ID: 353629
Sample Name: 602b97e0b415b.png.dll
Cookbook: default.jbs
Time: 17:12:47
Date: 16/02/2021
Version: 31.0.0 Emerald

Table of Contents

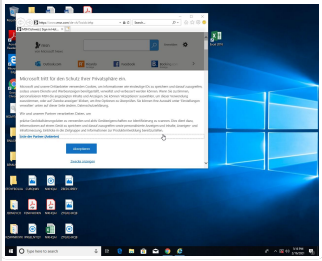
Analysis Report 602b97e0b415b.png.dll

Overview

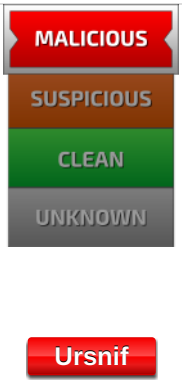
General Information

Sample Name:	602b97e0b415b.png.dll
Analysis ID:	353629
MD5:	262590037c93a5..
SHA1:	29616a643f896d6.
SHA256:	eaeb42576fb19b8.
Tags:	dll

Most interesting Screenshot:



Detection

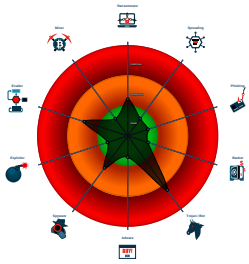


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- Abnormal high CPU Usage
- Contains functionality to call native f…
- Contains functionality to check if a d…
- Contains functionality to query CPU …
- Contains functionality to query locale…
- Contains functionality to read the PEB
- Creates a process in suspended mo…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6928 cmdline: loaddll32.exe 'C:\Users\user\Desktop\602b97e0b415b.png.dll' MD5: 8081BC925DFC69D40463079233C90FA5)
  - regsvr32.exe (PID: 6936 cmdline: regsvr32.exe /s C:\Users\user\Desktop\602b97e0b415b.png.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - cmd.exe (PID: 6944 cmdline: C:\Windows\system32\cmd.exe /c 'C:\Program Files\Internet Explorer\iexplore.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - iexplore.exe (PID: 6964 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
      - iexplore.exe (PID: 7028 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6964 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
      - iexplore.exe (PID: 5456 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6964 CREDAT:17428 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
      - iexplore.exe (PID: 1916 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6964 CREDAT:82958 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
      - iexplore.exe (PID: 3132 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6964 CREDAT:17436 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
      - iexplore.exe (PID: 5456 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6964 CREDAT:82964 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "server": "12",
  "whoami": "user@061544hh",
  "dns": "061544",
  "version": "250177",
  "uptime": "279",
  "crc": "1",
  "id": "4355",
  "user": "ef15d01308f8d2d8cdc8873a46d8f622",
  "soft": "3"
}
```


Yara Overview

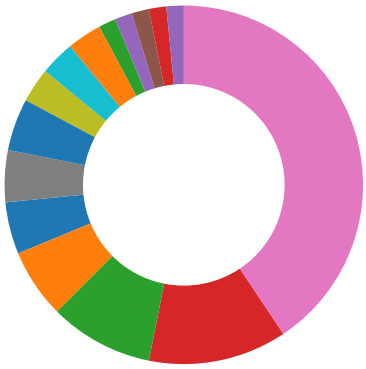
Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.504046984.0000000005048000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.503943251.0000000005048000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.504289437.0000000005048000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.504009334.0000000005048000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.656990122.0000000004D4E000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 6 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- 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

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

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

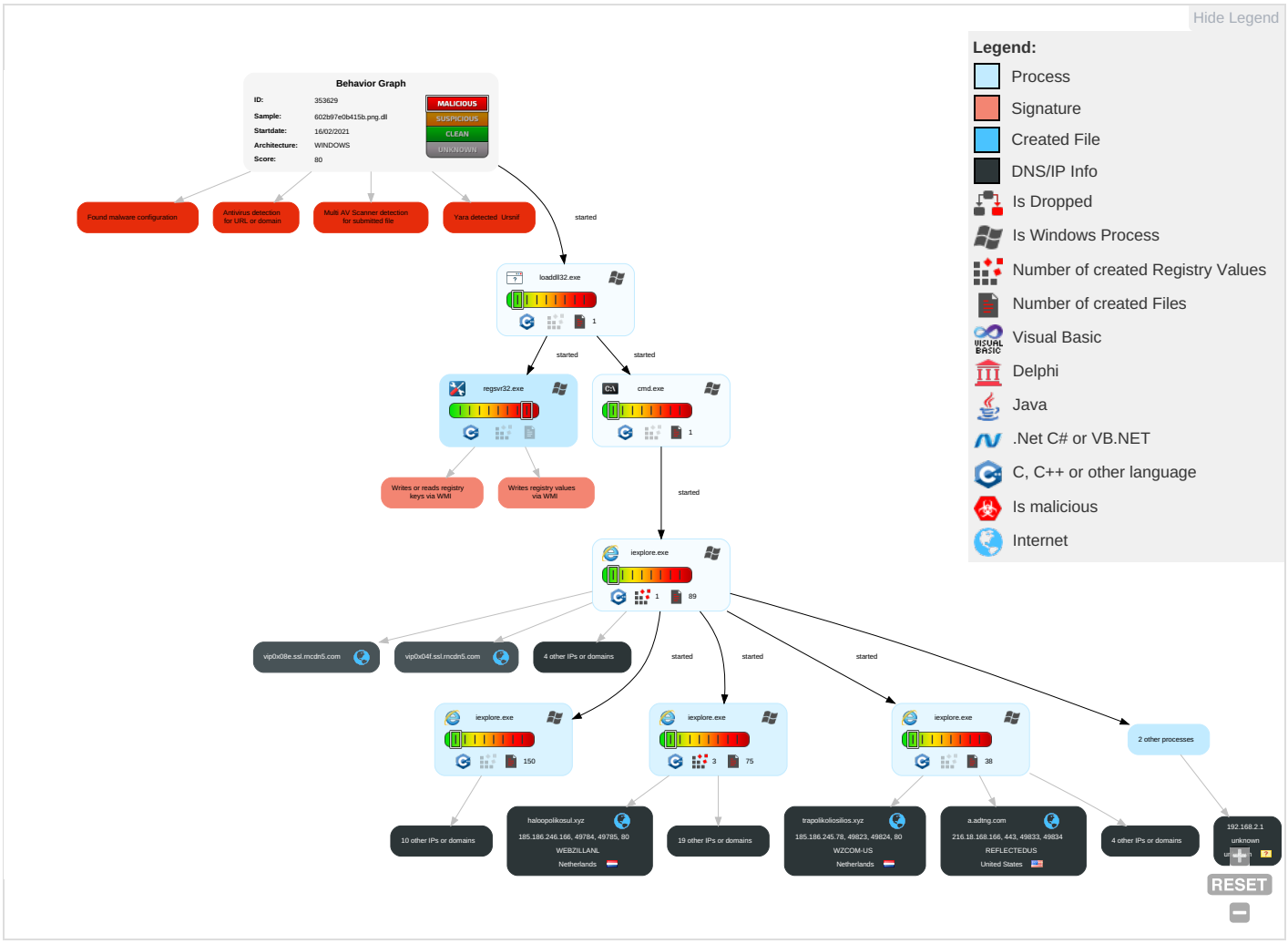
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Valid Accounts	Windows Management Instrumentation 2	DLL Side-Loading 1	Process Injection 1 2	Masquerading 1	OS Credential Dumping	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communication	
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 1 2	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location	
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Regsvr32 1	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 2	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	System Information Discovery 2 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	

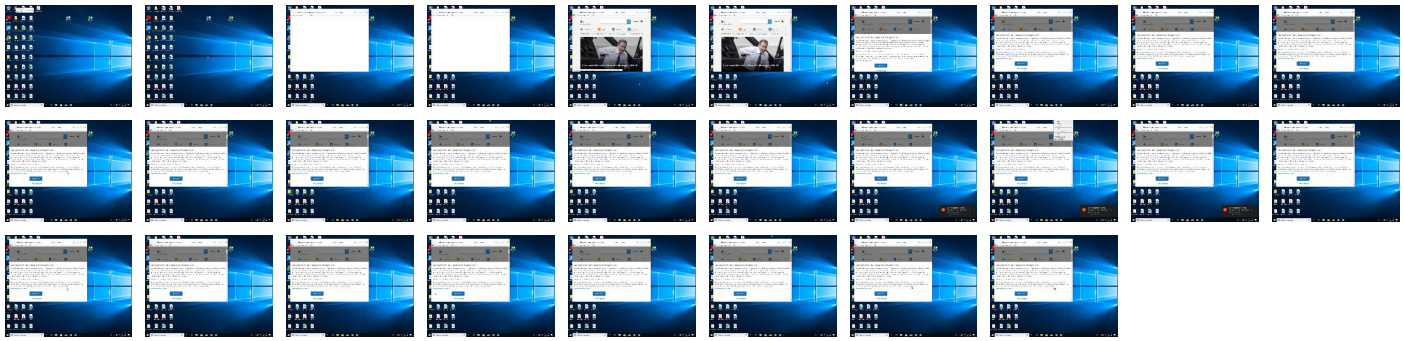
Behavior Graph

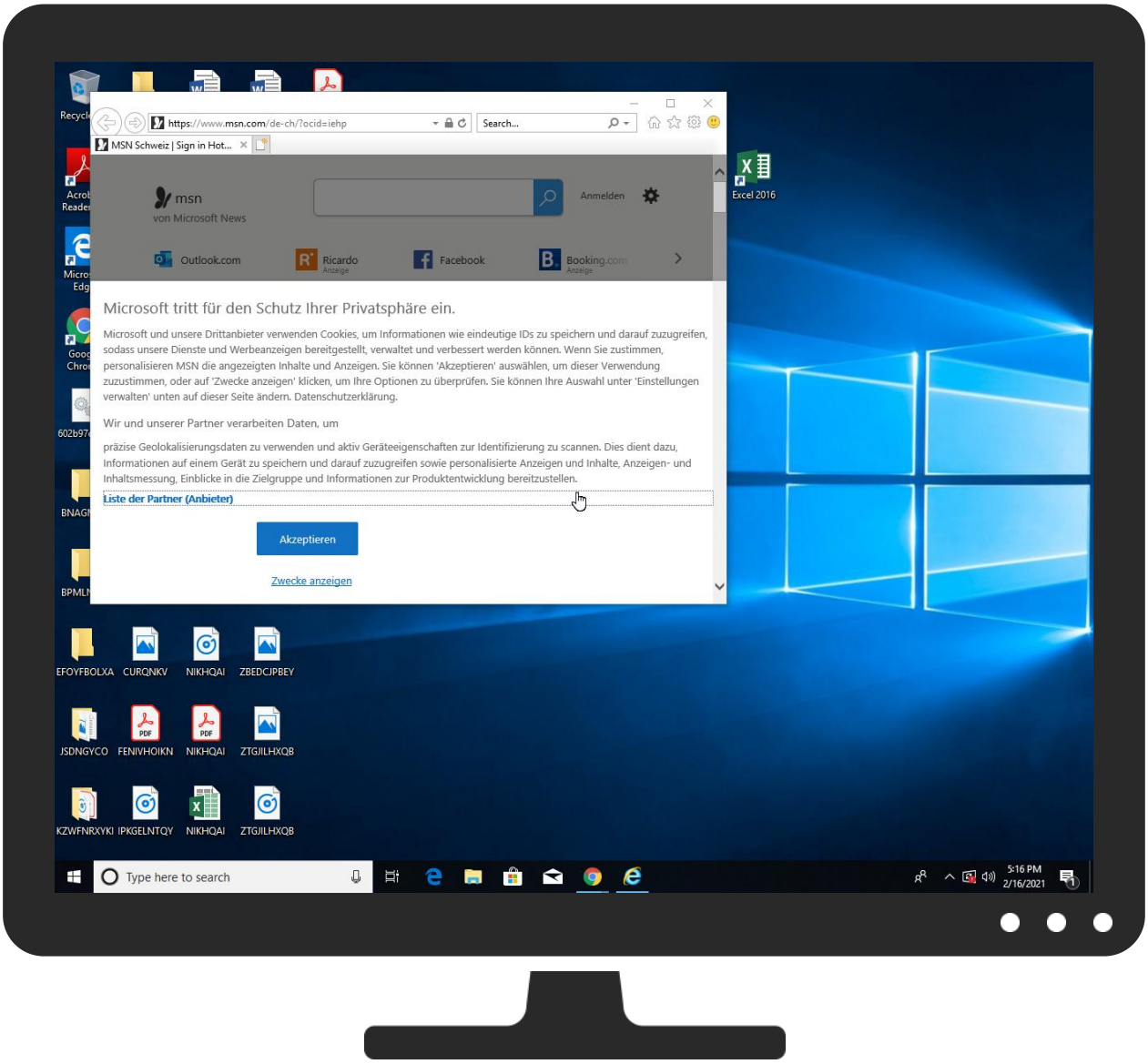


Screenshots

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
602b97e0b415b.png.dll	10%	Virustotal		Browse
602b97e0b415b.png.dll	3%	Metadefender		Browse
602b97e0b415b.png.dll	13%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.regsvr32.exe.810000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
trapolikoliosilios.xyz	1%	Virustotal		Browse
cs742.wpc.rncdn4.com	0%	Virustotal		Browse
tls13.taboola.map.fastly.net	0%	Virustotal		Browse
haloopolikosul.xyz	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://haloopolikosul.xyz/manifest/YcHhvzqnGV3dy_2/FvEnS_2F9p1dXR5ImF/Zp9nA6_2B/trDvtMc01BMk6W10nS4b/nBY6Ro9NIYZgB4PdSB2/i1mhjy8xHpcjAa_2BlE3Kc/q_2FYOvC1J7aP/FNI18_2F/AG7vxeQbhoSEjouJBbqlUsR/JPS1_2BPEm/2lxmo_2BYnZJRzpXG/9_2FrnCKa8_2/B0uAY1BCgPp/SFeeWzcA5y/lCN_2FD.cnx	100%	Avira URL Cloud	malware	
http://https://www.etahub.com/trackn?app_id=	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
trapolikoliosilios.xyz	185.186.245.78	true	false	• 1%, Virustotal, Browse	unknown
cs742.wpc.rncdn4.com	192.229.221.215	true	false	• 0%, Virustotal, Browse	unknown
tls13.taboola.map.fastly.net	151.101.1.44	true	false	• 0%, Virustotal, Browse	unknown
stats.l.doubleclick.net	74.125.206.156	true	false		high
redtube.com	66.254.114.238	true	false		high
haloopolikosul.xyz	185.186.246.166	true	false	• 2%, Virustotal, Browse	unknown
ht-cdn2.adtng.com.sds.rncdn7.com	67.22.48.100	true	false		unknown
contextual.media.net	184.30.24.22	true	false		high
vip0x04f.ssl.rncdn5.com	205.185.208.79	true	false		unknown
hubtraffic.com	66.254.114.32	true	false		high
hblg.media.net	184.30.24.22	true	false		high
ei.rdtcdn.com.sds.rncdn7.com	67.22.48.100	true	false		unknown
www.google.co.uk	216.58.208.131	true	false		unknown
a.adtng.com	216.18.168.166	true	false		unknown
lg3.media.net	184.30.24.22	true	false		high
ads.trafficjunky.net	66.254.114.38	true	false		high
geolocation.onetrust.com	104.20.185.68	true	false		high
vip0x08e.ssl.rncdn5.com	205.185.208.142	true	false		unknown
cdn.speedcurve.com	unknown	unknown	false		high
srtb.msn.com	unknown	unknown	false		high
www.redtube.com	unknown	unknown	false		high
hw-cdn-ap.trafficjunky.net	unknown	unknown	false		high
img.img-taboola.com	unknown	unknown	false		unknown
stats.g.doubleclick.net	unknown	unknown	false		high
web.vortex.data.msn.com	unknown	unknown	false		high
vz-cdn.trafficjunky.net	unknown	unknown	false		high
ht.redtube.com	unknown	unknown	false		high
static.trafficjunky.com	unknown	unknown	false		high
www.msn.com	unknown	unknown	false		high
di.rdtcdn.com	unknown	unknown	false		high
ht-cdn2.adtng.com	unknown	unknown	false		unknown
cdn1d-static-shared.phncdn.com	unknown	unknown	false		high
ei.rdtcdn.com	unknown	unknown	false		high
cvision.media.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://haloopolikosul.xyz/manifest/YcHhvzqnGV3dy_2/FvEnS_2F9p1dXR5ImF/Zp9nA6_2B/trDvtMc01BMk6W10nS4b/nBY6Ro9NIYZgB4PdSB2/i1mhjy8xHpcjAa_2BlE3Kc/q_2FYOvC1J7aP/FNI18_2F/AG7vxeQbhoSEjouJBbqlUsR/JPS1_2BPEm/2lxmo_2BYnZJRzpXG/9_2FrnCKa8_2/B0uAY1BCgPp/SFeeWzcA5y/lCN_2FD.cnx	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://di.rdtcdn.com/m=bIa44NVg5p/media/videos/202002/27/28743511/original/9.webp	3FSF6RAW.htm.31.dr	false		high

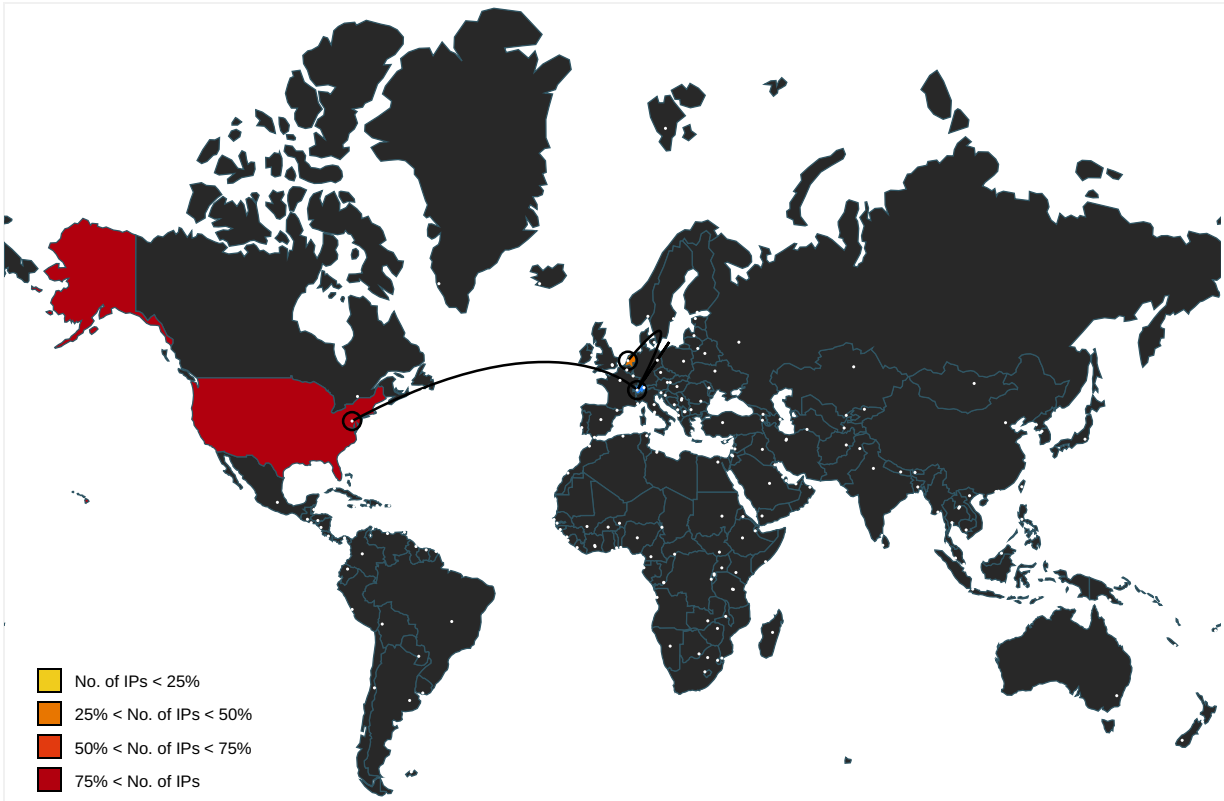
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ci-ph.rdtcdn.com/videos/202010/27/364493701/original/(m=bIaMwLVg5p)(mh=swxomuRbeznEZPbV)0.we	43C0QGGY.htm.28.dr	false		high
http://https://di.rdtcdn.com/m=bIaMwLVg5p/media/videos/201906/09/17354301/original/13.webp	3FSF6RAW.htm.31.dr	false		high
http://https://cdn.speedcurve.com/js/lux.js?id=609859533	3FSF6RAW.htm.31.dr	false		high
http://https://ci-ph.rdtcdn.com/videos/202012/30/379343432/original/(m=bIa44NVg5p)(mh=8JzX8bCfGEtmOXHd)0.we	3FSF6RAW.htm.31.dr	false		high
http://https://di.rdtcdn.com/m=eGJF8f/media/videos/201905/28/16860471/original/	3FSF6RAW.htm.31.dr	false		high
http://https://di.rdtcdn.com/m=bIaMwLVg5p/media/videos/202002/27/28743511/original/9.webp	3FSF6RAW.htm.31.dr	false		high
http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/images/pc/network-bar-sprite.png?v=6f521479622948	3FSF6RAW.htm.31.dr	false		high
http://https://ei.rdtcdn.com/m=eGJF8f/media/videos/201910/09/22850761/original/	3FSF6RAW.htm.31.dr	false		high
http://https://www.tube8.com/?utm_source=redtube&utm_medium=network-bar&utm_campaign=redtube-networkbar	3FSF6RAW.htm.31.dr	false		high
http://https://github.com/jquery/jquery-color	jquery-ui-1.10.3[1].js.28.dr	false		high
http://https://ci-ph.rdtcdn.com/m=e_rU8f/pics/pornstars/000/061/671/thumb_105631.jpg	3FSF6RAW.htm.31.dr	false		high
http://https://di.rdtcdn.com/m=bIaMwLVg5p/media/videos/201905/28/16860471/original/12.webp	3FSF6RAW.htm.31.dr	false		high
http://https://di.rdtcdn.com/m=eGJF8f/media/videos/202007/11/33841811/original/	3FSF6RAW.htm.31.dr	false		high
http://https://di.rdtcdn.com/m=eah-8f/media/videos/201904/09/15630541/original/12.jpg	3FSF6RAW.htm.31.dr	false		high
http://https://di.rdtcdn.com/m=eah-8f/media/videos/202007/24/34428911/original/10.jpg	3FSF6RAW.htm.31.dr	false		high
http://https://www.redtube.com/?page=2	3FSF6RAW.htm.31.dr	false		high
http://https://dw.rdtcdn.com/media/videos/202002/03/27917611/360P_360K_27917611_fb.mp4	3FSF6RAW.htm.31.dr	false		high
http://https://ei.rdtcdn.com/m=eW0Q8f/media/videos/202011/19/38164441/original/4.jpg	3FSF6RAW.htm.31.dr	false		high
http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/images/pc/category/amateur_001.jpg	3FSF6RAW.htm.31.dr	false		high
http://https://res-a.akamaihd.net/__media__/pics/8000/72/941/fallback1.jpg	{5B2D87FA-70BD-11EB-90E5-ECF4BB2D2496}.dat.3.dr	false		high
http://https://ci-ph.rdtcdn.com/videos/202012/30/379343432/original/(m=eGJF8f)(mh=38RzzpmO7YHWdTc5)	3FSF6RAW.htm.31.dr	false		high
http://https://www.onenote.com/notebooks?WT.mc_id=MSN_OneNote_Recent&auth=1&wdorigin=msn	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://di.rdtcdn.com/m=bIa44NVg5p/media/videos/202003/28/29931511/original/15.webp	3FSF6RAW.htm.31.dr	false		high
http://https://di.rdtcdn.com/m=eah-8f/media/videos/202011/02/37489741/original/5.jpg	3FSF6RAW.htm.31.dr	false		high
http://https://cv-ph.rdtcdn.com/videos/201809/28/185193891/360P_360K_185193891_fb.mp4?VPWEe8g3Vde2H4N-pbLjR	3FSF6RAW.htm.31.dr	false		high
http://https://di.rdtcdn.com/m=bIa44NVg5p/media/videos/202007/11/33841811/original/13.webp	3FSF6RAW.htm.31.dr	false		high
http://https://ei.rdtcdn.com/m=eGJF8f/media/videos/202008/24/35368101/original/	3FSF6RAW.htm.31.dr	false		high
http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/images/pc/ajax-loader.gif	3FSF6RAW.htm.31.dr	false		high
http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/images/pc/category/mature_001.jpg	3FSF6RAW.htm.31.dr	false		high
http://https://ei.rdtcdn.com/m=eah-8f/media/videos/201910/09/22850761/original/2.jpg	3FSF6RAW.htm.31.dr	false		high
http://www.reddit.com/	msapplication.xml4.3.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dw.rdtcdn.com/media/videos/202011/09/37808811/360P_360K_37808811_fb.mp4	3FSF6RAW.htm.31.dr	false		high
http://https://ei.rdtcdn.com/m=eGJF8f/media/videos/201907/14/18927751/original/	3FSF6RAW.htm.31.dr	false		high
http://https://hw-cdn-ap.trafficjunky.net/uploaded_content/creative/101/814/192/1/1018141921.png	ads_batch[2].json.31.dr	false		high
http://https://ads.trafficjunky.net/deep_click?adtype=static&ar=www.redtube.com&click_data=m-8rYAAAAACJmJ47	ads_batch[1].json.28.dr	false		high
http://https://ei.rdtcdn.com/m=eah-8f/media/videos/201907/14/18927751/original/5.jpg	3FSF6RAW.htm.31.dr	false		high
http://https://ci-ph.rdtcdn.com/videos/202010/27/364493701/original/(m=eW0Q8f)(mh=EAfqUkqacw_m4_HW)0.jpg	43C0QGGY.htm.28.dr	false		high
http://https://di.rdtcdn.com/m=bIaMwLVg5p/media/videos/202012/02/38585811/original/15.webp	3FSF6RAW.htm.31.dr	false		high
http://https://ci-ph.rdtcdn.com/m=bIWpYLVg5p/pics/pornstars/000/001/630/thumb_385962.webp	3FSF6RAW.htm.31.dr	false		high
http://https://sp.booking.com/index.html?aid=1589774&label=travelnavlink	de-ch[1].htm.4.dr	false		high
http://https://ei.rdtcdn.com/m=bIijsHVg5p/media/videos/201706/02/2182127/original/9.webp	3FSF6RAW.htm.31.dr	false		high
http://https://di.rdtcdn.com/m=eah-8f/media/videos/201908/21/20680141/original/4.jpg	3FSF6RAW.htm.31.dr	false		high
http://https://di.rdtcdn.com/m=eGJF8f/media/videos/201908/21/20680141/original/4.jpg	3FSF6RAW.htm.31.dr	false		high
http://https://ci-ph.rdtcdn.com/m=e_rU8f/pics/pornstars/000/035/562/thumb_1261201.jpg	3FSF6RAW.htm.31.dr	false		high
http://https://dw.rdtcdn.com/media/videos/201903/21/15059681/360P_360K_15059681_fb.mp4	3FSF6RAW.htm.31.dr	false		high
http://https://dw.rdtcdn.com/media/videos/202007/06/33655051/360P_360K_33655051_fb.mp4	3FSF6RAW.htm.31.dr	false		high
http://https://di.rdtcdn.com/m=eah-8f/media/videos/201903/02/14329691/original/12.jpg	3FSF6RAW.htm.31.dr	false		high
http://https://amzn.to/2TTxhNg	de-ch[1].htm.4.dr	false		high
http://https://www.skype.com/go/onedrivepromo.download?cm_mmc=MSFT_2390_MSN-com	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://static.trafficjunky.com/invocation/embeddedads/	3FSF6RAW.htm.31.dr	false		high
http://designer.videojs.com	video-js[1].css.28.dr	false		high
http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/images/pc/category/lesbian_001.jpg	3FSF6RAW.htm.31.dr	false		high
http://https://ci-ph.rdtcdn.com/videos/202102/02/382881362/original/(m=eGJF8f)(mh=KcOd3zrwWRqQbpfr)0.jpg	3FSF6RAW.htm.31.dr	false		high
http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/css/generated/pc/default-redtube.css?v=6f52147962	3FSF6RAW.htm.31.dr	false		high
http://https://di.rdtcdn.com/m=eGJF8f/media/videos/202012/02/38585811/original/	3FSF6RAW.htm.31.dr	false		high
http://https://di.rdtcdn.com/m=eGJF8f/media/videos/201905/20/16689701/original/	3FSF6RAW.htm.31.dr	false		high
http://https://www.msn.com/de-ch	de-ch[1].htm.4.dr	false		high
http://https://www.etahub.com/trackn?app_id=	timings-1.0.0[1].js.28.dr	false	• Avira URL Cloud: safe	unknown
http://https://ci-ph.rdtcdn.com/m=bIWpYLVg5p/pics/pornstars/000/007/562/thumb_520742.webp	3FSF6RAW.htm.31.dr	false		high
http://modernizr.com/download/#-video-shiv-cssclasses-load	modernizr[1].js.28.dr	false		high
http://https://di.rdtcdn.com/m=bIa44NVg5p/media/videos/201908/08/20135061/original/12.webp	3FSF6RAW.htm.31.dr	false		high
http://https://di.rdtcdn.com/m=eGJF8f/media/videos/202002/24/28658531/original/	3FSF6RAW.htm.31.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://di.rdtcdn.com/m=eW0Q8f/media/videos/202012/02/38585811/original/15.jpg	3FSF6RAW.htm.31.dr	false		high
http://https://ci-ph.rdtcdn.com/m=bIWpYLVg5p/pics/pornstars/000/245/441/thumb_1180331.webp	3FSF6RAW.htm.31.dr	false		high
http://https://di.rdtcdn.com/m=eGJF8f/media/videos/201903/15/14834671/original/	3FSF6RAW.htm.31.dr	false		high
http://https://di.rdtcdn.com/m=bIaMwLVg5p/media/videos/201908/30/21082181/original/3.webp	3FSF6RAW.htm.31.dr	false		high
http://https://ei.rdtcdn.com/m=bIa44NVg5p/media/videos/202009/17/36095301/original/13.webp	3FSF6RAW.htm.31.dr	false		high
http://https://ei.rdtcdn.com/m=ejrk8f/media/videos/201409/08/885303/original/4.jpg	3FSF6RAW.htm.31.dr	false		high
http://https://di.rdtcdn.com/m=eW0Q8f/media/videos/201904/29/16202841/original/12.jpg	3FSF6RAW.htm.31.dr	false		high
http://https://dw.rdtcdn.com/media/videos/201912/27/26372111/360P_360K_26372111_fb.mp4	3FSF6RAW.htm.31.dr	false		high
http://https://www.msn.com/de-ch/?ocid=iehp&item=deferred_page%3a1&ignorejs=webcore%2fmodules%2fjsb	de-ch[1].htm.4.dr	false		high
http://https://di.rdtcdn.com/m=eGJF8f/media/videos/202003/07/29111521/original/	3FSF6RAW.htm.31.dr	false		high
http://https://ev-ph.rdtcdn.com/videos/202007/16/333596592/360P_360K_333596592_fb.mp4?validfrom=1613488548&	3FSF6RAW.htm.31.dr	false		high
http://https://di.rdtcdn.com/m=bIa44NVg5p/media/videos/201908/30/21082181/original/3.webp	3FSF6RAW.htm.31.dr	false		high
