ID: 457500
Sample Name: YfDl.bin
Cookbook: default.jbs
Time: 15:00:27
Date: 01/08/2021
Version: 33.0.0 White Diamond

Table of Contents

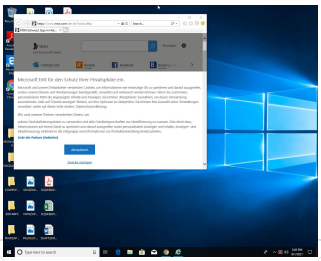
Windows Analysis Report YfDl.bin

Overview

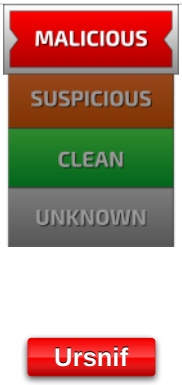
General Information

Sample Name:	YfDl.bin (renamed file extension from bin to dll)
Analysis ID:	457500
MD5:	499200f6a8e223c.
SHA1:	ef46f9c62b94715..
SHA256:	d7e64f8e65ce586.
Infos:	

Most interesting Screenshot:



Detection



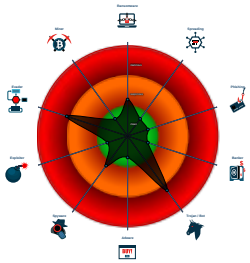
Ursnif

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected Ursnif
- Creates an undocumented autostart …
- Found stalling execution ending in A…
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- Antivirus or Machine Learning detec…
- Contains functionality to call native f…
- Contains functionality to dynamically…
- Contains functionality to query CPU …
- Contains functionality to read the PEB

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6124 cmdline: loaddll32.exe 'C:\Users\user\Desktop\YfDl.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 3376 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\YfDl.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 3440 cmdline: rundll32.exe 'C:\Users\user\Desktop\YfDl.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 5768 cmdline: regsvr32.exe /s C:\Users\user\Desktop\YfDl.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - iexplore.exe (PID: 5412 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - iexplore.exe (PID: 4464 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6760 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:17426 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6400 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:82960 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6524 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:82964 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 7064 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:17442 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 2152 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:82978 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6276 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:17446 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 5216 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:17476 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 5348 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:17480 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6716 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:17484 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 1236 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:83022 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - rundll32.exe (PID: 3292 cmdline: rundll32.exe C:\Users\user\Desktop\YfDl.dll,Opisthotonos MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6184 cmdline: rundll32.exe C:\Users\user\Desktop\YfDl.dll,Hydrazo MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6344 cmdline: rundll32.exe C:\Users\user\Desktop\YfDl.dll,Overlock MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6440 cmdline: rundll32.exe C:\Users\user\Desktop\YfDl.dll,Automobilist MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6612 cmdline: rundll32.exe C:\Users\user\Desktop\YfDl.dll,Swampland MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6868 cmdline: rundll32.exe C:\Users\user\Desktop\YfDl.dll,Subarachnoid MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7164 cmdline: rundll32.exe C:\Users\user\Desktop\YfDl.dll,Bechained MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6316 cmdline: rundll32.exe C:\Users\user\Desktop\YfDl.dll,Unforeseenness MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6504 cmdline: rundll32.exe C:\Users\user\Desktop\YfDl.dll,Incrimination MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6852 cmdline: rundll32.exe C:\Users\user\Desktop\YfDl.dll,Oversystematic MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6496 cmdline: rundll32.exe C:\Users\user\Desktop\YfDl.dll,Shieldless MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2596 cmdline: rundll32.exe C:\Users\user\Desktop\YfDl.dll,Tsarevitch MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6104 cmdline: rundll32.exe C:\Users\user\Desktop\YfDl.dll,Torchbearer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5200 cmdline: rundll32.exe C:\Users\user\Desktop\YfDl.dll,Moler MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5340 cmdline: rundll32.exe C:\Users\user\Desktop\YfDl.dll,Hyperpigmented MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1328 cmdline: rundll32.exe C:\Users\user\Desktop\YfDl.dll,Adipous MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5428 cmdline: rundll32.exe C:\Users\user\Desktop\YfDl.dll,Undazzled MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6988 cmdline: rundll32.exe C:\Users\user\Desktop\YfDl.dll,Peckishness MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.428802489.0000000001D88000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000017.00000003.310250645.0000000006638000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000002E.00000003.368506549.0000000006CE8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000032.00000003.385717547.0000000006DE8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000029.00000003.367471901.0000000006D38000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 117 entries

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Boot Survival:

Creates an undocumented autostart registry key

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Malware Analysis System Evasion:

Found stalling execution ending in API Sleep call

Stealing of Sensitive Information:

Yara detected Ursnif

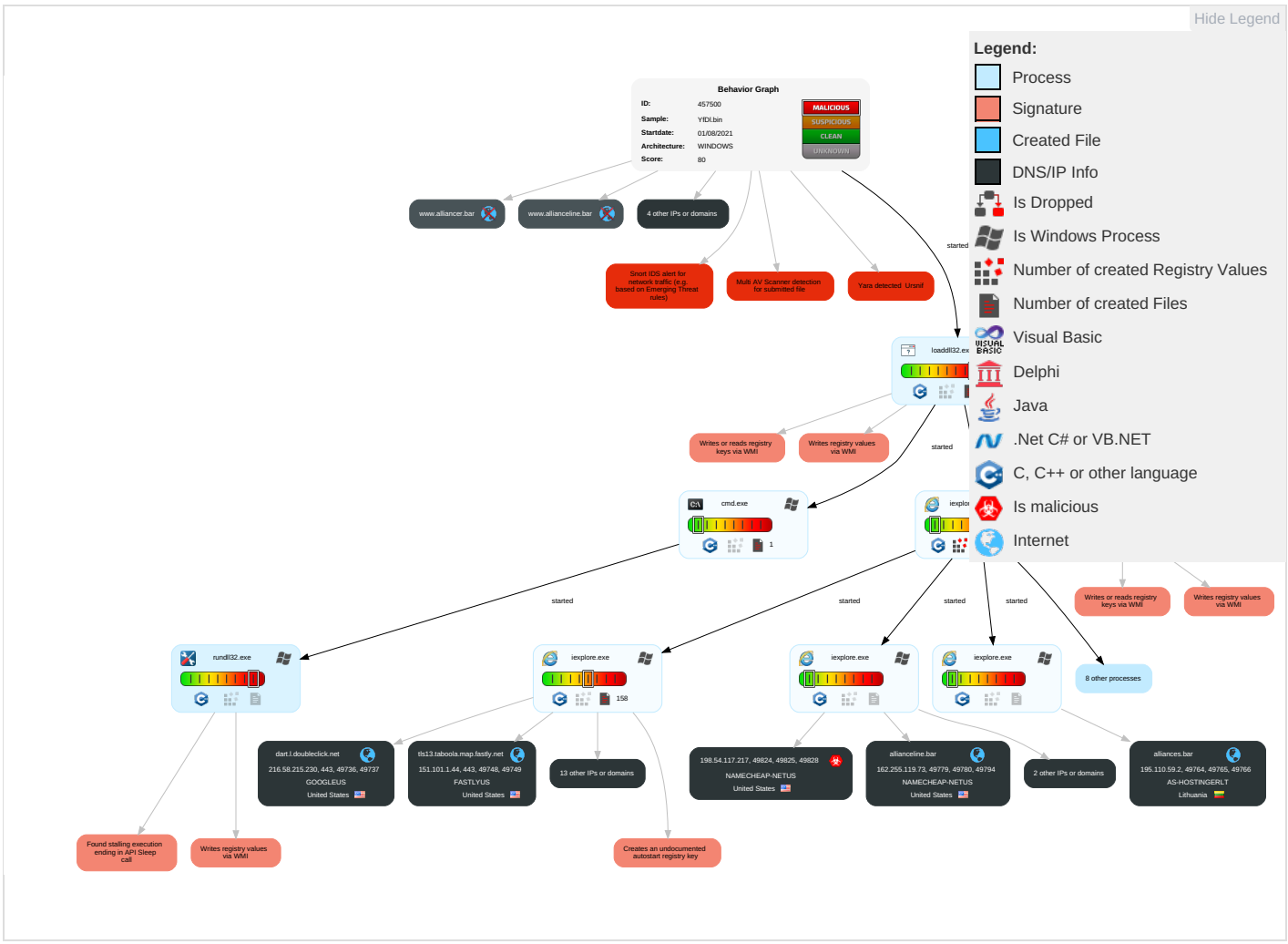
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 2	Registry Run Keys / Startup Folder 1	Process Injection 1 2	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdr Insecure Network Commur
Default Accounts	Native API 2	DLL Side-Loading 1	Registry Run Keys / Startup Folder 1	Virtualization/Sandbox Evasion 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Process Injection 1 2	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Regsvr32 1	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commur
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rundll32 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial o Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access I
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	System Information Discovery 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocol

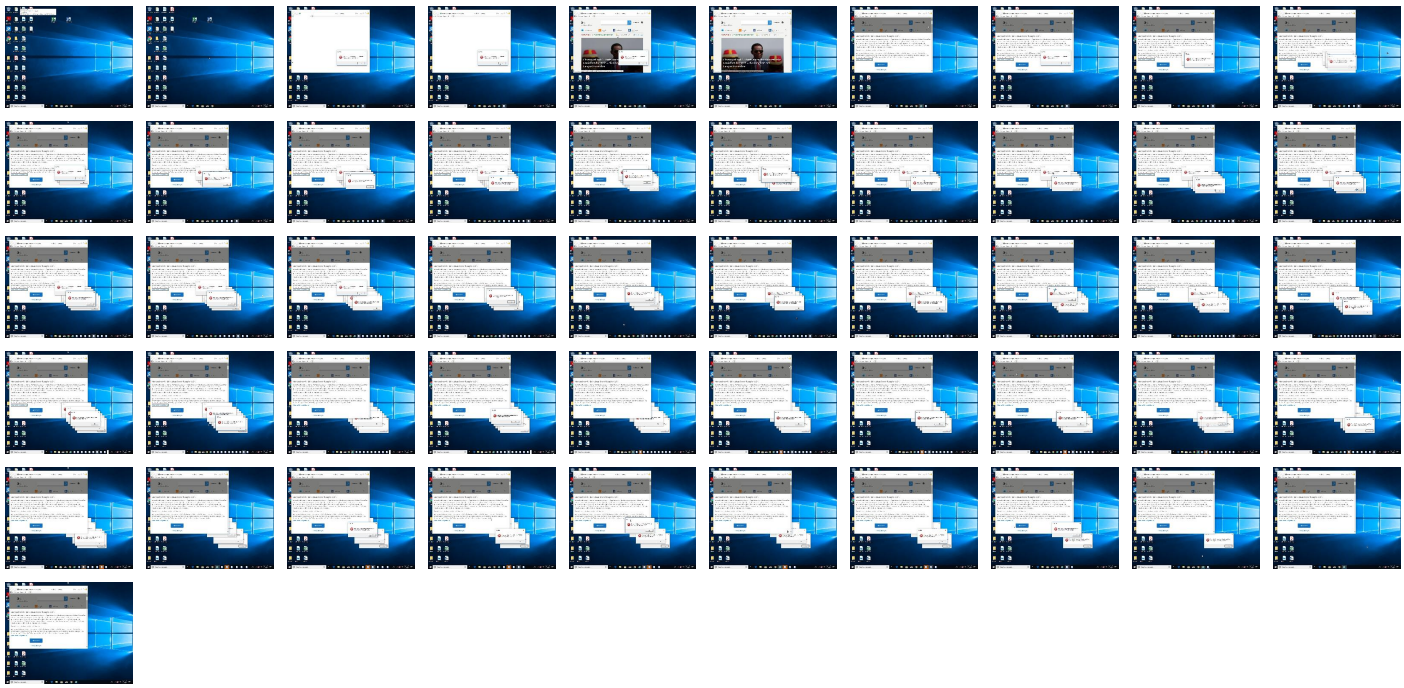
Behavior Graph

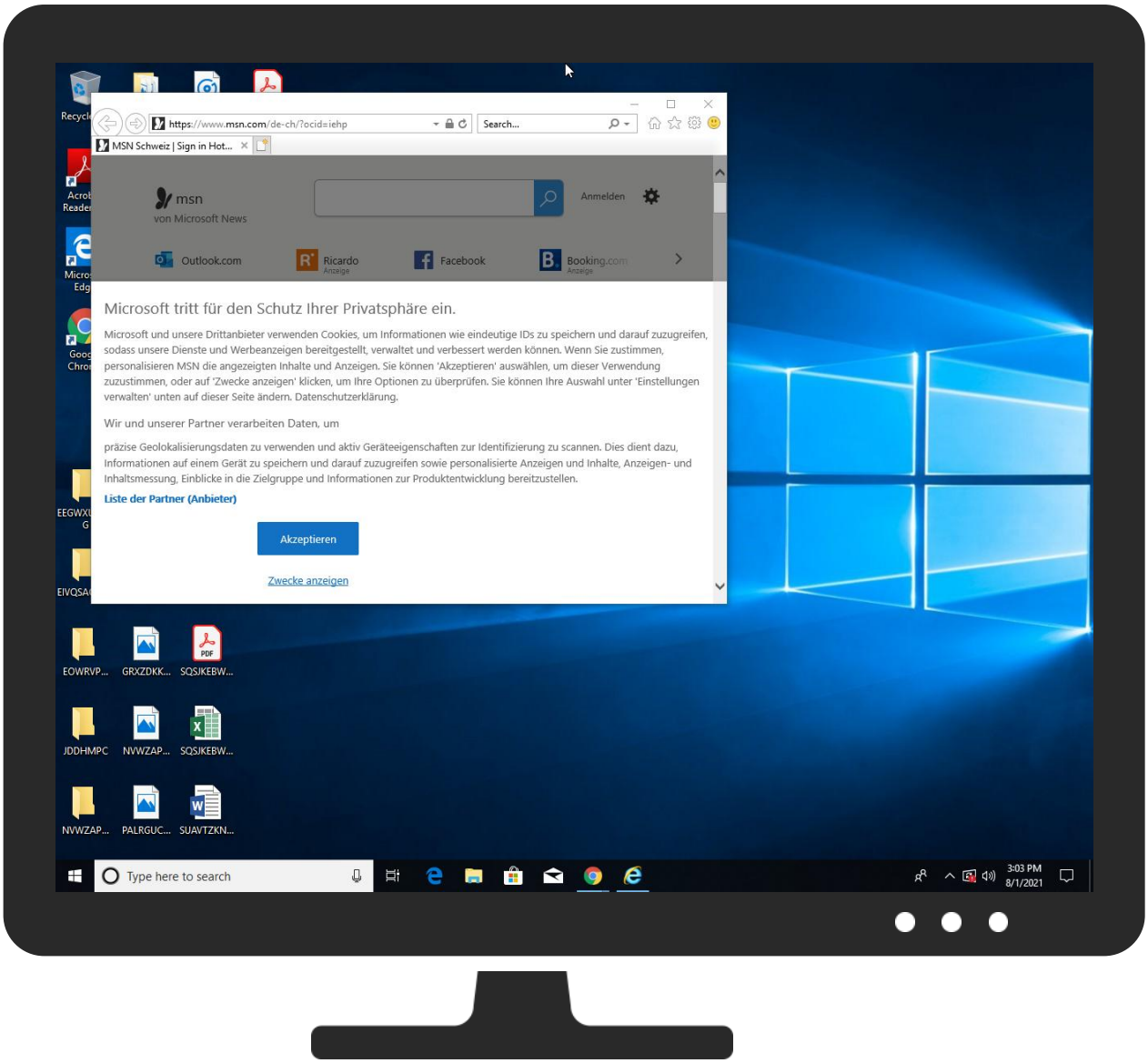


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
YfDl.dll	69%	Virustotal		Browse
YfDl.dll	51%	Metadefender		Browse
YfDl.dll	68%	ReversingLabs	Win32.Trojan.Ursnif	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.47d0000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
36.2.rundll32.exe.4440000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
37.2.rundll32.exe.4d70000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
13.2.rundll32.exe.4cf0000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
3.2.regsvr32.exe.10000000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
46.2.rundll32.exe.2f50000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
12.2.rundll32.exe.840000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
41.2.rundll32.exe.4b60000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
22.2.rundll32.exe.6ba0000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
23.2.rundll32.exe.4660000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.ca0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
42.2.rundll32.exe.52c0000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
18.2.rundll32.exe.4f80000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
14.2.rundll32.exe.34c0000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
3.2.regsvr32.exe.d20000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
4.2.rundll32.exe.10000000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
48.2.rundll32.exe.4920000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
50.2.rundll32.exe.4e20000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.2.loaddll32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://allianceline.bar/jdraw/dLL7q72MwgF/_2BKoRFjbhgJAS/vzNzOQYcs22fS9PZmGiqk/ImBn4ZbMkjp0c79n/fXFEqaYEWVKY_2F/_2FJyGoOXr4VTVC0eg/LUPZCf_2B/C1_2BlEDEf8ijbPT3XDP/4GbLjdNj_2Ft1xIX937/olnPKLY6LOBYxvJBmWK5iG/ofDL9uajZoReh/gnTfiCz_/2FJnM9VsOUm_2FxBFWygfHA/WN_2FWTfKr/cGyLVu_2BuD/D0vz.crw	0%	Avira URL Cloud	safe	
http://allianceline.bar/jdraw/dLL7q72MwgF/_2BKoRFjbhgJAS/vzNzOQYcs22fS9PZmGiqk/ImBn4ZbMkjp0c79n/fXFE	0%	Avira URL Cloud	safe	
http://https://onedrive.live.com;Fotos	0%	Avira URL Cloud	safe	
http://allianceline.bar/jdraw/_2FYs4QtMw9_2FVqLpLk2/u2LhzC7LFlqce_2B/EJ5CkL6CyTor06H/h9Yb_2BSjV6Rt1S	0%	Avira URL Cloud	safe	
http://alliancer.bar/jdraw/6t2TJPVp8r4_2Fuvh2KKhY/8YV_2B_2BRJ82/6nGE2eYA/7HHAwpkhVWuf8lW4yXxIq9d/P3s	0%	Avira URL Cloud	safe	
http://allianceline.bar/jdraw/cryAR_2BXe/tfZsZbCTIFSKEc_2F/fRFkFMDrwQ2J/nrfzPEYzAHe/Wx7an4ijbM8zE_/2FhpezUV4yO_2FfukN7U6/uBGYkZ4E31D33UZl/2HgOfw9U8TtlGcU/RO3AW2pv4UBCdojWiG/XAiw8U4II/LFIW7fzb6NeZ11ktdY_2/BmSX_2BpD6QEHKNSkw3/GsrABMXgDqbSFWjB/BiqFiS.crw	0%	Avira URL Cloud	safe	
http://allianceline.bar	0%	Avira URL Cloud	safe	
http://alliances.bar/jdraw/PjuRunwYj4Bhvxk9T/FkaG6F1W0LAq/7ctDH_2F3Sg/7ugfKJqoxNQwsg/2ypZ1ap9U9TAmPN	0%	Avira URL Cloud	safe	
http://alliances.bar/jdraw/_2Fgi_2F0q9mbLIMOTyI/MSZHR0hHa_2BmeQiSR3/W8oggZpI5myExagD6_2BTj/ey2UGr7NbceZG/WQBy5MHE/7qXKpRH7zu077im_2F1dGJV/DbKkDe7jsz/yWoZjzp1UojMkJrXW/XsiPUNe_2BZ8/DIfEiNMAFM1/A0a2dGIo685cVI/iUyIhZAYyWsoPEjMSHZWX/6iyEp102eL/_2F_2FrX.crw	0%	Avira URL Cloud	safe	
http://alliances.bar/jdraw/AZ9j6FN_2FTyei6/Zf0uCNl_2FdnsseDLQ/aAlru6mfg/_2BxJ18hXN8l3o6HRZtg/iMkRHAWOXQH7Sonii2y/ZUDDqy42horX1ipsJquAAp/PE_2BV88LYzPh/_2BwspqN/QHL0gRAjrGmh0Ze8EXmvwJx/w8RwH_2Fv_/2FEesIeaXL2YGMyBr/PGDsr7HWeSeF/e3J46D1VO9zlgcp/85Zp5.crw	0%	Avira URL Cloud	safe	
http://allianceline.bar/jdraw/4trhqHpiyJW/gPL61gbH3V3gm2/GiN8WmuvnoRNfvQO06HHD/TolcFVz_2FK8ZYP2/IZQ7	0%	Avira URL Cloud	safe	
http://alliancer.bar/jdraw/6t2TJPVp8r4_2Fuvh2KKhY/8YV_2B_2BRJ82/6nGE2eYA/7HHAwpkhVWufpkhVWuf8lW4yXxI	0%	Avira URL Cloud	safe	
http://alliances.bar/jdraw/KzfCuU1nYQ/2jKJWMeBiltqUkBZk/bJHRs3aRSUlv/cI63tiCHI_2/F5uaZGCIn42HAA/37yNTKIJLuVjIBN3j61BH/f_2F7jKyVaT3WSHP/Idyt_2BFxwVV7Ez/wF0a5CSrL3svyQDzt7/z5kTlRVsI/o_2BijKkihsvPwp7ObK8/nGfEqkF_2BV9O_2BYHe/y7YIFWRDvDFDsnXQU1dk4w/ugyqJTKGN21dPtrvVHSLW/X.crw	0%	Avira URL Cloud	safe	
http://allianceline.bar/jdraw/cryAR_2BXe/tfZsZbCTIFSKEc_2F/fRFkFMDrwQ2J/nrfzPEYzAHe/Wx7an4ijbM8zE_/2	0%	Avira URL Cloud	safe	
http://alliances.bar/jdraw/AZ9j6FN_2FTyei6/Zf0uCNl_2FdnsseDLQ/aAlru6mfg/_2BxJ18hXN8l3o6HRZtg/iMkRHAW	0%	Avira URL Cloud	safe	
http://alliances.bar/jdraw/i1UnGotMRZpYX5QI846/jmFIJI_2FNDz7pkL8TrBB5/fMotNSc0eJn6p/utqPXHuH/Wff27J_	0%	Avira URL Cloud	safe	
http://alliances.bar	0%	Avira URL Cloud	safe	
http://alliances.bar/jdraw/TAmAcu8EQ5dbq_2FLn/jmsAPZU0N/O3d42v1YOxC8LCsNcUdI/hBRtAVsuP0wmqk3iAnH/V7a2yIwEeWGhi2w2781UJd/XfMuL5OGMx46D/tX7UDvFf/Y_2BiaZRVpr3DW0jCRNM81D/ubtn4Y0mDo/Zf69CqE_2FlQ0hZy6/_2B_2BpRSoEQ/klrzoZkO8B_/2BwdYmhPaHQxFS/cUtgYxD_2/F.crw	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://alliancer.bar/jdraw/8hMkfU_2BkV2Ho4GURNxe/X8MBAAmtf27latmq/SxWCuMHAvCWenY2/OeooX6vNMX17Ym3H7Q	0%	Avira URL Cloud	safe	
http://https://tools.applemediaservices.com/api/badges/download-on-the-app-store/black/de-de?"	0%	URL Reputation	safe	
http://allianceline.bar/jdraw/eNEjgfypiWX/qzBN0pjHkXaIJy/uSQAHTqmu7LUbuntarKiK/xwqbRspQk1D8qp6M/HWl7	0%	Avira URL Cloud	safe	
http://https://onedrive.live.com;OneDrive-App	0%	Avira URL Cloud	safe	
http://alliances.bar/jdraw/_2Fgi_2F0q9mbLIMOTyI/MSZHR0hHa_2BmeQiSR3/W8oggZpI5myExagD6_2BTj/ey2UGr7Nb	0%	Avira URL Cloud	safe	
http://alliances.bar/jdraw/b812tUOw/5vOcsr2Qa7HjSQYaeUGfQDe/A8EgAMSWJM/_2FFmfetjQhRMnISV/eMe6aV6DLPB	0%	Avira URL Cloud	safe	
http://alliances.bar/jdraw/KzfCuU1nYQ/2jKJWMeBiltqUkBZk/bJHRs3aRSUlv/cI63tiCHI_2/F5uaZGCIn42HAA/37yN	0%	Avira URL Cloud	safe	
http://https://www.stroeer.com/fileadmin/com/StroeerDSP_deviceStorage.json	0%	URL Reputation	safe	
http://www.alliancer.bar/jdraw/T1Oye5dXOyO7X2/W2Jf88M5e37Kz6KOh7AdL/wY5JZWvpnXF42vVg/l7s4mKoV_2FqPNE/dhTHk84TOdHYwxXQ3F/ZDAxuudp3/D1Qs8omUsHmDB_2FVyG9/fdORbAiNcjwPXWrQQ0O/25Y_2BweBhA69miE0hz3Mk/RqfVs38U7EbR6/7NRpQCUV/WpJhqepI5X3UmOUCA7tjaJ_/2FPWDLDzx0/6EjYsFZMbGs/q1m.crw	0%	Avira URL Cloud	safe	
http://allianceline.bar/jdraw/4trhqHpiyJW/gPL61gbH3V3gm2/GiN8WmuvnoRNfvQO06HHD/TolcFVz_2FK8ZYP2/IZQ72utUu8FkRq_/2F067OV_2FLlPUB9yd/i0sqdLKlL/TufDKlZhewFrgjSOjZoV/kw8l6gL0iujBb8tryKS/RGvMacSQhLHBDOTrqNLG4m/uP_2BKAulmZfa/zQq7CHkj/_2F1r9d83Jng_2Fktvq5Alz/Ls6WH3GEdzGxn/iTBX.crw	0%	Avira URL Cloud	safe	
http://alliances.bar/jdraw/Rb3_2FHxtxhMSM8zm/gYEt3B3r9PE_/2FfL3q236io/GFNEH8CEcSGt3Q/Xgu6vIh5KIqx2S1	0%	Avira URL Cloud	safe	
http://alliances.bar/jdraw/	0%	Avira URL Cloud	safe	
http://https://www.stroeer.de/konvergenz-konzepte/daten-technologien/stroeer-ssp/datenschutz-ssp.html	0%	URL Reputation	safe	
http://https://www.bidstack.com/privacy-policy/	0%	URL Reputation	safe	
http://alliancer.bar/jdraw/T1Oye5dXOyO7X2/W2Jf88M5e37Kz6KOh7AdL/wY5JZWvpnXF42vVg/l7s4mKoV_2FqPNE/dhT	0%	Avira URL Cloud	safe	
http://alliances.bar/jdraw/PjuRunwYj4Bhvxk9T/FkaG6F1W0LAq/7ctDH_2F3Sg/7ugfKJqoxNQwsg/2ypZ1ap9U9TAmPNK3Mj4E/1tkWj6xiOwNb06Ci/nMiIDTqZjqNR3Sl/Be2FTUJy9LUIgqGDgy/uKg22hRQ4/Py3DVyO8YWF3rk9X3HQr/yNaCoWiag_2BmQ7jPMJ/8l4YPxQA8wBHHEka2W3QS6/U7.crw	0%	Avira URL Cloud	safe	
http://alliances.bar/jdraw/_2FrlUhAClUiRyd8MwHtotk/I15TfspZAu/z01In076RAgynlo0F/aYBbR51uD1ML/uqQjbpx	0%	Avira URL Cloud	safe	
http://allianceline.bar/jdraw/eNEjgfypiWX/qzBN0pjHkXaIJy/uSQAHTqmu7LUbuntarKiK/xwqbRspQk1D8qp6M/HWl7bj_2FWhMbP8/Uujd82PrM7mxT3Qzg0/MWYHS6cay/F6rvctGR9QcGUIn_2BcA/FoEllX9k6apV8hveoXo/zNk4xAZcRLb7MRvJXwEutR/loIAT32m6_2BY/8Nz5PjSgzU6nn7nO/fTwM.crw	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
contextual.media.net	23.211.6.95	true	false		high
alliancer.bar	162.255.119.245	true	false		high
dart.l.doubleclick.net	216.58.215.230	true	false		high
tls13.taboola.map.fastly.net	151.101.1.44	true	false		high
hblg.media.net	23.211.6.95	true	false		high
allianceline.bar	162.255.119.73	true	false		high
parkingpage.namecheap.com	198.54.117.210	true	false		high
lg3.media.net	23.211.6.95	true	false		high
btloader.com	104.26.7.139	true	false		high
geolocation.onetrust.com	104.20.184.68	true	false		high
ad-delivery.net	104.26.3.70	true	false		high
alliances.bar	195.110.59.2	true	false		high
www.msn.com	unknown	unknown	false		high
ad.doubleclick.net	unknown	unknown	false		high
srtb.msn.com	unknown	unknown	false		high
img.img-taboola.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.allianceline.bar	unknown	unknown	false		high
web.vortex.data.msn.com	unknown	unknown	false		high
www.alliancer.bar	unknown	unknown	false		high
cvision.media.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://allianceline.bar/jdraw/dLL7q72MwgF/_2BKoRFjbhgJAS/vzNzOQYcs22fS9PZmGiqk/ImBn4ZbMkjp0c79n/fXFEqaYEWVKY_2F/_2FJyGoOXr4VTVC0eg/LUPZCf_2B/C1_2BlEDEf8ijbPT3XDP/4GbLjdNj_2Ft1xIX937/olnPKLY6LOBYxvJBmWK5iG/ofDL9uajZoReh/gnTfiCz_/2FJnM9VsOUm_2FxBFWygfHA/WN_2FWTfKr/cGyLVu_2BuD/D0vz.crw	true	• Avira URL Cloud: safe	unknown
http://allianceline.bar/jdraw/cryAR_2BXe/tfZsZbCTIFSKEc_2F/fRFkFMDrwQ2J/nrfzPEYzAHe/Wx7an4ijbM8zE_/2FhpezUV4yO_2FfukN7U6/uBGYkZ4E31D33UZI/2HgOfw9U8TtlGcU/RO3AW2pv4UBCdojWiG/XAiw8U4II/LFIW7fzb6NeZ11ktdY_2/BmSX_2BpD6QEHKNSkw3/GsrABMXgDqbSFWjB/BiqFiS.crw	true	• Avira URL Cloud: safe	unknown
http://alliances.bar/jdraw/_2Fgi_2F0q9mbLIMOTyI/MSZHR0hHa_2BmeQiSR3/W8oggZpI5myExagD6_2BTj/ey2UGr7NbceZG/WQBy5MHE/7qXKpRH7zu077im_2F1dGJV/DbKkDe7jsz/yWoZjzp1UojMkJrXW/XsiPUNe_2BZ8/DIfEiNMAFM1/A0a2dGIo685cVI/iUylhZAYyWsoPEjMSHZWX/6iyEp102eL/_2F_2FrX.crw	true	• Avira URL Cloud: safe	unknown
http://alliances.bar/jdraw/AZ9j6FN_2FTyei6/Zf0uCNl_2FdnsseDLQ/aAlru6mfg/_2BxJ18hXN8l3o6HRZtg/iMkRHAWOXQH7Sonii2y/ZUDDqy42horX1ipsJquAAp/PE_2BV88LYzPh/_2BwspqN/QHL0gRAjrGmh0Ze8EXmvwJx/w8RwH_2Fv_/2FEesIeaXL2YGMyBr/PGDsr7HWeSeF/e3J46D1VO9zlgcp/85Zp5.crw	true	• Avira URL Cloud: safe	unknown
http://alliances.bar/jdraw/KzfCuU1nYQ/2jKJWMeBiltqUkBZk/bJHRs3aRSUlv/cI63tiCHI_2/F5uaZGCIn42HAA/37yNTKIJLuVjIBN3j61BH/f_2F7jKyVaT3WSHP/Idyt_2BFxwVV7Ez/wF0a5CSrL3svyQDzt7/z5kTlRVsl/o_2BijKkihsvPwp7ObK8/nGfEqkF_2BV9O_2BYHe/y7YIFWRDvDFDsnXQU1dk4w/ugyqJTKGN21dPtrvVHSLW/X.crw	true	• Avira URL Cloud: safe	unknown
http://alliances.bar/jdraw/TAmAcu8EQ5dbq_2FLn/jmsAPZU0N/O3d42v1YOxC8LCsNcUdI/hBRtAVsuP0wmqk3iAnH/V7a2ylwEeWGhi2w2781UJd/XfMuL5OGMx46D/tX7UDvFf/Y_2BiaZRVpr3DW0jCRNM81D/ubtn4Y0mDo/Zf69CqE_2FlQ0hZy6/_2B_2BpRSoEQ/klrzoZkO8B_/2BwdYmhPaHQxFS/cUtgYxD_2/F.crw	true	• Avira URL Cloud: safe	unknown
http://www.alliancer.bar/jdraw/T1Oye5dXOyO7X2/W2Jf88M5e37Kz6KOh7AdL/wY5JZWvpnXF42vVg/l7s4mKoV_2FqPNE/dhTHk84TOdHYwxXQ3F/ZDAxuudp3/D1Qs8omUsHmDB_2FVyG9/fdORbAiNcjwPXWrQQ0O/25Y_2BweBhA69miE0hz3Mk/RqfVs38U7EbR6/7NRpQCUV/WpJhqepI5X3UmOUCA7tjaJ_/2FPWDLDzx0/6EjYsFZMbGs/q1m.crw	true	• Avira URL Cloud: safe	unknown
http://allianceline.bar/jdraw/4trhqHpiyJW/gPL61gbH3V3gm2/GiN8WmuvnoRNfvQO06HHD/TolcFVz_2FK8ZYP2/IZQ72utUu8FkRq_/2F067OV_2FlIPUB9yd/i0sqdLKlL/TufDKlZhewFrgjSOjZoV/kw8l6gL0iujBb8tryKS/RGvMacSQhLHBDOTrqNLG4m/uP_2BKAulmZfa/zQq7CHkj/_2F1r9d83Jng_2Fktvq5Alz/Ls6WH3GEdzGxn/iTBX.crw	true	• Avira URL Cloud: safe	unknown
http://alliances.bar/jdraw/PjuRunwYj4Bhvxk9T/FkaG6F1W0LAq/7ctDH_2F3Sg/7ugfKJqoxNQwsg/2ypZ1ap9U9TAmPNK3Mj4E/1tkWj6xiOwNb06Ci/nMiIDTqZjqNR3Sl/Be2FTUJy9LUIgqGDgy/uKg22hRQ4/Py3DVyO8YWF3rk9X3HQr/yNaCoWiag_2BmQ7jPMJ/8l4YPxQA8wBHHEka2W3QS6/U7.crw	true	• Avira URL Cloud: safe	unknown
http://allianceline.bar/jdraw/eNEjgfypiWX/qzBN0pjHkXaIJy/uSQAHTqmu7LUbuntarKiK/xwqbRspQk1D8qp6M/HWl7bj_2FWhMbP8/Uujd82PrM7mxT3Qzg0/MWYHS6cay/F6rvctGR9QcGUIn_2BcA/FoEIIX9k6apV8hveoXo/zNk4xAZcRLb7MRvJXwEutR/loIAT32m6_2BY/8Nz5PjSgzU6nn7nO/fTwM.crw	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.26.3.70	ad-delivery.net	United States		13335	CLOUDFLARENETUS	false
198.54.117.217	unknown	United States		22612	NAMECHEAP-NETUS	true
162.255.119.73	allianceline.bar	United States		22612	NAMECHEAP-NETUS	false
195.110.59.2	alliances.bar	Lithuania		47583	AS-HOSTINGERLT	false
216.58.215.230	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false
151.101.1.44	tls13.taboola.map.fastly.net	United States		54113	FASTLYUS	false
104.26.7.139	btloader.com	United States		13335	CLOUDFLARENETUS	false
104.20.184.68	geolocation.onetrust.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	457500
Start date:	01.08.2021
Start time:	15:00:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	YfDl.bin (renamed file extension from bin to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	53
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:	mal80.troj.evad.winDLL@87/254@35/9
EGA Information:	• Successful, ratio: 78.9%
HDC Information:	• Successful, ratio: 90.4% (good quality ratio 85.2%) • Quality average: 78.4% • Quality standard deviation: 29.8%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:01:49	API Interceptor	7x Sleep call for process: rundll32.exe modified
15:01:55	API Interceptor	1x Sleep call for process: regsvr32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\A9VUXYF1\www.msn[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	152
Entropy (8bit):	5.144362423003052
Encrypted:	false
SSDEEP:	3:D90aK1ryRtFwsx6wmxvFuqLHIfwEYPJGX7T40AAexTRK3sqSeV0bFKb:JFK1rUFkduqswEkIXH40AAeHK3Ifbkb
MD5:	0AE89BEE0FCCB762940393E485768FE3
SHA1:	6F3C792C30AE6F4C174EE8EA4D5E4E5E76BBBF8F
SHA-256:	129A26C8A079DF1663D006CCB9E50AFFA9C9056F1CB8FF1CF42EB001DE24AC27
SHA-512:	8672CFC082591613725ED0541328F035BDD425B2CBD00E2D3E995D4B05E068B5A6A4B65CDC12215B4A50979D3FDA4147192C4500989A783D44BC46808B3AF5A
Malicious:	false
Reputation:	unknown
Preview:	<root></root><root><item name="BT_AA_DETECTION" value="{"ab":false,"acceptable":true}" ltime="3363367792" htime="30902048" /></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\Y7FEA6TK\contextual.media[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3158
Entropy (8bit):	4.927792080167545
Encrypted:	false
SSDEEP:	96:WVVVnVMMOMMCCCsCCCCCfW4I4CfW4I4CfW4I4CfW4I4CfW4I4UCfW4I4C:L
MD5:	EBDEB410E95002CE81642F4BA2C50A38
SHA1:	0D3FED89A4F16C94F53E1E69BE90C45D1606B1F1
SHA-256:	021EABEACF483E2BBBC0AA5BC1093947A9CDA4388E347A147B3E7B55398CEF65
SHA-512:	0EA4E7C7126EB1D637DE6B916989A862B92F550A338358DDCDE593AF3E13254FF050FE62C5697F6A5127F93EDB6527F5B845E7CCF61004713804B813A90273BB
Malicious:	false
Reputation:	unknown
Preview:	<root></root><root></root><root><item name="HBCM_BIDS" value="{}" ltime="3345357792" htime="30902048" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3345357792" htime="30902048" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3345357792" htime="30902048" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3345357792" htime="30902048" /><item name="mntest" value="mntest" ltime="3345357792" htime="30902048" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3345357792" htime="30902048" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3345877792" htime="30902048" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3345877792" htime="30902048" /><item name="mntest" value="mntest" ltime="3345877792" htime="30902048" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3345877792" htime="30902048" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3345877792" htime="30902048" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3351867792" htim

