEnableBlurBehindWindow
Imagebase:	0x7ff767900000
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: 00000014.00000002.291132273.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6700 Parent PID: 6312

General

Start time:	11:09:28
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmEnableComposition
Imagebase:	0x7ff767900000
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: 00000017.00000002.298078907.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 7124 Parent PID: 6312

General

Start time:	11:09:32
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmEnableMMCSS
Imagebase:	0x7ff767900000
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: 00000018.00000002.306023387.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 7156 Parent PID: 6312

General

Start time:	11:09:35

Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmExtendFrameIntoClientArea
Imagebase:	0x7ff767900000
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: 0000001A.00000002.313866092.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 5212 Parent PID: 6312

General

Start time:	11:09:39
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmFlush
Imagebase:	0x7ff767900000
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: 0000001B.00000002.320703611.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 1000 Parent PID: 6312

General

Start time:	11:09:42
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmGetColorizationColor
Imagebase:	0x7ff767900000
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: 0000001C.00000002.328825836.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6748 Parent PID: 6312

General

Start time:	11:09:46
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false

Commandline:	rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmGetCompositionTimingInfo
Imagebase:	0x7ff767900000
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: 0000001D.00000002.335325271.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6764 Parent PID: 6312

General

Start time:	11:09:49
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmGetGraphicsStreamClient
Imagebase:	0x7ff767900000
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: 0000001E.00000002.342840550.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 1256 Parent PID: 6312

General

Start time:	11:09:53
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmGetGraphicsStreamTransformHint
Imagebase:	0x7ff767900000
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: 0000001F.00000002.350560741.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 5340 Parent PID: 6312

General

Start time:	11:09:56
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmGetTransportAttributes
Imagebase:	0x7ff767900000
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: 00000020.00000002.357565041.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 5284 Parent PID: 6312

General

Start time:	11:09:59
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmGetUnmetTabRequirements
Imagebase:	0x7ff767900000
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: 00000021.00000002.365133450.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 3952 Parent PID: 6312

General

Start time:	11:10:03
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmGetWindowAttribute
Imagebase:	0x7ff767900000
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: 00000022.00000002.431388502.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: wlrmdr.exe PID: 3060 Parent PID: 3472

General

Start time:	11:10:05
Start date:	28/09/2021
Path:	C:\Windows\System32\wlrmdr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wlrmdr.exe
Imagebase:	0x7ff7ce160000
File size:	65704 bytes
MD5 hash:	4849E997AF1274DD145672A2F9BC0827
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 3232 Parent PID: 6312

General

Start time:	11:10:07
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmInvalidateIconicBitmaps
Imagebase:	0x7ff767900000
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: 00000025.00000002.381961674.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 7112 Parent PID: 6312

General

Start time:	11:10:10
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmIsCompositionEnabled
Imagebase:	0x7ff767900000
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: 00000027.00000002.392634921.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: wlrmdr.exe PID: 6320 Parent PID: 3472

General

Start time:	11:10:12
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\BAz\wlrmdr.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\BAz\wlrmdr.exe
Imagebase:	0x7ff6e3c60000
File size:	65704 bytes
MD5 hash:	4849E997AF1274DD145672A2F9BC0827
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: 00000028.00000002.392891461.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: isoburn.exe PID: 4012 Parent PID: 3472

General

Start time:	11:10:15
Start date:	28/09/2021
Path:	C:\Windows\System32\isoburn.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\isoburn.exe
Imagebase:	0x7ff6d5bc0000
File size:	117248 bytes
MD5 hash:	46A0538BD86F949DF1E40802AB6BFFC7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6148 Parent PID: 6312

General

Start time:	11:10:16
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\FROqdaZTXE.dll,DwmModifyPreviousDxFrameDuration
Imagebase:	0x7ff767900000
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: 0000002A.00000002.401652535.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Disassembly

Code Analysis