http://https://di.rdtcdn.com/m=eW0Q8f/media/videos/202009/19/36157701/original/11.jpg	3FSF6RAW.htm.31.dr	false		high
http://https://ci-ph.rdtcdn.com/m=bIWpYLVg5p/pics/pornstars/000/005/221/thumb_305561.webp	3FSF6RAW.htm.31.dr	false		high
http://https://de.redtube.com/	3FSF6RAW.htm.31.dr	false		high
http://https://di.rdtcdn.com/m=bIa44NVg5p/media/videos/201907/14/18927751/original/5.webp	3FSF6RAW.htm.31.dr	false		high
http://https://ci-ph.rdtcdn.com/videos/202007/16/333596592/original/(m=eGJF8f)(mh=wTIcX7GkEsQERyzS)0.jpg	3FSF6RAW.htm.31.dr	false		high
http://https://di.rdtcdn.com/m=bIaMwLVg5p/media/videos/201907/14/18927751/original/5.webp	3FSF6RAW.htm.31.dr	false		high
http://https://dw.rdtcdn.com/media/videos/201908/30/21082181/360P_360K_21082181_fb.mp4	3FSF6RAW.htm.31.dr	false		high
http://https://cdn1d-static-shared.phncdn.com/timings-1.0.0.js	3FSF6RAW.htm.31.dr	false		high
http://https://onedrive.live.com/?qt=mru;OneDrive-App	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://www.skype.com/de	85-0f8009-68ddb2ab[1].js.4.dr	false		high
http://https://cw.rdtcdn.com/media/videos/201906/09/17354301/360P_360K_17354301_fb.mp4	3FSF6RAW.htm.31.dr	false		high
http://https://ci-ph.rdtcdn.com/m=bIWpYLVg5p/pics/pornstars/000/035/562/thumb_1261201.webp	3FSF6RAW.htm.31.dr	false		high
http://https://dv-ph.rdtcdn.com/videos/202010/27/364493701/360P_360K_364493701_fb.mp4?ttl=1613495723&ri	43C0QGGY.htm.28.dr	false		high
http://https://ci-ph.rdtcdn.com/videos/201907/01/232605451/original/(m=eGJF8f)(mh=_XdyfjpQjKb1ue5F)3.jpg	3FSF6RAW.htm.31.dr	false		high
http://https://jp.redtube.com/	3FSF6RAW.htm.31.dr	false		high
http://https://www.msn.com/de-ch/news/other/z%c3%bcrcher-finanzdirektor-fordert-einen-corona-ausstiegsplan/	de-ch[1].htm.4.dr	false		high
http://https://di-ph.rdtcdn.com/videos/201809/28/185193891/original/(m=bIa44NVg5p)(mh=UEMIxBRwTvtYu0dM)3.we	3FSF6RAW.htm.31.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://di.rdtcdn.com/m=eW0Q8f/media/videos/201903/15/14834671/original/12.jpg	3FSF6RAW.htm.31.dr	false		high
http://https://di-ph.rdtcdn.com/videos/201809/28/185193891/original/(m=eW0Q8f)(mh=Y0NNJ5GholpF9zE7)3.jpg	3FSF6RAW.htm.31.dr	false		high
http://https://di.rdtcdn.com/m=eGJF8f/media/videos/201910/17/231977181/original/	3FSF6RAW.htm.31.dr	false		high
http://https://onedrive.live.com/?wt.mc_id=oo_msn_msnhomepage_header	de-ch[1].htm.4.dr	false		high
http://https://ci-ph.rdtcdn.com/videos/202010/27/364493701/original/(m=eGJF8f)(mh=EXJlJkCRUNs_a08Y)0.jpg	43C0QGGY.htm.28.dr	false		high
http://https://cw.rdtcdn.com/media/videos/201903/15/14834671/360P_360K_14834671_fb.mp4	3FSF6RAW.htm.31.dr	false		high
http://https://di.rdtcdn.com/m=eW0Q8f/media/videos/202002/27/28743511/original/9.jpg	3FSF6RAW.htm.31.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.254.114.238	unknown	United States		29789	REFLECTEDUS	false
74.125.206.156	unknown	United States		15169	GOOGLEUS	false
66.254.114.38	unknown	United States		29789	REFLECTEDUS	false
66.254.114.32	unknown	United States		29789	REFLECTEDUS	false
67.22.48.100	unknown	Netherlands		29789	REFLECTEDUS	false
216.58.208.131	unknown	United States		15169	GOOGLEUS	false
192.229.221.215	unknown	United States		15133	EDGECASTUS	false
151.101.1.44	unknown	United States		54113	FASTLYUS	false
185.186.245.78	unknown	Netherlands		40824	WZCOM-US	false
104.20.185.68	unknown	United States		13335	CLOUDFLARENETUS	false
216.18.168.166	unknown	United States		29789	REFLECTEDUS	false
185.186.246.166	unknown	Netherlands		35415	WEBZILLANL	false
205.185.208.142	unknown	United States		20446	HIGHWINDS3US	false
205.185.208.79	unknown	United States		20446	HIGHWINDS3US	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	353629
Start date:	16.02.2021
Start time:	17:12:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	602b97e0b415b.png.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:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.troj.winDLL@16/197@34/15
EGA Information:	Failed
HDC Information:	• Successful, ratio: 21.5% (good quality ratio 20.8%) • Quality average: 80.7% • Quality standard deviation: 27.1%
HCA Information:	• Successful, ratio: 71% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 51.104.139.180, 40.88.32.150, 13.88.21.125, 23.211.6.115, 13.64.90.137, 88.221.62.148, 131.253.33.203, 92.122.213.187, 92.122.213.231, 65.55.44.109, 184.30.24.22, 152.199.19.161, 92.122.213.194, 92.122.213.247, 205.185.216.10, 205.185.216.42, 2.20.142.209, 2.20.142.210, 51.103.5.159, 52.155.217.156, 20.54.26.129, 184.30.20.56, 151.101.2.217, 151.101.66.217, 151.101.130.217, 151.101.194.217, 142.250.186.78, 209.197.3.98, 142.250.180.100, 51.11.168.160, 216.58.209.46 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, vip1-par02p.wns.notify.trafficmanager.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, www.google.com, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, www.google-analytics.com, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, cvision.media.net.edgekey.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, updates.microsoft.com, a1999.dscg2.akamai.net, web.vortex.data.trafficmanager.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, a3.shared.global.fastly.net, blobcollector.events.data.trafficmanager.net, cs9.wpc.v0cdn.net, cds.q7x2a8v5.hwcdn.net, au.download.windowsupdate.com.edgesuite.net, store-images.s-microsoft.com-c.edgekey.net, a-0003.dc-msedge.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, go.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, www-google-analytics.l.google.com, ie9comview.vo.msecnd.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, cds.e9q5t8x5.hwcdn.net, www-msn-com.a-0003.a-msedge.net, cds.d2s7q6s2.hwcdn.net, a767.dscg3.akamai.net, e607.d.akamaiedge.net, web.vortex.data.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, icePrime.a-0003.dc-msedge.net, go.microsoft.com.edgekey.net, static-global-s-msn-com.akamaized.net, skypedataprdcolwus15.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
66.254.114.38	DSC_Canon_23.12.2020.exe	Get hash	malicious	Browse	
	LGwzOM1BAN.exe	Get hash	malicious	Browse	
	invoice_order_57832.zip.exe	Get hash	malicious	Browse	
	5f291381b8e10png.dll	Get hash	malicious	Browse	
	5f291fa0130fcrar.dll	Get hash	malicious	Browse	
216.58.208.131	NordVPN 4.17.6.apk	Get hash	malicious	Browse	
	skripsi.apk	Get hash	malicious	Browse	
	skripsi.apk	Get hash	malicious	Browse	
	http://app.eq.intuit.com/e/er?s=113755760&lid=62441&elqTrackId=4b615073902b48dc9d66fc98052408f2&elq=cbdf3bcb965644b38a2e3ce069e60868&elqaid=27000&elqat=1	Get hash	malicious	Browse	
	http://https://rebrand.ly/we9zn	Get hash	malicious	Browse	
	http://purchase900923.zizera.com	Get hash	malicious	Browse	
	http://https://www.canva.com/design/DAENr9VVSBY/j0BB1RmEldachKWw-1swmQ/view?utm_content=DAENr9VVSBY&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	Get hash	malicious	Browse	
	http://https://facialxpressions.com/mox/	Get hash	malicious	Browse	
	http://https://www.women.com/alexa/quiz-dialect-test	Get hash	malicious	Browse	
	http://https://app.box.com/s/3yqx9qlp6f5g2u6hojzof8xiz970by12	Get hash	malicious	Browse	
	http://technoraga.com/Doc.htm	Get hash	malicious	Browse	
	Zped7c3dam.exe	Get hash	malicious	Browse	
	http://naturalhub-diet.world/shake.php?a=1nou&c=diet&s=330788,UEMRADAPDP38712	Get hash	malicious	Browse	
	eLaaw7SqMi.exe	Get hash	malicious	Browse	
	OvhEqDMY2H.exe	Get hash	malicious	Browse	
	8Hyg1V4APN.exe	Get hash	malicious	Browse	
	nL0Rdebyri.exe	Get hash	malicious	Browse	
	1o38UBif0L.exe	Get hash	malicious	Browse	
	8SXG5TeTQf.exe	Get hash	malicious	Browse	
	65QroIPnO1.exe	Get hash	malicious	Browse	
66.254.114.238	DSC_Canon_23.12.2020.exe	Get hash	malicious	Browse	
	invoice_order_57832.zip.exe	Get hash	malicious	Browse	
	5f291381b8e10png.dll	Get hash	malicious	Browse	
	5f291fa0130fcrar.dll	Get hash	malicious	Browse	
74.125.206.156	http://https://us18.campaign-archive.com/?u=c411c1f1b730b2e13b3b995f2&id=b5f83c2121	Get hash	malicious	Browse	
	INVOICES.pdf	Get hash	malicious	Browse	
	http://email.lyftmail.com/c/eJwtkE1vgkAQhn8N3iDLsi5w4ACl2hqjsSaiXsiyO8o07EL4EO2vLzRN5jLJM-_MMyoSoXJhUb1ufa6h68QdclQRYVT5VHHbJa6wGQCxQ1rcbF8EoVAFdYPAW2BEiRuQJQkoYd6SOa7D3tNVzAlJg9TnPAktRuZoLbByZK0XZQQBDakMVSEplx5l3PNdqRjzfe5KEHJRRWXfN53lxRZdTTWOozNnzPNTWwwdmulQu2nrG1YwgStZK7C8NHttvsXHppHeV3M9LsutSWqRPTtxTn4O61V_PZfmYg7DhYb9J454yU5MrneP4rhRTqr2Cu8OGI18n11jZrJ6W-_KePN2ojkkobQoH3qdd_XQynkdmgf2oKa36QLavAWNRkH7j0mhG4F3M4ECns0s30aybLHrERzhNCVWFU6ejAgNz3vxJ_gLZsmCsQ	Get hash	malicious	Browse	
	http://diana-clairvoyance.com/H2qPF8N48pg/QeNoIoaJbBKRmYfbnO1sulYlUcteAQwH/page.html	Get hash	malicious	Browse	
	SUPERsetup.exe	Get hash	malicious	Browse	
	ow.ly/u8cg30gnek9	Get hash	malicious	Browse	
66.254.114.32	DSC_Canon_23.12.2020.exe	Get hash	malicious	Browse	
	LGwzOM1BAN.exe	Get hash	malicious	Browse	
	invoice_order_57832.zip.exe	Get hash	malicious	Browse	
	5f291381b8e10png.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	5f291fa0130fcrar.dll	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
stats.l.doubleclick.net	Ve8rhkTls5.exe	Get hash	malicious	Browse	• 64.233.184.157
	dPWf8DPe5x.exe	Get hash	malicious	Browse	• 64.233.184.157
	y0CRLCaQxA.exe	Get hash	malicious	Browse	• 142.250.102.154
	CONSTANTINE.xlsx	Get hash	malicious	Browse	• 108.177.15.157
	Document0098.html	Get hash	malicious	Browse	• 108.177.15.156
	yVn2ywuhEC.exe	Get hash	malicious	Browse	• 108.177.127.155
	VM859-7757.htm	Get hash	malicious	Browse	• 108.177.127.157
	Acunetix Premium v13.0.201112128 Activation Tool.exe	Get hash	malicious	Browse	• 74.125.133.157
	Jasper-6.10.0.docx	Get hash	malicious	Browse	• 74.125.140.157
	e-card.htm .exe	Get hash	malicious	Browse	• 108.177.15.154
	e-card.jpg .exe	Get hash	malicious	Browse	• 108.177.15.154
	http://https://new-fax-messages.mydopweb.com/	Get hash	malicious	Browse	• 108.177.15.156
	http://https://ozmmdmfly0ob6rsgyfcjja-on.drv.tw/GAIAFw&flowName=GlifWebSignIn&flowEntry=AddSession&response_mode=form_post&response_type=code+id_token&scope=openid+profile&state=OpenIdConnect.AuthenticationProperties=7l5fOQe2aVADfQrM2gnSPpnNXdJDFVEswOkTEzvRpizt0MxezF-fEHwkij9KPoULqpUnkx2n_0Dud0uKVG57peviUxksCdnZyX7ab0n1hx9UpfkPdjMq2wNzHOC_K3ig&nonce=636810071538546755.OTdjZTIwMDItYjU4Yy00ODAxLTkzMDgtMzAzNGIwNThmY2ZkZWI3OTkzNDUtN2NlZC00MDIxLWFlZDQtNzhkNmM0ODhmMzAz&/	Get hash	malicious	Browse	• 108.177.15.155
	http://https://web.tresorit.com/l/JG7xl#7YqXRnhV6spRT3ekJskNaw	Get hash	malicious	Browse	• 108.177.15.157
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 108.177.15.155
	http://https://wfuwdbjwquoiynfb-dot-tundasma.el.r.appspot.com/#test@test.com	Get hash	malicious	Browse	• 108.177.15.156
	http://bit.ly/3nlGvk0	Get hash	malicious	Browse	• 74.125.140.156
	http://https://cypressbayhockey.com/NO	Get hash	malicious	Browse	• 74.125.140.156
	http://https://pdfsharedmessage.xtensio.com/7wtcdlta	Get hash	malicious	Browse	• 74.125.140.154
	http://https://viewer.desygner.com/-M7QpDHAe3Y/	Get hash	malicious	Browse	• 74.125.140.157
tls13.taboola.map.fastly.net	SecuriteInfo.com.Generic.mg.44669e0ff064dfc9.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Generic.mg.3964ec2fe493ed56.dll	Get hash	malicious	Browse	• 151.101.1.44
	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
	RI51uAlUyL.dll	Get hash	malicious	Browse	• 151.101.1.44
	ZRz0Aq1Rf0.dll	Get hash	malicious	Browse	• 151.101.1.44
	mon44_cr.dll	Get hash	malicious	Browse	• 151.101.1.44
	mon41_cr.dll	Get hash	malicious	Browse	• 151.101.1.44
	mon4498.dll	Get hash	malicious	Browse	• 151.101.1.44
	e888888888.dll	Get hash	malicious	Browse	• 151.101.1.44
	1233.exe	Get hash	malicious	Browse	• 151.101.1.44
	Server.exe	Get hash	malicious	Browse	• 151.101.1.44
	2200.dll	Get hash	malicious	Browse	• 151.101.1.44
	mon48_cr.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Generic.mg.5db96940e68acc98.dll	Get hash	malicious	Browse	• 151.101.1.44
	SecuriteInfo.com.Generic.mg.fac603176f7a6a20.dll	Get hash	malicious	Browse	• 151.101.1.44
cs742.wpc.rncdn4.com	DSC_Canon_23.12.2020.exe	Get hash	malicious	Browse	• 192.229.221.215
	5f291fa0130fcrar.dll	Get hash	malicious	Browse	• 192.229.221.215

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
REFLECTEDUS	DSC_Canon_23.12.2020.exe	Get hash	malicious	Browse	• 66.254.114.32

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.CIL.StupidStealth.Heur.exe	Get hash	malicious	Browse	• 216.18.168.166
	http://https://signup.kwikvpn.com/	Get hash	malicious	Browse	• 66.254.118.170
	http://cloudz.pw/go?green=carrier%2048gs-036060301%20operation%20manual	Get hash	malicious	Browse	• 208.99.69.133
	http://cloudz.pw/go?green=carrier 48gs-036060301 operation manual	Get hash	malicious	Browse	• 66.254.111.99
	LGwzOM1BAN.exe	Get hash	malicious	Browse	• 66.254.114.41
	http://https://www.google.com/url?q=https%3A%2F%2Fbit.ly%2F34lVoM1&sa=D&sntz=1&usg=AFQjCNGItNrIAWHjWOHF3rvz8pNqtmAYtg	Get hash	malicious	Browse	• 208.99.69.233
	2svozs0lnii.exe	Get hash	malicious	Browse	• 216.18.168.122
	invoice_order_57832.zip.exe	Get hash	malicious	Browse	• 66.254.114.32
	5f291381b8e10png.dll	Get hash	malicious	Browse	• 216.18.168.166
	5f291fa0130fcrar.dll	Get hash	malicious	Browse	• 66.254.114.32
REFLECTEDUS	DSC_Canon_23.12.2020.exe	Get hash	malicious	Browse	• 66.254.114.32
	SecuriteInfo.com.CIL.StupidStealth.Heur.exe	Get hash	malicious	Browse	• 216.18.168.166
	http://https://signup.kwikvpn.com/	Get hash	malicious	Browse	• 66.254.118.170
	http://cloudz.pw/go?green=carrier%2048gs-036060301%20operation%20manual	Get hash	malicious	Browse	• 208.99.69.133
	http://cloudz.pw/go?green=carrier 48gs-036060301 operation manual	Get hash	malicious	Browse	• 66.254.111.99
	LGwzOM1BAN.exe	Get hash	malicious	Browse	• 66.254.114.41
	http://https://www.google.com/url?q=https%3A%2F%2Fbit.ly%2F34lVoM1&sa=D&sntz=1&usg=AFQjCNGItNrIAWHjWOHF3rvz8pNqtmAYtg	Get hash	malicious	Browse	• 208.99.69.233
	2svozs0lnii.exe	Get hash	malicious	Browse	• 216.18.168.122
	invoice_order_57832.zip.exe	Get hash	malicious	Browse	• 66.254.114.32
	5f291381b8e10png.dll	Get hash	malicious	Browse	• 216.18.168.166
	5f291fa0130fcrar.dll	Get hash	malicious	Browse	• 66.254.114.32
GOOGLEUS	InterTech_Inquiry.exe	Get hash	malicious	Browse	• 34.102.136.180
	Firefox Browser fast private safe web browser_v85.1.3_apkpure.com.apk	Get hash	malicious	Browse	• 142.250.184.42
	Firefox Browser fast private safe web browser_v85.1.3_apkpure.com.apk	Get hash	malicious	Browse	• 142.250.180.142
	PO copy.pdf.exe	Get hash	malicious	Browse	• 35.246.6.109
	RFQ 2-16-2021-.exe	Get hash	malicious	Browse	• 34.102.136.180
	upload-1070618585-617329914.xls	Get hash	malicious	Browse	• 216.239.38.21
	Microsoft Outlook Secure email calendars files_v4.2104.2_apkpure.com.apk	Get hash	malicious	Browse	• 142.250.180.132
	Gspace_1.0.2.apk	Get hash	malicious	Browse	• 142.250.180.131
	Gspace_1.0.2.apk	Get hash	malicious	Browse	• 142.250.180.74
	Gspace_1.0.2.apk	Get hash	malicious	Browse	• 142.250.180.132
	fedex.apk	Get hash	malicious	Browse	• 142.250.184.42
	NEW ORDER - VOLVO HK HKPO2102-13561,pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	LeaveHomeSafe_v1.1.6_apkpure.com.apk	Get hash	malicious	Browse	• 142.250.180.132
	Request for Quotation76584454.ppt	Get hash	malicious	Browse	• 216.58.208.161
	02-016.exe	Get hash	malicious	Browse	• 34.102.136.180
	ORDER FRD91PM7.xlsx	Get hash	malicious	Browse	• 35.186.253.211
	ORDER FRD91PM7.xlsx	Get hash	malicious	Browse	• 216.58.198.35
	wfEePDdnmR.exe	Get hash	malicious	Browse	• 34.102.136.180
	D200821ROB.ppt	Get hash	malicious	Browse	• 216.58.208.161
	D200821ROB.ppt	Get hash	malicious	Browse	• 216.58.208.161

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	PO 20191003.exe	Get hash	malicious	Browse	• 67.22.48.100 • 216.58.208.131 • 66.254.114.238 • 74.125.206.156 • 192.229.221.215 • 151.101.1.44 • 66.254.114.38 • 104.20.185.68 • 216.18.168.166 • 205.185.208.142 • 205.185.208.79 • 66.254.114.32