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{01B84D60-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	1066104

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{01B84D60-F314-11EB-90E4-ECF4BB862DED}.dat	
Entropy (8bit):	2.9306645707387795
Encrypted:	false
SSDEEP:	384:rlM6qtKhjDnOy2s6F3oKKfspBQXG5fRdsfs0TzUXQL7p71WszDz8zbDVdrQ4r2io:B2TcyTBH75oa5S
MD5:	6958A10476A4F60AEBE5D831D99FB918
SHA1:	0E8359A03C15A8E6C45E614CF59AF51035E5CE30
SHA-256:	A9FBF4D986BD1F020B594B4730EF890773988901BDBFE1364006420C2E222AF9
SHA-512:	93359229F4408D9E5A0C6E23C96F555C42958E294B882DECDB46A07C2C03CC879384D131187EF370A497D8FD10D1365F8170BA532315DC90E7B08DA2EB1C8E0
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{01B84D62-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	197566
Entropy (8bit):	3.583386104625758
Encrypted:	false
SSDEEP:	3072:PZ/2Bfcdmu5kgTzGtaZ/2Bfc+mu5kgTzGtY:WZB
MD5:	49D26981020636367CE90563E09A69C5
SHA1:	96CFE67CB8D52932F46729BD06B69D48EA435F19
SHA-256:	325114CC4D43EDDBF58C3CD05B92B2C7E6DBC0CD581DFA3C9EBE021CA0BAD1C2
SHA-512:	F902C48FD479058928527043B6C5E4843C1334BECFBA54599E796EA9AC3F184B6D4E7CBC1BE5005610A5F9B83315CABD52FEDBEC288B9928E18249F02B9484F
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{07B78121-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5830201777277748
Encrypted:	false
SSDEEP:	48:IwbGcprqGwpaU7G4pQ8GrapbSoGQpKEG7HpRLTGIpX2NGApm:rBZyQA66BSQAPThFAg
MD5:	F43CABF0BC5A7EBC6CC69176C1F8E151
SHA1:	238915A81713E9B833D45C8D2FE5386AF5AFE865
SHA-256:	C62B0121163F62A7456249F5407970089809C58A05927F40F3E0FDBEC7F2615B
SHA-512:	C3FF4C310DAEC14682E9B8E9131A9677982DCE4B7D5F1C69948D9457147F584A746FCA3ACFA3BA31EC9E08DFF3FB8AB8B27CA647EA8E6B7B890C9271988F2F5
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{07B78123-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27364
Entropy (8bit):	1.8427674575567963
Encrypted:	false
SSDEEP:	96:rmZdQJ6XBSwjh21WUMgGy08rARy08rb0dA:rmZdQJ6Xkwjh21WUMgG68R6gA
MD5:	90BBE90D33FE2B0DE7092FECDF1B4366
SHA1:	985C82A74DB7B702C17998D656E3F942F5D80CA6
SHA-256:	580D4848CFC9D833081DFB6B9ADECE51435743B374B12F875B92BD39BAA495AD
SHA-512:	93ACD70D7CC7442FAA7ED45C9D4B3104D88E520FBA66326D3F7E023773FF44BE5818ACFD4CF0FC16D0C5423510912722CB68F5D77C21BE78EA0B9C136714897

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{07B78123-F314-11EB-90E4-ECF4BB862DED}.dat	
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{11855471-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27368
Entropy (8bit):	1.844056057872779
Encrypted:	false
SSDEEP:	96:rkZjQX6hBSQjt2pW/QMspirYL9xrYLSYOA:rkZjQX6hkQjt2pW/QMspiExxA
MD5:	79EECE24B0067436CEA7C6F7B36D950B
SHA1:	014929D5AA9CF26FE34FA805E55D64769BFEEEF1
SHA-256:	EED0094A36F7CA1F3E27A7D186A06DF4FC1F2B4A96E298FBA96B3D48A5722239
SHA-512:	E63CBD2267103C572744995E65E8A648FF68FCACC3F449FC8B964FFA75DF58175EB4CD46F00656316152CB408625014C42A8FCC0F28492C9F9D4DDD261671450
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{11855473-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5739708932321852
Encrypted:	false
SSDEEP:	48:IwwGcpr1GwpaFG4pQNGrapbSxGQpB1GHHpcITGUpG:r0ZfQX6tBSLj42wA
MD5:	853F3CECDE5983CF3405EF012A3403CD
SHA1:	BBBD09A224C552D737EEF274FB07B738DFE35A76
SHA-256:	68F019774554D8597426D5C5022081B49CAFA87972739081A9488A733D7D0D1F
SHA-512:	32F1C673FDAE2371FE84314EBC5C91F62EE64AA6E054DD3CE733459DC09D30AC2EAA8150D1C9C6917DB1FA0BD99AF36E205985B2166C429938D87CF7AECE0F F3
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{11855475-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27376
Entropy (8bit):	1.8490437165531572
Encrypted:	false
SSDEEP:	192:rRZCQS6gkNjD2HW6MC6NXFHmxNXFHOXHA:rXv9tpa27RN1HCN1HOQ
MD5:	C257016FFE8FE28885D81EDB483F897C
SHA1:	294E1B31C88DDD075CAA30BDBAFEC1DC5323077A
SHA-256:	56AF92406C032DED3699FF6804CCE311F4A1FCC7CC134B6F8B6BC83D2613E46A
SHA-512:	F236C6C0F8C20DCD2C59C5A8113A0F930D44161CAC2D244B3A748EB6A45B218F54E6122ABB41AD82593163F652EAA3DC4449623179F402202138F725CF774011
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{19D46F2A-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27376
Entropy (8bit):	1.846073478514319
Encrypted:	false
SSDEEP:	96:rBZmQa60BSGjN2FWNM56f/9mF8bJxf/9mF8b4/9mIA:rBZmQa60kGjN2FWNM56ndJxndGfA
MD5:	03068357A723AB3A31D30D01D081014D
SHA1:	9B789256E26D9884196638AF5E541047FE14F6AD
SHA-256:	A4E9CBDB1FFDD26CC4460D58EDA3E8BB2BB5F6FAB201751C8B8A383A9BC2B207
SHA-512:	BC2A67C9CC9D8E6D1172BECEBB3CB0A5C166008367943E9152D418C6A17EB2F362F9C3EA5ADC59E82C4BFE8CFD7DD697B2F6F72BE50CC7AD2AF0B897F651 CC1
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{19D46F2C-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27356
Entropy (8bit):	1.8411421469581968
Encrypted:	false
SSDEEP:	96:rdZKQi6cBSiejd2EWaMiuqTyGPRqTyG4A:rdZKQi6ckiejd2EWaMiugbRg0A
MD5:	1A0FA9A4FA0C12CAD95AF592C46DD48E
SHA1:	30418DB12D4D888BF00507FC7D0734A9B9209822
SHA-256:	0F6882316CECF6785CB17811C80758102C9CCE580E69682C371D9AC782A03C0F
SHA-512:	CED54ACC3068295556C2216F78ACB495D24A952DCB66F20FAA7E6C92F7E5834C9F8F26BC48CCFF16412FA2C3EF76A8AE4413CEA4A9BB5BADC84E304CF412A E8
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{19D46F2E-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27432
Entropy (8bit):	1.868235326999151
Encrypted:	false
SSDEEP:	192:riZBQl67kiejd2VWkMsiESCqG3xESCqGPSjA:reWQAiYUsRDESpMESpeSU
MD5:	72430003E19071E23B28F28D09DCF99D
SHA1:	8C217AC1D167DB52A2E6E778F6F4846EAA95100B
SHA-256:	59947F44AA0D5F13B6832ADB7786A377257075A5FBE7E9DE0B533CFBFB34CDF1
SHA-512:	FE2F5547723AB984C28725D5E3BD5C08350474F149E1593B2001024E62843A8795E8EE6265141F23E62166960F45D176B44EC263A16E70244A27F31C00C671A0
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{19D46F30-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27364
Entropy (8bit):	1.843855461559848
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{19D46F30-F314-11EB-90E4-ECF4BB862DED}.dat	
SSDEEP:	96:rvZI7QA6+BSJj92xWzMDGCtU26ORCtU26lthA:rvZEQA6+kJj92xWzMDGr9ORr9RA
MD5:	CD440B8E3C0CABB378E25647794E10BA
SHA1:	592C734FADEBF367D6469D6B3144813CFC9B4E55
SHA-256:	CAE94E045FA121F8E936B3F183E5A6DEB16CD739B9983287339D72AD4A793C9B
SHA-512:	F23DE7B280BDFFE1E26CB083CF765E3FA3E8EEE45BDBF3F113AA0ED3CC13F6038C846F937DD9449039B34A868E5F54F4178E2C59198E4AB9C738B1CDD4F410D2
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1FE27CB5-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27364
Entropy (8bit):	1.8426307352798483
Encrypted:	false
SSDEEP:	192:rTZgQw6uksjN2BWEMMG/wEk2R/wEkDwjA:rV5bPeEwxP/jkK/jkD5
MD5:	7B4511B00E56D0EC760D0E08711540C8
SHA1:	B57C8FA948AA4256A47D5E02E9993F25971AC834
SHA-256:	B738045716EEE36C73354106B6A688E01CAC8A15898B12ED206699CCEDC25745
SHA-512:	2659D6189E62054F131D5D241B24BDDADF0A617986949156566EBA7431949FBC057B18F764C94CCD4649BB5C3D667D06263E2C408F9B7FFFB56AA4A9E0C93F1
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1FE27CB7-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27928
Entropy (8bit):	1.8461790871201937
Encrypted:	false
SSDEEP:	96:rrZ4QU6yBS1jJ2RW9MhSnjZUyjFSRnjZUyjFBjYr:rrZ4QU6yk1jJ2RW9MhSjWsSRjWsVYr
MD5:	DB602B5730286D9853F02185ACB03424
SHA1:	85F8601A30015936A06708C8B2717B916ABAF61F
SHA-256:	537043A53776781CB9707C952527EAB8B38602EEA29B54D388C3AAC9F237DD52
SHA-512:	3521762A010D99A027DA334DB4192D797054F7334DB97A8479A8627FA4373841778E7069028D0368359F48F2F469133BB1AFECC6748BC945ACCDDCF5AC568E00
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1FE27CB9-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27356
Entropy (8bit):	1.841851028361465
Encrypted:	false
SSDEEP:	96:r91ZzMQ56bBScjx2RWHM2GuglX45/VRglX45/iXjoA:r91ZzMQ56bkcjx2RWHMrugeVRgeiEA
MD5:	062D85ED525E52457DD4FED7030A695A
SHA1:	630ECD7C987564E9B4FFA43527D0BC561185AC74
SHA-256:	3AD8B7AAE7AEE4688D1E4402DF493272A745FB07B04CD014D371C65ACD27D1F2
SHA-512:	8D5653064D8561BD7DF46382E48374339136D28412631A3279782F51646526DD0DFE7D5A94C1219493EEEC6A46081DCAD30410DB4CFEA80B0D60F5E1D232BD8
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1FE27CB9-F314-11EB-90E4-ECF4BB862DED}.dat	
Preview:	.... R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{27D0DC27-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27864
Entropy (8bit):	1.8241650382004335
Encrypted:	false
SSDEEP:	96:rsZPQf6pBS/jZ29WJMBS8EeGYZ3R8EeGYZBRr:rsZPQf6pk/jZ29WJMBSHejRHePr
MD5:	3AEEEB8EDED88B5419636D5910D3050F
SHA1:	19E78DCBAB54D3BD3074BF8DB8A7684A688EB73C
SHA-256:	24FE35FEE48A347036D02ADD45AD252251956A2ABC4017A6C56830C53B86CADE
SHA-512:	E32D4FDA17A02759B07DE4E0B50FEF9ECEC2458BBC3D8B54D36713A6B1289282B450802E4A41CC057B631D92FF88D72DA6A29D2B501161A284C05A8D8667C8 1
Malicious:	false
Reputation:	unknown
Preview:	.... R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{27D0DC2A-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27404
Entropy (8bit):	1.858192114467452
Encrypted:	false
SSDEEP:	96:r1Z2Qa63BS/j52ZWMMoeEuE0skBMxEuE0skBaE0sYiA:r1Z2Qa63k/j52ZWMMoepFaxpFgFWA
MD5:	940025642138DD8A58F868D5B6CA2804
SHA1:	2DBC90AEA99676180DD6EAA1EDE9F0E588EEECB8
SHA-256:	4C922EFCAF592D76A896BD91730EEFED822C69DDDAB8502C649EB5455B43F818
SHA-512:	2369C36D3880587D5CE59F881CD62B9274B2D934AA6FAE40AC7BD3539EECA2515595E47714F9B031C18E490134AAE86E5E51B3845F6CB6C1346BD2AF5754B2C
Malicious:	false
Reputation:	unknown
Preview:	.... R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{27D0DC2B-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27364
Entropy (8bit):	1.8433651982131196
Encrypted:	false
SSDEEP:	48:IwAGcprxGwpahG4pQ1GrapbS1GQpBiGHHpcPTGUp8IGzYpmkzGopU2CqTWNIxG/E:rkZrQz6lBS/j52ZWMMoG1RrNR1RrzjA
MD5:	DACFA9F57C3E690B7D2D63DDD740D83F
SHA1:	66FB4926732EEAF3309061067EC510D57514895E
SHA-256:	3D56FA11D6C6897FDF2E01BDA830FF2BC6766496D3FB31ACA421CDD56B8C322A
SHA-512:	0DD15766A040DC43EA7E5B8FF32CF0A76DB834E87F8C643E371A34204E773B685EAC7BF9AB08E1968989404553AAAA2FB09A0A049489CA1939305F63C2DDCA7 A
Malicious:	false
Reputation:	unknown
Preview:	.... R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{27D0DC2D-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{27D0DC2D-F314-11EB-90E4-ECF4BB862DED}.dat	
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27384
Entropy (8bit):	1.8518842431923939
Encrypted:	false
SSDEEP:	96:rHZ8Q36dBS7jj2bWWMOyR7AO0Hs6RR7AO0HsU7AOhA:rHZ8Q36dk7jj2bWWMOy5ms6R5msEhA
MD5:	15E770F48CFAEF5A96029464AF027B6C
SHA1:	6130067B10845542328A4197FB64E8682C27BA66
SHA-256:	12A455AD959707B8C9B1C00AFB6B84CD1663DA93549CF47683A59EA7E2036330
SHA-512:	C54AB0470C84F5834B71CDE5BC6673BF687393F221F5D58618B50BD3B671BD92EA81B3317CFE62DB2F7B8262555E94DB8B6DF96B144F3C02A362D8614203B0C
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{27D0DC2F-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27436
Entropy (8bit):	1.8686211578187273
Encrypted:	false
SSDEEP:	96:rYZ7QX6NBShSjvF2rVWVMO+qgDOjoxqgDOjlUCA:rYZ7QX6Nk0jN2RWVMO+3/x3LCA
MD5:	793EF154DF7D40823DEF49CDEA0D0CEF
SHA1:	DFC423A48FE29B2F0C89CB4837C4594C72986869
SHA-256:	1BB1FE87C9AE5A52C6CEEFEF1EE3D336EC337C3BDFB1270928B9218382560177
SHA-512:	3ADB09F5857459B68CD5EDDDC2F7ADB5EFFD6CFBDE2FF5B5D0AB27A68970C1B78C3DCA5C080623CE195A71EC65729A4AAF1FECAFF592B9857D0256102101313 B2
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{27D0DC31-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27360
Entropy (8bit):	1.8418656626877872
Encrypted:	false
SSDEEP:	96:rcZnQP6FBSmjx21WnMLq0lQUjpR0lQUj51A:rcZnQP6Fkmjx21WnMLqMQ6RMQMA
MD5:	D639A497D9F9A510A91E38785CD4F650
SHA1:	42C12739F8121E3718EBBE580A67FC5CD2C4137B
SHA-256:	770B264A961AD300ECD2FECA99A2816C7D868895F5D0845320224290B65EEFFA
SHA-512:	610A3BA034CB9E22FD2AF7735AF312EBDA57FF82B3CAC1CEE070B3F7AE818B2D723AE9D5DD85F3241C503FE14FAA74161CA63651257944C1EA03936E69C8AD 12
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{27D0DC33-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27928
Entropy (8bit):	1.847540449123775
Encrypted:	false
SSDEEP:	48:IwgGcprlGwpa9G4pQNGrapbSgGQpB+GHHpcDTGUp88GzYpmpeGopQzz69AtgK6e9:rEZvQ/6tBSIjN2dWoMoS/cAoR/cAOjr

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{27D0DC33-F314-11EB-90E4-ECF4BB862DED}.dat	
MD5:	A71D7E8B9A4D1EA79686156A3451A04F
SHA1:	15A6A4426D6AD679591DF7B68058D0244A3A3F6F
SHA-256:	57F9FD260908087AB7AC1A59B758FA3350FB06BB38DB058BDF5CDCFBF3A40F97
SHA-512:	5FBCE97A04D7824BE1939DD62BE0E2FE21B757F48CF0307331E7D7E220C8A552129476FC1CF60C839931F72E0308FA512CB159AC738C8AE18B5CEC129F6F99B
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{27D0DC35-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27340
Entropy (8bit):	1.8345329674363398
Encrypted:	false
SSDEEP:	96:rFZ+QV63BStjN2FWPMbe3MqdGTx3MqdGaqMA:rFZ+QV63ktjN2FWPMbecMGTxcMGapA
MD5:	BD4643DBCBCB5163D0973326B2283FF8
SHA1:	20864ABC83B1710424C9B7704F2C90D5517F3E7D
SHA-256:	49E14F085D0D38550B901A468095763DD95F21B91591E610BA424FA4D062535B
SHA-512:	92E83CEED3BF0650D420DCE60B2B37B93E4D0FF918FB0EC01FF619F22212CFD7C2B9CA7D7FEA4D2471F87D2F959F6D99A95C4CE6BC8B0767E6F0C4719E0EB 91
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{27D0DC37-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27376
Entropy (8bit):	1.847723168005921
Encrypted:	false
SSDEEP:	192:rGZ1Qp6nk4ejgIJ2gRWgoMgA6SXiXMmrDFePxSXiXMmrDFehiXIA:rCqEkbYD6c4t4dY
MD5:	C5A22F768FC1939FEFB8A2D0EFF05854
SHA1:	2FAC68541AEC72A5DD2C78A30A651EAD6D01CC45
SHA-256:	68A30946C9D633B6FC4C27F5F094D066AC37CD6E609CB6CA9D84A2B8F9AB7188
SHA-512:	E592D0DEB37B1A20BA91291D358D581E51BA42D6CFDBC6EC1A0E8E5F00738EDA676140AEBF433079D64CBC1825040B23DBC36D1A5B356B773B9BAC0BF96C8 74
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{27D0DC38-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.565461645571475
Encrypted:	false
SSDEEP:	48:IwtGcprFGwpa8G4pQoGrapbS7GQpKSG7HpRFTGIpG:rzZPQc62BS1A9TTA
MD5:	14AD0CBE78B2FCB06F9B1DC2D528E8AB
SHA1:	CD55C379AA0869554970EFE5B38F6B97030E31DA
SHA-256:	492840C57A14B15202C3947BAD788F5175C9A972D75B32629FC3F9DD802A916B
SHA-512:	CBA8F2A2ED510F87EF79C819D9CD1868F6D5821F145C8DDFE625BE0FEF022B7F29C2D0A553E548C8C0CCA4EFFB07A7FC2918545736630CCCBF7B56E3A0321D C7
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{27D0DC38-F314-11EB-90E4-ECF4BB862DED}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{2F1D94D8-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27368
Entropy (8bit):	1.8422155494685488
Encrypted:	false
SSDEEP:	48:IwkGcprRGwpawG4pQYGrapbSkGQpBOGHHpcrTGUp8ByGzYpm90xGopA3VUxGt+4a:r4ZLQw6mBS8jd2FWcMciFpVtxFpVowzA
MD5:	73257088D0DBE8C687E9FBB98A045649
SHA1:	F188650BBADB5EDA6DD73C5CCD0C4E31A9E0D90A
SHA-256:	5B18F05BB0AB63B9787A1FEED3B147E5FCE8E3A15AFA66A3433243B741EAC18B
SHA-512:	5CA75134829CCA889D711C0AADE5B2B4496FB2856B38716692C3D9B12B424674EC414D19DE62C93D7923A1B9A23DF4E6438E26FF797AF163C7A478DEA7372EA
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{2F1D94DA-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27216
Entropy (8bit):	1.8625593114796777
Encrypted:	false
SSDEEP:	96:rjZUQA6iBSTjB2LWqMka6xA8rRx6xbA8rqA:rjZUQA6ikTjB2LWqMka2Rx6qA
MD5:	13226ABC3ED62296E58DA833F86A070E
SHA1:	9FE7C0B7F817A1F666334220079F3EFFB1C30F26
SHA-256:	A2DCA5A3C948E85475C494E75763CA9C002B63F49FD5F6F636475457A17D9711
SHA-512:	B74BFD131C100E8EB05511E9DCB9B57D03340F9FBA9439EB2917FA0662EAC3D2740CE92D9FCE6B21B98ED9EB9384C7CA7860D2866DB103552BF1ADEFA308F9 6A
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{2F1D94DD-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27924
Entropy (8bit):	1.8466062842527826
Encrypted:	false
SSDEEP:	96:rWZZQp6jBSXh1j/Os2/5W/dM/V2N5SJKxN5SJfcr:rWZZQp6jkx1jN2hWFMN26Kx6Ur
MD5:	228B272005A53DD7318EC942D06B9119
SHA1:	FACF9D38349F8AB66AFD5224D0DA75F490EBEE4D
SHA-256:	DDA61D170AD98EC8B990734390907AFC6CCEE7B60904471EC0D2A688A5DE16E3
SHA-512:	4177426B0B39530ED0F8304704818750B93CE8F69C5319A3FADF57EE2E3A576C229C5AF0147B331307D4932728C7576405D06AF94C679DBCBAD40F58A1D3E013
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{2F1D94DE-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{2F1D94DE-F314-11EB-90E4-ECF4BB862DED}.dat	
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27440
Entropy (8bit):	1.8688703621253206
Encrypted:	false
SSDEEP:	96:r9ZqQO6wBSXh1j/Z2/5W/pM/VzmNHgH30DYxNHgH30DNkA:r9ZqQO6wkx1jR2hWRMN6eH30sxeH30CA
MD5:	1849B9ED451F7DD3FBC305A99EE2EB6B
SHA1:	E8298B388359ED4BA2C8185439A276D39AA80712
SHA-256:	30E8C1D5F1F1F2BAF3C8378B3AA6241CBC27A19BEB77BF220F56CC68643E0595
SHA-512:	76D34D7163A41D45F1A8979E227DDFB4C34084160C6EA2F345446C716014EF323190664517B26C56E26B86851598C83B4B424DB1CD25ABC70DA99ADCA12899CE
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{351E906A-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27340
Entropy (8bit):	1.8362022515397163
Encrypted:	false
SSDEEP:	96:rYZbQT6xBSL0jD5L2DTVWDvvMDiqeN7yCUkBgVLxN7yCUkBgTCUkKA:rYZbQT6xkoj92FWrvM+qePgLxP+A
MD5:	11FD074C5F59D641D6B3BA7BDB77DD70
SHA1:	22F0B154E74043B599C509983A75EBA7F036F3F1
SHA-256:	405DE3791B672326189533D856FB80D0B37EBDC7C6D595D09C068D5DD5CA02E4
SHA-512:	7F3F52AA1E54B631A3382F65690D6736B59F640DA2AA76F4CB0134F6796DC4F9D155951A81A74DD5F3B00ADC25ADF3F59632466B9AC774F4275693F2C9B433A4
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{351E906C-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27088
Entropy (8bit):	1.839191442721295
Encrypted:	false
SSDEEP:	192:rVZWQS6Akr0jzRL2zDVWzkMzUTmNZhxNifA:rbj9NrmzRCzDszRzImNZfNiI
MD5:	317A7887F60D142058D3A5F6B538D575
SHA1:	5C08E65BC435F5303F964CD9FECFC7326ED56CB1
SHA-256:	404AF5D19945557CBAEFE09A0D8F0192CFC1A05C685E57BB2E48FCB6C4CF223D
SHA-512:	1D15CA779C9105BB171F4D1B5463F57300D2CEC9BB996859A7FD4F4D98E137D3EDB236B510F4A0FD9493B0F4668BEBDA1C3958F6796E4419C5B91B148106EEB
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{351E906E-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24612
Entropy (8bit):	1.722268620833721
Encrypted:	false
SSDEEP:	48:IwnGcprjGwpa3G4pQjGrapbSfGQpBKGHHpc3TGUp8oGzYpmelGopUsjvBujRPu6I:rNZ9Q56HBSJjR2BWsM8GOBYRPuIg
MD5:	0DC3DD4B81F3E46F36B269E3859AE659
SHA1:	5695FBD95208EF0B1F5EA76BD9C3549E737CF486

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{351E906E-F314-11EB-90E4-ECF4BB862DED}.dat	
SHA-256:	17F4A95ECF3C9A3258A52B4662D15E081315C411A47E2C0966457ABFFA964E79
SHA-512:	F6E08889738AD3DE77A18B8E4A9CC327380C55F32AEC7499A5D8C55B167E4486E82B84EE99090F3264ECCEC6F47DEE73A80216254175BE198DC72A3298E5B71
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{351E9070-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27088
Entropy (8bit):	1.8407459619885356
Encrypted:	false
SSDEEP:	96:r1ZCQ/6JBS1jJ2hWJMhTmMRF83xMRvF8fA:r1ZCQ/6Jk1jJ2hWJMhTmh3x5fA
MD5:	70858837F12CDF209D3F6AB8644224CD
SHA1:	C443D1DCC96A18ED384494DF66A50014888B7E8F
SHA-256:	3CFC393DF723F43BDCF2706AEC5EEF82DA9CFD4562BCC8303802B819F1BC33B4
SHA-512:	AA8200627A15CC7B0A0B82C349ECA46FD049C7A42F538A34B64C5BF3481981E0731DD2A060181AF8F8A76A1B71AF5D7E861494CAD175B3C758D2F9869ED2433
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{351E9072-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27392
Entropy (8bit):	1.8519815644026607
Encrypted:	false
SSDEEP:	48:IwBGcproGwpaZG4pQ9GrapbSoGQpByGHHpcXTGUp8TGzYpmKWGopZmI9EQPmuA7V:r3ZwQ76dBSQjJ2hWJMhKArmORArmHm2A
MD5:	6100BD10C92FEA80EB39D2323835F85B
SHA1:	5E6524B214156497D7EFA495DFF67A6DBCC0B252
SHA-256:	5D3270F734BFE61A3E004BBEE640A12305806B609C00C30D5C4844A34AD87F39
SHA-512:	A0B6F3C9E2AE3571A5D31E32C493DEDCF69656008969C11BDF401D32198ABBD057C3A84894F89BBED789A7443AB25AF91689E601B0880A39E47ED74FA6823F4
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{351E9074-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27428
Entropy (8bit):	1.865849157833868
Encrypted:	false
SSDEEP:	48:IwqGcprPGwpazG4pQnGrapbSzGQpBCGHHpckcTGUp81MGzYpmGzHGopUs83zlaZP:rOZ5QF67BSNjZ2hW1YMQhGxTGRxTcA
MD5:	2C2B91BE5D750260B61338D85A450376
SHA1:	DFB7CFB1695C8A9E5AF15A86591513B712EA9C03
SHA-256:	3E25C4033BE84D6C562FA5790CF654EBAEBC98EDE5857344031A990A593E9BC2
SHA-512:	6B93156D83771272E3354875AF6942DB4E2B80073026E4E1E08999F3BB67F211FC101DEA22D1B19D61E86D2E40107D58D6A6E876D9F19ADEE12BB51ED047AFD2
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{3BB8EFEA-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27364
Entropy (8bit):	1.8398780486609683
Encrypted:	false
SSDEEP:	192:rLZYQb6pk5jd2UnWsMMGMMF7bRMMF7yMF/A:rdBe61UUWpPfFZfF1Fo
MD5:	93E77464E0CC7C7C72F94534E6684875
SHA1:	666CAB60D6B302A82C958A13C01CD851CE678F44
SHA-256:	9B568C211121271CBB07497F2ACA2CE7F2D10B4FD116DF4D83D4BF0302E49184
SHA-512:	92DB0440B3A3195042BBEB4FDE5430615E11F83688FF748F7D889C09087EAF491152DA2ED0EA4C43C5BD43B4DC28E6894753868429A50FE6B04EFE1BF625F708
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{4205BD41-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27396
Entropy (8bit):	1.8531647487837244
Encrypted:	false
SSDEEP:	96:rbZQQE6CBS5jx22WtMdmSKt/PRSKt/OiA:rbZQQE6Ck5jx22WtMdm5t3R5tGiA
MD5:	008165AEC02EF974CF561C96268D0314
SHA1:	46AA1710705E8C755B501E61F6480B9F28CD9ABD
SHA-256:	0B3AB327E8D7CACD013511403E6E01EF516B8B4DABBA686F5CC3BF05B26C1F53
SHA-512:	9930D53258083D6B686D35DDA796B08AF92AE63B1E3A3B26F46959DB2128B9E4598ACF9FA217B9BFE3160974482864291C41FF5B83B9170D323BAD768CC81A17
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{4205BD42-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27368
Entropy (8bit):	1.8383790286769315
Encrypted:	false
SSDEEP:	96:rwZWQy6EBS5jx21WtMdiYZBH1bxYZBH1EBH1hYA:rwZWQy6Ek5jx21WtMdiYH1bxYH1YH1uA
MD5:	0511CE32D5FCD05A458C780D42859ED3
SHA1:	CC3318F79468289A9969898D3B32A55F38EA3494
SHA-256:	6B5E0FD8DA79F317C875ECBF8B28860D3ECD819F3B4EDD44D848B326CC2AFCBF
SHA-512:	6CF0E7971947A01A7787057568C2DFEE42ABBCC14C2B929637B144267CB31BAD0AF0F592D089E22EE0313BFD7E2D4CF36140FDF0A71229333C2A306269FAD62
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{4205BD44-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27368
Entropy (8bit):	1.843753557957144
Encrypted:	false
SSDEEP:	192:ryZpQl6XkfjI2hWBM3iNKA/llxNKA/lVKAAA:ruOQUbcQaS8A/Z8A/qAT
MD5:	2C25510728442603066E35E811C1544C

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{4205BD44-F314-11EB-90E4-ECF4BB862DED}.dat	
SHA1:	E12082F410F1CA9BADA31E0783F2F112D55D4ABD
SHA-256:	1BA11EF4902C91A22E116728BDD747B290D38179A27E4ADC39FFE01B33B6CC56
SHA-512:	A637496682674F882EAA556ED483DB8E0E1804721514DD9637BD17E73090D62B90AA0726BFAC60960A7E9D751D8DFCA75B1FD744A2D01AD87671CE83928FC73
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{4205BD46-F314-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	27364
Entropy (8bit):	1.8436635470860712
Encrypted:	false
SSDEEP:	96:rIZTQH6dBSQ0jR2RWOM6G/VFLV9R/VFLVnA:rIZTQH6dkQ0jR2RWOM6G/B9R/BnA
MD5:	B2F067E6AC3762634F8367F0C3B8A7A7
SHA1:	7E5AEABED611B2352C43EE9A2B86665AD3D720B0
SHA-256:	93DA21B765B23BBA8C4592631C078BA331F7342B3A623D9869803BEFEE65A120
SHA-512:	B3BD145C0377C59DA8ABE0700239304F7E3843B33FA7FD2E9664EF5E543E282AF6C4A619E6151C04C7BA4E35A387ADEB2BDA19F77E864D427A1965F5017CECE D
Malicious:	false
Reputation:	unknown
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	934
Entropy (8bit):	7.040045848455702
Encrypted:	false
SSDEEP:	24:u6tWaF/6easyD/iCHLSWWqyCoTTdTc+yhaX4b9upGi:u6tWu/6symC+PTCq5TcBUX4bY
MD5:	0AF76835485904283AB595532949CD19
SHA1:	E2CD5E452747AC104796466AD4502C4F1EAE479E
SHA-256:	ACDCA7DB85E18F849207AB6E15DA849392A3D652BC0D37DD9625CDF07B935E66
SHA-512:	5A5A5C8D2082F34FF39F32ABA34B8288693570D99358E0520EA7D02FA80C63788E0BB0F23CCAA28EE00F825ACFE83C19CD9FC63538D8CF6BF35E357EC1CA0B 2
Malicious:	false
Reputation:	unknown
Preview:	E.h.t.t.p.s.:././.s.t.a.t.i.c.-.g.l.o.b.a.l.-.s.-.m.s.n.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.h.p.-.n.e.u./.s.c./.2.b./.a.5.e.a.2.1...i.c.o.....PNG.....IHDR... ... .pHYs..... .vpAg... ... .eIDATH...o.@../..MT..KY..P!9^....:UjS..T."P.(R.PZ.KQZ.S. ....,v2.^.....9/t....K..;_ }'.....~..qK..i.;.B..2.`.C...B.....<...CB.....).....;..Bx..2.}.. ._>w!..%B..{.d... LCgz..j/.7D.*.M.*.....'.HK..j%.!DOf7.....C.]._Z.f+..1.I+.;.Mf....L:Vhg..[.. ..O:..1.a....F..S.D...8<n.V.7M.....cY@.....4.D..kn%.e.A.@IA.,>\.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`. ... .a.....a....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\17-361657-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1238
Entropy (8bit):	5.066474690445609
Encrypted:	false
SSDEEP:	24:HWwAaHZRRIYfOeXPmMHUKq6GGiqIlQCQ6cQflgKioUInJaqzrQJ:HWwAabuYfO8HTq0xB6XfyNoUiJaD
MD5:	7ADA9104CCDE3FDFB92233C8D389C582
SHA1:	4E5BA29703A7329EC3B63192DE30451272348E0D
SHA-256:	F2945E416DDD2A188D0E64D44332F349B56C49AC13036B0B4FC946A2EBF87D99
SHA-512:	2967FBCE4E1C6A69058FDE4C3DC2E269557F7FAD71146F3CCD6FC9085A439B7D067D5D1F8BD2C7EC9124B7E760FBC7F25F30DF21F9B3F61D1443EC3C214E3F F
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\17-361657-68ddb2ab[1].js	
Preview:	define("meOffice",["jquery","jqBehavior","mediator","refreshModules","headData","webStorage","window"],function(n,t,i,r,u,f,e){function o(t,o){function v(n){var r=e.local Storage,i,t,u;if(r&&r.deferLoadedItems)for(i=r.deferLoadedItems.split(","),t=0,u=i.length;t<u;t++)if(i[t]&&i[t].indexOf(n)!==-1){f.removeItem(i[t]);break}}function a(){var i=t.find ("section li time");i.each(function(){var t=new Date(n(this).attr("datetime"));t&&n(this).html(t.toLocaleString())})}function p(){c=t.find("[data-module-id]").eq(0);c.length&&(h=c. data("moduleId"),h&&(l="moduleRefreshed-"+h,i.sub(l,a)))}function y(){i.unsub(o.eventName,y);r(s).done(function(){a();p()})}var s,c,h,l;return u.signedin||(t.hasClass("of fice")?v("meOffice"):t.hasClass("onenote")&&v("meOneNote")),{setup:function(){s=t.find("[data-module-deferred-hover], [data-module-deferred]").not("[data-sso-de pendent]");s.length&&s.data("module-deferred-hover")&&s.html("<p class='meloading'><\/p>");i.sub(o.eventName,y)},teardown:function(){h&&i.un

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\7cedbf13-ebf9-416a-817e-7df06701ed63[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:	downloaded
Size (bytes):	65113
Entropy (8bit):	7.9705869459743255
Encrypted:	false
SSDEEP:	1536:+yENxRQgREqV8Cg/srYWx7HU9sAAofGyA1tqzpgOX1ZdZW9B58Lc:5CBM1/srYGEJAfsD1ZWL53
MD5:	F2627B2C529912FC3250B55DAE65F9E2
SHA1:	A8E58798AD0A90B28A78B2556DA78E00F21CBE85
SHA-256:	5989B6E705D8550B793C70607B378B17338FBA33BDB8908ABB48F922CAF120C1
SHA-512:	B34BD85215042887B5340862D2590DE96C58249AF5AB47A0231B4D5B1C6FB48A07CFC4D89080AAE713AF612E627B705D76A04133DAE7CA263B5F816DCC9CF0E
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://cvision.media.net/new/300x300/3/128/70/89/7cedbf13-ebf9-416a-817e-7df06701ed63.jpg?v=9
Preview:	......JFIF.....C.....C.....!...1.AQ."aq.2.....#B....3R...$brCDS4..%E.....?.#[u.U.+u(t.....O..o....e[9.....v..+.EW`.i bGH..`...{.6.8.?N.m.4.....V.\.!w+.....qFP.)6....~.o..u.....l9.`...:...o..q..#...~...._f.?1.w..?..0J.W.#.....8S..P...2.8.?.|.m....>..=:..Z..2.{c.}.$....s.>...{...+.o....~.p?...YA.Q..1.#.9? O~....?..?.S.....=.N3&g....;. ..D.a....9...|}...A.'.J.~....Lg.~.yEV..8.....c...,*....v..{.....H....F..{p.....H8#c.....k:.+.q.....c.uKI....'m.w..... ..m.....<{..... .....?.....}...y....._m .....#.V.grH..o.o.o.$.....=...o....BS.v.....S....c=..C.....ZG..H8.a.....RW.M#.....o.....%.E8.+...oo...n;.Q...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AAMEUCC[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:	downloaded
Size (bytes):	744
Entropy (8bit):	7.656229901379694
Encrypted:	false
SSDEEP:	12:6v/7X74api+Na/rDBxHmXcGqPU1A+w8MrXwpfBRJcdF3YfO7G9gbSoslt/PFP7M5:sEd+NaTdxGHqPYUJXwp5RGb37KC2os/i
MD5:	517323FF602732E216DE18C212FD43E4
SHA1:	F8697D4BD32D90793B57C6F0510AE8F9847B418E
SHA-256:	86426C336EE1FED57463CEAD16D924DC5143B35363C95A38595ED0344194F42B
SHA-512:	D4BBAC9AB24CD198F39DAE90108CFFCA16BD991F0B07422FF4F202AAD9310D863E966BFB21ADF4788DB9247D22F86ADF7DF4525F378E9CF3663C28923436FB 4
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAMEUCC.img?h=27&w=27&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....U....pHYs.....+.....IDATx....k.A..Sc.P....A. ..^T,E..^....A.R..d...?.. ..lAD..D/R../D....A.E.M..~g7.....y.....}3I.Y.5y.R.F%.'i.l0...d..O...]6.p...X.aU. ...V.....1..s...m}`....C...*.e.....q.!..._C.....,.....8Jy....B..... ..Wx",...N/w4N.....%5...^.l..x..e:+.*;.;...|..4..U.a.:..tQx../...(.....X.....wv}..&..s....Y..@j...Y..r.{!.7..L.0.....X..ji..|G..- .!E<..dB. ..>.Xu@.s...X.....a.j..Z...Z4FhN.`S..R..*..MuS2.P.w.U...{i.....z... .....l....z..z..1....K..:S....t.....Z..(.s...qVc..;S.v^.N=.,-g.....B.}16.U.x.GYkf..0..\....4....x.....7L.y.{"P).# .A..u....c..+(?)L..v}r.=.2;.1`....."YI...=gWf...S_..M.s...$...X.4.}2....n..>.K...z.#l..-..U.A..k..(....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AAMJPjh[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:	downloaded
Size (bytes):	2666
Entropy (8bit):	7.8178309068182905
Encrypted:	false
SSDEEP:	48:QfAuETAX+T/L4TZodR2NVEBA0qPVJAL5qhUNZBwDDu:Qf7EcukTZ/NV0A0YJAL5qhUNZBwDS
MD5:	75EB6D1BEE405463FA72DA1C31CEA046
SHA1:	DBB29FA5A5C1E313972C0B8072EDE09863C54ACE
SHA-256:	90DA10EE3D723285E6E8AB38106F9214724D6D973C1ACABBEA5451CCFE8427E9
SHA-512:	DFE095C60890491BCA1918DAAB8951095212EB9CF630DF05802C642B2321D840832FCFD23056061C429B0FDC468C93446D20ADDEED3B3947C32624CF5111A45
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAMJPjh.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f&f=jpg&x=476&y=246