	ce8fe9f746c521ecc687fb0482c663fc.exe	Get hash	malicious	Browse	• 67.22.48.100 • 216.58.208.131 • 66.254.114.238 • 74.125.206.156 • 192.229.221.215 • 151.101.1.44 • 66.254.114.38 • 104.20.185.68 • 216.18.168.166 • 205.185.208.142 • 205.185.208.79 • 66.254.114.32
	POCM 202100322.exe	Get hash	malicious	Browse	• 67.22.48.100 • 216.58.208.131 • 66.254.114.238 • 74.125.206.156 • 192.229.221.215 • 151.101.1.44 • 66.254.114.38 • 104.20.185.68 • 216.18.168.166 • 205.185.208.142 • 205.185.208.79 • 66.254.114.32
	ORDER FRD91PM7.xlsx	Get hash	malicious	Browse	• 67.22.48.100 • 216.58.208.131 • 66.254.114.238 • 74.125.206.156 • 192.229.221.215 • 151.101.1.44 • 66.254.114.38 • 104.20.185.68 • 216.18.168.166 • 205.185.208.142 • 205.185.208.79 • 66.254.114.32
	CHT International.exe	Get hash	malicious	Browse	• 67.22.48.100 • 216.58.208.131 • 66.254.114.238 • 74.125.206.156 • 192.229.221.215 • 151.101.1.44 • 66.254.114.38 • 104.20.185.68 • 216.18.168.166 • 205.185.208.142 • 205.185.208.79 • 66.254.114.32
	SecuriteInfo.com.Generic.mg.44669e0ff064dfc9.dll	Get hash	malicious	Browse	• 67.22.48.100 • 216.58.208.131 • 66.254.114.238 • 74.125.206.156 • 192.229.221.215 • 151.101.1.44 • 66.254.114.38 • 104.20.185.68 • 216.18.168.166 • 205.185.208.142 • 205.185.208.79 • 66.254.114.32

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Generic.mg.3964ec2fe493ed56.dll	Get hash	malicious	Browse	• 67.22.48.100 • 216.58.208.131 • 66.254.114.238 • 74.125.206.156 • 192.229.22 1.215 • 151.101.1.44 • 66.254.114.38 • 104.20.185.68 • 216.18.168.166 • 205.185.20 8.142 • 205.185.208.79 • 66.254.114.32
	SecuriteInfo.com.Generic.mg.f76b81b0397ae313.dll	Get hash	malicious	Browse	• 67.22.48.100 • 216.58.208.131 • 66.254.114.238 • 74.125.206.156 • 192.229.22 1.215 • 151.101.1.44 • 66.254.114.38 • 104.20.185.68 • 216.18.168.166 • 205.185.20 8.142 • 205.185.208.79 • 66.254.114.32
	SecuriteInfo.com.Generic.mg.f77e7bd43f365593.dll	Get hash	malicious	Browse	• 67.22.48.100 • 216.58.208.131 • 66.254.114.238 • 74.125.206.156 • 192.229.22 1.215 • 151.101.1.44 • 66.254.114.38 • 104.20.185.68 • 216.18.168.166 • 205.185.20 8.142 • 205.185.208.79 • 66.254.114.32
	NJPcHPuRcG.dll	Get hash	malicious	Browse	• 67.22.48.100 • 216.58.208.131 • 66.254.114.238 • 74.125.206.156 • 192.229.22 1.215 • 151.101.1.44 • 66.254.114.38 • 104.20.185.68 • 216.18.168.166 • 205.185.20 8.142 • 205.185.208.79 • 66.254.114.32
	Ne6A4k8vK6.dll	Get hash	malicious	Browse	• 67.22.48.100 • 216.58.208.131 • 66.254.114.238 • 74.125.206.156 • 192.229.22 1.215 • 151.101.1.44 • 66.254.114.38 • 104.20.185.68 • 216.18.168.166 • 205.185.20 8.142 • 205.185.208.79 • 66.254.114.32
	13xakh1PtD.dll	Get hash	malicious	Browse	• 67.22.48.100 • 216.58.208.131 • 66.254.114.238 • 74.125.206.156 • 192.229.22 1.215 • 151.101.1.44 • 66.254.114.38 • 104.20.185.68 • 216.18.168.166 • 205.185.20 8.142 • 205.185.208.79 • 66.254.114.32

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DUcKsYsyX0.dll	Get hash	malicious	Browse	• 67.22.48.100 • 216.58.208.131 • 66.254.114.238 • 74.125.206.156 • 192.229.22 1.215 • 151.101.1.44 • 66.254.114.38 • 104.20.185.68 • 216.18.168.166 • 205.185.20 8.142 • 205.185.208.79 • 66.254.114.32
	7eec14e7cec4dc93fbf53e08998b2340.exe	Get hash	malicious	Browse	• 67.22.48.100 • 216.58.208.131 • 66.254.114.238 • 74.125.206.156 • 192.229.22 1.215 • 151.101.1.44 • 66.254.114.38 • 104.20.185.68 • 216.18.168.166 • 205.185.20 8.142 • 205.185.208.79 • 66.254.114.32
	RI51uAIUyL.dll	Get hash	malicious	Browse	• 67.22.48.100 • 216.58.208.131 • 66.254.114.238 • 74.125.206.156 • 192.229.22 1.215 • 151.101.1.44 • 66.254.114.38 • 104.20.185.68 • 216.18.168.166 • 205.185.20 8.142 • 205.185.208.79 • 66.254.114.32
	L257MJZ0TP.htm	Get hash	malicious	Browse	• 67.22.48.100 • 216.58.208.131 • 66.254.114.238 • 74.125.206.156 • 192.229.22 1.215 • 151.101.1.44 • 66.254.114.38 • 104.20.185.68 • 216.18.168.166 • 205.185.20 8.142 • 205.185.208.79 • 66.254.114.32
	brewin-02-02-21 Statement_763108amFtZXMubXV0aW1lcg ==.htm	Get hash	malicious	Browse	• 67.22.48.100 • 216.58.208.131 • 66.254.114.238 • 74.125.206.156 • 192.229.22 1.215 • 151.101.1.44 • 66.254.114.38 • 104.20.185.68 • 216.18.168.166 • 205.185.20 8.142 • 205.185.208.79 • 66.254.114.32
	658908343Bel.html	Get hash	malicious	Browse	• 67.22.48.100 • 216.58.208.131 • 66.254.114.238 • 74.125.206.156 • 192.229.22 1.215 • 151.101.1.44 • 66.254.114.38 • 104.20.185.68 • 216.18.168.166 • 205.185.20 8.142 • 205.185.208.79 • 66.254.114.32

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	P178979.htm	Get hash	malicious	Browse	• 67.22.48.100 • 216.58.208.131 • 66.254.114.238 • 74.125.206.156 • 192.229.221.215 • 151.101.1.44 • 66.254.114.38 • 104.20.185.68 • 216.18.168.166 • 205.185.208.142 • 205.185.208.79 • 66.254.114.32
	03728d6617cd13b19bd69625f7ead202.exe	Get hash	malicious	Browse	• 67.22.48.100 • 216.58.208.131 • 66.254.114.238 • 74.125.206.156 • 192.229.221.215 • 151.101.1.44 • 66.254.114.38 • 104.20.185.68 • 216.18.168.166 • 205.185.208.142 • 205.185.208.79 • 66.254.114.32

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\EQAWN5DV\www.msn[2].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FED
Malicious:	false
Reputation:	high, very likely benign file
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\IB42RK38\contextual.media[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3172
Entropy (8bit):	4.844878245634065
Encrypted:	false
SSDEEP:	96:XKZKZKJKZKgKgKOKgKgK7KgKAKAKyKAKAKAK6K6KMK6K6K3dKjK6K3dKjKtK6K3D:a00E0zzBzzOzTT1TTTtfttomtomItoq
MD5:	E6D72352A8D8BA82324D2CB98E7C2474
SHA1:	D807AF6547FBC88054C1F1B86F6718BA0919C7C9
SHA-256:	D80FC98DCF8F5E2F179DF0BCD03D88D9091886831BC1CD6B24996DC302CA5DA2
SHA-512:	AEC305CC00BC2DBC38B3EE1A165B53F66184ABB4607D286FED7FFF39479D524F9761AD8C5C28DAB4E2BDD643CCB7861ED4A78CFAFC7887753B743725B29E3F4
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\IB42RK38\contextual.media[1].xml	
Preview:	<root></root><root><item name="HBCM_BIDS" value="{}" ltime="553006128" htime="30868682" /></root><root><item name="HBCM_BIDS" value="{}" ltime="553006128" htime="30868682" /></root><root><item name="HBCM_BIDS" value="{}" ltime="553006128" htime="30868682" /><item name="mntest" value="mntest" ltime="553206128" htime="30868682" /></root><root><item name="HBCM_BIDS" value="{}" ltime="553006128" htime="30868682" /></root><root><item name="HBCM_BIDS" value="{}" ltime="553326128" htime="30868682" /></root><root><item name="HBCM_BIDS" value="{}" ltime="553326128" htime="30868682" /><item name="mntest" value="mntest" ltime="553366128" htime="30868682" /></root><root><item name="HBCM_BIDS" value="{}" ltime="553326128" htime="30868682" /></root><root><item name="HBCM_BIDS" value="{}" ltime="553326128" htime="30868682" /><item name="mntest" value="mntest" ltime="557046128" htime="30868682" /></root><root><item name="HBCM_BIDS" value="{}" ltime="553326128" htime="30868682" /></root><root><item nam

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\IB42RK38\www.redtube[1].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\Recovery\High\Active\RecoveryStore.{5B2D87F8-70BD-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	111976
Entropy (8bit):	2.2490087099943112
Encrypted:	false
SSDEEP:	384:roNMCgCcCNCsClC9CnCyC+CtCaCMQCV1d11CQJFCVxCDCgBdFOdbC2CjCVCRdGdT:MVBbJSiVq
MD5:	3A7048D04B1962E78746849DF21F5BE0
SHA1:	EA619CFC38F6B1A09D92B777971F20614A8485B3
SHA-256:	06E194475BF7CD995A83E2C3034160477A1EA3E83165CBE301817AA333BDE17A
SHA-512:	46E2E9E4A8044A51E3B095C0208E5B91A57CCC1722E21463C2E092A09A1FFC759CAE1BAD233E30AACBC0AA925B161AB777BE8BCA74ED97556FF64A6A007AE0 F6
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{5B2D87FA-70BD-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	194810
Entropy (8bit):	3.5857337805403073
Encrypted:	false
SSDEEP:	3072:mZ/2BfcYmu5kLTzGt/Z/2Bfc/mu5kLTzGtn:feA
MD5:	5CF5A534B771884AAFA6A5D8A589AA9E
SHA1:	ABBBA646ED89402FB7B989A8B891CF2541F0EF1D
SHA-256:	8F8014D3A93ADF1878CFE1C01EE6ECE09245B2CC3094533E1805519AF85809E4
SHA-512:	D1ED8354540787A3E57945D2FE4CB0D219202EC218906A08537BE389544F47B4EDFD31FCB95220F160D2C45C88C9590982727C0AFB238110EF79CCBCDCF523E
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{8D06893B-70BD-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27924

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{8D06893B-70BD-11EB-90E5-ECF4BB2D2496}.dat	
Entropy (8bit):	1.8457957327612562
Encrypted:	false
SSDEEP:	96:rjZqQ66gBSEjl2JWLM422fXldgDx2fXldmGcr:rjZqQ66gkEjl2JWLM422XgDx2X0r
MD5:	9312C8019197D6678D65A3FF1C97F324
SHA1:	8DFD2D9D82769ADABBA6CD7E09BE2E60E59957CA
SHA-256:	C1F16965A3E310E93D9215E086DB6557A3297D166FA70A1D8A23CD32444ECC61
SHA-512:	15F80CFFEA98EC488F8912E82E889A154DC57CB226ADD3A9C5BB2CC4E6FA08207D476225647CA0A0E359672F1548132AD668D50FA00E40A801C8CC659A7495E
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9A78D51B-70BD-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	31344
Entropy (8bit):	1.6771859449923778
Encrypted:	false
SSDEEP:	48:IwRGcprUGwpaoG4pQwGrapbSL9GQpB6GHHpcUTGUp8EoGzYpmrnGopGNfajGyXpB:rnZsQ46OBSLjB2MWZMFsQ/N2tFJA
MD5:	E2FB86CE4535CEBB62740604D0A72AE9
SHA1:	B8FB0A0B8F04B8C4915EC60C020CAFE2A05E5F86
SHA-256:	91F9DEB94FD1920B4509CE367B595F2A1E76BF55515073DB52CE71602E545C9C
SHA-512:	37456F0A5C297EDFE91737F1A89A841061CDA8BC94A56B7D58C78F18C5862E122309D89A311F71A921582D97E3B7359A26D8CBA8426E2D5985572CBA5E51F4E
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{A9200887-70BD-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	31344
Entropy (8bit):	1.6752519800811727
Encrypted:	false
SSDEEP:	48:IwrGcprKGwpaiG4pQxGrapbSY9GQpBaGHHpcPTGUp8Y/GzYpmTBGopGBfacGyXpD:rxZSQS6BBSsjh2ZWOM3sJ/528FWA
MD5:	891CEC05C9E8C9CE211C942638BEF832
SHA1:	0745C0B157401F381B43402D9D3F0FB8950A4D20
SHA-256:	80E8DCD4697DCB133FDCD5750249E165F32187B545E62B9E7BBE977015706B36
SHA-512:	630AFC7A79F5DB46104C14EDE2EAB9233A6C94AE46AB901651EE7D4C76EC57D55DB1D107AA2FF6E674DDBE405A1A25B860268AC01F7AA54138797DAC54A538 80
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B78472F4-70BD-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	27432
Entropy (8bit):	1.8654256902371216
Encrypted:	false
SSDEEP:	192:rAZ3Qb6hk+j423WqM2ifDU4ghxfDU4gm1A:rwgeS4Pmr1fo/for
MD5:	2C02E9D0822C1C110E0320BB3A3058B9
SHA1:	73EF4CDB56DA80266CD1FD00F183C0489A06E320
SHA-256:	7E7D9F4B56E14873B312024E950A82B325343DA6FACA32F86876221BD68733ED
SHA-512:	A8311551DEAE47F635FCEF44AE5AABCD5F46589F9A223BF81B7EC41692156E404A07E344AD68A82656A09C0013140520267DE19B88DF2F93E53186B78E0E84A9
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B78472F4-70BD-11EB-90E5-ECF4BB2D2496}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.098487390045104
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEeuoquoy4nWimI002EtM3MHdNMNxOEeuoquoy4nWimI00OVbVbkEtMb:2d6NxOtuZuV4SZHKd6NxOtuZuV4SZ7VM
MD5:	2208FBE39C38A111CDA0F2FC3F47408D
SHA1:	9E90BC9E06A1B81D03D4E1DF5F80AA438D3AB325
SHA-256:	A4B74BCB53E12B377D2249EBAEABA3029857195B1EAC8DD98B5204D63F6BF761
SHA-512:	7C993E076743A3A3DBB9207A0191A4F843B8A0C734FB84F1A3F145CFBDD67AF03A6FFCF38E6828F2030FDA5E487DF037FEAF97E6B49C5EE1A49F9EC485277ED2
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x3238924f,0x01d704ca</date><accdate>0x3238924f,0x01d704ca</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>0x3238924f,0x01d704ca</date><accdate>0x3238924f,0x01d704ca</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):	656
Entropy (8bit):	5.093760111946404
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kr0wX0wy4nWimI002EtM3MHdNMNxe2kr0wqx4nWimI00OVbkak6Ety:2d6NxrJ4SZHKd6Nxr5x4SZ7VAa7b
MD5:	0B7D1AB6507E0495F71EC50418BB2F9C
SHA1:	8C7F1ECB5197341C05B14E139DDB8ABAE54CF0B7
SHA-256:	9565962D99B02040821B0B697AD61576108C1CE60BD40101CA6C756B4E449CE0
SHA-512:	40B6D549EACAB8491F1DE9BCBF938ECEF624B9846FAB63498302545A8D1C4DBDD283A2EDF8251A50CD4488641DC7FE9FF1462C82BFA444724FA96A5187865704
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x322f08af,0x01d704ca</date><accdate>0x322f08af,0x01d704ca</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>0x322f08af,0x01d704ca</date><accdate>0x32316b18,0x01d704ca</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	665
Entropy (8bit):	5.083611464246636
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLeU44nWimI002EtM3MHdNMNxvLeU44nWimI00OVbmZEtMb:2d6Nxv6U44SZHKd6Nxv6U44SZ7Vmb
MD5:	746FE939A4906D2783EE1C1846FB1B77
SHA1:	4D42A86AAD8E55BABC0DB94E88A3B308881ADDB1
SHA-256:	E0779E5FFA11861FC0796F1E0124775E3C76A5FE0D5733206811D2B763111F50
SHA-512:	5E4506B8FCCDD593E6CBA3E75EAA9BFFAC742ED5132C82DDB31AC31C05EBACE4E4E3A1769388C811353F130665D9664C93F9343F3B110DF9E28084C2FF60A63
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x323af49c,0x01d704ca</date><accdate>0x323af49c,0x01d704ca</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>0x323af49c,0x01d704ca</date><accdate>0x323af49c,0x01d704ca</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	650
Entropy (8bit):	5.085103028849672
Encrypted:	false
SSDEEP:	12:TMHdNMNxie8H8n4nWimI002EtM3MHdNMNxie8H8n4nWimI00OVbd5EtMb:2d6NxD8H8n4SZHKd6NxD8H8n4SZ7VJjb
MD5:	C6104C1E149805CC7F072934491208FF
SHA1:	B17E753708E2F741940C0AA795DD5AAB5E8E60A9
SHA-256:	F2F630A0B88FD27AD1ADE01B7CD06D74A22217292BCDDBC2A298D576FCB8326B
SHA-512:	EC81293FD24B239F71D8EE1B858BC7916D62D99226C559D10C8A9791DC992560DBD463B710B1012453416570F74156E7AA11324A399ED4E1B4483789B1C5D7B5
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x32362fdc,0x01d704ca</date><acc date>0x32362fdc,0x01d704ca</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>0x32362fdc,0x01d704ca</date><accdate>0x32362 fdc,0x01d704ca</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):	659
Entropy (8bit):	5.099606495149208
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGweU44nWimI002EtM3MHdNMNxhGweU44nWimI00OVb8K075EtMb:2d6NxQBU44SZHKd6NxQBU44SZ7VYKajb
MD5:	FD7EF7C8CD258810FB1D5137F90C0F15
SHA1:	0DCE67C64B1DFB6E91991D36213FEC12BC0AED53
SHA-256:	06594404B321B91C696846745D6BDD501BABCA0FF91380177BD9E82CADC53D25
SHA-512:	72505D1465BD4853DB082C8D48E48AC4E0FB8877308741AD73CAF8E2D7D1FDB6D1EA6FADAD7E39F3BA5891A62807F56DE65BDF77CB9E2B3F4ABFCF1B1F811 25
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x323af49c,0x01d704ca</date>< accdate>0x323af49c,0x01d704ca</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>0x323af49c,0x01d704ca</date><accdate>0 x323af49c,0x01d704ca</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):	656
Entropy (8bit):	5.102314745739643
Encrypted:	false
SSDEEP:	12:TMHdNMNx0neuoquoy4nWimI002EtM3MHdNMNx0neuoquoy4nWimI00OVbxEtMb:2d6Nx0euZuV4SZHKd6Nx0euZuV4SZ7Vb
MD5:	42518E6DE4E3C6B61067756E7DD15951
SHA1:	A2286727DB99BDD0ECA0F500FEAC6F250DDD6073
SHA-256:	F8AA78E20BD0BFAA436E00F8EF50180B9B3D6EF92797A44A55119CCB39C8EF03
SHA-512:	C025775A02B5204AB1FDE4A43F584AD4513B97BC10B1988B54A770D79B88633DDF9B5ACC1C3E5F4D7DCE4F34BF6C351B92F5B981C1F029AE0C1532FB97B9F3 E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x3238924f,0x01d704ca</date><a ccdate>0x3238924f,0x01d704ca</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>0x3238924f,0x01d704ca</date><accdate>0x3 238924f,0x01d704ca</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):	659
Entropy (8bit):	5.123548106255583
Encrypted:	false
SSDEEP:	12:TMHdNMNxxe8H8n4nWimI002EtM3MHdNMNxxe8Huoy4nWimI00OVb6Kq5EtMb:2d6Nxw8H8n4SZHKd6Nxw8HuV4SZ7Vob
MD5:	5BA519E6059AFEBBD9D440B79F86118B

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
SHA1:	1AB97E831AFDF886D9A7E16D2602DEFBDA4F9E8C
SHA-256:	C6A3F76D6EC3FBCCF289430E23BDA0E1DA6D95D3A7F6D2BDE2710E82440EA3DE
SHA-512:	E35EC75B5E964CC596A8434B617211F7AC2C98CF835600EAB87940E49D3867F883D838161E1D97C38D593F10683D1ECC148994BA5B9180E3ED19E0A2F7C3C0B
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x32362fdc,0x01d704ca</date><accdate>0x32362fdc,0x01d704ca</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>0x32362fdc,0x01d704ca</date><accdate>0x3238924f,0x01d704ca</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):	662
Entropy (8bit):	5.079499032731856
Encrypted:	false
SSDEEP:	12:TMHdNMNxce34Bq34By4nWimI002EtM3MHdNMNxce34Bq34By4nWimI00OVbVEtMb:2d6NxlIEIo4SZHKd6NxlIEIo4SZ7VDb
MD5:	89371D5F24181F89ADDC0BFB8A1E936D
SHA1:	3E94BC1C5858022D8EF1F09E2326D50AF1ADD7AC
SHA-256:	E2CECB5828640154E6F1C6EECC3D345199988D97BAACA0A79EB7EBC3B9319377
SHA-512:	A7EC5629EDFDE5C66A81FBE9F2E7AACF597F0938B538610E49BF12CE9C0030B31CBFB863F04E0856108A4AACB68469AD6E8DBEC300C58BCAB19B23A4CE58CA04
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x3233cd6f,0x01d704ca</date><accdate>0x3233cd6f,0x01d704ca</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>0x3233cd6f,0x01d704ca</date><accdate>0x3233cd6f,0x01d704ca</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):	656
Entropy (8bit):	5.070755001395612
Encrypted:	false
SSDEEP:	12:TMHdNMNxfne8H8n4nWimI002EtM3MHdNMNxfne8H8n4nWimI00OVbe5EtMb:2d6Nx28H8n4SZHKd6Nx28H8n4SZ7Vijb
MD5:	02C04685A3BF2650BC7DB76EB5258E5F
SHA1:	9E477E76C78F934CF70B798D29C8E0E3CFDED6DC
SHA-256:	2CF3C3E0EF3C25A4338CAFB2857A86F3CC427DC425A9A4E9DCF2EB6970165134
SHA-512:	7F84F1F3C3BB78DCBCDF575B788D24C45B77A2B5D3A701A939B8C53D7EAA9BD08DF1B61ACF4A57F7FF419FBB20CFA629ECD0FAAF56B817448A663F5D53A39FC
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x32362fdc,0x01d704ca</date><accdate>0x32362fdc,0x01d704ca</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>0x32362fdc,0x01d704ca</date><accdate>0x32362fdc,0x01d704ca</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\wlm7n14\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	7372
Entropy (8bit):	7.88293022117834
Encrypted:	false
SSDEEP:	192:f0fSy3NwU5TIm/ZppBpo2UesiW7xLoo6m:sf/tTIuZpFqeQ6o5
MD5:	B7A0CBC051DF120E998BFA80C8068AA1
SHA1:	F160D16742E25046158465B0E986036B8F64E386
SHA-256:	C5076B5979BD9A6D95E29C5E49E40BBB24EB00D3F67513CF1E4B174E9E4AFFD8
SHA-512:	D290C2A1E3CF98765BC554322A0D60EC13E8B0A8DAF6FC67AAD249D80A80795F1EA07DCC0761EE4777E85A76A4AA11B19F948572F8809692C7315F3F3EDCAE
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat	
Preview:	o.h.t.t.p.s.:././.e.i...r.d.t.c.d.n...c.o.m./.w.w.w.-.s.t.a.t.i.c./.c.d.n._.f.i.l.e.s./.r.e.d.t.u.b.e./.i.c.o.n.s./.f.a.v.i.c.o.n...p.n.g.?.v.=.6.f.5.2.1.4.7.9.6.2.2.9.4.8.1.2.4.4.d.c.0.3.c.6.1.2.9.e.f.d.7.9.f.6.0.b.d.5.5.2.....PNG.....IHDR.....%.\.....sRGB.....IDATx..].x.E.>...!..H."-..4C... ~.....E....C. .....(.]..:!...$!..$..@.....e.....gggO}.=[fwf|..oZ.../E...\.*..j.....,kv..ee...6.h..))AA...I..RW..T(.....0c..N.@..).....(X....=..bq...J.E.q.I....QE.!...P...=...I.G..w....+.$...."....Q+.CH.Z"O..F....w....JV.q..."...c...Q...D..q_..Dj..-.y.@.I.....u).zQ{....6.R..uOPy...[..]V.>z...YE.J.....i.).yRJ].....c.c@]..DS...k..Y.Ux.@._.X..t..sF{.$..Z.Z...^....L.so..U!...VdT.,..z ....i.....T..<.c.....c .=v.....4oe=(,((f5.AI...9....k.@.g...+f,..?.....R.h..Z....2.m.Fw.5.k..A1..v.^t...9.bm...q.;.$.7...@.E`h.b..w<..".1.?J.:.].k...T...Q.D$:.+.....zh.#..(.....Z4h.>..O.Z....>~~ZH..d.;.k.c....!:..%.....K.....K..1.}b....|.%.....M.....8.cb.^'.9 *

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\mms\9GUNE2VU\409721[1].dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	589824
Entropy (8bit):	6.264033516229162
Encrypted:	false
SSDEEP:	12288:BeB03pEkmGuDye9Cc1zQMeVGkMItIOl5F4OVMS4iuvf:Q7kmGuDB18Dalttd5Vj4RX
MD5:	A10D802BF8B1EDCE5FEA1D212F0DFFA4
SHA1:	0FF32BCE3AAD381171926ED7D783995A93700D69
SHA-256:	2EE0D0EED52ABEB570D47318CF11C1F522B94B00F48DB97B8EDA25197C7DFDA3
SHA-512:	C6ED5D77B0B07328CD3F74391DD8FC2A8385867C9DCE11F491DE2906FF43DCD251C68BB905E365F9609589A4678E39D27C827216C2C2D6579815A0E76B75212
Malicious:	false
Preview:	......4L3.\.... .#...2>z/.3..8...$..`[...g. .../V..A.....m2h...{XM.x....^.:{k.P.[....b..c ..J0N..).R.j.d}d...z=m.-:.*...`.h]<..N..Fr..p.....F..K/.D.3i_.+@.t.Y3d.H..w...z9Z...\9w...0..w" ..RN...._..(...a.....-mWd%~..\..w...).ot.?l._.Wu...E+).5..0.Tyz..H" .J`Mz%.9c..;..F_...t-....q..^C.....p{"c..?.....zm.....N..8,v7\.x...Ad...._z.Nmk....-r.O1@.^...F.i._..a/..h.h.FKA....$..M\s3.b..~BA.A.[.:.....)zI.m.Lf.....F.W!....Q..,kM..t;.=^...Yw.MY.j.a.q...&Z.Z.i...M.t.S.....:.\.].p..|`x..<....&..)_?.7.A.....p'..@.c....<.$....5?.....uF.....`sR.3..G....`...x.\s.N.1V.X.I.z.T..zZ.*...(.cL.}..6>.....Cc.....T.....EG4;.x5...h..3[.....0x...O5.....$.^...uL..^$SS..4.j...G~...9.1.i. .....,...i..#.....>.E..G..O...q..q.a8.#..?..A.;..%U0H+.z:a..;....c6[.c+3,=`.F4.R"t..t.....{.Y...O!..8.W*.|.S?..R....&.M..F.....|....<...{.8.0....C...@.y5.sp.*?.xgm....re.t..._.`1Z.y....U1.....[..Z...1...v.\".B.. .?.2...[....iR3...A...tE..u.J

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\10009606[1].htm	
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):	20732
Entropy (8bit):	5.6321176140669635
Encrypted:	false
SSDEEP:	192:+i6rMA8yf+yXDvqzaFASuxeCUMyyX8H9t3JqysSC/SElM+isWDs7ObNUv1kruZ+d:mrMA8yf+c6sAOCeVoys9z7ObmKrmDs
MD5:	0756357287623CBA5A3A148D4075F0C9
SHA1:	B8018C5331C9B9CEE12584746AEE929E9EB907FB
SHA-256:	A42F2F2CA5CA967BB26DF5B15F3CF6FCCCF85D7998BF3CB4F955077FE8D285F8
SHA-512:	28F1F198E77369E447A50E654FBFC978E4CA903C931BFD27C018993F7F1F57F34CF6AD942448EECE8D24B441835A128C09D8C9337492678CF02A7805C0FEB47B
Malicious:	false
IE Cache URL:	http://https://a.adtng.com/get/10009606?1=1&uuid=7914946031748631396&impid=43_1613492148363030103_35962_1016&tj_zid=11531&tj_cid=1005167111&tj_aid=1476640231
Preview:	<!DOCTYPE html><html lang="en"><head><link rel="dns-prefetch" href="//ht-cdn2.adtng.com"><meta charset="UTF-8"><meta name="viewport" content="width=device-width"><style>body {background: #000;height: 100%;margin:0;padding:0;}.container-fluid {padding: 0;margin: 0;background: #000;}.ad {position: relative;display: block;width: 315px;height: 300px;}img#logo {position: absolute;top: 0;left: 0;z-index: 200;width: 315px;height: 300px;}img.fallback_image {position: relative;display: block;background: #000;z-index: 1;width: 315px;height: 300px;height: auto;}video {width: 315px;height: 300px;height: auto;position: relative;display: block;background: #000;z-index: 1;}.IIV::-webkit-media-controls-play-button,.IIV::-webkit-media-controls-start-playback-button {opacity: 0;pointer-events: none;width: 5px;}.canvid{width:315;}.adaptive_video_player{display:block !important;}</style><script type="text/javascript" src="https://ht-cdn2.adtng.com/delivery/vortex/vortex-simple-1.0.0.js"></script><script t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\1018141921[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 950 x 250, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	266318
Entropy (8bit):	7.984577108629215
Encrypted:	false
SSDEEP:	6144:G1Dv+30F5W58kwQP9gHi6NGKtbKVC3D59MMKE:GVvVm5pr0i6NrwGDUS
MD5:	43F4A5683EF4E64197EBCAB4BEF5C9F5
SHA1:	C4BBB71605C2B297A39C3605CD439A8411117C85
SHA-256:	CEAADB3F4CC1F40E8FEE82090B657E7CF61BD2474FFB528877AAFC457EE07E2F
SHA-512:	9D84FEEE3074E6A5A89FD66B7997BB6A1873C68BDA2B17A31B309713EF55768710F312F6D7765126DD34447645810D1DC92AA885AD6A9FCAEF202A38A5DBC0F
Malicious:	false
IE Cache URL:	http://https://vz-cdn.trafficjunky.net/uploaded_content/creative/101/814/192/1/1018141921.png
Preview:	.PNG.....IHDR.....LE.. .IDATx..y.]Gu7.....<JW.5X.,y.....b0..S._R&P.JR!/....T.^..I..y.....16.....e[.$.,].Ww.....n.{. ...)-[...w.....`o.....?n.]..W:.1..@.....f@`....F..!."k.. $p.....`.A.k.. .0 .....00.3 .3 ..".7!.....H..4.. .2"..HD.0.....(@.....R.... 3.A.@.!...a!.....<b.A...Z.3...`d.....8...u...(% .$@d..2..1... .<\hS.m!:...#...."#.D.J+`3.....S.:k.4..i8hk... ...0...../....W9...p..../..,W.sc.g.H.....{..(.H@BD`.3..|5 #.i.....D.W....X..#&.....}.-...+...`..|1..v`.....~..".1f....33.|.4.s.j..c.....S.ND..]zQ.m.vC.4.....k5./..^k...*e.....Q}.."....e..0....l.n.....o..+{.?.....{.....WN.{5....T+.7+...F&....L..s.m.0.....\X-.a..s`.R.jA.'P..Qb.. W.C...~&.e.....PP.$.HJ!..V*I.J.....$2..X. 2.\)s.\.....jF..k.J.\..+l.|?..7..aP.T.a\CB.....p.%t.. ...q.YJ....y..\.....5103....u.D.....8Q10;....|.GD.:_.vu...4.r^Kk.uhfj|rb,.....A.6.,..X . d2."....c....}..!r.L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\13[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, 304x171, frames 3
Category:	downloaded
Size (bytes):	12502
Entropy (8bit):	7.949015024281783
Encrypted:	false
SSDEEP:	384:UzXBkuYIZ8aDoBjAHVLucqXvK6pxmPKE6aMAtp:0bYzF01yHfDpxmPL6hAtp
MD5:	142582611F479702A43EC6B7032CCEFB
SHA1:	8133661829261FB2665DFEB7797E457920677A81
SHA-256:	989CF3206156828AE6B2415C6D5FDC37EAE1A01FC53F95D6F0F4E2277F204792
SHA-512:	8A2E39CF045846D71978926207DE3FCEF7108425238A94F854B7BC36D5ADA0579024F05DAB10EC849DA796A51350145E26043E69B146C6C41CE4A6F1FC4DD9F(
Malicious:	false
IE Cache URL:	http://https://di.rdtcdn.com/m=eW0Q8f/media/videos/202007/11/33841811/original/13.jpg
Preview:	......JFIF.....C.....!......"$".$.....C.....0.."..... 2e..`B.....W=\..h..A...!N_.....B1.Ck.~...jk..q.5.m.!a..... l6...#....1..#B$.0(.ECG.....$.....1.....,..Xf.!1.|...].0sl..i4,J.....|.....^.F..22.*.v:.~wB..)@YHy#.G..O.q[FB.....3..c .E...6..3..\i..$....X..*.n.E.$.8....$m.m...L.....q].s..1.....;..H.j...=.w....2Q".EaB.[&..+..?-)..R._...9.:.3"`....H`-...6k.....J...J..d.....9.....\].....h/.$.....Br.XA[.....3%....r..=..>.....Y. ....xd...N3F[....6.p.1...I.j.4p.T.XM4.k+....I..s.....<.....T%..g.I.. ..q...R.cT.b<.h....8.-;h..Gi.....=..".8...o49.{.%i...2.I.769...3g$U../"4O.#4.f<M.f.-I.H.....u-.xiB...r..N.J...Z..u.g.}. ..Y.bV...SMr.v|..;#.L...5...o.....F..)z.....q...K..w.q.z...9....._1...^.....<M.iI...].I.]....E.y..{I.^U=a.m.....c..NOIz...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\2[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, 304x171, frames 3
Category:	downloaded
Size (bytes):	12687
Entropy (8bit):	7.945750330667033
Encrypted:	false
SSDEEP:	192:HyDGfw87cEGNWDSK5u9g65Vtxtu2606tlcCAd5qmTNvvw83NpVs:SSfxcEo9Kn65xtuWc58GNHw83Npy
MD5:	B6713D9B745EE19802117F846474926D
SHA1:	09B125F4C578031C2C9E68DFA289186C430529AA
SHA-256:	0AD2126AEA04940EBDBA9E0958E0F4DD8888BE37B347B27EDF042CE6F4D2EF94
SHA-512:	2CD24E2A02108D0152D9E49CE2CF01CA39CA941CED0845F9FEF448DCD2A6EFDB17225DA8C265D983BB1A104025120B98433925ABF97C1A23E5C908858E040C 5
Malicious:	false
IE Cache URL:	http://https://di.rdtcdn.com/m=eW0Q8f/media/videos/201910/09/22850761/original/2.jpg
Preview:	......JFIF.....C.....!......"$".$.....C.....0.."..... ...so)*;.W...H0;...C...8t5..cr.....8.....J..v.....-.(z%.$OR.q.1T..E?O....B.)IP.e...i.%.2.Dt9...N6=e....$F..^..`d.q..j..p.^%R.4^.TXj.F.O..KM..S.....1.....%..(o2.}....2..L.{...'".[..4. ..}6.Js.....IN=..oN.5~.9.....=.mR.k.....$k.8.....>:.....Q.Z8s..8.D.p...G/ur.z..c.eV...m6.....mUi...Q...(l..H...s....y=a...^.1*..2]o,bvH.3....ki.....!...t.../F.Y.U.....[.;.Dc..i..d.y*+....jd. G..Y.c.....fB....H.3.....O...&$..2.`..P.....F...q'Z.pz.Z.`.^k..;J.89.Tv.:...SO...0.....rGG%D.....i..8..k..E.0...s.....`..Y(R3F.&....E.u.i....hu.E....x.di*)a...E.....H.z..:.....t.u.c...d...it..; a.....$3....rd.....u.VPN.5sm.b....Vr+v...E.T.....x..L^'pH.L..~.c....L..[.x7".S..R...%.Z.A....0.Y..?-`...v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\409711[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 315 x 300, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	135570
Entropy (8bit):	**7.992579878890036**
Encrypted:	**true**
SSDEEP:	3072:cVqkYVr2y0wvrW1ofyH+iclo52N4U7Fof:sqkOyJoraH+icg2Nv7F0
MD5:	4E3C86CA72855FAF53B7CE0BAA6A5EA9
SHA1:	9BB096205F6CC2A79D22EC4CF5D0EDA69575F0C7
SHA-256:	B86A148E0725BF73A574109B7ED452110FE86339F44647C3EDA343408DD69F70
SHA-512:	19775D29D3378BAEBAA441C9CEFB61EEBBE494964877DDDEC7F1E2C3A13DF6892CB27C1BB24D4E555735B264DFA7DE000495C0F47192D272E566A4E140EE51 D3
Malicious:	false
IE Cache URL:	http://https://hw-cdn-ap.trafficjunky.net/uploaded_content/poster/000/409/711/409711.png
Preview:	.PNG.....IHDR...;...,.....8iTXtXML:com.adobe.xmp.....<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?>.<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk=" Adobe XMP Core 6.0-c002 79.164360, 2020/02/13-01:07:22 ">. <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">. <rdf:Description rdf:about="". xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/". xmlns:stEvt="http://ns.adobe.com/xap/1.0/sType/ResourceEvent#". xmlns:xmp="http://ns.adobe.com/xap/1.0/". xmlns:xmpDM="http://ns.adobe.com/xmp/1.0/DynamicMedia/". xmlns:stDim="http://ns.adobe.com/xap/1.0/sType/Dimensions#". xmlns:dc="http://purl.org/dc/element s/1.1/". xmpMM:InstanceID="xmp.iid:4b090224-bca1-4f41-8084-9e785fe2b565". xmpMM:DocumentID="32487ef8-9fe0-7b05-f1ed-539e0000004f". xmpMM:Origina lDocumentID="xmp.did:c971dab5-620f-bd48-a59c-c1ba83d783f9". xmp:MetadataDate="2020-10-13T12:36:16+03:00". xmp:ModifyDate="2020-10-13T12:36:16+03:00". xmp:CreateDate="2020-10-13T12:35:46+03:00"

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\58-acd805-185735b[1].css	
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\3Y2ADQKS\85-0f8009-68ddb2ab[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	391843
Entropy (8bit):	5.323521567582823
Encrypted:	false
SSDEEP:	6144:Rrf9z/Y7Sg/FDMxqkhmnid1WPqIjHSjae1dWgxO0Dvq4FcG6Ix2K:dJ/Ynznid1WPqIjHdYltHcGB3
MD5:	CDD6C5E31F58A546B6F9637389B2503B
SHA1:	0ADA1E1C82B8E7636F6DAF4CE78D571C80A3E81A
SHA-256:	4CC5BC89E9F4E54FE905AB22340FA3793FE04F30453DC17CE2780D61DB35D5D4
SHA-512:	11FD84FE2EAB4FFEBAF45D8D509E7E8E927540A3D67CCADB65AB7C7A7F22F1922411A02157B404D2CA652D6AEF8809B659C0D4106F2F57B6B02911D85B06A4B
Malicious:	false
Preview:	var awa,behaviorKey,Perf,globalLeft,Gemini,Telemetry,utils,data,MSANTracker,deferredCanary,g_ashsC,g_hsSetup,canary;window._perfMarker&&window._perfMarker("TimeToJsBundleExecutionStart");define("jqBehavior",["jquery","viewport"],function(n){return function(t,i,r){function u(n){var t=n.length;return t>1?function(){for(var i=0;i<t;i++)n[i]()}:t?n[0]:f}function f(){}if(typeof t!="function")throw"Behavior constructor must be a function";if(i&&typeof i!="object")throw"Defaults must be an object or null";if(r&&typeof r!="object")throw"Exclude must be an object or null";return r=r||{},function(f,e,o){function c(n){n&&(typeof n.setup=="function"&&l.push(n.setup),typeof n.teardown=="function"&&a.push(n.teardown),typeof n.update=="function"&&v.push(n.update))}var h;if(o&&typeof o!="object")throw"Options must be an object or null";var s=n.extend(!0,{},i,o),l=[],a=[],v=[],y=!0;if(r.query){if(typeof f!="string")throw"Selector must be a string";c(t(f,s))}else h=n(f,e),r.each?c(t(h,s)):(y=h.length>0,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\9[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, 304x171, frames 3
Category:	downloaded
Size (bytes):	11583
Entropy (8bit):	7.943825788713623
Encrypted:	false
SSDEEP:	192:yOWSU32NotW54ALNG1sYpe6jSnwt5XvUVdC1aAvvOjFR8Pz8uy8UN2YNX3o:yOWSU9OLlWY46unZVM1a8pPguId3o
MD5:	BEAFBB5F2790B328CBF4630029998E77
SHA1:	8B1B53239712870EF85EFB41F5C90022E203921E
SHA-256:	CC3718CC7F12945D7DD881CF486F505B45DE46C79E5E9EAEE7AD4C909C1EA3E1
SHA-512:	01A21789BDC1BD943FE1746B6F784B5B8174F8407BB3EFB53FA2A8363AA0564FAE64485577BBE58E935FBF898C6ACFC4E8B09C00AF6F4A1FCF244923C6DB9995
Malicious:	false
IE Cache URL:	http://https://di.rdtcdn.com/m=eW0Q8f/media/videos/202011/16/38051871/original/9.jpg
Preview:	......JFIF.....C.....!......"$".$.....C.....0.."....{ O..Y.....Y.....@.!.1....u.....!l.d..l..l..d.....Ig....&x...F.....Nr..c..O.m..g.r.E.....Z)....N..K..\.%...s.}.:.\...D."#.-.|.3:.hY....>..4.....>..i.g.y5..S./...l.{.&,..d...c-5.....tA2I.N.gI.I..Ie...H(..z.. ...GO...N.F8..M.....X.}{9".n.%...M.IPYKcj.sK.a.O..t.b..HU.....6.,...Q.U...s...3M.31.....X.b..4..O._..S...'.....s...i.Is.5...<..e$6.....*..>{e....B@l..\...Sg..1...`& .l....7;..Z.h.U.R:.F .....7C.0..E.....c..\0I.d.%.k./7..:....Ay..-..2L...n..2.kJ...P9I.#..".-E.7.@AwD.E.)....7...3F.Y!.....H.. d%..R...:.T ...Jf.....2.w.#9...."...f..1$fwqC.rNx.wUv....=...3.v\..&.Dl...I7 ...)..."}.D.....%..E.c.l..Z".po...%.>h.....<.....2.....wS3.^.S....u7t$.v/...7 Y....K..1..#....yN..X.....^....vj.x.MH.