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AAMJPjh[1].jpg	
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......K.d..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?..cH...@pq..*.;.')q..L.[..y....r.r.P.5E..B...X.u....BZ4.. ...HCn.9bA.....[.k}v.....4..I.z..i...V...6...y.Y.#;.P1.AR.q.$...P.{}6UH..I.. .Rj.J..U.....#.z.FX...$+..H...u...e-....J.}O...z.{.....M.N.fr.M...U..2R.W...7I..K...w......I....n....LK.....U.&.&).`..:H...=L..Iv-.t..Z!.I...E...e..43N.d..q..$e.oA...j......Dz...{......#;].9.=.[.50..5 .S...JP.#.......'...ln..Vi.&-".A.n|.RR.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AAMJU5k[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:	downloaded
Size (bytes):	2164
Entropy (8bit):	7.779027315370886
Encrypted:	false
SSDEEP:	48:QfAuETAGBLUQg1BLPTpzHG0ipH/IXAjrnRFHwMCu/:Qf7Ei00EsAnr/
MD5:	179297A78E7A39A8004C2BD86C175A1E
SHA1:	8F59B564E5723F998B3BC737C7D2600C469C9150
SHA-256:	9426225B5372A722D4CFFD1E8A3459E1A16D7EAF7F73B7B2E26A1D7D65D37217
SHA-512:	5E4B3AE54478D1FEF26498CAA46C575D58E72E7A37214C63016CFCDF9D5CD25E9BA0192B1059AA27CDC77DEDC50996BB84FB3F8B0B96FFB69DFC69734A846 DC
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAMJU5k.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f&f=jpg&x=413&y=321
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......K.d..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?.....fcI..Lj.E!..g.8....".$..\./...).L.G..+.r4P2..$b..\3.....T.r.lQ[....A...acV..0.....8;...i.8.v.e....Kg......CV/(...4..bT..f...8.......\....F. .09.Y..u..[...p~..jN...s..\|=gd.D...s.W3...Z.c.n]"..h..qF.....~.yQ.'..$W..8.G......k.2.9g..Y.5.t.....u.EW.....efE..U. .U\..e..\R....fJ..........i....4........d.......*.r..J.7:.;...6....TZ..-..6.g.....g P..Q.gR..wz...H...RF/..y.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AAMJyjX[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:	downloaded
Size (bytes):	36980
Entropy (8bit):	7.959120589962446
Encrypted:	false
SSDEEP:	768:IjvGCqTL1HB+3O7Rdt8tunCjHRE+UjsimV0n6lgQai3faNm:ITGCq9H3v88nCzRG9mOn4mNm
MD5:	D14D33ACD908CE88D82B884773E330B8
SHA1:	31717EE81C09E0D0B6D126B7F9C38AB8DAF0A247
SHA-256:	818F34F3D878B33DC4A5EB21A3D22A6B96297D8181B62ABEF546BFC3D332810C
SHA-512:	3F172108CBE10AD96F5AF50A76C335686070A34EDC86DC63BB1A55E63463D8CD101D8BBD063488AF7005FACCDE08ECC7092E4A93904F476D297BC4AD5070E3 1
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAMJyjX.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=766&y=410
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......p.n..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?.."F..a..H...@.8...).c...3.Svi1.........[.o..@w...mf.........FE.d>.3."..:....b... 3ml.p.<.l...a..VNE..".l....b.X...../.@.G0X.H.lh..j.d ...}*.I.G.X...6-/8.YH..e.0.H....5..7\|.R@.^.Ng.OW.6.,1.........;+....U.j&y.A.f....[B.........r>$.{.....N.z.WU8.\...P....m.T.rq.....={U.0..b.A.J71.M7Q....V.%.K..%.I ...e&..H..T.P.........cB... <.#..I....,.^c....f.V.........7F....ZfmX.4.s..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AAMKJNj[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:	downloaded
Size (bytes):	6760
Entropy (8bit):	7.8318645236045015
Encrypted:	false
SSDEEP:	192:QoxIQM9gbBFIybJUblQRxHy51nj7ggScfBrwfIh9PEJ:bxIFgdFI2JUbl2yDjKSB8fwg
MD5:	C0D71968C479EE935C28D5C8BA0771BA
SHA1:	41FFB62046D9593E197250C486E27607767E7776
SHA-256:	FED4F84ED64C74CB53A04AD8F7DC1A09258D43F8461E30C93FB9749B87776B36
SHA-512:	5706EA310C7CF72C53EC53FEF48BE85BB3CC8C7FFC4CA0C5E981653684CF1C3D3EF05DB90537665182F1E97D4C4045D1651A64CE18E48773026D82C8435E3B5
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AAMKJNj[1].jpg	
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAMKJNj.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..I.E.b..R...- ..1@.....(...P...P.@....S.kE.....7..pbe.X.....:..1....k..A.....SY..i.|.;.z.....}..^..p..9...z....UHrJ..d.(...1q@ ...P1h.....R.b..Qp.P.L.....].f...H:.d..:.Mu0..:..d.dX....\...dS...x..0]F.e=^>..*.b.;++.{.....=+6.....!.!...zS...q...S.\.u..+..[U.....p...X.....r...Z...b....R.b....(.qH...@.h.9.0.A@....%...-\.5}Nc_...$...#m....j&.d..4...W

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AAMKkTf[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:	downloaded
Size (bytes):	20461
Entropy (8bit):	7.957890447661892
Encrypted:	false
SSDEEP:	384:NlO3eXbCKeR34a9Kl1ZKf/zW1fb9uJq4xer7aamUpHWc707Hr:NlkeX2KeRj9K9Kifb9uVcp25Hr
MD5:	B195792EB54BF918056EEEC80FD8C312
SHA1:	F3DF77734B629B5C11F9EC6FA6185F27ABC9345B
SHA-256:	3768DE71C889214E6F2B4D4334FC2A2ACC8A86A1B46D9C5EE8554833F0E697E3
SHA-512:	C4893F1F201F5E85E9532800936B82418ED638C7D80E4B54CD40A2269BBFAD2A79D704EC4AC886180FE0B0AF99C992F4FBA99BFAAE33B693AB7102FE2B7FDD4C
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAMKkTf.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg&x=509&y=247
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...`....)..[8S.....B..-...'.U.3.E+...c8.ey'.p).W/...56-....Vv.+.3s.....f.K!.#7.cv ....6n.t.*...o^...P..YE.....s.k.1.1...+.TR..R!F*z.B....J.i.Y.$.P..\.8....il..Tr....H.6.w...S.. `.i-.[."."s\....."S.....H8....1^.,h.....^$`rj..i..F..!.+)...R%...q['s6...`...q..a.....G5Qw....W..L.E.m.,f.j.....P...0'. 5.Z'..A.....E.N..4..'...3LC...MZBe.yV5.4..R..{.[....P..:#-....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AAMKqfT[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:	downloaded
Size (bytes):	6781
Entropy (8bit):	7.849606854330859
Encrypted:	false
SSDEEP:	192:QnqQqaSCJipS+prWV30SYuUJLYGQjuWkt3wN/Z7AP9e4U:0qdCJicKI30vBtmjupFA95
MD5:	A0A2F91A40EE5BC49842D11374A8A630
SHA1:	0970B0D5D6B5F344C9861B48DE083B949DC5E18F
SHA-256:	E709F74A9F272BB9CDB201A43E50190973D48212C8213D7C2F9B78F745E90676
SHA-512:	C623E7DDC8ECBE22093B3D1B55CF122D90F1C41D71C94172131E7735AADA2340A7B1EA02ED9AC08583F6A636EB4918DD4AD495E0E92C2CA32024774E41F19C0
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAMKqfT.img?h=166&w=310&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...@.....h..... "...H....`G...^..f]..j[)"..:.s../....s.(.Q}i..(.....M=h..QF.....H....9IV..w..VBh.X.\..J.N. z._2..2R..4.E..o4\,&I.....0..-.-.(....Xf...@.a..JV...Vf-....@.4.cR..P.....F .H..i]?.(.&..&R#.&...c.....Q..y....#...R.....`.T.....9..K..w.E.s".X..CE.....T.a\.....2..."E..b..1.@....P...@....S..B.....b..S.@S$(.4..@.L..@&B...z...ut#.!R.1..ZM.va....w>.Qp....B~.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AAMKt8K[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:	downloaded
Size (bytes):	14696
Entropy (8bit):	7.915581819968147
Encrypted:	false
SSDEEP:	384:N3FVaf2mUs0w1QL4YrRNGeMYbZ/Lwkkwb4Uc:N37a+msw1QL4kGeMYbbzb4Uc
MD5:	18814F7522831FAB54C39F965018E478
SHA1:	FC880C98CFABB3B45686C19C0E79CB2D56C25963
SHA-256:	C4407D0995D4BF84C4EA4C986A1F2AE2C290406D91C9FFB1085430387894226A
SHA-512:	8A775D192F5460E1C0C3DA28AB402CC3504AFE480BC27346B48C39144C44CFDA1AC50E0FD7EAC6C645C7C777BAC444D70D77CB1847F1ED5C730178AC0C18D11

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AAMKt8K[1].jpg	
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAMKt8K.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg&x=313&y=184
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..B.STH.G..`..=.J`..z@V.....4....[...i.I....Cz..k.75.0...R0.....P.....>.*.K.L...i\,9C.....&8/....I.@+...)..O..3.B.....*.....J.M...@.....(.....P+1B.f.b.....v7g.p.k..E.....u..av.}.....x.p..?../....\....E.<.....g.....W...?..+.i.yi@.Z....]...I..+..&..S.....w.....e.y.....\yh..P...}.....~.....@...I<.....}..a...s..sS&kMw,...C..GJ.#:.w.I..:S3...(..c.|.Q.a@....Rl

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AAMjuzS[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:	downloaded
Size (bytes):	2159
Entropy (8bit):	7.731681602282935
Encrypted:	false
SSDEEP:	48:QfAuETALnY6CxhgHzdGDfhvIY0f5PudE32UNd+fplwfk:Qf7EMyrgHBG7tItxP0E3FawM
MD5:	5A1E0DAB6EA7AB9CDB45852733345397
SHA1:	715AC0D7ED3E7A7EED663B71A4D4B1C7EA52D665
SHA-256:	316C78E11CC62D16A2F2E45C551DAFDFD8F4501DC9681BC451D425D7178D1130
SHA-512:	2F465342DDE7A5A37EA1D91193E791D272489A007DFF21E77FE263CAAC5FAD78D51C7AAC625B364C8A8903659382C20CEEFC3AF5D5CFF3B828C9C348E4816A3
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAMjuzS.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....C..}...6.}{.T.....,nVI.c.'.S.<...Rn!..\.C.n./..Y.K.2..q.Vr...!....#S.....hG%..3.e.m...>T6+M90....J...T\..r...l..1..._....E.....z.k.6.Q.8.f.....1..s..\.....$...dbx..yf.L...z.T0....6M'H.$.j1@..c.(%..9".s9g..4d.$x....y...5@...w)-.(....z..O.....F....g..H.$U.....Q..F...h..+ .n.....q1...@.<.....Y.....>..y..'.z.n.AX.....@.$/".Uc .$c46.=g.0..W...M+..Yv.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\AAuTnto[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:	downloaded
Size (bytes):	777
Entropy (8bit):	7.619244521498105
Encrypted:	false
SSDEEP:	12:6v/7/+Qh6PGZxqRPb39/w9AoWC42k5a1lhpzlnlA7GgWhZHcJxD2RZyrHTsAew9:++RFzNY9ZWcz/ln2aJ/Hs0/ooXw9
MD5:	1472AF1857C95AC2B14A1FE6127AFC4E
SHA1:	D419586293B44B4824C41D48D341BD6770BAFC2C
SHA-256:	67254D5EFB62D39EF98DD00D289731DE8072ED29F47C15E9E0ED3F9CEDB14942
SHA-512:	635ED99A50C94A38F7C581616120A73A46BA88E905791C00B8D418DFE60F0EA61232D8DAAE8973D7ADA71C85D9B373C0187F4DA6E4C4E8CF70596B7720E2238
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAuTnto.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx.]S]HSa.~.s.k...Y.....VF.)EfWRQQ.h%]..e.D)..]DA.%...t...Q.....y.Vj.j.3...9.w..}.....w...<..>..8xo...2L.....Q....*.4.)../'~.....<.3.#....V....T..[M..I).V.a.....EKI-4...b... 6JY...V.t2.%....."Q....`.....`.5.o.)d.S...Q..D....M.U...J.+.1.CE.f.(.....g.....z(..H...^~.:A.....S...=B.6....w..KNGLN..^..^.o.B)..s?P....v.....q.....8.W.7S6....Da`..8.[.z1G"n.2.X.....2>..q...c.....fb...q0..{...GcW@.Hb.Ba.....w....P.....=.)...h..A..`.....j.....o...xZ.Q.4..pQ.....>.vT..H..'Du.e..~7..q.`7..QU...S.....d...+..3.....%*m\.../.....M..}y.7..?8....K.I.|;5....@...u..6<.yM.%B",.U..].+...$...%$....3...L....%.8...A9..#.0j.\lZcg...c8..d.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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:	downloaded
Size (bytes):	936
Entropy (8bit):	7.711185429072882
Encrypted:	false
SSDEEP:	24:IJJuYNKuGlZLocJZlxAgAbiuoSrZzi1g3+:IJn94F/lxAZiuoSNYgO
MD5:	19B9391F3CA20AA5671834C668105A22
SHA1:	81C2522FC7C808683191D2469426DFC06100F574
SHA-256:	3557A603145306F90828FF3EA70902A1822E8B117F4BDF39933A2A413A79399F
SHA-512:	0E4BA430498B10CE0622FF745A4AE352FDA75E44C50C7D5EBBC270E68D56D8750CE89435AE3819ACA7C2DD709264E71CE7415B7EBAB24704B83380A5B99C66C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\BB10MkbM[1].png	
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB10MkbM.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG........IHDR................a....pHYs..........+.....ZIDATx.m._hSW....?....E...U.Z.M..a.1.}P..6+.....l......LDA......u.a.U..P..&k..Iz...&....R_.q.=p8....~.'...5..}......_.I$FS.\.c][4#... ......+...U@fZz.Y.......\|.7....r.x..S.?.ws....B9.P.-Yt*..N.}.'V......G...5....uc....XV.=.{..ai.pw.v)...(.9.z\\|.3:Q..,qr.es...ZTp..Mt.iB.2.{w.C*WB..F...b../.H..\..*.).0l.R......c........@S5.? 3...q..:..8.?....p.=6`..T...5.nn........]..b.j.,..pf.....8...".M..?.@K...L.='.1.O.2Kb.p..(..\.D.......n..._.....0............w^bR....v\..)..l..f..l..M.m.6t.7....U.Y3?.h=..!.<.._........pL..V"[....... {[P....e07...Wc....IH.T@...*..A@.......;....>Gt&...}...o...KP...7W1.sm~...&.......00.....>/....l.#.t......2.....L_Owu.*.A)...-.w.*.1/+.)....XR.A#;..X...p..3!...H.....f.ok;..\|x..1.R.\W.H\...<.. <&.M!mk:\|....%.<..,.%.g..g..G@z^Q..I...T.D^..G.&v6$.J.2J....~..Y\kX.j.......c.&.>.3..........ek..+..~B.\......IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\BB15AQNm[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:	downloaded
Size (bytes):	29565
Entropy (8bit):	7.9235998300887145
Encrypted:	false
SSDEEP:	384:I1cMsjB7+C2bbAEB2SUZRT+kXoMRRJhp5xvHapIzf7m41tgaYi9PIVKnHNVMP2Nm:IHsjkC2YEB2SUPTT48FPHTgf3VKn2Uc
MD5:	6B79D1438D8EFAF3B8DE6163107CEC71
SHA1:	E54E651A8A0FDAFCAD60B137D806D8CEC2F769C0
SHA-256:	2F00C9B0C23EE995091A90ACC7A8FA3AA773612A464F558D78664636C8B7B8D8
SHA-512:	745B822F9E21DB98B909F3AE762C439C376A35AD5C08655861B05539ACD5C47BCDCF24FAB2FB5A56712BC3BEDE6493FD5152E92D065AC5E9ECCE2DF93C4B7 B7
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB15AQNm.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=868&y=379
Preview:	......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......p.n..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?....(...4.m.!....4..i..4..l.C..u .pi....dRe#J..\..t..bC3.)..l.".W.#..&.....-&2.".&.(l..y...r...cE.7..h(#......t..E.....H.^b..../...5 ..r..4&R.>F.. ~..$..R.....1..WDV.L..j.^q..!...T.+..x.$.+._..<{Tc4!.^\$q.ZR`q...Y........A.Ld...(HM.....Z#2b.u40 ...J.F.j.*...Fy.."h..g.&...+H..$2...A....N.c.L...^..c...<Qa..[.. -..v.....-....xg.K.e+..'5[.... !@.ZM.b."....<.........~....(..".~

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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:	downloaded
Size (bytes):	1088
Entropy (8bit):	7.81915680849984
Encrypted:	false
SSDEEP:	24:FCGPRm4XxHvhNBb6W3bc763IU6+peaq90IUkiRPfoc:/pXBvkW3bc7k1FqWIUkSfB
MD5:	24F1589A12D948B741C2E5A0C4F19C2A
SHA1:	DC9BB00C5D063F25216CDABB77F5F01EA9F88325
SHA-256:	619910A3140A45391D7D3CB50EC4B48F0B0C8A76DC029576127648C4BD4B128C
SHA-512:	5D7A17B05E1FD1BC02823EC2719D30BC27A9FA03BCFFE30F3419990E440845842F18797C9071C037417776641AB2CDB86F1F6CD790D70481B3F863451D3249EE
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cEP3G.img?h=27&w=27&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG........IHDR................U....pHYs..........+......IDATx...]..U.....d..6YwW(.UV\.v.>.>..`.K}X).i..Tj...C..RD. ..AEXP.............]).vQ../$.%.l2.....dH&.YiOr93.....~..u.S...5........J. &..;.JN..z....2..;q.4..I .....c!....2;*J........l(......?.m+......V...g3.0.............C..GB.$..M.....jl.M..~6?.........../a%...;....E.by.J..1.$...".&.DX..W..jh.....=...aK...[.#....].. ....:Q....X.........uk.6 .0...e7..RZ..@@H..k........#......[..C.-.AbC.fK.(a.<.^p.j`...._>{<....`.........%.L...q.G...).2oc{....vQ...N5..%m-ky19..F.S....&..../..F......y.(.8.1..>?Zr......Q.`.e.\|0.&m.E....=[aN..r.+... .2B/f8.v..n...N..=........i.^....s&..Hr.z.....M......:........EF.....0.. .N.x...........N.pO.#2...df=...Fa..B#2yU....O.;.g....b.}ct.&.7x*..t.Y..yg....]..){.,.v.F.e.ZF.z..Ur+..^..].#.]....~..}..{g.W0? ....&....6n....p\.=.]..X...F.]...\s5OK.3Wb.#.M/fT...:^.M}...:t.......!..g......0t.h..8..4cB....px.............1.!...}=...Qb$W.*..."............V....!.y......<H

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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:	downloaded
Size (bytes):	368
Entropy (8bit):	6.811857078347448
Encrypted:	false
SSDEEP:	6:6v/lhPahm7HmoUvP34NS7QRdujbt1S+bQkW1oFjTZLKrdmhtIargWoaf90736wDm:6v/7xkHA2QRdsbt1pBcrshtvgWoaO7qZ
MD5:	C144BE9E6D1FA9A7DB6BD090D23F3453
SHA1:	203335FA5AD5E9D98771E6EA448E02EE5C0D91F3
SHA-256:	FAC240D4CA688818C08A72C363168DC9B73CFED7B8858172F7AD994450A8D459
SHA-512:	67B572743A917A651BD05D2C9DCEC20712FD9E802EC6C1A3D8E61385EB2FEBB1F19248F16E906AF0B62111B16C0EA05769AEA1C44D81A02427C1150CB035EA 8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\BB6Ma4a[1].png	
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB6Ma4a.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....''IDATx.cy. ..?...|.UA....GX...43.!:.o(f..Oa`..C...+Z0.y.....~..0...>.....(....X3H.....Y....zQ4.s0....R.u.*t..|....)....(.$.`..a...d.qd.....3.. .W_...}.*...;.....4.....>....N....)d.....p.4.....`i.k@QE....j....B....X.7....|..0.....pu?.1B,...J..P.....`F.>R..2.l.(..3J#.L4...9[...N....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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:	downloaded
Size (bytes):	489
Entropy (8bit):	7.208309014650151
Encrypted:	false
SSDEEP:	12:6v/7wmcW0JYErMXrLYTh/BBoqavcAccySLY:jmx0aaM7LYtTpaWcy4Y
MD5:	C090E4C7C513884E6B10030FCE2F2B37
SHA1:	2BE9AD7D8CE94A585F0EA58DBC0B0A9A9933E854
SHA-256:	C18187F3EF7089F6EA948C35797228FC4DFD3F90DBD2E78E531C6D2A92740471
SHA-512:	DA9A5F97B70845AECD6BA20F87DA7FC2D6947AC9E2CFBA299B402459CE5ED8A1AA918A140B11879038961A3FA6B986736813CD1707D05B4A1BB9C195F52005E
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBRUB0d.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx.c.....B.^.V..0..2..D0...3.J.1|\w....].L.....Km...M...|gx^<.....7.5.....k.1(n.f.v...}.....3.1|.w.....%@gr2..Y.....0...?Q.Q\ ....m.....W./..(.q....D5 ..,.e.Y..?.aj..(.p.+...;u.....A..n.FFF0...;.wLRQ.D1...?...w .....p5..a.n.. .....=c.4Vg.q..\!..&...._.....a...>....?/.....IP..y....c...v.:..T_.69q..k..Y.x...jA...@1../.wm...&.....&..}.x..~.0.....j.....Bb.._.\.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\BBUZVvV[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:	downloaded
Size (bytes):	415
Entropy (8bit):	7.093730449593416
Encrypted:	false
SSDEEP:	12:6v/7C7Stjm5n9HPBQrd/9a5cFWziVYbALUO1:BAm59irna55uYMb1
MD5:	16B34C1836A5FC244145527EC79361D4
SHA1:	18CB908457B380545D89D8A4D3F91CDABF3ADC78
SHA-256:	DB797DF4F1E320C21BD6019E89E6CCC5569C5CED57E1D3BDD736F3B4A9371BC0
SHA-512:	3FFFFB5F6876B8C246F2728A3AEA8EDF2997032F8CD9CE375497D8063939F810BB819E4CDC56B1ECA5E8A70B27E7355C2A9B7F23BDF8919307F01536008D4D7
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBUZVvV.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....QIDATx.cy.(.....B.^.V.....6..OD9... .b..1.o.c.y....v.+..sK..>N.....W.... .....aL....Z..<I.`..ek.~.<.W.....`..O..~C. .....%. .3..1..~....h(...[...}...u.J.....&=..?.....aa.....r...;..4q..3....[.....q...];.^^se`...K..6..UK...X..)..k;...X.U..2....0.....f.t.....p.....[]..n;H...P ..va....'..N.....!.....).&O...Fqo.%.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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:	downloaded
Size (bytes):	316
Entropy (8bit):	6.917866057386609
Encrypted:	false
SSDEEP:	6:6v/lhPahmxj1eqc1Q1rHZI8lsCkp3yBPn3OhM8TD+8lzjpxVYSmO23KuZDp:6v/7j1Q1Q1ZI8lsfp36+hBTD+8pjpxy/
MD5:	636BACD8AA35BA805314755511D4CE04
SHA1:	9BB424A02481910CE3EE30ABDA54304D90D51CA9
SHA-256:	157ED39615FC4B4BDB7E0D2CC541B3E0813A9C539D6615DB97420105AA6658E3
SHA-512:	7E5F09D34EFBFCB331EE1ED201E2DB4E1B00FD11FC43BCB987107C08FA016FD7944341A994AA6918A650CEAFE13644F827C46E403F1F5D83B6820755BF1A4C13
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBVuddh.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx....P..?E....U..E..|.....|...M.XD.`4YD...{.\6....s..0.;....?..&.../. .....$.\|Y....UU)gj...]..;x..(.''..$l.(.\.E.....4....y.....c...m.m.P...Fc...e.0.TUE....V.5..8..4..i.8.}.C0M.Y..w^G..t.e.l..0.h.6.|.Q...Q..i~.|...._...'..Q..."".....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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:	downloaded
Size (bytes):	879
Entropy (8bit):	7.684764008510229
Encrypted:	false
SSDEEP:	24:nbwTOG/D9S9kmVgvOc0WL9P9juX7wlA3lrvfFRNa:bwTOk5S96vBB1jGwO3lzfxa
MD5:	4AAAEC9CA6F651BE6C54B005E92EA928
SHA1:	7296EC91AC01A8C127CD5B032A26BBC0B64E1451
SHA-256:	90396DF05C94DD44E772B064FF77BC1E27B5025AB9C21CE748A717380D4620DD
SHA-512:	09E0DE84657F2E520645C6BE20452C1779F6B492F67F88ABC7AB062D563C060AE51FC1E99579184C274AC3805214B6061AEC1730F72A6445AEBDB7E9F255755F
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBX2afX.img?h=27&w=27&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....U....pHYs.....+.....!IDATx...K.Q..wfv.u.....*.,I"...)...z.....>.OVObQ.....d?|.....F.Ql$....qf.s.....">y`.....{~.6.Z.`.D[&.cV`..-8i...J.S.N..xf.6@.v.(E..S.....&...T...?.X)${.....s.l."V..r...PJ*!..p.4b}.=2...[.....:.....LW3...A.eB.;...2...~...s_z.x|..o....+..x....KW.G2..9.....<.\....gv...n..1..0...1}....Ht_A.x...D..5.H.....W..$_\G.e;./.1R+v....j.6v.....z.k.....&..(....,F.u8^..v...d-.j?.w..;..O.<9$..A..f.k.Kq9..N..p.rP2K.0.).X.4..Uh[..8..h....O..V.%.f.....G..U.m.6$.....X...../.=....f:.....\|c(,.....l.\..<./..6...!...z(.....# "S..f .Q.N=.0VQ._..\|....>@....P.7T.$./)s....Wy..8..xV.....D....8r."b@....:.E.E....._(....4w....Ir..e-5..zjg...e?./...|X..."!..'*/.....OI..J"I.MP....#...G.Vc..E..m.....wS.&.K<...K*q..\...A..$.K .....,...[..D...8.?..)..3....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
Reputation:	unknown
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
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: #000000;.. 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\0W10PBUV\NewErrorPageTemplate[2]	
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
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
Reputation:	unknown
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: #000000;.. 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\0W10PBUV\adb3478e-c94c-4cdb-9882-fa384ccec861[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\adb3478e-c94c-4cdb-9882-fa384ccec861[1].jpg	
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 300x300, frames 3
Category:	downloaded
Size (bytes):	86424
Entropy (8bit):	7.979519378625907
Encrypted:	false
SSDEEP:	1536:oXVk5kODvwkyh626qFydrCrE8rxd5mvXlz3QqlAXoX+wkrRsZtAVl:oXVk5hYkyhtzFy3O5WlrDlAw+FEAVl
MD5:	D3CFBC30017E38E6EEEBADEDFD8A3503
SHA1:	A9E354219DB237A4C0632B203C2260DDB977F5F1
SHA-256:	2F3719AD8F485C5B7244E36693E03A942EA6AAC5B0F17E88718881C3F480D64A
SHA-512:	6C74FE3FF4301C78C29119FF0BCCD19893003236C1DDBA229292F181C3CD6017AD23C72FA57F56B4C6800EB0004896AA3319117426378BBD95A45955736F95D6
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://cvision.media.net/new/300x300/3/178/41/161/adb3478e-c94c-4cdb-9882-fa384ccec861.jpg?v=9
Preview:	......JFIF.....C.....C.....,,..".....B.....!."1.#A .2Q.$a3B.q.%4R....Cr....&S.....A.....!..."1.A#2Qa..q.$3BR.....C...%ESbc.....?...=..Q%..c.....%<|....1....U/.._.....#...|.....s....T0..J....D... ...D@.....%H...s a.].?0q0233<...G..q...w."......a....<{..NBEl.9d....f.Fc....?....7EWRj.b..u.O.....=..|wq=..??....}.r.\..[PO..... .'.....f.k.f....3.e.8.....&9..._.._m.....K.|.....i.K..b.J|.)..c .....b#.....|..?.._3?l.....<X..v8.aL6.].....8....._p!K...q1 P>NFf#.....~....x..r4.....xbNNV...{.O.{.....8....li.l.....DfR.T2yi.|}.....33..}G..u.>.'.ri[hT..G.kX..\@..wp-..8. .....J.....r.%.1>.....c..Y.Y.....<.._.....|k...E.A'.m.k_.....j.8[..E.....!.g...~>~fb}-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493 AC6D
Malicious:	false
Reputation:	unknown
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(); initMo reInfo('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\0W10PBUV\dnserror[2]	
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:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493 AC6D
Malicious:	false
Reputation:	unknown
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(); initMo reInfo('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\0W10PBUV\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\down[1]	
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	unknown
Preview:	.PNG.....IHDR.....ex....PLTE....W..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\0W10PBUV\down[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	unknown
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..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\0W10PBUV\errorPageStrings[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):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	unknown
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";....//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[2]	
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):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[2]	
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	unknown
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\httpErrorPagesScripts[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):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Reputation:	unknown
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.su bstring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var pound Index = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\httpErrorPagesScripts[2]	
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):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Reputation:	unknown
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.su bstring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var pound Index = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\http___cdn.taboola.com_libtrc_static_thumbnails_26b7c43e8735f7408c60e41fb7e91ecd[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:	downloaded
Size (bytes):	15272
Entropy (8bit):	7.746669724171038
Encrypted:	false
SSDEEP:	384:+hq4/wYNg7d8qq/uRzBpSPnDyOfia52jvHa:EoYyp8qvGaaE7a
MD5:	3D15488C4E13B562DF2958C9C5DFBC8A
SHA1:	6EB1FFA4BFC5AC5D1EF77333787957DC73879D16
SHA-256:	92C55F09D5705690AA849771A368CB4F1B0EAB9ACCFFA8E62FD9A1C28168EB97