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\AA6SFRQ[1].png	
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\3Y2ADQKS\BB15AQNm[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 192x192, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	23518
Entropy (8bit):	7.93794948271159
Encrypted:	false
SSDEEP:	384:7XNEQW4OGoP8X397crjXt1/v2032/EcJ+eGovCO2+m5fC/lWL2ZSwdeL5HER4ycP:7uf4ik390Xt1vP2/RVCqm5foMyDdeiRU
MD5:	C701BB9A16E05B549DA89DF384ED874D
SHA1:	61F7574575B318BDBE0BADB5942387A65CAB213C
SHA-256:	445339480FB2AE6C73FF3A11F9F9F3902588BFB8093D5CC8EF60AF8EF9C43B35
SHA-512:	AD226B2FE4FF44BBBA00DFA6A7C572BD2433C3821161F03A811847B822BA4FC9F311AD1A16C5304ABE868B0FA1F548B8AEF988D87345AEB579B9F31A74D5BF3C
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB15AQNm.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=868&y=379
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....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..IR2...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\3Y2ADQKS\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.S.i,..]........)..N...Xn.U.i.67.h.i.1I>.....}.e.0A.4{Di."E...P.....w.....|.O.~>..=.n[G..../...+.....8.....2....9.!.....].s6d.....r.....D:A...M...9E..`.,.I..Q..],k.e..r`.l..`..2...[.e<.....|m.j...,~...0g....<H..6.....|..zr.x.3...KKs..(.j..aW....\.X...O.....?v...."EH...i.Y..1..tf~....&..I.()p7.E..^.<..@.f'..|.[....{.T_?....H.....v....awK.k..l{9..1A.,...%.!...nW[f.AQf.....d2k{7..&i.....o.....0...=.n.\X....Lv.....;g^.eC...[*).....#..M..i..mv.K.....Y"Y.^..JA..E).c...=m.7,.<9..0-..AE..b.....D*.;...Noh]JTd.. .....pD..7..O..+...B..mD!.....(..a.Ej..&F.+...M]..8..>b..FW,....7....d...z.....6O).8....j.....T...Xk.L..ha..{.....KT.yZ....P)w.P....lp.../.....=....kg.+

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1cG73h[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	917
Entropy (8bit):	7.682432703483369
Encrypted:	false
SSDEEP:	24:k/6yDLeCoBkQqDWOIotl9PxlehmoRArmuf9b/DeyH:k/66oWQiWOIul9ekoRkf9b/DH
MD5:	3867568E0863CDCE85D4BF577C08BA47
SHA1:	F7792C1D038F04D240E7EB2AB59C7E7707A08C95
SHA-256:	BE47B3F70A0EA224D24841CB85EAED53A1EFEEFCB91C9003E3BE555FA834610F

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1cG73h[1].png	
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\3Y2ADQKS\BB1dIWNG[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):	31657
Entropy (8bit):	7.953609989496633
Encrypted:	false
SSDEEP:	768:7SKzUWNCp30+go8a5WEVg6gL4crgQaSav1/fNC:7SW4t8cq6ylrgQHavq
MD5:	75154A46DACA6A1C8D6387FA11383F13
SHA1:	E17C8232F1CC528897BD6DA39D46CC24F6BDC736
SHA-256:	99556C3F74D394396C91DACA2EDD70D239D2C0109238578600B0ECB9D6A69686
SHA-512:	44BC4A1103AA8A122E4E56C2CAF30C22E2A350D6378B1D9ED7B86A1FE746327A20FB76A37B3009B7E6CF901A65E70EC65C980C05D0C640C862FE694635546D7
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dIWNG.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=1635&y=1278
Preview:	.....JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOOOOOO.....p.n..''.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?...Zo.J...QE....P..IFh.h...(...)(...)(...JZ(.(..@.E.....-.P..IE.-.Q@.&)h...)(.....(...J.Z(.H(.h.....4.R..)3K...'4....0..QI ..Z)2h. ....i.~4R...K..!.y.NG...Z`|K...@.RQG..w.E.Z>..R.....'8.u.$....h...R..h....-%&h..R.Z@.....Q.Jb.E&h.....~.....4.....h..1@...)h....@.IE...Hh...E..P.E.P.KI.;...IK@..Q...ZJ (..4.3E...QE.....4.Q@...f..(...3HM...3Fh..=(.....(..Q.P..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1dIyJo[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):	33720
Entropy (8bit):	7.960738170360026
Encrypted:	false
SSDEEP:	768:7+a10DT3jV7rmtieBdKG538r9Ms9T+4DwLOLPHmyvfkzEJxlW:7/2DT3J/6ie335mN9kaH58oJxc
MD5:	BEFCFC553A30BAF11243409150F3813D
SHA1:	2A4467B21C94D2D005F1D0088149A610EA8BAF21
SHA-256:	56ED932DA7197D84C156AF628F16CFA967BBD848C9DE60FE00FC89145E5F6CC9
SHA-512:	DCADE55559BB2548F35BC0BC71E6E50CC298E853D78DD4256FADF236C6F98B71472910E67D448BBA5112D922362BE7C105DDB3B3D488D9653FC2EF30E47D7A 6
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dIyJo.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 OOOOOOOOOOOOOOOOOO.....p.n..''.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..j(..aHih.....(....F;..4....)(....(....R.P.Q...H~....&}. R...&..x..PSJzP!..b..)9...~..4*.i..I..)..HO.(.$. +M).K.A&.....&1..M? Z.0F...r)2i.....O_ZFr3.+.sQ..bl..9....].!.O.0m...P..RFrc..>}z..7u..iA$`..~.,...51.I.....iI.....a.-....rq....f.9>....TRE..8''.mO'8;.i..V.1q#.....O.2A9.....C..<w..$.3....2.....sX.v..#].pO*}*... {.....%..T(GQM.V..M...U.f.A..Z.#6.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1dJ26y[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):	23477
Entropy (8bit):	7.939629881591871
Encrypted:	false
SSDEEP:	384:7ChBA/QqYlW4BYdqX0AKq2SwN1q3s0CG9YkNQ4tJdog4BZ9W3YqYGTklXSoXDpoc:7ChBAlvuqXkq2Fvq3h9YkNQSog4g3Yqi
MD5:	42FBB1DFC67671A2C824F040238A43A2
SHA1:	9230ED9053074D8B3F3EE6986A51F8C8C768F3D8
SHA-256:	FFA08DAEF72AE8730B4234FA67334B9002E08954D50B4EF6D570C89D1556A05D
SHA-512:	59688BC9F47EF3EC3004424679AF1B81F06182364FBB98C3EB84FBDDA2E5AEBF74F0E7D42C4DE249B229387879026F88CC4292DE887BDB8EF6CB284C4CCB5B 5
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dJ26y.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=550&y=661

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1dJ26y[1].jpg	
Preview:	.....JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..4Jc.y.g.].5}.|{{.m.-..Z.Y.[...6....5Sp..Z.Nd..i3.z..{.X.*..o.....b#.8.....ey852.U~Z.....S[N.@.T.W...4.(W.3I.-.g ..Y..2H*..,..m3...`_.;...5.9...Z.D....6(.:....)E0*],...W.NN.Z.i.h.(-R!..`...A...f...|..E..\I...Xr*..bv.Q@.}....M...$...V.vQF8Zr.+.Q@..."P.I...bW...)..K..>Mg...A..D[.4....@.....*..A3..S.@.Z M>...P...,c.Z...e.... .Tr".....A.]-....).YF.n`+Q.8...)\eT.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1dJ53U[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):	7216
Entropy (8bit):	7.923896523194403
Encrypted:	false
SSDEEP:	192:BC3QrmY4q3Nj+X8XIQi73euGzx01UwVR+7r0kBI513X:k3e3Njjm4aRR+kJ513X
MD5:	D6249190461AB068544CB4B3EBD0EBDD
SHA1:	19986F345ACCE2C23C9FC2912FE61067BBFCE960
SHA-256:	BD6BFBE5ADC8F654B53A8706D3F47725BF2F96279066AE6643EB7DCB92F7D01F
SHA-512:	0EB4505FF30899663B26A61653EBAC4529B216B0E360655BBFEFB9BF254BE84B6EB291757D12F8B7546899D7CAF6EA939893A111F8AD777C35E15DB3437F5AC1
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dJ53U.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=525&y=272
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..E-.....\P.b....1F)h.u....]..L...C.H.....6Y..l..:.".5.Uc..1..6....c.2?...n.,NU. ..?Z.6R...$..c..j....G.V..[...>cY.d..iE..?..L .&..).nJ..[..XR.\..GbT.Wln.").....KE.D..)..Rb...J)h.....\P)q@....\P.R.K@.+;T.....>....K7.....+H.9..(..3.....A..9..~:..a..d.....[..#...V.....),...\.B...?....&.&.eNx..E...?...X..z.}j..,I.P. V...i#M..`w...b]B...#..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1dJct9[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):	7944
Entropy (8bit):	7.936162480196688
Encrypted:	false
SSDEEP:	192:BC/URo0KPrTbGdZc/vhD4qUCuzb6XjWgLdUrXTcSku3zFavt:ksuXGZcHhEMuyCgdUrXT9L3zI
MD5:	EF0146C5C6B59A65DF476D633082F692
SHA1:	C393C07AB32BFB7BA7B40D899835E952195B010F
SHA-256:	A6904D777244D30A63127BCFC5A503E349F62653A264F81401C7C7FFDE71D9A5
SHA-512:	B6CFADC532EA6B54BDCFE3F1D07147E5629DE96B07A02F4DFD99D7F0E3C252E1025E2D33DED75CE90C439CC02EEC709E7572F407CE333CB977275BB079120 57
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dJct9.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	.....JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..;Xu+...X.u.... .-....G...u.)!...-...c?.`x.....@.)...7..S.N....(X..Z.i....F.....T.K{..Ku..^g$&.....u..K...s.*.H....3.NX..+ ..c$....g[....*6.....i..y'V'&L..SC.!..<d.r....@u.^....:b.8d.a[5...*.o..m.....l.q<U.T.....Wc.....A.e..%....b.z;..].....v.k)9}._....E^...q...67.:\...2<.....v..f...q.<.. .Z.t~V.....r}.S%.w....f...}.a .V...:'...Z..i.....5i.8a.5...W.f..0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1dJeLF[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):	13852
Entropy (8bit):	7.945689629224677
Encrypted:	false
SSDEEP:	192:BYzFOJq7pU0+Heuv3n4+ArvuVB302Yyln8gMKjrlmetF7AOP/+sqa0B03HPCFLLk:ehOJFTfv3/V/58gMkx7/PaHsHPmexwm
MD5:	9DCAA872081EE05150E27DBB4FCD67A0
SHA1:	4BFECCD4EC97C5919D38C4F5C5572CF6A21B8820
SHA-256:	052E0996C0DDEACE5CF33664B0D9526BEC3413584DA8E1F521C790DDC205EB40
SHA-512:	29DCA4C12A9DBB234768FEA622C1F0E28265823A02BB08E0BB43B96F0A88B561ED243F667F65CD2FEA509120207A1AAD5E1AA5D63B7312691306991273 1EB7E
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dJeLF.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1dJeLF[1].jpg	
Preview:	.....JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?..i(..C4.....4f...\.J(.sFi)h...i(.....J(.h.%....4.P..3E.....a.jz.fK+)....U...U....r.PK...:.E....E....J.(...(...(.. ..4RQ@.IE..QE..Z(....(...(...(...(.....Z)(.....(...)..`..'..6.....n....E....y.)0=.I..M.....;....a....!u.;..CG..h.gp.N..F..+.)m.....L.E.B..0+.tm.l5Q,.s...). ...&4....].yf.v."P."..z..r.;..v...[ .)2H.`.8#.}..f....E.S.QE%..QE .(...(...(...(.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1dJmD5[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 310x166, frames 3
Category:	downloaded
Size (bytes):	10386
Entropy (8bit):	7.947497747751832
Encrypted:	false
SSDEEP:	192:BFW/oFn+EA4amgMOqQykxJolhwTWCceZgSm7Vkv7WicnqNM5ppu6Nh93Qog:vl+E4mgM+HI/CcGgjKGnqNkpnAN
MD5:	04F0AAE02374B1F777E73E2793559C09
SHA1:	A345D007C751B15E0437F174EDB8CEEC358838BD
SHA-256:	3FD766A771723F6776B04B09EA43CF5C071E7C53113712B14B029022D531A434
SHA-512:	5E503676556D162CE3E22EA5B467E241F2AA8BD58A02CFA1A350109DB179C1B3C3A559924745B71C90BE85E8CC4B0FB37DAB6E3BC90CC4C967539FCA001603 9
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dJmD5.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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....6..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..`.g...o.rT..Z.. `...3..G&....R(.....8LqH..p=s.@..S.....`.i{.....E....pp...w.....Q.V>..r..l4.Tz...Q..M.GZ.....F..K.... .....u.v=".HO2i.....>".UV..1J.%I.#..^.kqa.\]k.bx.6[.....{.n..\.\...@:..q@.....Y..8D...?: .;p...?...NMCc0.K..3;..(5.j.....k{.h..bR...0/.F#...s.....1.2..=.*..q.f&..A2.;d.@C..T..y..SO... m....;..c.C.....)*....\..Z.h.(.rrB.SS"$J.@..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1dJmLq[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):	12001
Entropy (8bit):	7.940265361206707
Encrypted:	false
SSDEEP:	192:BYB68ia6APD/vs0HRHuDGRt6s3UgY8P3q19bMccIEYU0:eBytis0HEDwkgjP3CbXcIK0
MD5:	9DC2EC4A7806F824337299B13A297B0A
SHA1:	1818EA9DD7928437B337A73AD4C610A822004306
SHA-256:	A42711AD1D03D59D3787113DADFC44DD1A8C9B5426B1B87235B93C1BE3B8AC1E
SHA-512:	8225DAD41495253EAE43870256D4AFBB2C46FBE9F6964B2BFA639174BE9B34FF077A4E70D658638956B1A4467CE8655F7A196B148CC5452DC6698EFCB05159D9
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dJmLq.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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?....S.....s.jz..(.u4w.....e(.1..`4..(u%....K.JZ.(..H....4f..E74..AF)3Fh.h...h...f...b.R.h.1I.Z).....CqJ.. (.....Q..i.^Z.zUI..D..- 4U.....@X.`..Y.9Z.....tO.j..H)i...4.Z.....QM.4....ZJ3H....C.KM.....JL.....f.KLB.4..4...(4.....f.4..4XW..3M...c.K.....KM.R....R..J(.(....S....R..H..".).*.....])..S....+ .....pT.T.I.SG2.Q...[.|1..6..{V.....*z....P9..)....8

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1dJxQ5[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):	24511
Entropy (8bit):	7.960696531016436
Encrypted:	false
SSDEEP:	384:7s7MkinrvfiwzzuYYXNgiKH3ZONJeBHUvifY6CrdO/Fufd/060PPBT1wl4nT7ZWH:7yMN2wuL+H3ZONSvfil/06s5ilT1WH
MD5:	414E33567EEF0D7D61290D4E4425512F
SHA1:	52FB21A849CBA919CBCD61F4090C7AE561B1C689
SHA-256:	CF74814FDA317181D85DAD9BC75839A8B1428DF0B9687C1779F8E946526EE9ED
SHA-512:	B1573E6A67CF88085EB6F4A6CEB01967F271EB7903ED4FC0202AB32DAA62E889C9A7A12701A991BBDCF923A9F1E05B1D49A5412FDD939CDD00133D4F0E1BAA 31
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dJxQ5.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=744&y=334

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1dJxQ5[1].jpg	
Preview:	.....JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?...;5(q... .....t..<...y.cZ.$.@...7.YL$.....0e.f.1.U..4.>..M#AI...F)1@....'.k-.....>...+#&.X..]...s.....^.@..N.y.[w.....~5.,{X.M.$'.....S..m.+.X.^Emi....8. ?.4....eQ.+..o.V..l.....\.....MG....B.$C."....J.....3.6..YO.V..5u.....W.{.O.<6....&%..c...&4....tq.i.=VC...i....l'.|..yOU>....#e% nz.EO._.iWkqj...z0.4...[..IT..N.T...=..U>.z..(...(..
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB1dsRun[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):	7897
Entropy (8bit):	7.942677850200005
Encrypted:	false
SSDEEP:	192:BCjnHNFZq95sZFAjxvKKK6e9jpKe8C/zxhEld7xP:kB0sf6NJKt98Kzb29
MD5:	4FD5E237B39311DE264E02CCE95B46F1
SHA1:	737A3C7EC86FC252873ADEC6A455B1498171501A
SHA-256:	F793AFD70F3C0E00EC3109312D95CA7DC3B4286F9CAD0C2689FD68BC6E184539
SHA-512:	E6DE784197C61F7B3F7C38003E015D5ACAD1B20BB97A143AF55F142B9EC32F1187B838F68209FF1A3767208C3209524884CACB1A0A9F8790FC464E3103F3D97A
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dsRun.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.....?..i.O5.V.!.S..IM.4.B...N....BV.V.".E.!".....2D....?a@.....H.....WB.....?..S....f..e....X.X.I...4...2.V...5..Td<....+. ....18...9....=.;0.{...i.....T...z"...@.;.c..x...E<9....z...!..^..JL..i.\B.....r...e...^(..5S....C.P.Wz.....;T..%.=.QsVPT..*..1....AN..b.Z).H..<...%.4.R))..... .....&)j...vp.1.....\..k*".v....s4vQ.f`.w. Oe.....I....Vw'.I...{.z..W..%g....3.?/..-.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BB6Ma4a[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	396
Entropy (8bit):	6.789155851158018
Encrypted:	false
SSDEEP:	6:6v/lhPkR/CnFPFaUSs1venewS8cJY1pXVhk5Ywr+hrYYg5Y2dFSkjhT5uMEjrTp:6v/78/kFPFnXleeH8YY9yEMpyk3Tc
MD5:	6D4A6F49A9B752ED252A81E201B7DB38
SHA1:	765E36638581717C254DB61456060B5A3103863A
SHA-256:	500064FB54947219AB4D34F963068E2DE52647CF74A03943A63DC5A51847F588
SHA-512:	34E44D7ECB99193427AA5F93EFC27ABC1D552CA58A391506ACA0B166D3831908675F764F25A698A064A8DA01E1F7F58FE7A6A40C924B99706EC9135540968F1A
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB6Ma4a.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J....!IDAT8Oc|. ..?...|.UA....GP.*`|. .....E...b.....&.>..*x.h....c.....g.N...?5.1.8p.....>1..p...0.EA.A...0...cC/...0 Ai8...._....p.....)....2...AE....Y?.....8p..d.....$1l.%.8.<.6..Lf..a.....%.....-.q...8...4...."...`5..G!.|..L....p8 ...p.....P...,..l.(..C]@L.#....P...).....8.....[.7MZ.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BBI9mKZ[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):	545
Entropy (8bit):	7.319481666711111
Encrypted:	false
SSDEEP:	12:6v/78/W/6T3uqnIh2ppl50x90SGBencVJmfJmPO:U/67Ih2pJWJGBecOYG
MD5:	35AB807913DD76237F320B94AA9A665E
SHA1:	CC741C888CBD3D79CB6A8A2C9C0DD7E898CFCF04
SHA-256:	DD90963806AED00038191EF275421ACC18B08C8B6B5AAD71D47AA903C24BBDC2
SHA-512:	B2B9787EA5C65C040B0A961D36EBDF93DE87E1F93E5543BDCBC1BCBDCC790EF494ABDEE4AEFC8316CDB046801C2BD31C9939940015798BE9690535D85FEC4 EE0
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBI9mKZ.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...N.@....&..p....a`f 0(..L,.<..l.....l.&..$@Xp.O..k...\|....].....m8.z....I I.L.D ....#.c.j...A... .J. C...c...2TU.....(/.*..}=....^O.....n.....~./6.}P..Lf.@.wG.E...G.?j..$.....U.....>??l...*r.....X....(..X|...X,.N..M.Y.p21.....v[.5M..F...+btL..mp..g.r.....dR4...N...N.....O ...\...jY&.. ._..+[...jV..L.BQ.lu..7'.a<...@>..1n.I.,....D.y?D...R..M$.....}..r...b..~...j.f...]G(.B".D&.....2....I:w.z.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BBX2afX[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\BBX2afX[1].png	
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:	2A8FA8652CB92BBA624478662BC7462D4EA8500FA36FE5E77CBD50AC6BD0F635AA68988C0E646FEDC39428C19715DCD254E241EB18A184679C3A152030FD9F8
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\3Y2ADQKS\BBih5H[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	930
Entropy (8bit):	7.648838107672973
Encrypted:	false
SSDEEP:	24:4Blz5F/i83HMOlt4Ol9Okcvz7v590ZIVkQ/k8xMd:4Bl9F/iCN7ikcHv5CZIbMV
MD5:	F1AEB21B524DE2509415284BB45C9D1B
SHA1:	9C5D17A573FE2DC2ACB2729381BC777C9C8474A3
SHA-256:	EFD678CBFA67BBD38DCF9BFBDBA90804EA2425B93F0A7447DACA21F9ECCCD458
SHA-512:	5FDD9593498D0C5C479CEB7CD51CE39F47F27A7ECA75D66372E9F633C5D35AC5350B6D3DBD5F3830C2F2A45E53C80340D2B3502A48CF0051D02EB13C844786A
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBih5H.img?m=6&o=true&u=true&n=true&w=30&h=30
Preview:	.PNG.....IHDR.....;0.....sRGB.....gAMA.....a.....pHYs.....o.d...7IDATHK.UKHUA..f.....HQ((_`.K,'',..P..(..ha.%QPR..B.T.Dw-2.B`..W{(..Y....K.....i.....{0.9.^.'HS..''t'....=u...]..!.:=.F..W.Q.M:...1.....e...bZ.4(5 .@DJ..7.....Z..&.....jf.aW_.Ndj.[$.k.*.Q. .0.ot.P....pu.1.5...}.....Y...a....<..Mt.....d..$>.|.g@....`...15.^..X..R=.6.Jd..y...(F..T..(. 7ew.`..Ay.5.....9..d.n3....7<...^.m4.&$JH|'].::.R....d.j.!...[i4.QT...|.....6.....,g.b...."db.{..N:..sj..c..5...,ZX.a.=..*O.P*.:...7Lg.ND...<....c.9Jd.....]5R..!._..:..x..>H..!,`.;...J.#....9..Q.... 8....s..#DQ.u....}|k.1...e6.6p...V.q.\K....B?..=..40A....#.....n._X.Z..+*.r....>>%..G]..<...:z...f.!.w<....n.Y..%g..W...G..W.....C..NKNv.....:..>...F.....7.z..<....\...;.Q..1.| ..`Z.OZ.@...`.I|...^..SNe%V...<.6.....o.@#.>.~.... {.....n..>@9..u._.wx.....N}..6.^.P....0....').....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\checksync[1].htm	
Entropy (8bit):	5.3018084083386
Encrypted:	false
SSDEEP:	384:RqAGcVXlblcqnzleZSug2f5vzBgF3OZOfQWwY4RXrqt:+86qhbz2RmF3OsfQWwY4RXrqt
MD5:	F20E359D299221FAA621EEED8710C7CE
SHA1:	CDE9D4EAA1954C0BDC907377024AB11A62EBC3C6
SHA-256:	BC6612574C7F898BCA97BB62CEB242821B9EDEE9B5A01F30113E0C4189CA72A0
SHA-512:	477A7A1D520D0A580358B36F368FB625A692D5F6701FE4AD5FAA617A87A5C1027ECF95FDB07ED0E5AB09A504C62DBDAF89FDD1A5B153D6B4AAEC460E8EB76A47
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\3Y2ADQKS\checksync[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	20808
Entropy (8bit):	5.3018084083386
Encrypted:	false
SSDEEP:	384:RqAGcVXlblcqnzleZSug2f5vzBgF3OZOfQWwY4RXrqt:+86qhbz2RmF3OsfQWwY4RXrqt
MD5:	F20E359D299221FAA621EEED8710C7CE
SHA1:	CDE9D4EAA1954C0BDC907377024AB11A62EBC3C6
SHA-256:	BC6612574C7F898BCA97BB62CEB242821B9EDEE9B5A01F30113E0C4189CA72A0
SHA-512:	477A7A1D520D0A580358B36F368FB625A692D5F6701FE4AD5FAA617A87A5C1027ECF95FDB07ED0E5AB09A504C62DBDAF89FDD1A5B153D6B4AAEC460E8EB76A47
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\3Y2ADQKS\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\dnserror[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\dnserror[2]	
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=9003
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\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\3Y2ADQKS\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\httpErrorPagesScripts[1]	
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\iab2Data[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	230026
Entropy (8bit):	5.150044456837813
Encrypted:	false
SSDEEP:	768:l3JqIWtk5N1cfkCHGd5btLkWUuSKQlqmPTZ1j5sIbUkjsyYAAA:l3JqIGk5Med5btLksSKkPnjNjh4A
MD5:	6AAA0F3074990A455B222A4D044E2346
SHA1:	6443AF82ED596527261B0F4367A67DD4D1BA855B
SHA-256:	1232E273F047113AB950CC141FC73D50640D2352B2ED16B89A1BAC01A80BEBEC
SHA-512:	EDE13CDE1DDEB45CD038042DCC6C1F75664EC259BC44100EB9C36361CFB657A7A661901DFEAD44DF6CEC555406A221970DF10F562AE222226546B7EFCE8E68D
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/e012d846/webcore/externalscripts/oneTrustV2/consent/55a804ab-e5c6-4b97-9319-86263d365d28/iab2Data.json
Preview:	{"gvlSpecificationVersion":2,"tcfPolicyVersion":2,"features":{"1":{"descriptionLegal":"Vendors can:\n* Combine data obtained offline with data collected online in support of one or more Purposes or Special Purposes.","id":1,"name":"Match and combine offline data sources","description":"Data from offline data sources can be combined with your online activity in support of one or more purposes"},"2":{"descriptionLegal":"Vendors can:\n* Deterministically determine that two or more devices belong to the same user or household\n* Probabilistically determine that two or more devices belong to the same user or household\n* Actively scan device characteristics for identification for probabilistic identification if users have allowed vendors to actively scan device characteristics for identification (Special Feature 2)","id":2,"name":"Link different devices","description":"Different devices can be determined as belonging to you or your household in support of one or more of purposes."},"3":{"de

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\idsync.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	29371
Entropy (8bit):	5.428910987980176
Encrypted:	false
SSDEEP:	384:8Vfp/WJ7LI4H/4LK9512/EV+MVmzRI+e2wpsIicDtUWPRLYVkKDwXp796jbYQkMi:8iLpgG4PImzdejeXwXKQF4SiW
MD5:	6405D2E39C0FE813C39C48C7B8B697C6
SHA1:	C3470077CCBF6EFF2C3D8A0824ABCCF86C69BC57
SHA-256:	F6386D0117112031B7C215D25EBC5144214E7271389DFED66B3136ED3C10E847
SHA-512:	531B6A48A04F53143E34C8DD1DEBE739004CD6B3FBCD15927796D4F6169EEBDF8CDB0CB04C865F0BFB9D004F0B94497ECBD5579BB61909FAC673246B536422E
Malicious:	false
IE Cache URL:	http://https://static.trafficjunky.com/invocation/idsync/production/idsync.min.js?v=1613462400000
Preview:	!function(t){var e={};function n(r){if(e[r])return e[r].exports;var o=e[r]={i:r,l:!1,exports:{}};return t[r].call(o.exports,o,o.exports,n),o.l=!0,o.exports}n.m=t,n.c=e,n.d=function(t,e,r){n.o(t,e)||Object.defineProperty(t,e,{enumerable:!0,get:r})},n.r=function(t){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(t,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(t,"__esModule",{value:!0})},n.t=function(t,e){if(1&e&&(t=n(t)),8&e)return t;if(4&e&&"object"==typeof t&&t&&t.__esModule)return t;var r=Object.create(null);if(n.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:t}),2&e&&"string"!=typeof t)for(var o in t)n.d(r,o,function(e){return t[e]}.bind(null,o));return r},n.n=function(t){var e=t&&t.__esModule?function(){return t.default}:function(){return t};return n.d(e,"a",e),e},n.o=function(t,e){return Object.prototype.hasOwnProperty.call(t,e)},n.p="",n(n.s=1)}([function(t,e,n){var r,o,i;o=[],void 0===(i="function"==typeof(r=function(){var t,e,n=6e4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\intersection-observer[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):	6944
Entropy (8bit):	5.094817989209454
Encrypted:	false
SSDEEP:	192:dNqiGQ2dWEKr1dTkeEvqAzD9JAx0GpJYhM0twC6Yx:L4dmjeiCYQt0Yx
MD5:	059853B159FD85F8CDE467314FFE566C
SHA1:	F279F588C2D30BC5EDC468EA5B1B0F7BFCF1C2AE
SHA-256:	B9E26E4A296DF7DF8A7C9DB4C2C51C23382E3CFA3E6CA8FCAAD577AA82539404
SHA-512:	077E5A387D8239F063C797650A19BD1340C4B28C3B23D39371146DE9F72EBA9543F6B533B7F245788BFA20856D3425778C3DB75C2DD5C519ABE98E7EA2FC403D
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/js/generated/common/intersection-observer.js?v=6f5214796229481244dc03c6129efd79f60bd552

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\intersection-observer[1].js	
Preview:	!function(){"use strict";if("object"==typeof window)if("IntersectionObserver"in window&&"IntersectionObserverEntry"in window&&"intersectionRatio"in window.IntersectionObserverEntry.prototype)"isIntersecting"in window.IntersectionObserverEntry.prototype||Object.defineProperty(window.IntersectionObserverEntry.prototype,"isIntersecting",{get:function(){return 0<this.intersectionRatio}});else{var g=window.document,e=[];t.prototype.THROTTLE_TIMEOUT=100,t.prototype.POLL_INTERVAL=null,t.prototype.USE_MUTATION_OBSERVER=!0,t.prototype.observe=function(e){if(!this._observationTargets.some(function(t){return t.element==e})){if(!e||1!=e.nodeType)throw new Error("target must be an Element");this._registerInstance(),this._observationTargets.push({element:e,entry:null}),this._monitorIntersections(),this._checkForIntersections()}},t.prototype.unobserve=function(e){this._observationTargets=this._observationTargets.filter(function(t){return t.element!=e}),this._observationTargets.length||(this._unmonito

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\jquery-2.1.1.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	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\3Y2ADQKS\lazyload.min[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):	6307
Entropy (8bit):	5.100857148211249
Encrypted:	false
SSDEEP:	192:+UBo5/5x5Po9M0BBa9AhGwy5bI4gKvXm7RABZeF0:+mK/5YvB3Gwy5xP0W
MD5:	8283E4E3E49C23283AADEF2DA054A964
SHA1:	D819FA0461D1660BDE6A3712CFF589FCAFEB0EF5
SHA-256:	70F740FC38200AED87924F4C9C661F205F71D97699B4AC56727CECFB927B12E7
SHA-512:	34258834CEC0216A2C5214C9B1B38DC65012ED76EF5AF56FB96295DBE22F2A9ED77D2A34DAB99AC47CB9978C0C151BD96A39C8583A797E7D4EC3F5C65FB860A
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/js/generated/common/lazyload.min.js?v=6f5214796229481244dc03c6129efd79f60bd552
Preview:	!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?module.exports=e():"function"==typeof define&&define.amd?define(e):(t=t||self).LazyLoad=e()}(this,function(){"use strict";function e(){return(e=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var n=arguments[e];for(var a in n)Object.prototype.hasOwnProperty.call(n,a)&&(t[a]=n[a])}return t}).apply(this,arguments)}var a="undefined"!=typeof window,s=a&&!("onscroll"in window)||"undefined"!=typeof navigator&&/(gle|ing|ro)bot|crawl|spider/i.test(navigator.userAgent),c=a&&"IntersectionObserver"in window,n=a&&"classList"in document.createElement("p"),w=a&&1<window.devicePixelRatio,o={elements_selector:"img",container:s||a?document:null,threshold:300,thresholds:null,data_src:"src",data_srcset:"srcset",data_sizes:"sizes",data_bg:"bg",data_bg_hidpi:"bg-hidpi",data_bg_multi:"bg-multi",data_bg_multi_hidpi:"bg-multi-hidpi",data_poster:"poster",class_applied:"applied",class_loading:"loading",class_loaded:"loaded",class

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\nrrV67478[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	88164
Entropy (8bit):	5.423101112677061
Encrypted:	false
SSDEEP:	1536:DVnCuukXGsQihGZFu94xdV2E4q35nJy0ukWaaCUFP+i/TX6Y+fj4/fhAaTZae:DQiYpdVGetuVLKY+fjwZ
MD5:	C2DC0FFE06279ECC59ACBC92A443FFD4
SHA1:	C271908D08B13E08BFD5106EE9F4E6487A3CDEC4
SHA-256:	51A34C46160A51FB0EAB510A83D06AA9F593C8BEB83099D066924EAC4E4160BC
SHA-512:	6B9EB80BD6BC121F4B8E23FC74FD21C81430EE10B39B1EDBDEFF29C04A3116EB12FC2CC633A5FF4C948C16FEF9CD258E0ED0743D3D9CB0EE78A253B6F5CB05D
Malicious:	false
IE Cache URL:	http://https://contextual.media.net/48/nrrV67478.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\nrrV67478[1].js	
Preview:	var _mNRequire,_mNDefine;!function(){"use strict";var c={},u={};function a(e){return"function"==typeof e}_mNRequire=function e(t,r){var n,i,o=[];for(i in t)t.hasOwnProperty(i)&&("object"!=typeof(n=t[i])&&void 0!==n?(void 0!==c[n]||(c[n]=e(u[n].deps,u[n].callback)),o.push(c[n])):o.push(n));return a(r)?r.apply(this,o):o},_mNDefine=function(e,t,r){if(a(t)&&(r=t,t=[]),void 0===(n=e)||""===n||null===n||(n=t,"[object Array]"!==Object.prototype.toString.call(n))||!a(r))return!1;var n;u[e]={deps:t,callback:r}}();_mNDefine("modulefactory",[],function(){"use strict";var r={},e={},o={},i={},n={},t={},a={};function c(r){var e=!0,o={};try{o=_mNRequire([r])[0]}catch(r){e=!1}return o.isResolved=function(){return e},o}return r=c("conversionpixelcontroller"),e=c("browserhinter"),o=c("kwdClickTargetModifier"),i=c("hover"),n=c("mraidDelayedLogging"),t=c("macrokeywords"),a=c("tcfdatamanager"),{conversionPixelController:r,browserHinter:e,hover:i,keywordClickTargetModifier:o,mraidDelayedLogging:n,macroKeyw

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\otTCF-ie[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	102879
Entropy (8bit):	5.311489377663803
Encrypted:	false
SSDEEP:	768:ONkWT0m7r8N1qpPVsjvB6z4Yj3RCjnugKtLEdT8xJORONTMC5GkkJ0XcJGk58:8kunecpuj5QRCjnrKxJg0TMC5ZW8
MD5:	52F29FAC6C1D2B0BAC8FE5D0AA2F7A15
SHA1:	D66C777DA4B6D1FEE86180B2B45A3954AE7E0AED
SHA-256:	E497A9E7A9620236A9A67F77D2CDA1CC9615F508A392ECCA53F63D2C8283DC0E
SHA-512:	DF33C49B063AEFD719B47F9335A4A7CE38FA391B2ADF5ACFD0C3FE891A5D0ADDF1C3295E6FF44EE08E729F96E0D526FFD773DC272E57C3B247696B79EE1168BA
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/e012d846/webcore/externalscripts/oneTrustV2/scripttemplates/6.4.0/otTCF-ie.js
Preview:	!function(){"use strict";var c="undefined"!=typeof window?window:"undefined"!=typeof global?global:"undefined"!=typeof self?self:{};function e(e){return e&&e.__esModule&&Object.prototype.hasOwnProperty.call(e,"default")?e.default:e}function t(e,t){return e(t={exports:{}},t.exports),t.exports}function n(e){return e&&e.Math==Math&&e}function p(e){try{return!!e()}catch(e){return!0}}function E(e,t){return{enumerable:!(1&e),configurable:!(2&e),writable:!(4&e),value:t}}function o(e){return w.call(e).slice(8,-1)}function u(e){if(null==e)throw TypeError("Can't call method on "+e);return e}function l(e){return I(u(e))}function f(e){return"object"==typeof e?null!==e:"function"==typeof e}function i(e,t){if(!f(e))return e;var n,r;if(t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;if("function"==typeof(n=e.valueOf)&&!f(r=n.call(e)))return r;if(!t&&"function"==typeof(n=e.toString)&&!f(r=n.call(e)))return r;throw TypeError("Can't convert object to primitive value")}function y(e,t){retur

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\timings-1.0.0[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):	3187
Entropy (8bit):	5.190303506246706
Encrypted:	false
SSDEEP:	48:tuStgz6UFeR9Rh+zj5Hzh9b4cuKIoc71TKPQrMIbxD8CD7:tu2gz6UFeXP+zj5H5VCBT7dD8CH
MD5:	71F3A664DEFDA2F5724EAA072FC45C3C
SHA1:	FA1F57C353C958870FC31BA122849A6018341598
SHA-256:	5D0FEC532F2E7D4DC5A759EA0967583C0886585C3765DD79D58E38F0BFB7E877
SHA-512:	579708C88646A626E0FAED55E587E92E706B207EE6FA1D10C81A27D82F9B77FBB90ED6DE5EF5B12FBF4386FA65B45B36EAF1DFF6C48F0B9E90CDD23AD2C3A90D
Malicious:	false
IE Cache URL:	http://https://cdn1d-static-shared.phncdn.com/timings-1.0.0.js
Preview:	function MGPerformance(a){var b=this;var c=performance.timing;b.interval=600;if(a!=null){b.interval=a}b.callbacks=[];b.listen=function(d){if(c.loadEventEnd>0){b.callback(d)}else{b.callbacks.push(d)}};b.setInterval=function(d){b.interval(d)};b.callback=function(g){var h=c.domainLookupEnd-c.domainLookupStart;var d=c.connectEnd-c.connectStart;var e=c.responseStart-c.navigationStart;var f=c.redirectEnd-c.redirectStart;var i=c.domComplete-c.navigationStart;var l=c.domInteractive-c.navigationStart;var k=c.domContentLoadedEventEnd-c.navigationStart;var j=c.loadEventEnd-c.navigationStart;g(h,d,e,f,l,i,k,j)};b.test=function(){if(c.loadEventEnd>0){for(var d in b.callbacks){if(b.callbacks.hasOwnProperty(d)){b.callback(b.callbacks[d])}}}else{b.interval-=200;if(b.interval<100){b.interval=100}setTimeout(function(){b.test()},b.interval)}};setTimeout(function(){b.test()},b.interval)}function MGPerformanceTiming(a,c){var b=this;b.settings=c;b.ajax=function(f){try{var d=new XMLHttpRequest();d.open("GET"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\12[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, 304x171, frames 3
Category:	downloaded
Size (bytes):	11106
Entropy (8bit):	7.946365036309197
Encrypted:	false
SSDEEP:	192:nGCTyfvlSjf8poBZXTkV4NhRDU62gmu/9dMa9jv+WKvL:nydkUUtRNzD+gfTX9jvOj
MD5:	49A08899E08C7D18766EBA508A2EABFB
SHA1:	F5B52FF9A8B98FBDAC0EB187244527B6B5E1E79A
SHA-256:	7E3D9C1A4015948212DE624372F7533FED19B5866DF71070672EAD9D1071D0B2
SHA-512:	F1887ADF6DC545DB028BB2AB678B72DB6671C61EDC3DA3266A3D438C06ABD9E762B131F66660D56C5C6F3844C191A8C950DBD54C368516055E5C86109763DC
Malicious:	false
IE Cache URL:	http://https://di.rdtcdn.com/m=eW0Q8f/media/videos/201903/10/14667861/original/12.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\12[1].jpg	
Preview:	.....JFIF.....C.....!......"$".$.....C.....0.."..... N :5.1....5VR...A....W..#.....oU..zK1...A..S[..JE.@Gm.P.5..G.....-+.h... .I.....0....!.t ..2N.9...B....bd...I.E.EH..$.`.2.Y.n..wBL.....I.B...O3_...w'..%..mbQX.:...S.M;3..C$7A.A!B:.. 7"f.L.jd8.....T...&].Z.rX.x.V.=..E].i.W..r:...8..n(....-...N&..r. j.j...,n..X3&D.}[/O...kZ..M...#..5N.?.Mh...4...4v.<9..(/;..:.O.g.Wg.$..lB.Tn....;...F....j'.^.W..y.).4....T.....\..d\.^.. i.H.-K1A...n .:....I8$l...n..7...Fr..>..wX.^.c..{.....m..9....JU..A.+...)O47.ON1..I.9+$..!g..@.V.....t.C.6}>..^.r....N..s....._5....-.^.\..J..j...2..i...R..mQ....fHH.....y...b8.c...vnr.X.[..x...?Q...^...\Y5 x|w.....`.3..$.:.%...g.5k4.>.F....Y0ty..X/:a!i....k....P|n...#.mCN..|{5z..n{.....xy..?..q.F....M..q.... .u).!...0.bm.<.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\15[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, 304x171, frames 3
Category:	downloaded
Size (bytes):	11922
Entropy (8bit):	7.933896253580004
Encrypted:	false
SSDEEP:	192:KKlkmSH9tyS4cAKiKNsJ0Wh6J9z2gMRYoax3M0k/9IRWi8HhZ+mZ4n+RV/9Bxsia:AmIDEcA5csaiZ0W9EVqv/w+RTsifi
MD5:	582EDB0754DAEEA480CEAD9CF3F65736
SHA1:	EEB90C614894A644B3C7A62A56B744BCA874DED1
SHA-256:	96481FB295896AFBA1B1F8C956F386D2DE2F1CB2D180D1A9B6FBBC295247A9F4
SHA-512:	FE0CEBFF951679F40F22C800E067F2E4CCFA1A5420E08EA939E73990A42C8EE9BFAADA374F59054F6337B86AB8384B1AA685A11647B0F11391A05062767D13A2
Malicious:	false
IE Cache URL:	http://https://di.rdtcdn.com/m=eW0Q8f/media/videos/202003/28/29931511/original/15.jpg
Preview:	.....JFIF.....C.....!....."$".$.....C.....0.."..... m..\? @?...=.h,Ix~.X.,....V.YV.....zw.<.....Uo.c....<.z.0M.A..i.+[U..X..y;...$.....z.YZ.T.6.}U.P.%....B.}..~...$.....v..xa...L...9.y.Wf+...%.....0.....S..Kj.e..!..c[X.....*.&..z.%..y...yra.. .|k..5... b.0.).f.0.g.....iBsw...t.#od.KU..Z.....t...}k...qL:..v.....g..T.XH..5zj...&p'...x.Aee)y..1.C.U%..E.]..._.T.E.f.=..''..)4..t6..Z*p....|.]&.c.8..Iok..D.PY.....F..Y..."d...8..U.[)k..^..m.T .}.F.9.-V..za...n_UU....r.&.U..P.,.^Y\.Q..8... ...G..Y..&.Q.X..&.....B....r..*.....[=..ca.....)....O+.x.jI)4..E&...gc.<`.>.k.P..V[F.Q.AJ.Z.!+,...&.>.+`.M.-sZ.p.].NAXH.u9I.$.L.....*g.-q... p...f-.....\tY6..E.6._q]d.)..1..c....+?.X7b..X..K].X!iL fF..>tq$.%.....V*...ZR.a...c.....j.H..]..C....._...o.l6v

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\3FSF6RAW.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	422829
Entropy (8bit):	4.898785154067777
Encrypted:	false
SSDEEP:	6144:MTbKGSGNyQm80Q40bKPNud2pYwsD8AyqsEmr+5MZ/MOi5BS/WSmAWb8vWuYM8KZX:MT32/WKWuYM8O/RirThpY
MD5:	4008AF5E1B2B5B041865219F75093367
SHA1:	992C66F383B22159B8E3E7A00252E36C95F8B15D
SHA-256:	5BDD26A5F03133C29B2443AAD86844486D7489EF951AAD672E5CDCC91FA8ECC4
SHA-512:	F974A26B07003911B4F88A154479C507481A6EDAC861FDEACAD378A092F4391F7D4837AB6E53B8D1ECB238A93DA949C7A4BEA1EE228C34F6275A3FE5F73AA83 E
Malicious:	false
Preview:	<!DOCTYPE html>. [if lt IE 7]><html class="ie ie6 language-en" lang="en"><![endif]-->. [if IE 7]><html class="ie ie7 language-en" lang="en"><![endif]-->. [if IE 8]><html class="ie ie8 language-en" lang="en"><![endif]-->. [if IE 9]><html class="ie ie9 language-en" lang="en"><![endif]-->. [if !(IE)]> <html class="language-en" lang="en"> <![endif]-->. <head>. <title>Free Porn Sex Videos - Redtube - XXX Movies - Home of Videos Porno</title>. .<meta http-equiv="Content-type" content="text/html; charset=UTF-8" />.<meta http-equiv="X-UA-Compatible" content="IE=edge" />.<meta name="msapplication-config" content=" none" />.<meta name="keywords" content="porn, sex,xxx" />. <meta name="description" content="Redtube brings you NEW porn videos every day for free. Enjoy our XXX movies in high quality HD resolution on any device. Get fully immersed with the latest virtual reality sex videos from top adult st

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\5[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, 304x171, frames 3
Category:	downloaded
Size (bytes):	10067
Entropy (8bit):	7.931951355822377
Encrypted:	false
SSDEEP:	192:ABZwi0P6HulG0WpwpL9VgBp+1v35J3gdXEhvFbi57b+du9Ma8OsKRxEmE:Lic6HulMpwm83bQdUNq+dUMaXsommE
MD5:	DCDF7EF0D71336473D27EF2204A8F3F4
SHA1:	A452B5B5B86F6AB5C3881EEE25CEF9F7F8B94FB1
SHA-256:	4ADAC6755C120341E597A670E1CB61F1ACD1E958F1ABD1ECDA7303A1B8FF20DA
SHA-512:	E63918C272D61B1251BA55AA035B244629F57D9D25598667F65B4F5F3FEC2BE2D3653A3E01B5B5EC6F13FB0F0103E2D441E120884F39C4B8D031872F71469688
Malicious:	false
IE Cache URL:	http://https://di.rdtcdn.com/m=eW0Q8f/media/videos/201907/14/18927751/original/5.jpg
Preview:	.....JFIF.....C.....!....."$".$.....C.....0.."..... ? .I..&.a.2^.D.D.Y9..NN..j...w).U".X..f).Vu...~...c....B.-...I..'+.....i....idZ..v.l.r.w.e.,.m../H.0/?E....8...._..O....[Tu..!..`.a...T.u.I.....ko.o.>.NS..n..F.W....h.n....9.....L....{...3V&9....ba.. (..F.Bp.\.....i..0.GGpT...:.yZ.kA.\.f.4...+5.j2.'k*...U..''..X....B. ....Y....v.3.<.s?.ydg6...]......%4..o$^.....z.-....}.)<z0.G."&...Z.m@..6."......N....x.].g.O=|..1.....$..tt.A.$nG}.....{... ..K..{.H.@z.QEmVV..Pd.C.CK....L.....2...U.0.#....R.;.j..{..t.._..4..Q...:._c!.}....u....Q..@.&....J\m.%._4.L.....^J.Z..o....GR!(....s..PQ#)+,a.%\.h.#.6~...]?To....u...M&..\U4....^.t.8 ..x]s#..Oi.zx..G.I..*YH.....E.7.F8:..Y3.....r....U5.G7../.h,...#:.....h..R./..;G*.p...Z...t...+@.zf..=..Y...x..G.k&.3..:.7..uq..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\AAuTnto[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	801
Entropy (8bit):	7.591962750491311
Encrypted:	false
SSDEEP:	24:U/6yrupdmd6hHb/XvxQfxnSc9gjo2EX9TM0H:U/6yruzFDX6oDBY+m
MD5:	BB8DFFDE8ED5C13A132E4BD04827F90B
SHA1:	F86D85A9866664FC1B355F2EC5D6FCB54404663A
SHA-256:	D2AAD0826D78F031D528725FDFC71C1DBAA21B7E3CCEEAA4E7EEFA7AA0A04B26
SHA-512:	7F2836EA8699B4AFC267E85A5889FB449B4C629979807F8CBAD0DDED7413D4CD1DBD3F31D972609C6CF7F74AF86A8F8DDFE10A6C4C1B1054222250597930555
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"..Ir.Th.....B..s.o.!...S...bT.81.y.Y....o...O.?.Z..v.....#h*;.E.....)p.<....'.7.*{.;.....p8...:..).O..c!.....5...KS..1....08..T..K..WB.Ww.V....=.)A.....sZ..m..e..NYW...E... Z].8Vt...ed.m..u.....|@...W...X.d...DR.....007J.q..T.V./..2&Wgq..pB..D....+...N.@e.....i..:.L...%....K..d..R.....N.V.....$.....7..3....a..3.1...T.`.]...T{.....).....Q7JUUID....Y... .$czVZ.H..SW$.C.....a...^T.....C..(.;]\|,.2..;.....p..#.e..7....<..Q...}..G.WL,v.eR...Y..y.`>.R.L..6hm.&,...5....u..[$_.t1.f...p..(.."Fw.I...'.....%4M..._....[.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\AAyuliQ[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	435
Entropy (8bit):	7.145242953183175
Encrypted:	false
SSDEEP:	12:6v/78/W/6TKob359YEwQsQP+oaNwGzr5jl39HL0H7YM7:U/6pbJPgQP+bVRt9r0H8G
MD5:	D675AB16BA50C28F1D9D637BBEC7ECFF
SHA1:	C5420141C02C83C3B3A3D3CD0418D3BCEABB306A
SHA-256:	E11816F8F2BBC3DC8B2BE84323D6B781B654E80318DC8D02C35C8D7D81CB7848
SHA-512:	DA3C25D7C998F60291BF94F97A75DE6820C708AE2DF80279F3DA96CC0E647E0EB46E94E54EFFAC4F72BA027D8FB1E16E22FB17CF9AE3E069C2CA5A22F5CC74 A4
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AAyuliQ.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....HIDAT8O.KK.Q.....v...me....H.}.D.....A$.=..=h.J..:..H...;qof?.M.....?..gg.j*.X..`/e8.10...T.. ....h..\?..7)q8.MB..u.-...?..G.p.O...0N.!.. .....M.....hC.tVzD...+?....Wz}h...8.+<..T._..D.P.p&.0.v....+r8.tg..g .C..a18G...Q.I.=..V1.....k...po.+D[^..3SJ.X..x...`..@4..j..1x'.h.V. ...3..48.{$BZW.z.>....w4~.`..m....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB10MkbM[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	965
Entropy (8bit):	7.720280784612809
Encrypted:	false
SSDEEP:	24:T2PqcKHsgioKpXR3TnVUvPkKWsvIos6z8XYy8xcvn1a:5PZK335UXkJsglyScf1a
MD5:	569B24D6D28091EA1F76257B76653A4E
SHA1:	21B929E4CD215212572753F22E2A534A699F34BE
SHA-256:	85A236938E00293C63276F2E4949CD51DFF8F37DE95466AD1A571AC8954DB571
SHA-512:	AE49823EDC6AE98EE814B099A3508BA1EF26A44D0D08E1CCF30CAB009655A7D7A64955A194E5E6240F6806BC0D17E74BD3C4C9998248234CA53104776CC00A0
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB10MkbM.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs...#...#.x.?v...ZIDAT8OmS[h.g.=s..$n...]7.5..(.&5...D..Z..X..6....O.-.HJm.B.....j..Z,.D.5n.1....^g7;;.;3.w../..... ..}....5....C==}..hd4.OO..^1.I..*.U8.w.B..M0..7}.....J....L.i...T...(J.d*.L..sr.....g?.aL.WC.S..C...(.pl..}[Wc..e.....[...K.....<...=S.....]..N/.N....(^N'.Lf....X4.....A<#c.....4fL.G.. 8..m..RYDu.7.>...S....-k.....GO.....R.....5.@.h...Y$..uvpm>(<..q,..PY....+...BHE..;.M.yJ...U<..S4.j..g....x.....t"....h.....K...~._....:...qg.).~..oy..h..u6....i._n...4T..Z.#.. ...0....L.....l..g!..z...8.I&....,iC.U.V,j_._...9.....8<...A.b.|.^..;..2...../v .....>....O^..;.o...n .'!k\l..C.a.I$8.~.0...4j..~5.\6...z?..s.qx.u....%...@.N.....@..HJh].....l.....#'.r.!../..N .d!m...@.....qV...c..X....t.1CQ..TL....r3.n..".t....`...$...ctA....H.p0.0.A..IA.o.5n.m..\.l.B>....x..L.+.H.c6..u...7....`....M....IEND.B`.