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\http___cdn.taboola.com_libtrc_static_thumbnails_26b7c43e8735f7408c60e41fb7e91ecd[1].jpg

SHA-512:	A48C0A9CBA3BB5A1A10991D8C446794BA4F5D87FDB628D3DEAADCAE52191616C782B09C10144CCA47EAE70CF78CD0B2C5A5C4A74376080A666E3155648F880AB
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F26b7c43e8735f7408c60e41fb7e91ecd.jpg
Preview:	......JFIF.....@ICC_PROFILE.....0appl....mntrRGB XYZ .....acspAPPL....APPL.....-appl.....desc...P...bdscm.....cprt.. .....#wtpt.....rXYZ.....gXYZ.....bXYZ...,...rTRC...@....aarg...L... vcgt...l...0ndin.....>chad.....,mmod.....(bTRC...@....gTRC...@....aabg...L... aagg...L... desc.....Display.....mluc....."....hrHR.....koKR.....nbNO.....id.....huHU.....csCZ.....daDK.....ukUA.....2ar.....NitIT.....broRO.....vnlNL.....heIL.....esES.....vfiFI.....zhTW.....viVN.....skSK.....zhCN.....ruRU...$....frFR.....ms.....caES.....@thTH.....XesXL.....vdeDE..... .denUS.....tptBR.....plPL.....elGR..."....svSE.....trTR.....jaJP.....ptPT.....L.C.D. .u. .b.o.j.i.... .L.C.D.F.a.r.g.e.-.L.C.D.L.C.D. .W.a.r.n.a.S.z...n.e.s. .L.C.D.B.a.r.e.v.n..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\http___cdn.taboola.com_libtrc_static_thumbnails_99e5c79b1689b75f0f0c1e3d399c6deb[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:	downloaded
Size (bytes):	18641
Entropy (8bit):	7.973309194563705
Encrypted:	false
SSDEEP:	384:/dpCkcmAmt2BoMRCQUwN0HLCqWnzJkshCb1gjpLPX08Go+PKeMyQQXoRrFr:/zcmXt26shNiLwzW/KA8vzHNJr
MD5:	E19ACE737EDDA4FBA47C2516C9F5760C
SHA1:	4C11DD22EE4E97FDBFC99D7A5C0724A2D9089554
SHA-256:	5084468B1251ECAA06AF81B773A1F2906B0ECEE33AA6236E549927D76106E6CE
SHA-512:	8D19E584B9B756B17C5D294C986B67EA71C7E0D463CABFE92FD734363A2739B8CD8C8F4A2743B9EE2E3AD9CDD1AFB571E971FA9EB48E0FBE91F56CDBC9F67CF2
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F99e5c79b1689b75f0f0c1e3d399c6deb.jpg
Preview:	......JFIF....."......".$...$.6*&&*6>424>LDDL_Z_||.....-" " -D*2**2*D<I;7;I<lUKKUl}ici}.....7.....5.....m.... @.....6.. ..d. ..3. @..... .d6fZ..3!... @...*@..... A. .6kfl,..Y.d. @..,...W...2..7..2.3f..... . @..<...y..x=.....ih2.f...A.d..`. @..B.i..C....vD;n^Y.l..". @.....0 Y.d6..dd...:u...d2.D. ..@.....|.fCql?@...@..tqvt.W4... .&d. @. ..../BZ7..qM..D.$f.....}A..v.:i.fA..... @..Z.....%Z....n.u.EK9..*...i...2.. @.....b.~H-2j....Y.....L.\.....Q.. @...,{l.n .k!....q...$..7H..,.....$.a.h...).".9....?/t.[.D..!?...~m32....dn. A...Z....1..hw<S.'.g+S..k.....i.Dzgb.q..@..B....WKy..\.\t.6.SR[e.s.C...8.....'.....r...4....(.....J...1.toO4UOCrt[H.[.Jk!.Q.....A%s].[...Ez.....\}Pn...)h *._\.*z3..Q..kdCR..~.{..d.[..c.. @.....YDma.5..@..7X=..qY...%.q.c*G..2.bh.....jH2..d(.c.7/.:.jF6.....]...Y..o.e..1..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\http___cdn.taboola.com_libtrc_static_thumbnails_d6d46d338affb3594713ba2d27fe615e[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:	downloaded
Size (bytes):	16004
Entropy (8bit):	7.968216701887388
Encrypted:	false
SSDEEP:	384:RBQcfqwBDiwmfywWo5SyNT5jNfzEV5JGqLa:b1jpVbI5rNTXfzyRa
MD5:	EE50C2CC9CA747B74709E3CF94095E69
SHA1:	40A7BA878F3C7B69E4F5C8320E039118D4C66D9F
SHA-256:	1BF1F868CA2530B9313A80E4A7164FC2E49E7DC67B6B16883E89895F3FE0ECE6
SHA-512:	9ACE4B5B282E47B483DE7F8093E39701DC988460F01CEC14C715D3B0FAAEE28152C2E3BBF71CFE38E2DBA88E57F822327521D283D7A7F23CF96ABD6BF1FA97D
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2Fd6d46d338affb3594713ba2d27fe615e.jpg
Preview:	......JFIF.....C.....!*$..(..%2%(,-/0/.#484.7*./....C.....'..'S7/7SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS.....7..... .....Y.&RHQ..&...a.+w#..a....!O.\.X%....rY.....Fu.q2.$...J.J*B.....e,....Y.1....7re>#.Z.P.M.....`..YcU2..k,..yW.`..M...;..$K.<.K.AC. ...+`{.....U.:F2U(.W....].M...5.6...O .x%.....M"..A.hm..s.B.4..Y.ez.....$6@....r..Z...t. .k]9s^.w(..%...q.u....t._.I...)W.N1...\..L.t....}>dl0FVu.{M.(..IX.....:j!.>.).D...y.."......F.& ..7.Y..1.).@.. ...:,...rK.....ma....z|..\Z.L.....L.A....6.,.Y.^..urb.).V...=-7..n.9.....Y.1. lMd..6)g.....,Sm.;+.....,.r..\xgo3x.tR.|u...cDgcZdC*.=VS;[.#.f....g.3.lwQ...y|...6..b.V..n} H...b0=..uG...\.V..d"..im...'...o.....t".|...%..Y.....u.....6..+...+.....{Z.x...vW..._.3.D.vodbn>.....Z..W..J.n..c.m.5.....n{.._..D.....:...4/R..C..h.....-bt.....t...}..}...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\https___console.brax-cdn.com_creatives_b9476698-227d-4478-b354-042472d9181c_59b51455-21ce-4d46-9f4f-9f6d1b718da4_756c7118509673334289d5dc86f79662[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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\https___console.brax-cdn.com_creatives_b9476698-227d-4478-b354-042472d9181c_59b51455-21ce-4d46-9f4f-9f6d1b718da4_756c7118509673334289d5dc86f79662[1].jpg	
Category:	downloaded
Size (bytes):	19143
Entropy (8bit):	7.974573739863761
Encrypted:	false
SSDEEP:	384:/8hYDnYqwprDwCk3iZIF6eCSVv3zqFVmJ1yQYhCO5N2wH5TWx87pu89Z:/8hYDYpJkOIFsSSVmJ1yQYYOJBWiuw
MD5:	E00963528631CCE455BA56BE6D206D17
SHA1:	11FD9E9F35E138C2495F30FAFE8562ADD4DF6D87
SHA-256:	6DA5863218E298BB3A3883E57C1399EDC5DB0B879630F1A3B9094C26B121680B
SHA-512:	6820C089E2648DBB8355FF1DD83E613D7D6476FE1A32DC93FD850B40AAFEB7903C66AC610304F12AEBE6EC8E98F007454777FA5C3DDE1F3A5FA737E5E76682C
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fconsole.brax-cdn.com%2Fcreatives%2Fb9476698-227d-4478-b354-042472d9181c%2F59b51455-21ce-4d46-9f4f-9f6d1b718da4_756c7118509673334289d5dc86f79662.jpeg
Preview:	......JFIF.....".....".$...$.6*&&*6>424>LDDL_Z_||.....".....".$...$.6*&&*6>424>LDDL_Z_||.....7....".....5.....N.u..E.n.z..x.....ud..R..F.....r...v..i.M`...M.....UhsO.w`.X....+.....&."B....Pn.....2.r[....H.$....N...5a.\....t+.D...r.t.....d..8....<.-\|.U..d..)..P.>Ro)+I.....mg....T.G.B..aM..,.t.h_..(..".sj..<R.r.o.z....M.7.Q.....z...8...kD..z.e._.....?k.3D.Y.z.n..;.V.Aj.@,Ad:..hK4-+)w.[N.)g....:... ...S.fUD..$.....T...CH...@.....lk.....(n.WF..H.1..k9..X.!..T{.l.{....bb...B.C.....7.G..ty..Y.i.>K.S..1.>.nS|..x....F.H..(.u.....rP.3.<^.P).....'...N9...'.....X..o.....$.....>`.g.h..%.=S..n.....a/.8.....k...t.,....U..$.....c.6...%.....m..s.l]..V-wc.6.X...IP...uC..)y]..-.9...MG.*<.....:..bX%~0%.%r.....w.D.v.~.n+.E.:.^=...j..*:|.)v;=.H..h.9.nI..un..wpfZ.zY.....j.a...$...h..V..&.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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:	downloaded
Size (bytes):	84249
Entropy (8bit):	5.369991369254365
Encrypted:	false
SSDEEP:	1536:DPEkjP+iADIOr/NEe876nmBu3HvF38NdTuJO1z6/A4TqAub0R4ULvguEhjzXpa9r:oNM2Jiz6oAFKP5a98HrY
MD5:	9A094379D98C6458D480AD5A51C4AA27
SHA1:	3FE9D8ACAAEC99FC8A3F0E90ED66D5057DA2DE4E
SHA-256:	B2CE8462D173FC92B60F98701F45443710E423AF1B11525A762008FF2C1A0204
SHA-512:	4BBB1CCB1C9712ACE14220D79A16CAD01B56A4175A0DD837A90CA4D6EC262EBF0FC20E6FA1E19DB593F3D593DDD90CFDFFE492EF17A356A1756F27F90376B50
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/_h/975a7d20/webcore/externalscripts/jquery/jquery-2.1.1.min.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\0W10PBUV\log[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	35
Entropy (8bit):	3.081640248790488
Encrypted:	false
SSDEEP:	3:CUnl/RCXknEn:/wknEn
MD5:	349909CE1E0BC971D452284590236B09
SHA1:	ADFC01F8A9DE68B9B27E6F98A68737C162167066
SHA-256:	796C46EC10BC9105545F6F90D51593921B69956BD9087EB72BEE83F40AD86F90
SHA-512:	18115C1109E5F6B67954A5FF697E33C57F749EF877D51AA01A669A218B73B479CFE4A4942E65E3A9C3E28AE6D8A467D07D137D47ECE072881001CA5F5736B9C0
Malicious:	false
Reputation:	unknown
Preview:	GIF89a.....,.....@..L..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\4996b9[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 45633, version 1.0
Category:	downloaded
Size (bytes):	45633
Entropy (8bit):	6.523183274214988

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\4996b9[1].woff	
Encrypted:	false
SSDEEP:	768:GiE2wcDeO5t68PKACfgVEwZfaDDxLQ0+nSEClr1X/7BXq/SH0Cl7dA7Q/B0WkAfO:82/DeO5M8PKASCZSvxQ0+TCPXtUSHF7c
MD5:	A92232F513DC07C229DDFA3DE4979FBA
SHA1:	EB6E465AE947709D5215269076F99766B53AE3D1
SHA-256:	F477B53BF5E6E10FA78C41DEAF32FA4D78A657D7B2EFE85B35C06886C7191BB9
SHA-512:	32A33CC9D6F2F1C962174F6CC636053A4BFA29A287AF72B2E2825D8FA6336850C902AB3F4C07FB4BF0158353EBBD36C0D367A5E358D9840D70B90B93DB2AE32
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/sc/ea/4996b9.woff
Preview:	wOFF.......A..........................,....OS/2...p...`...`B.Y.cmap............G.glyf.......,..,0..Hhead.......6...6....hhea...,...$...$....hmtx............($LKloca...`...f...f....maxp...P... ... .name... ....IU..post....... ... .*...........I.A_.<........... ....d.*......................^...q.d.Z..3.......3.....f.............................HL .@...U...f...................... ....\.d.\.d...d.e.d.Z.d.b.d.4.d.=.d.Y.d.c.d.].d.b.d.I.d.b.d.f.d._.d.^.d.(.d.b.d.^.d.b.d.b.d...d...d._.d._.d...d...d.P.d.0.d.b.d.b.d.P.d.u.d.c.d.^.d._.d.q.d._.d.d.d.b.d._.d._.d. b.d.a.d.b.d.a.d.b.d...d...d.^.d.^.d.`.d.[.d...d...d.$.d.p.d...d...d.^.d._.d.T.d...d.b.d.b.d.b.d.i.d.d.d...d...d...d.7.d.^.d.X.d.].d.).d.l.d.l.d.b.d.b.d.,.d.,.d.b.d.b.d...d...d...d.7.d.b.d.1. d.b.d.b.d...d...d...d...d.A.d...d...d.(.d.`.d...d...d.^.d.r.d.f.d.,.d.b.d...d.b.d._.d.q.d...d...d.b.d.b.d.b.d.b.d...d.r.d.I.d._.d.b.d.b.d.b.d.V.d.Z.d.b.d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAM8s6t[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:	downloaded
Size (bytes):	17348
Entropy (8bit):	7.3852538663577825
Encrypted:	false
SSDEEP:	192:QnCDfFwHDY5+op7iHZKvnKkin38985WVCsSKPe3My5SqA1jorfHMyrzMY5rwjc:ICDUD+p6ZuKkin38yWV9G3P5Z6jG5Mjc
MD5:	F86A6CF788645E7C03386AF6BC9EAC35
SHA1:	FC7BD8C2A221FED1C76398A15AD2D9F7C77E8EA3
SHA-256:	8C215E0E924C361D4D2D4DCD1363400C9C94276A637D5060B3F684C86D6D451F
SHA-512:	8218A47A6A41193BD251C20A41EF5B9A7658B73F35BB2871395C3DCC53A1D97287030476F630158496EC7AAA223374A0B5F5D0F44ED24B5B6FCCA638DC6FF91
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAM8s6t.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......p.n..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?.....(......(......(......(......(......(......(......(......(......(..........._.8k|lJ. .....(......(......(......(......(......(......(......(....'.....(......(......(......(......(. .....(......(......(......(......(..........._.8k|lJ. .....(......(......(......(......(......(......(......(....'.....(......(......(......(......(......(......(......(......(..........._.8k|lJ. .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAMGG6z[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:	downloaded
Size (bytes):	30693
Entropy (8bit):	7.867652895389005
Encrypted:	false
SSDEEP:	768:I57Ht9VPkODNPW9cvFVC+X0EgAL7JrxandGxEl/:I5r9kODpqOFPkEgEaYxEl
MD5:	2AF3E84059004E3FE4F813C043C7C111
SHA1:	85F1EE72B669836CE39BB77AFF4C0EBBCE23740A
SHA-256:	681128D080043007E34287A659B3921CD7FFDBAB8E83672C498BEF7E48CA44A5
SHA-512:	793B1EB1D289B5E008ECE278E5B45CD60269132DF7ACAE0D77F37F98023DDD3F145E91AC3CC48345F8BE7B8F6D3BAB491D1B0A5D00BF55860A700C2751F8A2 2
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAMGG6z.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......p.n..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?...>x(.....@..%1.@....(.....L........(..A@..-.%.-.%0....(......Z.J.Z.(..A@../z..@..8.$.z.O.-...-N...}.\W....F..ZrR../..u..pC".>...k... /....8..0.@.@.@........P.@......P.@....(............(......Z.J.Z.J.Z..Rj-.........).P.@....P.. .....(............).P.@....P.@..-...(.P ....G..{..5.J..z.B...Bk..@.#.8..d.W.Q.......nno....r..8>..... gM.5H.....\B.HL.pc.x....X.$.b....;N}Z...3F.#

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAMJ7BJ[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:	downloaded
Size (bytes):	33263
Entropy (8bit):	7.9292542201372065
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAMJ7BJ[1].jpg	
SSDEEP:	768:lasQo/DOZtV+GkP7umcHbeXY+K7dsYlBSJNUrFo7d6Ux1IFHVoix:II0TGkP7l0iXOZlYDUZo5dx1ILjx
MD5:	FB307F4B3A3F13087FBFE3AEAD8B96B7
SHA1:	82BEEF47833F0F3684152C00726525CE26E28B34
SHA-256:	9B35EDAA3CC1E682D74E794E8C794889D979CD05B4C1C6C6B6A235077C200D41
SHA-512:	E5BE508457D910697A0C8BD2C3809D091265E62B6B336FFAA79F0F6717045913D471046F178673DE767BB2792CEDACE10406FFF8DC7C66DEB7900074031D74BE
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAMJ7BJ.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..0.J.).g.Z.&m..^Z.1..]0.c.....Q2..H.UV..Q....k.....P .a@....P.@....)...).P.....!f..@.GS@.....B.@....P.@..%.....P.@.... P.@.....P.P.@.....).0..... .{.9Q.zxJWf.f=..]].|....j.5..c8..nn...}.....w)..qO..+..I.O...hHhQ..H.q.W..o....?.....x.Z.3.(.....P.@....P.@.....P.@..%4..).V...'...!i...J...P.@....P.@..-.....!.r...c..(.E...P.@.....P.@....P.@..-...P.@..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAMKD6i[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:	downloaded
Size (bytes):	37168
Entropy (8bit):	7.95166259437806
Encrypted:	false
SSDEEP:	768:Iz1RM0GwMQMPN63Qt7ANGFME2fvmQMg0BWi07s2gPeL2I800Tn7zuUJjwAe2yksy:IAd+cFME2fxV52ISnXuOMAepG4sRl
MD5:	D29898D73E388AF82E0DEE95E8578B31
SHA1:	60E5C86B247750A6802F6E042D6E0D8B24159AEB
SHA-256:	F7030121A90FA901333568B206AB999FA0BBB6A59C5F56C0928F6BBA28A97699
SHA-512:	912C038272369A3D9FB66E076DC7E6344FA76036F00672C55DEFFFEB3F158B5BA14993980FCF10F748E762E3B3B54F0688BD155A52C9DF8708C2534C3529ABB9
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAMKD6i.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..J..=.T...E.#jb.h!.n.....#5h.f..Fl..)..1..@<P...@.@.....R.....`..P..!h.....(.(...CLG'....jl.._....Y.t..(.us..B.#.)...Hd.....M.....Z..S .....J.Z.(.....(.....(.....[.C.f.....Z..h....[....8.>..9..d....g.[l<p.Y.?..`....P.cS.V.n[.....k_&..BO.q.....4.+.\.f.9.fc%.....Z#.F..VZ/..9}[_..r..\'.Y!..=.w=.._:..s ..zQc.Q.]l.a.U.k Q`q$..K..AE.u...Q82x.V...&...L%..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAMKDQv[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:	downloaded
Size (bytes):	16562
Entropy (8bit):	7.917168148567248
Encrypted:	false
SSDEEP:	384:NzDWOsdVhKAh2IMY+nNzxaiwzN58R9I6FxgqUrUbK+Y:NzvG7j2tHNsLNalFxgFrUw
MD5:	DAC8473687C2AF74FE2A10D1254F5059
SHA1:	BD3854B36BF1CEFE292FBC81D26D0ED9C270DBCF
SHA-256:	2FB8463D2271C6282964D438048442268A022CD116B674029322FBE6B5B409E2
SHA-512:	74944FA13035689FECC68F8C904DFC40DB802E9668D83F7F90352621A4879FCE14FCBDCC002C5AE9FB59061472BA98D418E8E1E472C4A3833B9814E70F5A2461
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAMKDQv.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..sH.s.....sH..f~..S.O...j.A.L..772....u.. ...5...4$..x..:]D.4.86E;.m %Jh.L.E0.8...s@...!s@..S....h.s@..@.h....&Fh..?..O.i.....O..9.. ....tv....H.....kJ.....v..2X..1.>...88.B..@.>.....H.h.....P..}i..9.[.\.S.....u.. ....5.../.@I...u=X...D...T.....2d|...&x..2P&!...h..Qp.W.....sE.CE.vh..4...@7<..n?.....r..=..PQ.]..... ..J@fx..CZ_..!3....Jd..'.`&y.#c.@...P ..@.....4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAMKEJB[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:	downloaded
Size (bytes):	9249
Entropy (8bit):	7.706507609385151
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAMKEJB[1].jpg	
SSDEEP:	192:Q2VQvYOfAT2vDz2NgfUj39OwvaduFpqgmg4Wk4//F31Y0yR4+hKb6V:NVgA4qDdvaC0gF4WJ1DO5A6V
MD5:	236D0B266FD4CB68BEBB70FCCF86376E
SHA1:	D16B4F54D923E58C7CA95C9CEFA0CE20CA80DC07
SHA-256:	FAE0FAC985750C4B14DA8E2B2018A4605B92DE3373FC64F8E2809FCA44E72201
SHA-512:	89D2B765DE2650127FF0FDE984C51195428B820929F362DE5743574841B84C32A10EFEF6F71D1913B31AC7A39751FC5D5397C8FD79F5601AFD6B967997D4B97F
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAMKEJB.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....``.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...{..4.1.*X...)."&....K..{V2.4Q/Cm.XJf.%...+.".!p..ey&...Y%.....$z...6kD.l`Bj.!..=.6.&Koj.".XK_j. H....-.be...M.bA.^.1F.+..".,FE. ,.....@..#...-. .H.3Z.P.|.....Q.....P..n(...`g..*50"q...j.a.Rr.(.sY....#.e*.....a*..%....r4H.HZ..5.. +.7.....DW"w..Hl...D...=.l.1.g.f.;.c...r*.....$.(.l`p)\.3P.....ni.b6...j...@.@.1..{Q` ..{R.....@...`.(...T...P....:...2l3@.\.4..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAMKJAA[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:	downloaded
Size (bytes):	16207
Entropy (8bit):	7.9264750058573314
Encrypted:	false
SSDEEP:	384:NU/3oJg4sjiW/MqKBFymgaFatbPN3vo6ILhRigGMA/Zf3SV:NUwJ8MqKny0FQ/jILXiglAxSV
MD5:	5B3C30F3C8ED6CBC9AF9BE422412DD0B
SHA1:	2DD6004CFC6D78D7D6916987BE4A1A10E67CEB44
SHA-256:	1DAFF15F1E0F6171A20EB38F5FFAFBF702B7E66C6BF8456CF8DE783404736C06
SHA-512:	A8129C56813A9A22F8033CDF21D264AA239CEBAD1103C3B8002E6B128944C072FD52CB475C8695AA5005242DEBE8ECCDE70E66DE1CEE3D83FBF87B6CCC9C9 37
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAMKJAA.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....``.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..K).kd`.N9...0....)x.t.f.....3F....f...I6.A..9;.N..FV(Nv.@..S.....9e\|e...[..k..\.;.n..N).K.gQ.x....,.....g..r#...(T..9..R...E,...7/.*.2/...B.\|. ....Vn...<.H..T.....*.F..".$..M..w..43w:]..".."s.).-.;..t. `.9..=..\...^.H...I..R..dvB.]..t.....n...;.....]<V.....B.m...e.A...G.Ue8.....S.....4....`.oz..Y..d(.GL..R...y.....s.Z.j.[2.....Y...8.....v .Y.;.*V..n.*..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAMKLyZ[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:	downloaded
Size (bytes):	14685
Entropy (8bit):	7.8803215392654815
Encrypted:	false
SSDEEP:	384:NRhz62w9Lj20zIbFJj9ZqX0EcfBwt0KUEjd6RFjH:NX62k2qoVE0EcJ0eKUZ
MD5:	4C0F3D2F3AD6994421D136587D9A4935
SHA1:	1246E2E129D2C0866E133F1426590210B2914C43
SHA-256:	8CED1C5A09845F5B03C8F19DD11DEDC00BA854595AD0BD8E29C06E7A43731A09
SHA-512:	177C2CF0D16354A1792B4004E23A69D6A0812E5FAA0D685EAF6C4069857F30B5A1F575A5F4C01C55AC68586F360AFB6251A28AB086D070EED6D74DC4FAC066D
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAMKLyZ.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....``.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...Mu...k#.8.j\.J,..D...Z.(.....Z.(.....Qp.P...(.....S.....@....b...J.....J2.....*..iK{..rL..$...>...j}..V....n@.:.U..S-$.....Z.N..@....P.@... .1.....e..LX...k;.r.....Z.;....".@.@..-.....Z.(...%...P.@..... ....P.P.....3....Yp....uq..B.....O.f.MY2.wh.K..O.c|.....T.b...*.+.....wFSVc....Z.(.P...)."...".#...3I.._4.8.h.\..5D.1@. .....Z.(...P...@.....P.@.(.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAMKgYD[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:	downloaded
Size (bytes):	9002
Entropy (8bit):	7.927579036767863
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAMKgYD[1].jpg	
SSDEEP:	96:QfQEfMwhQRsNPxxSt8oUCGcCS/4TwKNkUldpWbNeQjrip1jHvMFvHELvTFq1QKVW:QoJRA/StTGSWn8rinHvfrc1T1bVZi9
MD5:	1301F922F52A8F440559AF03FFED9F9E
SHA1:	9222AD39C2524A0D6F1DF9EF26A98B54DFF77531
SHA-256:	A30EA467B0887B9BFD29DE5789096CAF01D046463EF09B1C22E3734F293F5499
SHA-512:	7F024DED550D452DAA2B103EE6A5FE398B8430966C7E29B43DE80BC0B492F9115098892E38850BDCBF5B678EF3912F03E676C6328B7D895ED1254A820BF19FC
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAMKgYD.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=640&y=340
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..`A@.(.i.P0....@.....(..@.....-.-.-!.a@.@...4P .....P.S.q@.q@.....z...r.>c.d.;..t..Q..;.I.....UH..GJ..A@.....P.....@.....6..(.h.R.....h.h.Q...Z.....q..W<..;..EA.....q...$R.~{.....X.3:p.x..|.@..n...z..c+;.h....}k.b..r.b.e\....WT*Fj.>.A@.@.@.@.4..@....P!...Z.u....@.....Z..o.+.ry.J..v)!..3..j..&..h.m.o.&.x.....;H.]0f....0...K.....R.f{...\zd...-.....oz.#R.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAMKjKP[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:	downloaded
Size (bytes):	8279
Entropy (8bit):	7.906897836836859
Encrypted:	false
SSDEEP:	192:Qo8ShY8L9SVcdRSA2qIpxc2SppTKy9qU5K+/v5azDuqFoJn:bNLLwVvAuplSppTKo35KesXCx
MD5:	C0AB584D9CB4DA4CE2FEA2244B9FC064
SHA1:	5CE3EEC824A486E7FB1F4869CED8517176C67123
SHA-256:	9A76F19E6BB4A8E170520B1B3BD6957939CE0035105AFCAD30A5456E9DE9BB32
SHA-512:	F82CF43484C4FEBDF235C7200B8A256D90A1AFB7804EF263B26CC197F90A54AC2803772677CB90452A7901C0B5836DC76EF9868C7CC7CEB31E80A29FD0D627E
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAMKjKP.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=550&y=392
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...B.5-..#...e].a...$..|g.._B$.(.....,...x..b/=)....?..H...]q.H.....W..}h.X.....?..;..o....;.....c.OjW..Mn...G.....0.^N:.q.a.U.OZ.bc.#.....(....L.....2q.d.....0=O..#....1B.V.\.....'.... ..U.y>.\,.M+....qX.5.._. ..Z..D6....J.m.....Kv.....u"..!p7g.H..a.9...RZE.)..q..;ua.P..;....Ooj..0.c.....%...E.aR....;.XF.@ -.b%.....b....?w4....9..W...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAMqFmF[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	553
Entropy (8bit):	7.46876473352088
Encrypted:	false
SSDEEP:	12:6v/7kFXASpDCVwSb5I63cth5gCsKXLS39hWf98i67JK:PFXkV3lBKbSt8MVK
MD5:	DE563FA7F44557BF8AC02F9768813940
SHA1:	FE7DE6F67BFE9AA29185576095B9153346559B43
SHA-256:	B9465D67666C6BAB5261BB57AE4FC52ED6C88E52D923210372A9692A928BDDE2
SHA-512:	B74308C36987A45BC96E80E7C68AB935A3CC51CD3C9B4D0A8A784342B268715A937445DEB3AEF4CA5723FBC215B1CAD4E7BC7294EECEC04A2F1786EDE73E1A7
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAMqFmF.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx....RQ.....%AD.Vn$R...]n\.....Z..f.....\.A.~.f \H2(2.J.uT.i.u.....0P..s..}.....P.....l...*..P.....~...tb...f,.K.;.X.V...^..x<.b...lr8...bt.]..<.h.d2I.T2...sz...@.p8.x<..pH...g:...DX.Vt:.....eR..$...E.d2I..d..b.R.0...]. .j...v..A....j.....H...=....@.'Z^....E|>..tZv".^...#l.[yk(.B<j..#.H..dp.\..m....."#...b.l6.7.-.Q...l6.<.#.H.....|.....>/^.....eL.....9.z.....lwy....*.g..h?...<...zG...c\d.....q.3o9.Y.3.|..Jg...%.t.?>....+..6.0.m.....X.q.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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:	downloaded
Size (bytes):	322
Entropy (8bit):	6.966129933463651
Encrypted:	false
SSDEEP:	6:6v/lhPahmKxf8jCAw4DGQJe1kvnxIekdOgcKOtQExGTFDDv4bp:6v/7lxkjyzQEyaI1QmGTlW
MD5:	89E1141C659F2127DD80809F71326697