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB14hq0P[1].jpg	
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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."..... }.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?..ii(....(.h.....Z(....JZ.)i(....(.....(.....(....J...+h...@....+...e.9...V..'."!.@....|.....n...@My..w9;.5I...@....L..k...w2.'... M8)4..>.u9..5U.w9,M(....!E..!.[.5<v.?AV..s...VS....E5v.....Q.^jwp*3&MJrf..J..|p...n .j..qW#.5w.)&.&..E^..*..."..T.....y.U.4.lK.sK.ooj.....Z..3j..."..).c..~... .RqL...lcym..R.. gTa..a9.+....5-.W'.T@.N.8"...f.:....J.6.r.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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. lik...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\9QTQHWWN\BB1cyB6y[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):	11631
Entropy (8bit):	7.94205600072752
Encrypted:	false
SSDEEP:	192:xYKm5Rwuly+Lq3fRlZprmyUzNaV0LkYIovCg2rDR54NovYOoYCyk06qd+q3oXCSK:Op52doqPR/pr72NkItI+Cvp5mKYAV6Ty
MD5:	BD826FBAC90351ABC716E8334A3F756B
SHA1:	41D61260D04B28548D207305373BC0E184E49C88
SHA-256:	28B09F76157D6033B3C9EA9648CC79BB9444F0EE41A304B22C8DFCC0502141FD
SHA-512:	80E8C353BA4F97C5E67C1E9B5E5FB5C9503F0988BC6BE5B2914E99D107709703A7DFB9F188CEFE8EF54BF97599C9683CB2050168E2E564A3126F57CBDCED6F25
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cyB6y.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg&x=960&y=641
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...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?.....}....}....U.Um.;..j..T.A.....n[.4...I.nZ.....S.tW-h.cj5/.9.t...RkgC..h..QY.v.....<"oJ<..U.... @.5."5..c..2c.i4\.*&.....3..U....._'...S.XGHR..^..L\Q.J.T.J#>.`ER,F..q..O$.SLdv....:.t.*.(.mYd..c...hU.J.....J...T._..<.'2.%F.W..{...z.1.....j.BE0.+'..)\.m.j].m..;.m..Sm.m.. ...6.h.J.r,Q..m.h.\..T.h..s.~.V..jId...+.C..L..N..".<.)D..U...s...S...g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1dIP4i[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):	2418
Entropy (8bit):	7.8204944528043345
Encrypted:	false
SSDEEP:	48:BGpuERA4+taHweIhDvAGnsv6QZIC9CF0uuyXZd7S:BGAE0syoJHIC9QJXZo
MD5:	B7CC8E04F1E633F97351D2A97CF304B2
SHA1:	D4E63E320E28B3772B9AC713EF2DDD9804DF1D85
SHA-256:	D0BEA926F512EEDAE100B17BADA5B4168BB61CCDDD90517D4F8410978703F336

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1dIP4i[1].jpg	
SHA-512:	2B4F73DC0B4DF6838E33BC3202D25C2F43FDF68124FFECCED77DF384C65F7E0AB9ED0D8792A16FDDC15254EE4C866F4583F8277513FE172BD35DCBF15297101
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dIP4i.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f&f=jpg&x=544&y=201
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO......K.d.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..<...0.[....Tn.ib..P.zgk.Bk.{Q.....:V.awn..;n.....A-Me7! ..Z.R/.b....j...s...y...j.h.._....Kv..>....h..W.QGLw.oc;\.{;_\..6.....3.....@.k&..Q...GJ.<...$7.....MO6..7v3.|?.Z..,...A....v4.6..|....Kr..+...?.^E..m l..0....+2.AX.C%...u_..+5.Y|....SY$./</f...z..W..."..5..1..Aww...i....s.....D...x4..Y...*s...../..'#...v.k..5(...<.l.l...lz..J.f.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1dJ7bz[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):	2411
Entropy (8bit):	7.812817500188182
Encrypted:	false
SSDEEP:	48:BGpuERAhQfI2rz6rvm6mDTrOMPjoPenxIkJmId3eC33oKdMiAYNb7+Z:BGAEvnCmNnrOMUP8IkJmmPoKdMiAUc
MD5:	10D83416DDA33AEEC516DFB4DE9701F3
SHA1:	EFF3A913A92A2BC7D9E72228772C82B08E651E79
SHA-256:	D3D99614C406D8D543BA3F393EC93073D9220056AC7E1F8D918DE8243CA10417
SHA-512:	B140F92F795EBC6C1DE289A5E6168631749DB8ED171A011DEB23647165980C3354699AE6F5D117A3415664689180 90DBC91448CDCD1CE44BF224B9E5D48FA975
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dJ7bz.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:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....o.....Mt.....h_?.....]]..h}E!...J..r,...k&..2...koV].....g?.f.'...Q&;....d....N.T`..EEpY.....~.....G...c.oO..hbW+1s..1.k'.d..#!.{S.`.m.c..H....T.t=f.k{9..".`<....H.....+;G.KX.%x..9g...T..j....[#.j;G.uH.YBC+.-.....j....G.d4Y...y....e..+.4.H..7P...v.F...;...j.K'."..8.QJ...fW.y..?..36..(.=....y...0..u.X.G.G.S.....a.....blrZ....Z....#.r.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1dJbEd[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):	7299
Entropy (8bit):	7.930407473104593
Encrypted:	false
SSDEEP:	96:xGAaE6/OehVghKQNLd3QcE2QIUcJTwqtrVYYU6AP9K1aES2JtswDTAy0koPQznlL:xC+e3yVrX0qtIE1a7QtJDt0xPUnZrd5
MD5:	75845E11B39DF5DE004D1216577E7091
SHA1:	2B7F93ED82BC9A02B1464F20331545E6DBBB9FE2
SHA-256:	AE848C761A9C13805CCEF81911FEB4F2645FF11FAA8F0080ECEB3FC27F427214
SHA-512:	EA94E1F775652A5BAA53211503C644E51F0EE2014739371ACC3CC8EAEE829098DD3B770282E0E2A99EA4647FACBDC05C34B7DC1BB05391E05CA1E546A5A727AB
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dJbEd.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=526&y=167
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..\.[.....i.:.%c.\.....z...I.n_...`k...(.0.H...._...=L.l.i.x2.ReU..Q.h.....V.`..HV..{.....V..o. W....K.uc...kckB.....r.....E3N.[kT@9..{.....U..a.*&J.....W...*...@..q...EQ..<r.c..^..e\...V.fsGL..b..2.....k2....D.B..(.....q....M.\@.....u...Ih..e@ce.....@.....'..T....7...i.&.r.....=*.!#j.O0.....q.V.....@...#...s..Hr.z....O..^

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1dJc59[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):	7087
Entropy (8bit):	7.9229765060977995
Encrypted:	false
SSDEEP:	192:BCMcFlPV54BPG8o0kwl3CtDFkww1p4iACi+SaV:kMClz4BPPNhoqp4IV
MD5:	D53B1899A62B89CF7BA6D4FC4F5A4DCB
SHA1:	AE289CF4359516B6D456CC72DA8708A1E0DDA27E
SHA-256:	ABEF0E4BE3557DBC78F410A688DA16BDAC82E06989B086CBBFE2000F6DE7131A
SHA-512:	E5A7359AA5427C19155D3AB109A2F7311E0A10046D062347F5E0502960B6126A1A1247B5F145D6FBA211EA333304C47C3F53204CAC0270F5330B5A2C75F23776
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1dJc59[1].jpg	
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dJc59.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=607&y=317
Preview:	.....JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....m.qHE`u...\U....E"....X+L+AD.i.....f.s.BUO.i01..Es.).l..+.^E..#...^...+....-W.B....c..(....ed_...N.....!y.....sG....t.c..*.)D$..M..e'.b.F..I.....p1.U.d.p.....v..j?..h.3.k[L..s.....H.K...r2.8.....$f..1e.}j.....b(~.M.*....:\.r.|.W#>...5....w.#.x.:r).&...;._.b....0.CO..9.{..P..J..a..m.s....ZQ,w1.]...*.x.PG#..O...&G..2.D~q.C..Q....PEIt..(.O....._pN...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1dJejb[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):	6723
Entropy (8bit):	7.805670003516452
Encrypted:	false
SSDEEP:	192:BY13yERhmoesaFqiPCN3tIvRCMDY2+3W2Gr11:e8odaFnPkOi3WHrL
MD5:	E679E611A9C0C2D8469A6AA2C5C0888E
SHA1:	FA5C9912D7923FF83CE162F6D686C57CD84AF41E
SHA-256:	6E118FB19DE5C403477D584C0166156E3FE91886253EBA3A9F4154F22222AAC4
SHA-512:	9393AB9409CAF9E5D3B9E4AD05C6241F12D5B6AB8BC6AAF427F45F22691870E5685614B03C31FC52C2A37FB993B444D4B0D74A54E30806E3D57FECEE5CADBBF1
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dJejb.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:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..m...d./.oG..m...Fv..s]1..KC.m....T.SK.3O..PU...;..QHaE.P.E.P.E.P.E.P.d...sf....Md..j.v...=*jj..u.AE.....E9....E!..4..QE.5....Fh...z.....iMQ..5zQT%^j...C).h.....W.|c44.f.....56x.5*^.D.J..O.BS...k.u'..}+.5.....?.....(4%.<..k:....Z"Y....K.[.s.....=...(..k...|A...(.,(...(...(...(...(.....Q@..Q@....(.....s..*.....kTf.4.@.5D.#...@C .S..'J.p.R3.....qT....2.d&.(^

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1dJh9q[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):	50801
Entropy (8bit):	7.971779585893578
Encrypted:	false
SSDEEP:	1536:74ljqdPv0IKXR1rfE2yWZEeEZtuHL0RY8hTH:W2dn0Is1o2xuZtuHLL8RH
MD5:	892D706C7AAC69DEE828000ED537A9B5
SHA1:	55E1B8625B4612D83C50D15D59D9F07FC588D0D2
SHA-256:	86A82DAC813A4BAD345E8281B1603C612DD2FEC4D9AD116C9ACFB9E159C65E33
SHA-512:	787086F185784222770C921B8078B6603A43EA64214EDFFEC28BADA8C42E050BEF72EF155DF42D295A286DCFB649A3D1C2EB5693B07718624553C0FA2C7FAF3C
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dJh9q.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=1002&y=1956
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.....?..&f`..i..(.Y.@.=.3 ..TL...l.....,9|....>...nT..@:w..U....X..|.`..2."...G.}..M@..T....}0k.X..(.5...."m.>...5.,!VP.q.....#%l....K.y....#...Zi..3..,.d..5..l.3...l.?/'..-...A...%..x .R0.GC..W...P..0gf^...[b)...H..t..s.2.....9.O.5.u.>....QS..,..3D.....F;.\Q`6...\.v..X..T.['.5..a.P.~..h.).....A.V..g..U..bq.U.`5m.=...1.s.{VN)..H.....R.....9#N.*8..jB.`A..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1dJiYl[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):	11382
Entropy (8bit):	7.93026039760067
Encrypted:	false
SSDEEP:	192:BYNG3LsS3QP0db0Eaff/9rm5oyqKJmKxOzqX/MXm83gK819KAO:eNQLsSAREM0yIJmKx/iT3gKCVO
MD5:	8EA7FEADF38F8069595E1F0ADA93D382
SHA1:	B6B63C08937571976EBE854ACC21BF5D83811864
SHA-256:	97ED0A577012CAC864D7FBDA0CEF4980E484BFFAC12CA353E58810CF60C15255
SHA-512:	E7D3C26647F78CB8820703DFA9113B60627C16F11EBF9C017720231E3AD4EB69B74FD6B843783DB5AAE631234F7A1DBD3E118A63ABD66480D63603EDB1E45F2
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dJiYl.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1dJiYl[1].jpg	
Preview:	......JFIF.....,.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?..$...+.=.)$.H.i..y9.M.rC..2i...o..v.M).T..!..\.P.N.1R..X`.*..In..@..l.sR..6.rj.....W.s...@..?x~TG...{..v... .I....#..$H..;.....s.TD...V.....@..Sdl...d..t.....HS.....>..v....H...)...?Jc.>a....^.4.r.f..yS.E@T..".....R..px4.1".n.8 .=.V.O....M.@\.L..:L.@[..D.JC.J..../S@...J....;.@s. ..R..P.K. iS..F.....a....b...0i.sV.A.....E....)\dT'".$V...J.=i..(..>1EF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1dJjrz[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):	14328
Entropy (8bit):	7.947389866532409
Encrypted:	false
SSDEEP:	384:eUQ22pmSfA9/vvKXxZWSrWCWwYek+0vmv3Wlfx:eUNxSIXSrmwZZYmv3OZ
MD5:	C5ED3EF6608E476253E72558DA5C75E3
SHA1:	80C8A2DA2142AD1BCC413B1A7BF91292A4FA9942
SHA-256:	76921A9292D1B472E6FBD98B39AED60D8EE3506C9C97F28465D7B6418D965165
SHA-512:	1D01D012579626822AD03E90BDA2E88F5888D819B2FAAD9D2FF5F05C15E5D893A70AE5F67EA868A4365CED1CED6919A8B5B9769206E5A8E69467726D578E6FD
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dJjrz.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.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?.....4..Qa.(..Q..X..J?....s.N=)O..g..4.1.<..E6...b..SF=....iv.. .K..h.....q....m..:.1...7m.Gzq.. ..}+OK. <.e..w...t..9..X.....E...,{(.&c.#.PD.<t..Yn.l.+Fv.+..K..L...4..qM...(#=.N`wt.4P&....m..M...B.....g4...S...iq..q@>.P.V..S...@.y.@.....`m..h.....K.g4.&....s.ZA.j3.(.#..("'..q...z.sF.bh. ..z....I..@....Z.S.q.`i.m.....=)B..4.r)....(.=M4.^)H..J....Ou..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1dJnYR[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):	15463
Entropy (8bit):	7.957539218246347
Encrypted:	false
SSDEEP:	384:Ovj1qe4CXdcUYu6VKwr44GlEC5PhHWvQhGx7CdOKwXV3z:Ov0YYvB4JWC5PhHWvQhGx7CdOKwp
MD5:	906EFD3C1756061AFBBE0C5E32DD140F
SHA1:	76872EF09AD83DF3CEC1FFC2962D33413AB170E7
SHA-256:	725E0862953B3D6E2747281B41753389E69F6EAF29026979E774493BCFBED7BE
SHA-512:	5563F95714547AA8C1041060F85E40EDDEBBA2BE58F6B9CAAE4E7DB62BFC26D2B0C3DF1379568CB4F64BA0743F0635C00F7C9768A0F16E5359D3C25B0D5F969B
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dJnYR.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg&x=326&y=277
Preview:	......JFIF.....H.H.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefgh ijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXY Zcdefghijstuvwxyz.....?..s8.B.v.$....b..P.3y-.:qWe..e..oZH.#T.....9b.-.J....j.U%-....],...7..L..>.y.,d2.jE..w....*...&...._.l.... ...m|.d.J5.J..b...!U.....9=.-m1..V..u!O..bF.^...u.l..m.(.`....Y8.*Er.5...Jv..J&...H.bT.@4.+A...C.+.m....]..y.....-.:}....W.....2).L...R..})....(..."...%@.b..w...Q(h.W.0..,c^."[3..H.k ).uQ.x...(..k. Cmt..qs....^.`..#1c>....l.4..y$..#k.y..[.e.y

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1dJqc9[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 183x183, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	10542
Entropy (8bit):	7.95057323303207
Encrypted:	false
SSDEEP:	192:5C0nk51S2M11kk2yEBwMvTc2AaRmWxGDnhLsifbVtvHCK6WK:M0kXSb11jEBJvTvKhLsiDDvH7K
MD5:	D333DFAB6C6EA8A4BA125B016BD34246
SHA1:	E7ECFD877D9D4900CD1987D8D38465F573114E6D
SHA-256:	A25F09A70D4564475DA13B3D1C1CAC9E942AF442F08FCC27B56271C5E459CCB2
SHA-512:	1DD1E55244F26D6EA3C86F2719CC8E26F77E61326565E95C86B1B1D4F9F00387D9F0527B6A2B2AFCA337BA39C042DA66054158FDCD7515EDBCE062450506C24
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1dJqc9.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=100&y=205

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB1dJqc9[1].jpg

Preview:

......JFIF.............C................ .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOOOOOO..........."..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs
tuvwxyz...?..n.QK......PM...w.A.Z.t.....[3.m.?.1...W_...O%~.Nd..Q...f..(v<....G.].mR....Y..0o.....[...T..B..]...R.-.7..0.yg..#.W#
..:..'..ZK.=....z..$...(..b.JZ(.......+.|;.xj..N...2fdp0..8l..../.\.[....%..i!.....5.F......:BB....8.r. >..'?..e...(..,O.....p..uEy.......iC.W.p...;n..*..55.iP..\M..X.~xQ]..T.V..,..N...G.....a....F.7.........S.