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\AAzb5EX[1].png	
SHA1:	3262110C91000071FDBB0D33893EC1EC8026ADEC
SHA-256:	98763AAD3E2B7507E7729711ACD2DACCBD56164FE6DDB10410047B212275C279
SHA-512:	1D32DF0DB191F0A3FA152BC47F5F463234224F215A283A26E4EBAF95095A0977ABF5B9D9804FA4DDB276CA8DAE2865789802BB8A18B02B232A9DBB22D5F19E49
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAzb5EX.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx..=..@..C.....K..`-(.`...vb.....vV...`g.!D.....!.....7..../Qg.Z...Y.....c....t.....c..).....)@.:.....8..t1{P_\.1..3Ao.....A].....5G_.....\5..x5R....'...VS.....|.`...~.....+....H^..1E^...0.,')....qJ8!..D.!O}.i1..E(....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\BB1dCSOZ[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:	downloaded
Size (bytes):	432
Entropy (8bit):	7.252548911424453
Encrypted:	false
SSDEEP:	6:6v/lhPahm7saDdLbPvjAEQhnZxqQ7FULH4hYHgjtoYFWYooCUQVHyXRTTrYm/RTy:6v/79Zb8FZxqQJ4Yhro0Lsm96d
MD5:	7ED73D785784B44CF3BD897AB475E5CF
SHA1:	47A753F5550D727F2FB5535AD77F5042E5F6D954
SHA-256:	EEEA2FBC7695452F186059EC6668A2C8AE469975EBBAF5140B8AC40F642AC466
SHA-512:	FAF9E3AF38796B906F198712772ACBF361820367BDC550076D6D89C2F474082CC79725EC81CECF661FA9EFF3316EE10853C75594D5022319EAE9D078802D9C77
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dCSOZ.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....bIDATx..?..a..?.3.w`.x.&..d..Q.L..LJ^.o...,....DR,.$.O.....r.ws..<.<.|..|..x..?....^..j..r...F..v<.....t.d2.^...x<b6....\.WT...L".`.8.R.....m.N'..`0H.T..vc...@.H$..+..~..j....N.....~.O.Z%..+..T*.r...#.....F2..X,.Z.h4..R)z..6.s:...l2...l....N>...dB6.%..i...)....q...^..n.K&..^..X,>'..dT)..v:.0D.Q.y>.#.u:.,...Z..r..../h..u....#'.v ....._&^....~..ol.#....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\BB1ftEY0[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	497
Entropy (8bit):	7.316910976448212
Encrypted:	false
SSDEEP:	12:6v/7YEtTvpTjO7q/cW7Xt3T4kL+JxK0ew3Jw61:rEtTRTj/XtjNSJMkJw61
MD5:	7FBE5C45678D25895F86E36149E83534
SHA1:	173D85747B8724B1C78ABB8223542C2D741F77A9
SHA-256:	9E32BF7E8805F283D02E5976C2894072AC37687E3C7090552529C9F8EF4DB7C6
SHA-512:	E9DE94C6F18C3E013AB0FF1D3FF318F4111BAF2F4B6645F1E90E5433689B9AE522AE3A899975EAA0AECA14A7D042F6DF1A265BA8BC4B7F73847B585E3C12C262
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1ftEY0.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx....N.A..=.....bC...RR..`'.....v.{:.^..... ."1.2....P..p.....nA.....o.....1...N4.9.>..8....g.,...|."...nL.#..vQ.....C.D8.D.0*.DR).... kl..|.....m...T..=.tz...E..y..... ..S.i>O.x.l4p~w.....{...U..S....w<.;.A3...R*..F..S1..j..%...1.|.3.mG..... f+.,x....5.e..]lz..*.).1W..Y(..L`.J...xx.y{.*.\. ...L..D..\N.....g..W...}w:.....@].j ._$.LB.U..w'..S.....R...:^..[\.^@....j...t...?..<.....M..r..h....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\BBPfCZL[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 50 x 50
Category:	downloaded
Size (bytes):	2313
Entropy (8bit):	7.594679301225926
Encrypted:	false
SSDEEP:	48:5Zvh21Zt5SkY33fS+PuSsgSrrVi7X3ZgMjkCqBn9VKg3dPnRd:vkrrS333q+PagKk7X3ZgaI9kMpRd
MD5:	59DAB7927838DE6A39856EED1495701B
SHA1:	A80734C857BFF8FF159C1879A041C6EA2329A1FA
SHA-256:	544BA9B5585B12B62B01C095633EFC953A7732A29CB1E941FDE5AD62AD462D57
SHA-512:	7D3FB1A5CC782E3C5047A6C5F14BF26DD39B8974962550193464B84A9B83B4C42FB38B19BD0CEF8247B78E3674F0C26F499DAFCF9AF780710221259D2625DB86
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBPfCZL.img?h=27&w=27&m=6&q=60&u=t&o=t&l=f&f=png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\BBPfCZL[1].png	
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\MEEXW4H4\BBZ3zrM[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:	downloaded
Size (bytes):	763
Entropy (8bit):	7.621723844116318
Encrypted:	false
SSDEEP:	12:6v/7N5fvaQCJmEzDuMi5ld08fuKGi9o4eUTE5xDgic9NEm652PPanadeh7jteQ8c:IBihmEGMi5ltfDPu4E5iic9NEp52kl9
MD5:	CFE739AEAE33DC7C7BB02D24E081F0CE
SHA1:	CBE000F23A34635EF4518C919A234DC4A3635C1E
SHA-256:	A1F6D07C79B387A99C2550B0E24AD030964EB42ACBA18F21F2D790A05499BAF3
SHA-512:	E8CD4F90716E62E4A0A8B9817794F55517CA52EC75F634E55462BBFDFB288076C1992298DB5578C84EC695D3B23BE6FF1AD80EDEEBA8435AAF96B6B32C711C5 D
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBZ3zrM.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx.]SKO.Q...s;e:.}.}@.._....hb..b..kw.....M\..t.0j....|"..E.2..C...S..M...s..;.~W..<.....=>.....J.P..?.L.....Pf.eB.BU...@. ^"1(..05.]UA0....g..N.....H.K.L..P..z....;N..O.pi<...{oVpc*.[..D...@6.a,2....<..sq.h.h~.s.*..I.@L.....h8.....)$.4.B.*.....3...m.&..H.....1...8.7...0...u..k.)d..\.;@...:m..*.Tc.....$.v..a..v.x.(; {..G...+...QY..L.N....;E.....T..>@r(.;"d...0...../.nT.01...P!...5...P.....`...b.Q....k6.*..I....R.....P.Pw.t;..T.R...6[...\.l.7'Gpq$...[.Z.%....jb..`e..T.X...C.Y#.W..\.....B.B..mR...p.0.?.J..[. ....K...Sl....."B.b.A...@.-..w.`E*.-.w..@<(,Ki.^O...zY^.. 7..4E.oyN..e..'.j.4...4ST .?.D.G....(...C..<.....8E...<?......../..X^c..j....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
Reputation:	unknown
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\MEEXW4H4\NewErrorPageTemplate[2]	
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
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\NewErrorPageTemplate[2]	
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: #000000;.. 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\MEEXW4H4\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:	downloaded
Size (bytes):	758
Entropy (8bit):	7.432323547387593
Encrypted:	false
SSDEEP:	12:6v/792/6TCfasyRmQ/iyzH48qyNkWCj7ev50C5qABOTo+CGB++yg43qX4b9uTmMI:F/6easyD/iCHLSWWqyCoTTdTc+yhaX4v
MD5:	84CC977D0EB148166481B01D8418E375
SHA1:	00E2461BCD67D7BA511DB230415000AEFBD30D2D
SHA-256:	BBF8DA37D92138CC08FFEEC8E3379C334988D5AE99F4415579999BFBBB57A66C
SHA-512:	F47A507077F9173FB07EC200C2677BA5F783D645BE100F12EFE71F701A74272A98E853C4FAB63740D685853935D545730992D0004C9D2FE8E1965445CAB509C3
Malicious:	false
Reputation:	unknown
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/sc/2b/a5ea21.ico
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\MEEXW4H4\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):	21552
Entropy (8bit):	5.304993140573211
Encrypted:	false
SSDEEP:	384:gUAGcVXlblcqnzleZSweg2f5ng+7naMHF3OZOJQWwY4RXrqt:Z86qhbS2RpF3OsJQWwY4RXrqt
MD5:	8FF8B26EA37716845608082BF587A182
SHA1:	490F72551D0AA00A0933B5004AC03F0ECCEF37BA
SHA-256:	A81EE5C51FBCC5C19639A4999D0768B7DD5650C6B2DC2D741EC34C72DBAD9D2E
SHA-512:	BE67F40511D610DC6B8857FBEC47F614C7A29E9F10B809B8C59EF4C302C5C638A3C3D24D479931B1F81F641F0B93AF563CC54B22EBAB42C2A11308C146CFED F
Malicious:	false
Reputation:	unknown
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":77,"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}},"ussyncmap":[],"hasSam eSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui" ,"shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log": {"successLper":10,"failLper":10,"logUrl":{"cl":"https:\/\/hblg.media.net\/log?logid=kfk&evtid=chlog"}},"csloggerUrl":"http

Static File Info

General

File type:	MS-DOS executable, MZ for MS-DOS
Entropy (8bit):	6.4061376769323415
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% • VXD Driver (31/22) 0.00% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	YfDl.dll
File size:	258504
MD5:	499200f6a8e223c057c6e16701740721
SHA1:	ef46f9c62b94715b750173074c51100285ff6fe9

General

SHA256:	d7e64f8e65ce586ce2f0a857810b2a23f85140bf5e52e5a824f09787fb2bf45e
SHA512:	b32e3c480c7533d6fa745b3d22bf7d7bed1d0f52452b77c8232560e3d3e8979db53e0e45eb47e81757b6f20cfa01b20c55d5e63f423d89666ee74e6c9988a511
SSDEEP:	3072:SEF7LCAtgVteclWZuw72sQI6ja4IyXBiGqfWOSi7NTk+0UylJm2os4nd41RgVTo6:SEFXKVteapw7SlJ4G9dpNyjmJLsRGPhz
File Content Preview:	MZ.....!..L.!This -7Afram cannot be run in DOS mode....$.....PE..L..... .....!.....d..... .....N..... .....R.....

File Icon

Icon Hash:	9cdadaa6a6a6e400

Static PE Info

General

Entrypoint:	0x10059964
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, DLL, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x0 [Thu Jan 1 00:00:00 1970 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	d34313ce3555dec95480bcae2d5dea6b

Authenticode Signature

Signature Valid:	
Signature Issuer:	
Signature Validation Error:	
Error Number:	
Not Before, Not After	
Subject Chain	
Version:	
Thumbprint MD5:	
Thumbprint SHA-1:	
Thumbprint SHA-256:	
Serial:	

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.unsooth	0x1000	0x1be	0x200	False	0.74609375	data	5.05965650539	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.prekind	0x2000	0x5755	0x200	False	0.8359375	data	5.55991795387	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.aqueoig	0x8000	0x56bb	0x200	False	0.607421875	data	4.089974355	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.spiritr	0xe000	0x56b6	0x200	False	0.6171875	data	4.32537549194	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.nectaro	0x14000	0x5747	0x200	False	0.779296875	data	5.28600359483	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.philolo	0x1a000	0x191	0x200	False	0.6875	data	4.6969561979	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.pres	0x1b000	0x19f	0x200	False	0.703125	data	4.84520818639	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.outglad	0x1c000	0x56f5	0x200	False	0.6796875	data	4.69557672384	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.pogonir	0x22000	0xfc	0x200	False	0.484375	data	3.3261397334	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.taurico	0x23000	0x56cb	0x200	False	0.650390625	data	4.40534616445	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.untar	0x29000	0xec	0x200	False	0.435546875	data	2.96362208909	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.muskroo	0x2a000	0x5752	0x200	False	0.80859375	data	5.31594136919	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.cricoto	0x30000	0x56f1	0x200	False	0.67578125	data	4.63187162043	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.breaghe	0x36000	0x569b	0x200	False	0.576171875	data	3.95722657349	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.shunnab	0x3c000	0x1f8	0x200	False	0.83203125	data	5.3891798566	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.hemaut	0x3d000	0x190	0x200	False	0.677734375	data	4.65755245189	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.uncongr	0x3e000	0x1b3	0x200	False	0.75	data	5.10140119986	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tonner	0x3f000	0x5723	0x200	False	0.75	data	5.11518896506	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.jink	0x45000	0x220	0x400	False	0.4326171875	data	3.53364999014	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.stirles	0x46000	0x15f	0x200	False	0.60546875	DOS executable (COM)	4.18109406994	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.imper	0x47000	0x170	0x200	False	0.634765625	data	4.46625189416	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.unsubve	0x48000	0x576f	0x400	False	0.4345703125	data	3.47992565687	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.text	0x4e000	0x1336b	0x13400	False	0.55760450487	data	6.30608125945	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x62000	0xaa	0x200	False	0.236328125	data	1.73649757383	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x63000	0x21a9b	0x1c600	False	0.605004129956	data	6.00866637611	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x85000	0x8ca5	0x8e00	False	0.217814700704	data	4.84189780533	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8e000	0x1e10	0x2000	False	0.770629882812	data	6.65709646572	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Version Infos

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/01/21-15:02:04.697710	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49764	80	192.168.2.3	195.110.59.2
08/01/21-15:02:04.697710	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49764	80	192.168.2.3	195.110.59.2
08/01/21-15:02:04.763477	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49765	80	192.168.2.3	195.110.59.2
08/01/21-15:02:04.763477	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49765	80	192.168.2.3	195.110.59.2
08/01/21-15:02:04.861031	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49766	80	192.168.2.3	195.110.59.2

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/01/21-15:02:04.861031	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49766	80	192.168.2.3	195.110.59.2
08/01/21-15:02:04.913743	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49767	80	192.168.2.3	195.110.59.2
08/01/21-15:02:04.913743	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49767	80	192.168.2.3	195.110.59.2
08/01/21-15:02:05.009811	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49768	80	192.168.2.3	195.110.59.2
08/01/21-15:02:05.009811	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49768	80	192.168.2.3	195.110.59.2
08/01/21-15:02:05.061274	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49769	80	192.168.2.3	195.110.59.2
08/01/21-15:02:05.061274	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49769	80	192.168.2.3	195.110.59.2
08/01/21-15:02:05.149843	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49770	80	192.168.2.3	195.110.59.2
08/01/21-15:02:05.149843	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49770	80	192.168.2.3	195.110.59.2
08/01/21-15:02:14.062530	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49773	80	192.168.2.3	195.110.59.2
08/01/21-15:02:14.062530	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49773	80	192.168.2.3	195.110.59.2
08/01/21-15:02:21.440293	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49775	80	192.168.2.3	195.110.59.2
08/01/21-15:02:27.100181	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49777	80	192.168.2.3	195.110.59.2
08/01/21-15:02:27.100181	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49777	80	192.168.2.3	195.110.59.2
08/01/21-15:02:27.103624	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49778	80	192.168.2.3	195.110.59.2
08/01/21-15:02:27.286655	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49779	80	192.168.2.3	162.255.119.73
08/01/21-15:02:27.675948	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49782	80	192.168.2.3	198.54.117.210
08/01/21-15:02:39.063524	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49793	80	192.168.2.3	195.110.59.2
08/01/21-15:02:39.063524	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49793	80	192.168.2.3	195.110.59.2
08/01/21-15:02:48.879749	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49795	80	192.168.2.3	162.255.119.73
08/01/21-15:02:48.880715	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49794	80	192.168.2.3	162.255.119.73
08/01/21-15:02:48.880715	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49794	80	192.168.2.3	162.255.119.73
08/01/21-15:02:49.272887	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49797	80	192.168.2.3	198.54.117.210
08/01/21-15:02:49.273117	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49796	80	192.168.2.3	198.54.117.210
08/01/21-15:02:49.273117	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49796	80	192.168.2.3	198.54.117.210
08/01/21-15:02:50.284062	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49798	80	192.168.2.3	162.255.119.245
08/01/21-15:02:50.691088	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49801	80	192.168.2.3	198.54.117.211
08/01/21-15:02:53.774423	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49805	80	192.168.2.3	195.110.59.2
08/01/21-15:02:54.390725	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49806	80	192.168.2.3	195.110.59.2
08/01/21-15:02:54.390725	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49806	80	192.168.2.3	195.110.59.2
08/01/21-15:02:54.431533	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49807	80	192.168.2.3	195.110.59.2
08/01/21-15:02:54.431533	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49807	80	192.168.2.3	195.110.59.2
08/01/21-15:02:54.514118	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49809	80	192.168.2.3	195.110.59.2
08/01/21-15:02:54.514118	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49809	80	192.168.2.3	195.110.59.2
08/01/21-15:02:55.125911	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49810	80	192.168.2.3	162.255.119.73
08/01/21-15:02:55.125911	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49810	80	192.168.2.3	162.255.119.73
08/01/21-15:02:55.514761	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49813	80	192.168.2.3	198.54.117.210

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/01/21-15:02:55.514761	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49813	80	192.168.2.3	198.54.117.210
08/01/21-15:02:55.691240	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49812	80	192.168.2.3	198.54.117.210
08/01/21-15:02:55.691240	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49812	80	192.168.2.3	198.54.117.210
08/01/21-15:02:56.043194	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49814	80	192.168.2.3	198.54.117.210
08/01/21-15:02:56.043194	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49814	80	192.168.2.3	198.54.117.210
08/01/21-15:02:56.213545	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49815	80	192.168.2.3	198.54.117.210
08/01/21-15:02:56.213545	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49815	80	192.168.2.3	198.54.117.210
08/01/21-15:02:56.556169	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49816	80	192.168.2.3	198.54.117.210
08/01/21-15:02:56.556169	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49816	80	192.168.2.3	198.54.117.210
08/01/21-15:02:56.729962	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49817	80	192.168.2.3	198.54.117.210
08/01/21-15:02:56.729962	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49817	80	192.168.2.3	198.54.117.210
08/01/21-15:02:57.076040	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49820	80	192.168.2.3	198.54.117.210
08/01/21-15:02:57.076040	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49820	80	192.168.2.3	198.54.117.210
08/01/21-15:03:11.298734	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49822	80	192.168.2.3	162.255.119.245
08/01/21-15:03:11.298734	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49822	80	192.168.2.3	162.255.119.245
08/01/21-15:03:11.692329	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49825	80	192.168.2.3	198.54.117.217
08/01/21-15:03:11.692329	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49825	80	192.168.2.3	198.54.117.217
08/01/21-15:03:12.994152	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49827	80	192.168.2.3	162.255.119.73
08/01/21-15:03:13.446886	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49829	80	192.168.2.3	198.54.117.217
08/01/21-15:03:22.138170	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49831	80	192.168.2.3	195.110.59.2

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 1, 2021 15:01:24.468975067 CEST	192.168.2.3	8.8.8.8	0xd22b	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:26.523000002 CEST	192.168.2.3	8.8.8.8	0x95a8	Standard query (0)	web.vortex.data.msn.com	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:26.830293894 CEST	192.168.2.3	8.8.8.8	0x2cac	Standard query (0)	geolocation.onetrust.com	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:27.013653994 CEST	192.168.2.3	8.8.8.8	0x9dfb	Standard query (0)	contextual.media.net	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:27.145615101 CEST	192.168.2.3	8.8.8.8	0x1995	Standard query (0)	btloader.com	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:27.364810944 CEST	192.168.2.3	8.8.8.8	0xcbcd	Standard query (0)	ad-delivery.net	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:27.364912033 CEST	192.168.2.3	8.8.8.8	0x65d8	Standard query (0)	ad.doubleclick.net	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:28.159879923 CEST	192.168.2.3	8.8.8.8	0xb8c2	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:28.899947882 CEST	192.168.2.3	8.8.8.8	0x67e0	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 1, 2021 15:01:29.373080015 CEST	192.168.2.3	8.8.8.8	0x4114	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:29.736171961 CEST	192.168.2.3	8.8.8.8	0x2bab	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:30.333395004 CEST	192.168.2.3	8.8.8.8	0xb47e	Standard query (0)	img.img-taboola.com	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:04.548523903 CEST	192.168.2.3	8.8.8.8	0xbda3	Standard query (0)	alliances.bar	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:13.964167118 CEST	192.168.2.3	8.8.8.8	0x5f4b	Standard query (0)	alliances.bar	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:21.341387033 CEST	192.168.2.3	8.8.8.8	0x9056	Standard query (0)	alliances.bar	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:27.025634050 CEST	192.168.2.3	8.8.8.8	0xcc35	Standard query (0)	alliances.bar	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:27.065891027 CEST	192.168.2.3	8.8.8.8	0xe1c7	Standard query (0)	allianceline.bar	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:27.465254068 CEST	192.168.2.3	8.8.8.8	0x57ab	Standard query (0)	www.allianceline.bar	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:33.030208111 CEST	192.168.2.3	8.8.8.8	0xea56	Standard query (0)	alliances.bar	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:38.989789009 CEST	192.168.2.3	8.8.8.8	0x1379	Standard query (0)	alliances.bar	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:48.665577888 CEST	192.168.2.3	8.8.8.8	0x7536	Standard query (0)	allianceline.bar	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:49.050689936 CEST	192.168.2.3	8.8.8.8	0xe4a6	Standard query (0)	alliancer.bar	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:49.064676046 CEST	192.168.2.3	8.8.8.8	0x8224	Standard query (0)	www.allianceline.bar	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:50.062547922 CEST	192.168.2.3	8.8.8.8	0xe4a6	Standard query (0)	alliancer.bar	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:50.465974092 CEST	192.168.2.3	8.8.8.8	0xc7e1	Standard query (0)	www.alliancer.bar	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:51.356640100 CEST	192.168.2.3	8.8.8.8	0x2a37	Standard query (0)	alliances.bar	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:53.698822975 CEST	192.168.2.3	8.8.8.8	0x32cc	Standard query (0)	alliances.bar	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:54.312211037 CEST	192.168.2.3	8.8.8.8	0x519d	Standard query (0)	alliances.bar	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:54.899777889 CEST	192.168.2.3	8.8.8.8	0x5fda	Standard query (0)	allianceline.bar	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:55.312726974 CEST	192.168.2.3	8.8.8.8	0x5bf1	Standard query (0)	www.allianceline.bar	A (IP address)	IN (0x0001)
Aug 1, 2021 15:03:11.082987070 CEST	192.168.2.3	8.8.8.8	0x7522	Standard query (0)	alliancer.bar	A (IP address)	IN (0x0001)
Aug 1, 2021 15:03:11.480617046 CEST	192.168.2.3	8.8.8.8	0x91f5	Standard query (0)	www.alliancer.bar	A (IP address)	IN (0x0001)
Aug 1, 2021 15:03:12.730308056 CEST	192.168.2.3	8.8.8.8	0x7456	Standard query (0)	allianceline.bar	A (IP address)	IN (0x0001)
Aug 1, 2021 15:03:13.189273119 CEST	192.168.2.3	8.8.8.8	0xa826	Standard query (0)	www.allianceline.bar	A (IP address)	IN (0x0001)
Aug 1, 2021 15:03:22.073694944 CEST	192.168.2.3	8.8.8.8	0x24e0	Standard query (0)	alliances.bar	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 1, 2021 15:01:24.498075962 CEST	8.8.8.8	192.168.2.3	0xd22b	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 1, 2021 15:01:26.566648960 CEST	8.8.8.8	192.168.2.3	0x95a8	No error (0)	web.vortex.data.msn.com	web.vortex.data.microsoft.com		CNAME (Canonical name)	IN (0x0001)
Aug 1, 2021 15:01:26.868050098 CEST	8.8.8.8	192.168.2.3	0x2cac	No error (0)	geolocation.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:26.868050098 CEST	8.8.8.8	192.168.2.3	0x2cac	No error (0)	geolocation.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:27.054532051 CEST	8.8.8.8	192.168.2.3	0x9dfb	No error (0)	contextual.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:27.179785013 CEST	8.8.8.8	192.168.2.3	0x1995	No error (0)	btloader.com		104.26.7.139	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 1, 2021 15:01:27.179785013 CEST	8.8.8.8	192.168.2.3	0x1995	No error (0)	btloader.com		172.67.70.134	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:27.179785013 CEST	8.8.8.8	192.168.2.3	0x1995	No error (0)	btloader.com		104.26.6.139	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:27.402287006 CEST	8.8.8.8	192.168.2.3	0xcbcd	No error (0)	ad-delivery.net		104.26.3.70	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:27.402287006 CEST	8.8.8.8	192.168.2.3	0xcbcd	No error (0)	ad-delivery.net		172.67.69.19	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:27.402287006 CEST	8.8.8.8	192.168.2.3	0xcbcd	No error (0)	ad-delivery.net		104.26.2.70	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:27.408845901 CEST	8.8.8.8	192.168.2.3	0x65d8	No error (0)	ad.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Aug 1, 2021 15:01:27.408845901 CEST	8.8.8.8	192.168.2.3	0x65d8	No error (0)	dart.l.doubleclick.net		216.58.215.230	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:28.195055008 CEST	8.8.8.8	192.168.2.3	0xb8c2	No error (0)	lg3.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:28.938000917 CEST	8.8.8.8	192.168.2.3	0x67e0	No error (0)	hblg.media.net		23.211.6.95	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:29.407217979 CEST	8.8.8.8	192.168.2.3	0x4114	No error (0)	cvision.media.net	cvision.media.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Aug 1, 2021 15:01:29.763366938 CEST	8.8.8.8	192.168.2.3	0x2bab	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Aug 1, 2021 15:01:29.763366938 CEST	8.8.8.8	192.168.2.3	0x2bab	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 1, 2021 15:01:30.369585037 CEST	8.8.8.8	192.168.2.3	0xb47e	No error (0)	img.img-taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Aug 1, 2021 15:01:30.369585037 CEST	8.8.8.8	192.168.2.3	0xb47e	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:30.369585037 CEST	8.8.8.8	192.168.2.3	0xb47e	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:30.369585037 CEST	8.8.8.8	192.168.2.3	0xb47e	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Aug 1, 2021 15:01:30.369585037 CEST	8.8.8.8	192.168.2.3	0xb47e	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:04.594222069 CEST	8.8.8.8	192.168.2.3	0xbda3	No error (0)	alliances.bar		195.110.59.2	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:13.996819973 CEST	8.8.8.8	192.168.2.3	0x5f4b	No error (0)	alliances.bar		195.110.59.2	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:21.374216080 CEST	8.8.8.8	192.168.2.3	0x9056	No error (0)	alliances.bar		195.110.59.2	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:27.062108994 CEST	8.8.8.8	192.168.2.3	0xcc35	No error (0)	alliances.bar		195.110.59.2	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:27.111437082 CEST	8.8.8.8	192.168.2.3	0xe1c7	No error (0)	allianceline.bar		162.255.119.73	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:27.502639055 CEST	8.8.8.8	192.168.2.3	0x57ab	No error (0)	www.allianceline.bar	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Aug 1, 2021 15:02:27.502639055 CEST	8.8.8.8	192.168.2.3	0x57ab	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:27.502639055 CEST	8.8.8.8	192.168.2.3	0x57ab	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:27.502639055 CEST	8.8.8.8	192.168.2.3	0x57ab	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 1, 2021 15:02:27.502639055 CEST	8.8.8.8	192.168.2.3	0x57ab	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:27.502639055 CEST	8.8.8.8	192.168.2.3	0x57ab	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:27.502639055 CEST	8.8.8.8	192.168.2.3	0x57ab	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:27.502639055 CEST	8.8.8.8	192.168.2.3	0x57ab	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:33.065195084 CEST	8.8.8.8	192.168.2.3	0xea56	No error (0)	alliances.bar		195.110.59.2	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:39.025733948 CEST	8.8.8.8	192.168.2.3	0x1379	No error (0)	alliances.bar		195.110.59.2	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:48.701280117 CEST	8.8.8.8	192.168.2.3	0x7536	No error (0)	allianceline.bar		162.255.119.73	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:49.099817038 CEST	8.8.8.8	192.168.2.3	0x8224	No error (0)	www.allianceline.bar	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Aug 1, 2021 15:02:49.099817038 CEST	8.8.8.8	192.168.2.3	0x8224	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:49.099817038 CEST	8.8.8.8	192.168.2.3	0x8224	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:49.099817038 CEST	8.8.8.8	192.168.2.3	0x8224	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:49.099817038 CEST	8.8.8.8	192.168.2.3	0x8224	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:49.099817038 CEST	8.8.8.8	192.168.2.3	0x8224	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:49.099817038 CEST	8.8.8.8	192.168.2.3	0x8224	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:49.099817038 CEST	8.8.8.8	192.168.2.3	0x8224	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:50.091795921 CEST	8.8.8.8	192.168.2.3	0xe4a6	No error (0)	alliancer.bar		162.255.119.245	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:50.095215082 CEST	8.8.8.8	192.168.2.3	0xe4a6	No error (0)	alliancer.bar		162.255.119.245	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:50.504231930 CEST	8.8.8.8	192.168.2.3	0xc7e1	No error (0)	www.alliancer.bar	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Aug 1, 2021 15:02:50.504231930 CEST	8.8.8.8	192.168.2.3	0xc7e1	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:50.504231930 CEST	8.8.8.8	192.168.2.3	0xc7e1	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:50.504231930 CEST	8.8.8.8	192.168.2.3	0xc7e1	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:50.504231930 CEST	8.8.8.8	192.168.2.3	0xc7e1	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:50.504231930 CEST	8.8.8.8	192.168.2.3	0xc7e1	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:50.504231930 CEST	8.8.8.8	192.168.2.3	0xc7e1	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:50.504231930 CEST	8.8.8.8	192.168.2.3	0xc7e1	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:51.389395952 CEST	8.8.8.8	192.168.2.3	0x2a37	No error (0)	alliances.bar		195.110.59.2	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 1, 2021 15:02:53.734052896 CEST	8.8.8.8	192.168.2.3	0x32cc	No error (0)	alliances.bar		195.110.59.2	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:54.346115112 CEST	8.8.8.8	192.168.2.3	0x519d	No error (0)	alliances.bar		195.110.59.2	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:54.932179928 CEST	8.8.8.8	192.168.2.3	0x5fda	No error (0)	allianceline.bar		162.255.119.73	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:55.338815928 CEST	8.8.8.8	192.168.2.3	0x5bf1	No error (0)	www.allian celine.bar	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Aug 1, 2021 15:02:55.338815928 CEST	8.8.8.8	192.168.2.3	0x5bf1	No error (0)	parkingpag e.namechea p.com		198.54.117.210	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:55.338815928 CEST	8.8.8.8	192.168.2.3	0x5bf1	No error (0)	parkingpag e.namechea p.com		198.54.117.216	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:55.338815928 CEST	8.8.8.8	192.168.2.3	0x5bf1	No error (0)	parkingpag e.namechea p.com		198.54.117.217	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:55.338815928 CEST	8.8.8.8	192.168.2.3	0x5bf1	No error (0)	parkingpag e.namechea p.com		198.54.117.212	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:55.338815928 CEST	8.8.8.8	192.168.2.3	0x5bf1	No error (0)	parkingpag e.namechea p.com		198.54.117.218	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:55.338815928 CEST	8.8.8.8	192.168.2.3	0x5bf1	No error (0)	parkingpag e.namechea p.com		198.54.117.215	A (IP address)	IN (0x0001)
Aug 1, 2021 15:02:55.338815928 CEST	8.8.8.8	192.168.2.3	0x5bf1	No error (0)	parkingpag e.namechea p.com		198.54.117.211	A (IP address)	IN (0x0001)
Aug 1, 2021 15:03:11.119657993 CEST	8.8.8.8	192.168.2.3	0x7522	No error (0)	alliancer.bar		162.255.119.245	A (IP address)	IN (0x0001)
Aug 1, 2021 15:03:11.517740965 CEST	8.8.8.8	192.168.2.3	0x91f5	No error (0)	www.allian cer.bar	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Aug 1, 2021 15:03:11.517740965 CEST	8.8.8.8	192.168.2.3	0x91f5	No error (0)	parkingpag e.namechea p.com		198.54.117.217	A (IP address)	IN (0x0001)
Aug 1, 2021 15:03:11.517740965 CEST	8.8.8.8	192.168.2.3	0x91f5	No error (0)	parkingpag e.namechea p.com		198.54.117.212	A (IP address)	IN (0x0001)
Aug 1, 2021 15:03:11.517740965 CEST	8.8.8.8	192.168.2.3	0x91f5	No error (0)	parkingpag e.namechea p.com		198.54.117.218	A (IP address)	IN (0x0001)
Aug 1, 2021 15:03:11.517740965 CEST	8.8.8.8	192.168.2.3	0x91f5	No error (0)	parkingpag e.namechea p.com		198.54.117.215	A (IP address)	IN (0x0001)
Aug 1, 2021 15:03:11.517740965 CEST	8.8.8.8	192.168.2.3	0x91f5	No error (0)	parkingpag e.namechea p.com		198.54.117.216	A (IP address)	IN (0x0001)
Aug 1, 2021 15:03:11.517740965 CEST	8.8.8.8	192.168.2.3	0x91f5	No error (0)	parkingpag e.namechea p.com		198.54.117.211	A (IP address)	IN (0x0001)
Aug 1, 2021 15:03:11.517740965 CEST	8.8.8.8	192.168.2.3	0x91f5	No error (0)	parkingpag e.namechea p.com		198.54.117.210	A (IP address)	IN (0x0001)
Aug 1, 2021 15:03:12.762952089 CEST	8.8.8.8	192.168.2.3	0x7456	No error (0)	allianceline.bar		162.255.119.73	A (IP address)	IN (0x0001)
Aug 1, 2021 15:03:13.230506897 CEST	8.8.8.8	192.168.2.3	0xa826	No error (0)	www.allian celine.bar	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Aug 1, 2021 15:03:13.230506897 CEST	8.8.8.8	192.168.2.3	0xa826	No error (0)	parkingpag e.namechea p.com		198.54.117.217	A (IP address)	IN (0x0001)
Aug 1, 2021 15:03:13.230506897 CEST	8.8.8.8	192.168.2.3	0xa826	No error (0)	parkingpag e.namechea p.com		198.54.117.216	A (IP address)	IN (0x0001)
Aug 1, 2021 15:03:13.230506897 CEST	8.8.8.8	192.168.2.3	0xa826	No error (0)	parkingpag e.namechea p.com		198.54.117.212	A (IP address)	IN (0x0001)
Aug 1, 2021 15:03:13.230506897 CEST	8.8.8.8	192.168.2.3	0xa826	No error (0)	parkingpag e.namechea p.com		198.54.117.218	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 1, 2021 15:03:13.230506897 CEST	8.8.8.8	192.168.2.3	0xa826	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Aug 1, 2021 15:03:13.230506897 CEST	8.8.8.8	192.168.2.3	0xa826	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Aug 1, 2021 15:03:13.230506897 CEST	8.8.8.8	192.168.2.3	0xa826	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Aug 1, 2021 15:03:22.098493099 CEST	8.8.8.8	192.168.2.3	0x24e0	No error (0)	alliances.bar		195.110.59.2	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- alliances.bar
- allianceline.bar
- www.alliancer.bar
- www.allianceline.bar

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49764	195.110.59.2	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:02:04.697710037 CEST	3801	OUT	GET /jdraw/eWbkeEy29Mk9inNA7c/ATuO3Prha/DtolimWlXpnk8nFP0lSw/2yNlaC5cCiMklCCNwvu/sQNUZO_2Fm1xZzA1gS_2FG/9kTrosYW0_2Fm/VKROzRO8/gAsB4lDIAfyynMPz_2BNLur/ogiNTGjuy5/h8pifSL4zzmkbAEY1/43YSZu3Y6Aaj/v_2BXUswAoj/3H8D7Kh5Eubf1gg9Yf/HP.crw 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: alliances.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49765	195.110.59.2	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:02:04.763477087 CEST	3802	OUT	GET /jdraw/eWbkeEy29Mk9inNA7c/ATuO3Prha/DtolimWlXpnk8nFP0lSw/2yNlaC5cCiMklCCNwvu/sQNUZO_2Fm1xZzA1gS_2FG/9kTrosYW0_2Fm/VKROzRO8/gAsB4lDIAfyynMPz_2BNLur/ogiNTGjuy5/h8pifSL4zzmkbAEY1/43YSZu3Y6Aaj/v_2BXUswAoj/3H8D7Kh5Eubf1gg9Yf/HP.crw 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: alliances.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49778	195.110.59.2	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:02:27.103624105 CEST	4059	OUT	GET /jdraw/KzfCuU1nYQ/2jKJWMeBiltqUkBZk/bJHRs3aRSUlv/cI63tiCHI_2/F5uaZGCIn42HAA/37yNTKIJLuVjIBN3j61BH/f_2F7jKyVaT3WSHP/Idyt_2BFxwVV7Ez/wF0a5CSrL3svyQDzt7/z5kTlRVsI/o_2BijKkihsvPwp7ObK8/nGfEqkF_2BV9O_2BYHe/y7YIFWRDvDFDsnXQU1dk4w/ugyqJTKGN21dPtrvVHSLW/X.crw 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: alliances.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49779	162.255.119.73	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:02:27.286654949 CEST	4061	OUT	GET /jdraw/eNEjgfypiWX/qzBN0pjHkXaIJy/uSQAHTqmu7LUbuntarKiK/xwqbRspQk1D8qp6M/HWl7bj_2FWhMb P8/Uujd82PrM7mxT3Qzg0/MWYHS6cay/F6rvctGR9QcGUIn_2BcA/FoEIIX9k6apV8hveoXo/zNk4xAZcRLb7MRvJX wEutR/loIAT32m6_2BY/8Nz5PjSgzU6nn7nO/fTwM.crw 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: allianceline.bar Connection: Keep-Alive
Aug 1, 2021 15:02:27.459995985 CEST	4062	IN	HTTP/1.1 302 Found Server: nginx Date: Sun, 01 Aug 2021 13:02:27 GMT Content-Type: text/html; charset=utf-8 Content-Length: 271 Connection: keep-alive Location: http://www.allianceline.bar/jdraw/eNEjgfypiWX/qzBN0pjHkXaIJy/uSQAHTqmu7LUbuntarKiK/xwqbRsp Qk1D8qp6M/HWl7bj_2FWhMbP8/Uujd82PrM7mxT3Qzg0/MWYHS6cay/F6rvctGR9QcGUIn_2BcA/FoEIIX9k6apV8h veoXo/zNk4xAZcRLb7MRvJXwEutR/loIAT32m6_2BY/8Nz5PjSgzU6nn7nO/fTwM.crw X-Served-By: Namecheap URL Forward Data Raw: 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 77 77 77 2e 61 6c 6c 69 61 6e 63 65 6c 69 6e 65 2e 62 61 72 2f 6a 64 72 61 77 2f 65 4e 45 6a 67 66 79 70 69 57 58 2f 71 7a 42 4e 30 70 6a 48 6b 58 61 49 4a 79 2f 75 53 51 41 48 54 71 6d 75 37 4c 55 62 75 6e 74 61 72 4b 69 4b 2f 78 77 71 62 52 73 70 51 6b 31 44 38 71 70 36 4d 2f 48 57 6c 37 62 6a 5f 32 46 57 68 4d 62 50 38 2f 55 75 6a 64 38 32 50 72 4d 37 6d 78 54 33 51 7a 67 30 2f 4d 57 59 48 53 36 63 61 79 2f 46 36 72 76 63 74 47 52 39 51 63 47 55 49 6e 5f 32 42 63 41 2f 46 6f 45 6c 49 58 39 6b 36 61 70 56 38 68 76 65 6f 58 6f 2f 7a 4e 6b 34 78 41 5a 63 52 4c 62 37 4d 52 76 4a 58 77 45 75 74 52 2f 6c 6f 49 41 54 33 32 6d 36 5f 32 42 59 2f 38 4e 7a 35 50 6a 53 67 7a 55 36 6e 6e 37 6e 4f 2f 66 54 77 4d 2e 63 72 77 27 3e 46 6f 75 6e 64 3c 2f 61 3e 2e 0a 0a Data Ascii: Found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49791	195.110.59.2	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:02:33.110698938 CEST	8861	OUT	GET /jdraw/PjuRunwYj4Bhvxk9T/FkaG6F1W0LAq/7ctDH_2F3Sg/7ugfKJqoxNQwsg/2ypZ1ap9U9TAmPNK3Mj4E /1tkWj6xiOwNb06Ci/nMiIDTqZjqNR3Sl/Be2FTUJy9LUIgqGDgy/uKg22hRQ4/Py3DVyO8YWF3rk9X3HQr/yNaCoW iag_2BmQ7jPMJ/8l4YPxQA8wBHHEka2W3QS6/U7.crw 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: alliances.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49793	195.110.59.2	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:02:39.063524008 CEST	8911	OUT	GET /jdraw/_2Fgi_2F0q9mbLIMOTyI/MSZHR0hHa_2BmeQiSR3/W8oggZpI5myExagD6_2BTj/ey2UGr7NbceZG/W QBy5MHE/7qXKpRH7zu077im_2F1dGJV/DbKkDe7jsz/yWoZjzp1UojMkJrXW/XsiPUNe_2BZ8/DIfEiNMAFM1/A0a2 dGlo685cVI/iUyIhZAYyWsoPEjMSHZWX/6iyEp102eL/_2F_2FrX.crw 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: alliances.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49795	162.255.119.73	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:02:48.879749060 CEST	8980	OUT	GET /jdraw/4trhqHpiyJW/gPL61gbH3V3gm2/GiN8WmuvnoRNfvQO06HHD/TolcFVz_2FK8ZYP2/IZQ72utUu8FkRq_/2F067OV_2FLlPUB9yd/i0sqdLKlL/TufDKlZhewFrgjSOjZoV/kw8l6gL0iujBb8tryKS/RGvMacSQhLHBDOTrqNLG4m/uP_2BKAulmZfa/zQq7CHkj/_2F1r9d83Jng_2Fktvq5Alz/Ls6WH3GEdzGxn/iTBX.crw 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: allianceline.bar Connection: Keep-Alive
Aug 1, 2021 15:02:49.054338932 CEST	8981	IN	HTTP/1.1 302 Found Server: nginx Date: Sun, 01 Aug 2021 13:02:48 GMT Content-Type: text/html; charset=utf-8 Content-Length: 301 Connection: keep-alive Location: http://www.allianceline.bar/jdraw/4trhqHpiyJW/gPL61gbH3V3gm2/GiN8WmuvnoRNfvQO06HHD/TolcFVz_2FK8ZYP2/IZQ72utUu8FkRq_/2F067OV_2FLlPUB9yd/i0sqdLKlL/TufDKlZhewFrgjSOjZoV/kw8l6gL0iujBb8tryKS/RGvMacSQhLHBDOTrqNLG4m/uP_2BKAulmZfa/zQq7CHkj/_2F1r9d83Jng_2Fktvq5Alz/Ls6WH3GEdzGxn/iTBX.crw X-Served-By: Namecheap URL Forward Data Raw: 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 77 77 77 2e 61 6c 6c 69 61 6e 63 65 6c 69 6e 65 2e 62 61 72 2f 6a 64 72 61 77 2f 34 74 72 68 71 48 70 69 79 4a 57 2f 67 50 4c 36 31 67 62 48 33 56 33 67 6d 32 2f 47 69 4e 38 57 6d 75 76 6e 6f 52 4e 66 76 51 4f 30 36 48 48 44 2f 54 6f 6c 63 46 56 7a 5f 32 46 4b 38 5a 59 50 32 2f 49 5a 51 37 32 75 74 55 75 38 46 6b 52 71 5f 2f 32 46 30 36 37 4f 56 5f 32 46 4c 6c 50 55 42 39 79 64 2f 69 30 73 71 64 4c 4b 6c 4c 2f 54 75 66 44 4b 6c 5a 68 65 77 46 72 67 6a 53 4f 6a 5a 6f 56 2f 6b 77 38 6c 36 67 4c 30 69 75 6a 42 62 38 74 72 79 4b 53 2f 52 47 76 4d 61 63 53 51 68 4c 48 42 44 4f 54 72 71 4e 4c 47 34 6d 2f 75 50 5f 32 42 4b 41 75 6c 6d 5a 66 61 2f 7a 51 71 37 43 48 6b 6a 2f 5f 32 46 31 72 39 64 38 33 4a 6e 67 5f 32 46 6b 74 76 71 35 41 6c 7a 2f 4c 73 36 57 48 33 47 45 64 7a 47 78 6e 2f 69 54 42 58 2e 63 72 77 27 3e 46 6f 75 6e 64 3c 2f 61 3e 2e 0a 0a Data Ascii: Found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49794	162.255.119.73	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:02:48.880714893 CEST	8980	OUT	GET /jdraw/_2FYs4QtMw9_2FVqLpLk2/u2LhzC7LFlqce_2B/EJ5CkL6CyTor06H/h9Yb_2BSjV6Rt1SZIu/4F9iSiMa_/2FMSVlcf9Qu31roXh0J1/XT62QjG3DHbjtCzAO_2/B_2BsPQzjxGsde0UbMxPHp/SJcz88c_2Fs5k/867jz4YW/Gav8pspEQfvIQYY_2FHZoiA/PuUT_2Brpo/dSi_2Fsd7qdqVkqsa/uXH9U_2BtkCW/nt_2FeA79Sp7/ATp1A.crw 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: allianceline.bar Connection: Keep-Alive
Aug 1, 2021 15:02:49.057159901 CEST	8982	IN	HTTP/1.1 302 Found Server: nginx Date: Sun, 01 Aug 2021 13:02:48 GMT Content-Type: text/html; charset=utf-8 Content-Length: 316 Connection: keep-alive Location: http://www.allianceline.bar/jdraw/_2FYs4QtMw9_2FVqLpLk2/u2LhzC7LFlqce_2B/EJ5CkL6CyTor06H/h9Yb_2BSjV6Rt1SZIu/4F9iSiMa_/2FMSVlcf9Qu31roXh0J1/XT62QjG3DHbjtCzAO_2/B_2BsPQzjxGsde0UbMxPHp/SJcz88c_2Fs5k/867jz4YW/Gav8pspEQfvIQYY_2FHZoiA/PuUT_2Brpo/dSi_2Fsd7qdqVkqsa/uXH9U_2BtkCW/nt_2FeA79Sp7/ATp1A.crw X-Served-By: Namecheap URL Forward Data Raw: 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 77 77 77 2e 61 6c 6c 69 61 6e 63 65 6c 69 6e 65 2e 62 61 72 2f 6a 64 72 61 77 2f 5f 32 46 59 73 34 51 74 4d 77 39 5f 32 46 56 71 4c 70 4c 6b 32 2f 75 32 4c 68 7a 43 37 4c 46 6c 71 63 65 5f 32 42 2f 45 4a 35 43 6b 4c 36 43 79 54 6f 72 30 36 48 2f 68 39 59 62 5f 32 42 53 6a 56 36 52 74 31 53 5a 49 75 2f 34 46 39 69 53 69 4d 61 5f 2f 32 46 4d 53 56 6c 63 66 39 51 75 33 31 72 6f 58 68 30 4a 31 2f 58 54 36 32 51 6a 47 33 44 48 62 6a 74 43 7a 41 4f 5f 32 2f 42 5f 32 42 73 50 51 7a 6a 78 47 73 64 65 30 55 62 4d 78 50 48 70 2f 53 4a 63 7a 38 38 63 5f 32 46 73 35 6b 2f 38 36 37 6a 7a 34 59 57 2f 47 61 76 38 70 73 70 45 51 66 76 49 51 59 59 5f 32 46 48 5a 6f 69 41 2f 50 75 55 54 5f 32 42 72 70 6f 2f 64 53 69 5f 32 46 73 64 37 71 64 71 56 6b 71 73 61 2f 75 58 48 39 55 5f 32 42 74 6b 43 57 2f 6e 74 5f 32 46 65 41 37 39 53 70 37 2f 41 54 70 31 41 2e 63 72 77 27 3e 46 6f 75 6e 64 3c 2f 61 3e 2e 0a 0a Data Ascii: Found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49803	195.110.59.2	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:02:51.425579071 CEST	9027	OUT	GET /jdraw/_2FrlUhAClUiRyd8MwHtotk/l15TfspZAu/z01In076RAgynlo0F/aYBbR51uD1ML/uqQjbpxmeKc/L1amjLGDxOxIiq/2XLubSbffIPK0HbrHa2Lp/bjwJ7voTFzEKCY0F/aF6dVKQS112UAXS/aj4vTb6dDSsIFCUQVZ/qIZSdMQKF/8UI5q4eMPwG_2F8fIXwq/rx107CtEv/H.crw 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: alliances.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49805	195.110.59.2	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:02:53.774422884 CEST	9029	OUT	GET /jdraw/Rb3_2FHxtxhMSM8zm/gYEt3B3r9PE_/2FfL3q236io/GFNEH8CEcSGt3Q/Xgu6vIh5KIqx2S1Mrc6dl/0kCNyz0GTV6jaECQ/HiARcYhZ2Mqz_2B/BvbQ_2BHUEEnwRiksm/RXQ1zWOs_/2FRb8_2BzO0AkhcyX4o0/Pn9DN_2FJYMQOU8vTzr/Vm4hzNy1B7dqRs9x0qSEE3/RgCr9ZktG/Z3C.crw 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: alliances.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49806	195.110.59.2	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:02:54.390724897 CEST	9031	OUT	GET /jdraw/i1UnGotMRZpYX5QI846/jmFlJI_2FNDz7pkL8TrBB5/fMotNSc0eJn6p/utqPXHuH/Wff27J_2FTjxId_2BES1z1r/M_2BkcXpyD/K_2FeY_2Bil3S_2FY/RBcu0ZtleP_2/BPxc89E_2Bx/cUqugMTx_2BnBm/1nG_2BlJjtyEolJ_2BuVW/_2BuzYeRQBwowEX3/QOcwkE8Q_2Bp3En/Z4CKv0N41kvf6/f6QDpp.crw 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: alliances.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49807	195.110.59.2	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:02:54.431533098 CEST	9031	OUT	GET /jdraw/i1UnGotMRZpYX5QI846/jmFlJI_2FNDz7pkL8TrBB5/fMotNSc0eJn6p/utqPXHuH/Wff27J_2FTjxId_2BES1z1r/M_2BkcXpyD/K_2FeY_2Bil3S_2FY/RBcu0ZtleP_2/BPxc89E_2Bx/cUqugMTx_2BnBm/1nG_2BlJjtyEolJ_2BuVW/_2BuzYeRQBwowEX3/QOcwkE8Q_2Bp3En/Z4CKv0N41kvf6/f6QDpp.crw 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: alliances.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49766	195.110.59.2	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:02:04.861031055 CEST	3803	OUT	GET /jdraw/eWbkeEy29Mk9inNA7c/ATuO3Prha/DtolimWlXpnk8nFP0lSw/2yNlaC5cCiMklCCNwvu/sQNUZO_2Fm1xZzA1gS_2FG/9kTrosYW0_2Fm/VKROzRO8/gAsB4lDIAfyynMPz_2BNLur/ogiNTGjuy5/h8pifSL4zzmkbAEY1/43YSZu3Y6Aaj/v_2BXUswAoj/3H8D7Kh5Eubf1gg9Yf/HP.crw 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: alliances.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49808	195.110.59.2	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:02:54.512732029 CEST	9032	OUT	GET /jdraw/b812tUOw/5vOcsr2Qa7HjSQYaeUGfQDe/A8EgAMSWJM/_2FFmfetjQhRMnISV/eMe6aV6DLPBS/5MYu1aKdFNE/STasrOKiCBmv9X/eiZjDwcFHXNTS7hX6rpF6/PjKZwXlQvviQeyWd/_2BR0w7G5Pjv7Hi/LDxSArAenBlCjPFdb5/ZsL4oU8fF/CiH6rXpAguptoVX1zeJh/bT.crw 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: alliances.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49809	195.110.59.2	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:02:54.514117956 CEST	9033	OUT	GET /jdraw/i1UnGotMRZpYX5Ql846/jmFlJI_2FNDz7pkL8TrBB5/fMotNSc0eJn6p/utqPXHuH/Wff27J_2FTjxId_2BES1z1r/M_2BkcXpyD/K_2FeY_2Bil3S_2FY/RBcu0ZtleP_2/BPxc89E_2Bx/cUqugMTx_2BnBm/1nG_2BlJjtyEolJ_2BuVW/_2BuzYeRQBwowEX3/QOcwkE8Q_2Bp3En/Z4CKv0N41kvf6/f6QDpp.crw 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: alliances.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49810	162.255.119.73	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:02:55.125910997 CEST	9035	OUT	GET /jdraw/dLL7q72MwgF/_2BKoRFjbhgJAS/vzNzOQYcs22fS9PZmGiqk/ImBn4ZbMkjp0c79n/fXFEqaYEWVKY_2F/_2FJyGoOXr4VTVC0eg/LUPZCf_2B/C1_2BlEDEf8ijbPT3XDP/4GbLjdNj_2Ft1xIX937/olnPKLY6LOBYxvJBmWK5iG/ofDL9uajZoReh/gnTfiCz_/2FJnM9VsOUm_2FxBFWygfHA/WN_2FWTfKr/cGyLVu_2BuD/D0vz.crw 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: allianceline.bar Connection: Keep-Alive
Aug 1, 2021 15:02:55.299283028 CEST	9036	IN	HTTP/1.1 302 Found Server: nginx Date: Sun, 01 Aug 2021 13:02:55 GMT Content-Type: text/html; charset=utf-8 Content-Length: 310 Connection: keep-alive Location: http://www.allianceline.bar/jdraw/dLL7q72MwgF/_2BKoRFjbhgJAS/vzNzOQYcs22fS9PZmGiqk/ImBn4ZbMkjp0c79n/fXFEqaYEWVKY_2F/_2FJyGoOXr4VTVC0eg/LUPZCf_2B/C1_2BlEDEf8ijbPT3XDP/4GbLjdNj_2Ft1xIX937/olnPKLY6LOBYxvJBmWK5iG/ofDL9uajZoReh/gnTfiCz_/2FJnM9VsOUm_2FxBFWygfHA/WN_2FWTfKr/cGyLVu_2BuD/D0vz.crw X-Served-By: Namecheap URL Forward Data Raw: 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 77 77 77 2e 61 6c 6c 69 61 6e 63 65 6c 69 6e 65 2e 62 61 72 2f 6a 64 72 61 77 2f 64 4c 4c 37 71 37 32 4d 77 67 46 2f 5f 32 42 4b 6f 52 46 6a 62 68 67 4a 41 53 2f 76 7a 4e 7a 4f 51 59 63 73 32 32 66 53 39 50 5a 6d 47 69 71 6b 2f 49 6d 42 6e 34 5a 62 4d 6b 6a 70 30 63 37 39 6e 2f 66 58 46 45 71 61 59 45 57 56 4b 59 5f 32 46 2f 5f 32 46 4a 79 47 6f 4f 58 72 34 56 54 56 43 30 65 67 2f 4c 55 50 5a 43 66 5f 32 42 2f 43 31 5f 32 42 6c 45 44 45 66 38 69 6a 62 50 54 33 58 44 50 2f 34 47 62 4c 6a 64 4e 6a 5f 32 46 74 31 78 49 58 39 33 37 2f 6f 6c 6e 50 4b 4c 59 36 4c 4f 42 59 78 76 4a 42 6d 57 4b 35 69 47 2f 6f 66 44 4c 39 75 61 6a 5a 6f 52 65 68 2f 67 6e 54 66 69 43 7a 5f 2f 32 46 4a 6e 4d 39 56 73 4f 55 6d 5f 32 46 78 42 46 57 79 67 66 48 41 2f 57 4e 5f 32 46 57 54 66 4b 72 2f 63 47 79 4c 56 75 5f 32 42 75 44 2f 44 30 76 7a 2e 63 72 77 27 3e 46 6f 75 6e 64 3c 2f 61 3e 2e 0a 0a Data Ascii: Found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49824	198.54.117.217	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:03:11.691767931 CEST	9170	OUT	GET /jdraw/T1Oye5dXOyO7X2/W2Jf88M5e37Kz6KOh7AdL/wY5JZWvpnXF42vVg/l7s4mKoV_2FqPNE/dhTHk84TO dHYwxXQ3F/ZDAxuudp3/D1Qs8omUsHmDB_2FVyG9/fdORbAiNcjwPXWrQQ0O/25Y_2BweBhA69miE0hz3Mk/RqfVs3 8U7EbR6/7NRpQCUV/WpJhqepI5X3UmOUCA7tjaJ_/2FPWDLDzx0/6EjYsFZMbGs/q1m.crw 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 Connection: Keep-Alive Host: www.alliancer.bar

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49825	198.54.117.217	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:03:11.692328930 CEST	9171	OUT	GET /jdraw/6t2TJPVp8r4_2Fuvh2KKhY/8YV_2B_2BRJ82/6nGE2eYA/7HHAwpkhVWuf8lW4yXxIq9d/P3s_2FZHK D/oMUCAMgfPleHjs4l4/0BIh2qxT_2F_/2BqGTGuBqqr/qMuHlfbg722ygV/LdYTIqTAwZMOjKPe_2BwH/och7PytH C76QFgMR/zdGw0_2FoGJ7HxL/0oDAmlcPbJn2gUolv1/8hw0Ffgg.crw 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 Connection: Keep-Alive Host: www.alliancer.bar

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49827	162.255.119.73	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:03:12.994152069 CEST	9172	OUT	GET /jdraw/cryAR_2BXe/tfZsZbCTIFSKEc_2F/fRFkFMDrwQ2J/nrfzPEYzAHe/Wx7an4ijbM8zE_/2FhpezUV4yO_2FfukN7U 6/uBGYkZ4E31D33UZI/2HgOfw9U8TtlGcU/RO3AW2pv4UBCdojWiG/XAiw8U4II/LFIW7fzb6NeZ11ktdY_2/BmSX_ 2BpD6QEHKNSkw3/GsrABMXgDqbSFWjB/BiqFiS.crw 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: allianceline.bar Connection: Keep-Alive
Aug 1, 2021 15:03:13.168548107 CEST	9173	IN	HTTP/1.1 302 Found Server: nginx Date: Sun, 01 Aug 2021 13:03:13 GMT Content-Type: text/html; charset=utf-8 Content-Length: 278 Connection: keep-alive Location: http://www.allianceline.bar/jdraw/cryAR_2BXe/tfZsZbCTIFSKEc_2F/fRFkFMDrwQ2J/nrfzPEYzAHe/Wx 7an4ijbM8zE_/2FhpezUV4yO_2FfukN7U6/uBGYkZ4E31D33UZI/2HgOfw9U8TtlGcU/RO3AW2pv4UBCdojWiG/XAi w8U4II/LFIW7fzb6NeZ11ktdY_2/BmSX_2BpD6QEHKNSkw3/GsrABMXgDqbSFWjB/BiqFiS.crw X-Served-By: Namecheap URL Forward Data Raw: 3c 61 20 68 72 65 66 3d 27 68 74 74 70 3a 2f 2f 77 77 77 2e 61 6c 6c 69 61 6e 63 65 6c 69 6e 65 2e 62 61 72 2f 6a 64 72 61 77 2f 63 72 79 41 52 5f 32 42 58 65 2f 74 66 5a 73 5a 62 43 54 49 46 53 4b 45 63 5f 32 46 2f 66 52 46 6b 46 4d 44 72 77 51 32 4a 2f 6e 72 66 7a 50 45 59 7a 41 48 65 2f 57 78 37 61 6e 34 69 6a 62 4d 38 7a 45 5f 2f 32 46 68 70 65 7a 55 56 34 79 4f 5f 32 46 66 75 6b 4e 37 55 36 2f 75 42 47 59 6b 5a 34 45 33 31 44 33 33 55 5a 49 2f 32 48 67 4f 66 77 39 55 38 54 74 6c 47 63 55 2f 52 4f 33 41 57 32 70 76 34 55 42 43 64 6f 6a 57 69 47 2f 58 41 69 77 38 55 34 49 49 2f 4c 46 49 57 37 66 7a 62 36 4e 65 5a 31 31 6b 74 64 59 5f 32 2f 42 6d 53 58 5f 32 42 70 44 36 51 45 48 4b 4e 53 6b 77 33 2f 47 73 72 41 42 4d 58 67 44 71 62 53 46 57 6a 42 2f 42 69 71 46 69 53 2e 63 72 77 27 3e 46 6f 75 6e 64 3c 2f 61 3e 2e 0a 0a Data Ascii: Found.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49829	198.54.117.217	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:03:13.446886063 CEST	9174	OUT	GET /jdraw/cryAR_2BXe/tfZsZbCTIFSKEc_2F/fRFkFMDrwQ2J/nrfzPEYzAHe/Wx7an4ijbM8zE_/2FhpezUV4yO_2FfukN7U 6/uBGYkZ4E31D33UZI/2HgOfw9U8TtlGcU/RO3AW2pv4UBCdojWiG/XAiw8U4II/LFIW7fzb6NeZ11ktdY_2/BmSX_ 2BpD6QEHKNSkw3/GsrABMXgDqbSFWjB/BiqFiS.crw 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 Connection: Keep-Alive Host: www.allianceline.bar

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.3	49831	195.110.59.2	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:03:22.138170004 CEST	9189	OUT	GET /jdraw/TAmAcu8EQ5dbq_2FLn/jmsAPZU0N/O3d42v1YOxC8LCsNcUdI/hBRtAVsuP0wmqk3iAnH/V7a2yIwEe WGhi2w2781UJd/XfMuL5OGMx46D/tX7UDvFf/Y_2BiaZRVpr3DW0jCRNM81D/ubtn4Y0mDo/Zf69CqE_2FlQ0hZy6/ _2B_2BpRSoEQ/klrzoZkO8B_/2BwdYmhPaHQxFS/cUtgYxD_2/F.crw 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: alliances.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49767	195.110.59.2	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:02:04.913743019 CEST	3804	OUT	GET /jdraw/eWbkeEy29Mk9inNA7c/ATuO3Prha/DtolimWlXpnk8nFP0lSw/2yNlaC5cCiMklCCNwvu/sQNUZO_2F m1xZzA1gS_2FG/9kTrosYW0_2Fm/VKROzRO8/gAsB4lDIAfyynMPz_2BNLur/ogiNTGjuy5/h8pifSL4zzmkbAEY1/ 43YSZu3Y6Aaj/v_2BXUswAoj/3H8D7Kh5Eubf1gg9Yf/HP.crw 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: alliances.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49768	195.110.59.2	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:02:05.009810925 CEST	3806	OUT	GET /jdraw/eWbkeEy29Mk9inNA7c/ATuO3Prha/DtolimWlXpnk8nFP0lSw/2yNlaC5cCiMklCCNwvu/sQNUZO_2F m1xZzA1gS_2FG/9kTrosYW0_2Fm/VKROzRO8/gAsB4lDIAfyynMPz_2BNLur/ogiNTGjuy5/h8pifSL4zzmkbAEY1/ 43YSZu3Y6Aaj/v_2BXUswAoj/3H8D7Kh5Eubf1gg9Yf/HP.crw 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: alliances.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49769	195.110.59.2	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:02:05.061274052 CEST	3807	OUT	GET /jdraw/eWbkeEy29Mk9inNA7c/ATuO3Prha/DtolimWlXpnk8nFP0lSw/2yNlaC5cCiMklCCNwvu/sQNUZO_2F m1xZzA1gS_2FG/9kTrosYW0_2Fm/VKROzRO8/gAsB4lDIAfyynMPz_2BNLur/ogiNTGjuy5/h8pifSL4zzmkbAEY1/ 43YSZu3Y6Aaj/v_2BXUswAoj/3H8D7Kh5Eubf1gg9Yf/HP.crw 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: alliances.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49770	195.110.59.2	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:02:05.149842978 CEST	3808	OUT	GET /jdraw/eWbkeEy29Mk9inNA7c/ATuO3Prha/DtolimWlXpnk8nFP0lSw/2yNlaC5cCiMklCCNwvu/sQNUZO_2Fm1xZzA1gS_2FG/9kTrosYW0_2Fm/VKROzRO8/gAsB4lDIAfyynMPz_2BNLur/ogiNTGjuy5/h8pifSL4zzmkbAEY1/43YSZu3Y6Aaj/v_2BXUswAoj/3H8D7Kh5Eubf1gg9Yf/HP.crw 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: alliances.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49773	195.110.59.2	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:02:14.062530041 CEST	3872	OUT	GET /jdraw/AZ9j6FN_2FTyei6/Zf0uCNl_2FdnsseDLQ/aAlru6mfg/_2BxJ18hXN8l3o6HRZtg/iMkRHAWOXQH7Sonii2y/ZUDDqy42horX1ipsJquAAp/PE_2BV88LYzPh/_2BwspqN/QHL0gRAjrGmh0Ze8EXmvwJx/w8RwH_2Fv_/2FEesIeaXL2YGMyBr/PGDsr7HWeSeF/e3J46D1VO9zlgcp/85Zp5.crw 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: alliances.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49775	195.110.59.2	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:02:21.440293074 CEST	4009	OUT	GET /jdraw/p8BTc7rmN9rFz/dvVilNn8/1u0hUUFj3rLKVzUph9HCH9E/7PtciZB2lc/xpKpNIjlUqwM7Qoac/vY0xEhkDTdYg/zhCk8i_2Bc_/2BlBoMsKptZ_2F/zRnhMePPGQCsqYLwQD3Ue/lgSW5rDODttJ7i78/1NWLOGS4u6LI4sn/Z_2F736jFES7IEU0n1/BASM_2F10/Djh4bcFW/rXwgDHJ.crw 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: alliances.bar Connection: Keep-Alive

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49777	195.110.59.2	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Aug 1, 2021 15:02:27.100181103 CEST	4058	OUT	GET /jdraw/exPqHXDWoHjGDSQp9Aa/A_2B2jfV7Yu2z_2F81zrpc/4Hw3JjoG2C8FN/up0W_2Bg/2cOat_2FhB8XpeJI3Q4OrPd/3mcscxr_2F/XUcES9vbQCWR_2B2J/uVjKr_2FUQUP/ppEuzTVHGdh/cpJRHYjRekTIXl/zfM7YD6vGfq08eHNZhWho/thDyCd6IXfvgcRaJ/JjtQarSthDB/50HgVr4R/Z.crw 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: alliances.bar Connection: Keep-Alive

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
Aug 1, 2021 15:01:26.919608116 CEST	104.20.184.68	443	192.168.2.3	49728	CN=onetrust.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Feb 12 01:00:00 CET 2021	Sat Feb 12 00:59:59 CET 2022	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
							Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Aug 1, 2021 15:01:26.921531916 CEST	104.20.184.68	443	192.168.2.3	49729	CN=onetrust.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Feb 12 01:00:00 CET 2021 Mon Jan 27 13:48:08 CET 2020	Sat Feb 12 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Aug 1, 2021 15:01:27.219748974 CEST	104.26.7.139	443	192.168.2.3	49733	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Oct 06 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Wed Oct 06 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Aug 1, 2021 15:01:27.219862938 CEST	104.26.7.139	443	192.168.2.3	49732	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Oct 06 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Wed Oct 06 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Aug 1, 2021 15:01:27.462733984 CEST	104.26.3.70	443	192.168.2.3	49735	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Apr 21 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Thu Apr 21 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Aug 1, 2021 15:01:27.462809086 CEST	104.26.3.70	443	192.168.2.3	49734	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Apr 21 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Thu Apr 21 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	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=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

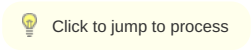
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Aug 1, 2021 15:01:27.527259111 CEST	216.58.215.230	443	192.168.2.3	49737	CN=*.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon Jul 05 03:35:32 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Sep 27 03:35:31 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	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=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Aug 1, 2021 15:01:27.528367043 CEST	216.58.215.230	443	192.168.2.3	49736	CN=*.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon Jul 05 03:35:32 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Sep 27 03:35:31 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	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=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Aug 1, 2021 15:01:30.484875917 CEST	151.101.1.44	443	192.168.2.3	49748	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		
Aug 1, 2021 15:01:30.490010023 CEST	151.101.1.44	443	192.168.2.3	49749	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
Aug 1, 2021 15:01:30.507484913 CEST	151.101.1.44	443	192.168.2.3	49750	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		
Aug 1, 2021 15:01:30.516846895 CEST	151.101.1.44	443	192.168.2.3	49751	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		
Aug 1, 2021 15:01:30.524878025 CEST	151.101.1.44	443	192.168.2.3	49752	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

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 6124 Parent PID: 5580

General

Start time:	15:01:17
Start date:	01/08/2021
Path:	C:\Windows\System32\loaddll32.exe

Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\YfDI.dll'
Imagebase:	0x220000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
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: 00000000.00000003.428802489.0000000001D88000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.428515499.0000000001D88000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.428837675.0000000001D88000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.428611848.0000000001D88000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.474906529.0000000001D88000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.428554224.0000000001D88000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.428457894.0000000001D88000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.428746719.0000000001D88000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.428583719.0000000001D88000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 3376 Parent PID: 6124

General

Start time:	15:01:17
Start date:	01/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\YfDI.dll',#1
Imagebase:	0xbd0000
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 Show Windows behavior

Analysis Process: regsvr32.exe PID: 5768 Parent PID: 6124

General

Start time:	15:01:18
Start date:	01/08/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\YfDI.dll

Imagebase:	0x1110000
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: 00000003.00000003.309722106.0000000005108000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.309589226.0000000005108000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.310021531.0000000005108000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.309505620.0000000005108000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.309660073.0000000005108000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.476957957.0000000005108000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.309399685.0000000005108000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.309887913.0000000005108000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.309772523.0000000005108000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 3440 Parent PID: 3376

General

Start time:	15:01:19
Start date:	01/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\YfDI.dll',#1
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 00000004.00000003.259140674.00000000053A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.259178122.00000000053A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.259099397.00000000053A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.259250940.00000000053A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.259222797.00000000053A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.258952943.00000000053A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000002.477641592.00000000053A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.259048645.00000000053A8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000004.00000003.259264233.00000000053A8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 5412 Parent PID: 6124

General

Start time:	15:01:22
Start date:	01/08/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Internet Explorer\iexplore.exe
Imagebase:	0x7ff7dad40000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 3292 Parent PID: 6124

General

Start time:	15:01:22
Start date:	01/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\YfDl.dll,Opisthotonos
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities Show Windows behavior

Analysis Process: iexplore.exe PID: 4464 Parent PID: 5412

General

Start time:	15:01:23
Start date:	01/08/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:17410 /prefetch:2
Imagebase:	0x7ff7488e0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6184 Parent PID: 6124

General

Start time:	15:01:26
Start date:	01/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\YfDl.dll,Hydrazo
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 6344 Parent PID: 6124

General

Start time:	15:01:29
Start date:	01/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\YfDl.dll,Overlock
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 0000000C.00000003.280402346.0000000004988000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000C.00000003.280442585.0000000004988000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000C.00000002.343816596.0000000004988000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000C.00000003.280372433.0000000004988000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000C.00000003.280191384.0000000004988000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000C.00000003.280276584.0000000004988000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000C.00000003.280138372.0000000004988000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000C.00000003.280343715.0000000004988000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000000C.00000003.280095345.0000000004988000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: rundll32.exe PID: 6440 Parent PID: 6124

General

Start time:	15:01:35
Start date:	01/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\YfDl.dll,Automobilist
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 6612 Parent PID: 6124

General

Start time:	15:01:38
Start date:	01/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\YfDl.dll,Swampland
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 0000000E.00000002.310335999.0000000005678000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: iexplore.exe PID: 6760 Parent PID: 5412

General

Start time:	15:01:40
Start date:	01/08/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:17426 /prefetch:2
Imagebase:	0x930000
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: rundll32.exe PID: 6868 Parent PID: 6124

General

Start time:	15:01:42
Start date:	01/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\YfDl.dll,Subarachnoid
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 00000012.00000003.321707074.0000000007408000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000012.00000003.321756107.0000000007408000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000012.00000003.321909022.0000000007408000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000012.00000003.321848683.0000000007408000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000012.00000003.321555066.0000000007408000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000012.00000002.446732830.0000000007408000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000012.00000003.322064190.0000000007408000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000012.00000003.322004343.0000000007408000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000012.00000003.321610655.0000000007408000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 7164 Parent PID: 6124

General

Start time:	15:01:45
Start date:	01/08/2021

Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\YfDl.dll,Bechained
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 00000016.00000003.295795718.0000000007198000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000016.00000003.295762368.0000000007198000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000016.00000003.295981429.0000000007198000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000016.00000003.295901229.0000000007198000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000016.00000002.353270821.0000000007198000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000016.00000003.295849373.0000000007198000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000016.00000003.295923025.0000000007198000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000016.00000003.295955814.0000000007198000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000016.00000003.295722944.0000000007198000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6316 Parent PID: 6124

General

Start time:	15:01:48
Start date:	01/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\YfDl.dll,Unforeseenness
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 00000017.00000003.310250645.0000000006638000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000017.00000003.310144792.0000000006638000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000017.00000002.460775914.0000000006638000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000017.00000003.310212383.0000000006638000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000017.00000003.309974225.0000000006638000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000017.00000003.309817966.0000000006638000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000017.00000003.309868338.0000000006638000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000017.00000003.309919627.0000000006638000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000017.00000003.310086165.0000000006638000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: iexplore.exe PID: 6400 Parent PID: 5412

General

Start time:	15:01:49
Start date:	01/08/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:82960 /prefetch:2
Imagebase:	0x930000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6504 Parent PID: 6124

General

Start time:	15:01:52
Start date:	01/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\YfDl.dll,Incrimination
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 6524 Parent PID: 5412

General

Start time:	15:01:52
Start date:	01/08/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:82964 /prefetch:2
Imagebase:	0x930000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6852 Parent PID: 6124

General

Start time:	15:01:55
Start date:	01/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\YfDl.dll,Oversystematic
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 7064 Parent PID: 5412

General

Start time:	15:01:57
Start date:	01/08/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:17442 /prefetch:2
Imagebase:	0x930000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6496 Parent PID: 6124

General

Start time:	15:01:59
Start date:	01/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\YfDl.dll,Shieldless
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 00000024.00000002.395162233.0000000006958000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000024.00000003.364869086.0000000006958000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000024.00000003.365062749.0000000006958000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000024.00000003.365099890.0000000006958000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000024.00000003.364977228.0000000006958000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000024.00000003.364937205.0000000006958000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000024.00000003.364804810.0000000006958000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000024.00000003.365132346.0000000006958000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000024.00000003.365018193.0000000006958000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 2596 Parent PID: 6124

General

Start time:	15:02:02
Start date:	01/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\YfDl.dll,Tsarevitch
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 00000025.00000003.336223581.0000000006E58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000025.00000003.336185061.0000000006E58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000025.00000003.336096103.0000000006E58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000025.00000003.336204746.0000000006E58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000025.00000002.408307408.0000000006E58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000025.00000003.336004164.0000000006E58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000025.00000003.336054371.0000000006E58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000025.00000003.336145332.0000000006E58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000025.00000003.335927438.0000000006E58000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: iexplore.exe PID: 2152 Parent PID: 5412

General

Start time:	15:02:03
Start date:	01/08/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:82978 /prefetch:2
Imagebase:	0x930000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 6276 Parent PID: 5412

General

Start time:	15:02:03
Start date:	01/08/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:17446 /prefetch:2
Imagebase:	0x930000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6104 Parent PID: 6124

General

Start time:	15:02:05
Start date:	01/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\YfDl.dll,Torchbearer
Imagebase:	0x7ff616cc0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 00000029.00000003.367471901.0000000006D38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000029.00000003.366983460.0000000006D38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000029.00000002.415488289.0000000006D38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000029.00000003.367322753.0000000006D38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000029.00000003.367645140.0000000006D38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000029.00000003.367145578.0000000006D38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000029.00000003.367427983.0000000006D38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000029.00000003.367564193.0000000006D38000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000029.00000003.367387100.0000000006D38000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 5200 Parent PID: 6124

General

Start time:	15:02:09
Start date:	01/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\YfDl.dll,Moler
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 5216 Parent PID: 5412

General

Start time:	15:02:09
Start date:	01/08/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:17476 /prefetch:2
Imagebase:	0x930000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 5340 Parent PID: 6124

General

Start time:	15:02:12
Start date:	01/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\YfDl.dll,Hyperpigmented
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 5348 Parent PID: 5412

General

Start time:	15:02:13
Start date:	01/08/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:17480 /prefetch:2
Imagebase:	0x930000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 1328 Parent PID: 6124

General

Start time:	15:02:16
Start date:	01/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\YfDl.dll,Adipous
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 0000002E.00000003.368506549.0000000006CE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002E.00000002.459586064.0000000006CE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002E.00000003.368421655.0000000006CE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002E.00000003.368551599.0000000006CE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002E.00000003.368346307.0000000006CE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002E.00000003.368531499.0000000006CE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002E.00000003.368451118.0000000006CE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002E.00000003.368293297.0000000006CE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002E.00000003.368387169.0000000006CE8000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: iexplore.exe PID: 6716 Parent PID: 5412

General

Start time:	15:02:16
Start date:	01/08/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:17484 /prefetch:2
Imagebase:	0x930000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 5428 Parent PID: 6124

General

Start time:	15:02:19
Start date:	01/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\YfDl.dll,Undazzled
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 1236 Parent PID: 5412

General

Start time:	15:02:20

Start date:	01/08/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5412 CREDAT:83022 /prefetch:2
Imagebase:	0x930000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6988 Parent PID: 6124

General

Start time:	15:02:22
Start date:	01/08/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\YfDl.dll,Peckishness
Imagebase:	0x8a0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 00000032.00000003.385717547.0000000006DE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000032.00000003.384858855.0000000006DE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000032.00000003.385510006.0000000006DE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000032.00000003.385353671.0000000006DE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000032.00000003.385676022.0000000006DE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000032.00000003.385602355.0000000006DE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000032.00000003.385558639.0000000006DE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000032.00000003.385639765.0000000006DE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000032.00000002.430581205.0000000006DE8000.00000004.00000040.sdmp, Author: Joe Security

Disassembly

Code Analysis