g.../.s];4. .....,3.=...[..~5.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BB7hg4[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	458
Entropy (8bit):	7.172312008412332
Encrypted:	false
SSDEEP:	12:6v/78/kFj13TC93wFdwrWZdLCUYzn9dct8CZsWE0oR0Y8/9ki:u138apdLXqxCS7D2Y+
MD5:	A4F438CAD14E0E2CA9EEC23174BBD16A
SHA1:	41FC65053363E0EEE16DD286C60BEDE6698D96B3
SHA-256:	9D9BCADE7A7F486C0C652C0632F9846FCFD3CC64FEF87E5C4412C677C854E389
SHA-512:	FD41BCD1A462A64E40EEE58D2ED85650CE9119B2BB174C3F8E9DA67D4A349B504E32C449C4E44E2B50E4BEB8B650E6956184A9E9CD09B0FA5EA2778292B01E A5
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB7hg4.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png

Preview:

.PNG........IHDR................a....sRGB.........gAMA......a.....pHYs..........(J...._IDAT8O.RMJ.@...&.....B%PJ.-.......... ...7..P..P....JhA..*$Mf..j.*n.*~.y...}...:...b...b.H<.)...f.U...f
s`.rL....}.v.B..d.15..\T.*.Z_..'.}..rc....(...9V.&.....|.qd...8.j..... J...^..q.6..KV7Bg.2@).S.l#R.eE.. ..:_.....l.....FR........r...y...eIC......D.c......0.0..Y..h....t....k.b..y^..1a.D..|...#.ldra.n
.0.......:@.C.Z..P....@...*......z.....p....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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/6rIcBfYxGoxfxfrLqHPKhif7T
MD5:	4F50C6271B3DF24A75AD8E9822453DA3
SHA1:	F8987C61D1C2D2EC12D23439802D47D43FED3BDF
SHA-256:	9AE6A4C5EF55043F07D888AB192D82BB95D38FA54BB3D41F701863239E16E21C
SHA-512:	AFA483EAFEAF31530487039FB1727B819D4E61E54C395BA9553C721FB83C3B16EDF88E60853387A4920AB8F7DFAD704D1B6D4C12CDC302BE05427FC90E7FAC 8
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\9QTQHWWN\BBPfCZL[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 50 x 50
Category:	downloaded
Size (bytes):	2313
Entropy (8bit):	7.594679301225926
Encrypted:	false
SSDEEP:	48:5Zvh21Zt5SkY33fS+PuSsgSrrVi7X3ZgMjkCqBn9VKg3dPnRd:vkrrS333q+PagKk7X3ZgaI9kMpRd
MD5:	59DAB7927838DE6A39856EED1495701B
SHA1:	A80734C857BFF8FF159C1879A041C6EA2329A1FA
SHA-256:	544BA9B5585B12B62B01C095633EFC953A7732A29CB1E941FDE5AD62AD462D57
SHA-512:	7D3FB1A5CC782E3C5047A6C5F14BF26DD39B8974962550193464B84A9B83B4C42FB38B19BD0CEF8247B78E3674F0C26F499DAFCF9AF780710221259D2625DB8
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBPfCZL.img?h=27&w=27&m=6&q=60&u=t&o=t&l=f&f=png

Preview:

GIF89a2.2.....7..;..?..C..I..H..<..9.....8..F..7..E..@..C..@..6..9..8..J..*z.G..>..?..A..6..>..8..:..A..=..B..4..B..D..=..K..=..@..<..:..3~.B..D.....,|.4..2..6..:..J..;..G....Fl..1}.4..R....
.Y..E..>..9..5..X..A..2..P..J../|.9.....T.+Z.....+..<.Fq.Gn..V..;..7.Lr..W..C..<.Fp.]......A.....0{.L..E..H..@.....3..3..O..M..K....#[.3i..D..>........I....<n..;..Z..1..G..8..E....Hu..1..>..
T..a.Fs..C..8..0}....;..6..t.Ft..5.Bi..:.x...E.....'z^~.......[....8`..........;..@..B.....7.....<.................F.....6..........>..?.n......g.......s...)a.Cm....'a.0Z..7....3f..<.:e.....@.q.....Ds..B....!P
.n...J............Li..=......F.....B.....:r....w..|..........`..[}.g...J.Ms..K.Ft.....'..>..........Ry.Nv.n..]..Bl........S..;....Dj.....=.....O.y.......6..J.......)V..g..5.......!..NETSCAPE2.0.....!...d...,....2.2......
..3.`..9.(|.d.C .wH.(."D...(D.....d.Y......<.(PP.F...dL.@.&.28..$1S....*TP......>...L..!T.X!.(..@a..IsgM..|..Jc(Q.+.......2.:.)y2.J......W,..eW2.!....!....C.....d...zeh....P.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\BBZ3zrM[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	762
Entropy (8bit):	7.614206271808948
Encrypted:	false
SSDEEP:	12:6v/78/W/6Tr7wRY1xnBIIpFHsY6ppwWyqx40riXsto+JLNLX8TW9SxOaJrJEQIYR:U/6AIOQFHsY6pGqBiXsttxsTLxOaJrJ9
MD5:	4948BCF4790FCC1A155C882BB00882E1
SHA1:	B99BA11A86E5D0798DF7EBA4EB3490DC8AAA8523
SHA-256:	6A989B924D2197375361EEA4F4BD018D02F664AE3A2B11F4255E486A5F8691B7
SHA-512:	ED70FACA673FD63076CC53DF9E9AE28E0A7FBF7DE177F5E1DA266220BBA136BA4F657DDBD3EEA3D20B5B7F938D389F62885E96BB03CFCB53C2D49B30536EA675
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBZ3zrM.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....IDAT8OeSOO.Q.....Bi.....&.h.!.h....x.....$.M.\|.o...9z.^.d...Q...."...t.m...8.-.....}o..q..@...O'.^9\|.).7]5H...'+M5.!.....M^@.....?]..m::..V.C.1.8..@.....t..1.fD.3}..y.w..#b(.:....~....$M...&...HGM....$.,?.X.X~.7..`.3.S...8....."Y.*..v.?....*.~5C.....d.CY;..!jh..aat~.k.'.....r.).Dtp..9.s.:.../..~..x2....l...g.rB'R..L.^-...t.p.p..S.U..r.>.[.E.GJ...t.\|..J.*.:m.....p2G.z...r.~.K.a`0.@."..F..]L.._\N.7....?..Lo:..jjt.....F.ke.#..x..."...B.#./.n(..9%..<\|/.....o...<n..;y.j.J6..G....`.3[c.....Q.G3.`86.>\..%.,.\.L-...p=...c..r.%.\|..... ..1f....w....$..2j..@x.....5.-.\};!s..C....5..'V6....&~[...I...j.]K...:....2.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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\9QTQHWWN\ads_batch[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):	10569
Entropy (8bit):	5.42381078610498
Encrypted:	false
SSDEEP:	192:/kNZktorNZ7gy4MjmqeqpG2UNZtCgy4MjmqeqpG2ZBQtorNZ7gy4MjmqeqpG2UNn:/MZTZkBqsZ5BqrPZkBqsZ9
MD5:	DF736C50F8E9F89001D59FC261D9857D
SHA1:	B204B84BA7CED744BC11B3A44177BB07D736DAE6
SHA-256:	B23B6B0CC91476EF64B81A9526705DEA17B81E5F2B1A14FA74E0F45D0745A8CB
SHA-512:	41829132DEE99BF21D81992663D5AA1201A67A20DC8476B213D5D3444BC1788C2E01955B7210B03362A37CB2595752063FC2B9466C22B0208F196EF9E1E088E7
Malicious:	false
IE Cache URL:	http://https://www.redtube.com/_xa/ads_batch?ads=true&clientType=mobile&channel[context_page_type]=home&channel[site]=redtube&site_id=16&device_type=tablet&hc=E55C1A81-A85A-4A89-8CEA-1C82F8033809&data=%5B%7B%22spots%22%3A%5B%7B%22zone%22%3A11531%7D%5D%7D%5D
Preview:	[{"ad_id":1476640231,"member_id":7290,"campaign_id":1005167111,"country_code":"CH","zone_id":"11531","link":"https://ads.trafficjunky.net/click?url=\u0026amp;click_data=QAAAAHocAAC07ytgAAAAAAAAAAALLQAACy0AAAAAAAAHouk7570DWFcIDj4AAAAAAAAAAAEAAAAAAAAAAAAAAA==\u0026amp;geo=CH%7C%3A%7CZH%7C%3A%7CZurich\u0026amp;ip=84.17.52.0\u0026amp;ar=www.redtube.com\u0026amp;ct=wifi\u0026amp;ot=windows\u0026amp;ret=--%7C%7C--\u0026amp;iid=43_1613492148363030103_35962_1016\u0026amp;s_kw=0\u0026amp;kw=%7B%7D\u0026amp;ano=5\u0026amp;imptype=0\u0026amp;adtype=iframe\u0026amp;brw=internet%20explorer\u0026amp;dmp_id=\u0026amp;ISP=Datacamp%20Limited\u0026amp;channel[context_page_type]=home\u0026amp;channel[site]=redtube\u0026amp;x=1\u0026amp;vf=55af3fae754e4f3c557a85d1728ec477fec77c70","img_url":"https://a.adtng.com/get/10009606?1=1","isdefault":0,"html":"\u003cHTML\u003e\u003cHEAD\u003e\u003cTITLE\u003eAd delivery system\u003c/TITLE\u003e\u003cmeta name=\"keywords\" content=\"1005167111\" def=\"0\" z_id=\"115

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\ads_batch[2].json	
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):	2528

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\ads_batch[2].json	
Entropy (8bit):	5.972907823771116
Encrypted:	false
SSDEEP:	48:YAlCWI7avLSbm4NemnvfUT447tDlZrY9kXxR5OMUT447tDlZNmqB:YJkLWWmnr47tDlZrckBSMr47tDlZNx
MD5:	1E95DCDC5877BE1D79DF2ADE2054E73A
SHA1:	92816DEA39F041553A8AEF9CF897A34D37276AE5
SHA-256:	31B7DB910C071A97B040BA13B718F5552EF2A73A5A943BE881D22764985BA2A0
SHA-512:	2FE7509E8682ACEE90B99CDBB235CADD260004CC241AB55A43922BFE94606900B9F46AAAD6CE500CB8B86FE43FC29E0313B77249C11DA2C447393877A1EF5DC
Malicious:	false
IE Cache URL:	http://https://www.redtube.com/_xa/ads_batch?ads=true&clientType=mobile&channel[context_page_type]=home&channel[site]=redtube&site_id=16&device_type=tablet&hc=E55C1A81-A85A-4A89-8CEA-1C82F8033809&data=%5B%7B%22spots%22%3A%5B%7B%22zone%22%3A11571%7D%5D%7D%5D
Preview:	[{"ad_id":1034867511,"member_id":1000249481,"campaign_id":1003661111,"zone_id":11571,"media_type":"image","html":"","full_html":"<!DOCTYPE html>\n<html>\n\t<head>\n\t\t c_id=1003661111 z_id=\"11571\" ad_id=\"1404581891\"-->\n\t\t<meta http-equiv=\"Content-Type\" content=\"text/html; charset=UTF-8\" />\n\t\t<title>Ad delivery system</title>\n\t\t<style type=\"text/css\">\n\t\t\t \n\t\t\ta img { border: 0; }\n\t\t\tbody { margin: 0; padding: 0; text-align: center; }\n\t\t\t-->\n\t\t</style>\n\t</head>\n\t<body style=\"background-color:transparent;\">\n\t\t<a href=\"https://ads.trafficjunky.net/deep_click?adtype=static&ar=www.redtube.com&click_data=tO8rYAAAAACJmJ47EAAAADMtAAAzLQAAAAAAADen0jsDOLhTN9OuPQM4uFMAAAAABaInZVJDGz8AAAAA&ct=wifi&geo=CH%257C%253A%257CZH%257C%253A%257CZurich&info=CiQyNTg3NjZlZC1jMGQ4LTRjNDEtODBhOS1jMWZlMGRkY2FjMTQQtN%2BvgQYaJjAwODkwMmNhLTlkYmEtNDlzZS05YmMzLTdkMzgyYmYwMjk5ZC0xMLNaOLNaSLfOyt4DUgIxNliJsfrcA2C3prvtA3ITNzkxNDk0NjAzMTc0ODYzMTM5NoEBBaInZVJDGz%2BSAQJDS

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\analytics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	47051
Entropy (8bit):	5.516264124030958
Encrypted:	false
SSDEEP:	768:ryOveCSBZfsnt5XqY/yPndFTkoWY3SoavqVy2rlebYUDTJC6g0stZm:ryJNDfs5hYdFTwY3SorSg0su
MD5:	53EE95B384D866E8692BB1AEF923B763
SHA1:	A82812B87B667D32A8E51514C578A5175EDD94B4
SHA-256:	E441C3E2771625BA05630AB464275136A82C99650EE2145CA5AA9853BEDEB01B
SHA-512:	C1F98A09A102BB1E87BFDF825A725B0E2CC1DBEDB613D1BD9E8FD9D8FD8B145104D5F4CACA44D96DB14AC20F2F51B4C653278BFC87556E7F00E48A5FA6231AD
Malicious:	false
IE Cache URL:	http://https://www.google-analytics.com/analytics.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var l=this||self,m=function(a,b){a=a.split(".");var c=l;a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c=c[d]&&c[d]!==Object.prototype[d]?c[d]:c[d]={}:c[d]=b};var q=function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},r=function(a){for(var b in a)if(a.hasOwnProperty(b))return!0;return!1};var t=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?:[/?#]|$))/i;var u=window,v=document,w=function(a,b){v.addEventListener?v.addEventListener(a,b,!1):v.attachEvent&&v.attachEvent("on"+a,b)};var x={},y=function(){x.TAGGING=x.TAGGING\|\|[];x.TAGGING[1]=!0};var z=/:[0-9]+$/,A=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponent(e[0]).replace(/\+/g," ")===b)return b=e.slice(1).join("="),c?b:decodeURIComponent(b).replace(/\+/g," ")}},D=function(a,b){b&&(b=String(b).toLowerCase());if("p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\auction[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	25803
Entropy (8bit):	5.6811104246276996
Encrypted:	false
SSDEEP:	384:RaZb2l4Fp5yhNsKprIKZDt7CbnRtGl0JUjD9RwxPdPQmTDRd+C8081JrC8EynaTG:RhtJr0bGuaD9n4F8081J0TpL8
MD5:	B29F33D38A47A9D74B5BE60D0583BEC2
SHA1:	B9D091C14B6BBA69D5D5FEAF472C0374A8AA43D8
SHA-256:	94FE5426BFF8A39B86A89A67739C4A3249D54391A0ABF52B1B6657635A7F3C9D
SHA-512:	04ED2B2870C532567F82636259B6A47B69F44E83F65512EC6B71F61D096FD20CC28F0F94C07D4A6B7BCC4A5B76B6C3821F4A4B3F4E3C50BBD25F00BD08B0B37
Malicious:	false
IE Cache URL:	http://https://srtb.msn.com/auction?a=de-ch&b=014b5567b7e447e6bb8818568dc78109&c=MSN&d=https%3A%2F%2Fwww.msn.com%2Fde-ch%2F%3Focid%3Diehp&e=HP&f=0&g=homepage&h=&j=0&k=0&l=&m=0&n=infopane%7C3%2C11%2C15&o=&p=init&q=&r=&s=1&t=&u=0&v=0&x=&w=&_=1613524419592
Preview:	.<script id="sam-metadata" type="text/html" data-json="{"optout":{"msaOptOut":false,"browserOptOut":false},"taboola":{"sessionId":"v2_2b4ec58c135ba026f01b1bc23eb93a93_4e97157c-3a47-4d54-85f9-d9b21244588d-tuct72574b9_1613492025_1613492025_CIi3jgYQr4c_GID769D9q7mXzQEgASgBMCs4stANQNCIEEje2NkDUP_____wFYAGAAaKKcqr2pwqnJjgE"},"tbsessionid":"v2_2b4ec58c135ba026f01b1bc23eb93a93_4e97157c-3a47-4d54-85f9-d9b21244588d-tuct72574b9_1613492025_1613492025_CIi3jgYQr4c_GID769D9q7mXzQEgASgBMCs4stANQNCIEEje2NkDUP_____wFYAGAAaKKcqr2pwqnJjgE","pageViewId":"014b5567b7e447e6bb8818568dc78109","RequestLevelBeaconUrls":[]}">.</script>.<li class="triptych serversidenativead hasimage " data-json="{"tvb":[],"trb":[],"tjb":[],"p":"taboola","e":true}" data-provider="taboola" data-ad-region="infopane" data-ad-index="3" data-viewability="">

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\checksync[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\checksync[1].htm	
Category:	dropped
Size (bytes):	20808
Entropy (8bit):	5.3018084083386
Encrypted:	false
SSDEEP:	384:RqAGcVXlblcqnzleZSug2f5vzBgF3OZOfQWwY4RXrqt:+86qhbz2RmF3OsfQWwY4RXrqt
MD5:	F20E359D299221FAA621EEED8710C7CE
SHA1:	CDE9D4EAA1954C0BDC907377024AB11A62EBC3C6
SHA-256:	BC6612574C7F898BCA97BB62CEB242821B9EDEE9B5A01F30113E0C4189CA72A0
SHA-512:	477A7A1D520D0A580358B36F368FB625A692D5F6701FE4AD5FAA617A87A5C1027ECF95FDB07ED0E5AB09A504C62DBDAF89FDD1A5B153D6B4AAEC460E8EB76A 47
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":75,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime" :"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data- v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0}},"hasSameSiteSupport":" 0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","y ld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"succe ssLper":10,"failLper":10,"logUrl":{"cl":"https:\/\/hblg.media.net\/log?logid=kfk&evtid=chlog"}},"csloggerUrl":"https:\/\/cslogger.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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):	5.3018084083386
Encrypted:	false
SSDEEP:	384:RqAGcVXlblcqnzleZSug2f5vzBgF3OZOfQWwY4RXrqt:+86qhbz2RmF3OsfQWwY4RXrqt
MD5:	F20E359D299221FAA621EEED8710C7CE
SHA1:	CDE9D4EAA1954C0BDC907377024AB11A62EBC3C6
SHA-256:	BC6612574C7F898BCA97BB62CEB242821B9EDEE9B5A01F30113E0C4189CA72A0
SHA-512:	477A7A1D520D0A580358B36F368FB625A692D5F6701FE4AD5FAA617A87A5C1027ECF95FDB07ED0E5AB09A504C62DBDAF89FDD1A5B153D6B4AAEC460E8EB76A 47
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":75,"visitor":{"vsCk":"visitor-id","vsDaCk":"data","sepVal":"|","sepTime" :"*","sepCs":"~~","vsDaTime":31536000,"cc":"CH","zone":"d"},"cs":"1","lookup":{"g":{"name":"g","cookie":"data-g","isBl":1,"g":1,"cocs":0},"vzn":{"name":"vzn","cookie":"data- v","isBl":1,"g":0,"cocs":0},"brx":{"name":"brx","cookie":"data-br","isBl":1,"g":0,"cocs":0},"lr":{"name":"lr","cookie":"data-lr","isBl":1,"g":1,"cocs":0}},"hasSameSiteSupport":" 0","batch":{"gGroups":["apx","csm","ppt","rbcn","son","bdt","con","opx","tlx","mma","c1x","ys","sov","fb","r1","g","pb","dxu","rkt","trx","wds","crt","ayl","bs","ui","shr","lvr","y ld","msn","zem","dmx","pm","som","adb","tdd","soc","adp","vm","spx","nat","ob","adt","got","mf","emx","sy","lr","ttd"],"bSize":2,"time":30000,"ngGroups":[]},"log":{"succe ssLper":10,"failLper":10,"logUrl":{"cl":"https:\/\/hblg.media.net\/log?logid=kfk&evtid=chlog"}},"csloggerUrl":"https:\/\/cslogger.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\de-ch[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	421560
Entropy (8bit):	5.43904312031383
Encrypted:	false
SSDEEP:	3072:AJkJULxx+vstaF/PAjkCGy4ag9tsHbQgXZiWDMsURvtILnWw3SdimGeX7mLX:AJkKOvDy4h8bQAZi8H4vtITWw3GGeX7G
MD5:	B32456A59C22A710D733801E4BEA1E6A
SHA1:	CE54E6E6E40A756DBCA4094C21901B8554E8FED0
SHA-256:	B7378E933811AB62671169FF839EA6562544E68FE3001C9964EAAD449E62E1F2
SHA-512:	7D600EBC1C4B3EE398C2E0E0C79130C026C8053757557822A474C8123BDDC149839C5028FFA2E85925E1002BC6BB409C30BAA8F562077771C055FE15155B2402
Malicious:	false
Preview:	<!DOCTYPE html><html prefix="og: http://ogp.me/ns# fb: http://ogp.me/ns/fb#" lang="de-CH" class="hiperf" dir="ltr" >.. <head data-info="v:20210208_312578 24;a:014b5567-b7e4-47e6-bb88-18568dc78109;cn:15;az:{did:951b20c4cd6d42d29795c846b4755d88, rid: 15, sn: neurope-prod-hp, dt: 2021-02-15T13:58:39.7944938Z, bt: 2021-02-08T21:20:57.5642255Z};ddpi:1;dpio:;dpi:1;dg:tmx.pc.ms.ie10plus;th:start;PageName:startPage;m:de-ch;cb:;l:de-ch;mu:de-ch;ud:{cid:,vk:homepage,n:,l:de- ch,ck:};xd:BBqgbZW;ovc:f;al:;fxd:f;xdpub:2021-01-12 22:59:27Z;xdmap:2021-02-16 16:12:26Z;axd:;f:msnallexpusers,muidflt12cf,muidflt17cf,muidflt52cf,muidflt5 6cf,mmxandroid1cf,pneedge3cf,audexhp2cf,tokenblockgc,bingcollabhp2cf,compliancehz1cf,artgly5cf,onetrustpoplive,1s-bing-news,vebudumu04302020,bbh202005 21msn,prong1aat,prg-gitconfigs-t11;userOptOut:false;userOptOutOptions:" data-js="{"dpi":1.0,"ddpi":1.0,"dpio":null,"forcedpi ":null,"dms":6000,"ps":1000,"b

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\de-ch[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	76785
Entropy (8bit):	5.343242780960818
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\de-ch[1].json	
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\9QTQHWWN\default-redtube_logged_out[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):	6043
Entropy (8bit):	5.105879346031891
Encrypted:	false
SSDEEP:	96:KM8zXfG6V2o+zScJzVTb20ogw+8zNzuIKD679d8b7fTpERQqA3W3DC:DZ6VNg7TKEo0679cbT2RQqA3W3DC
MD5:	6E0958AE85C65140246914D2EE46D5A9
SHA1:	2B7A8027F00F1F0F3F6F153EBC50838CB8E0C696
SHA-256:	6E4E6D59FEAEB182DBC41AC2A59E8EECBCCD2D0A53EA40D87127963C27BDF363
SHA-512:	D813FD5E049CD8A0181B8D472CB8F00ACAFB8F4FB435EB83697AE20B4D6319F0F8CE327162DB3C7D141611CBCC5430A23D0348DA488CE21D654672080EE5AB1
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/js/generated/pc/default-redtube_logged_out.js?v=6f5214796229481244dc03c6129efd79f60bd552
Preview:	var LoginForm=function(){"use strict";var _=this;_.defaultSettings={mainLoginDiv_id:"login_form",disableLoginDiv_class:"disable_login_container",usernameInput_id:"login_username",passwordInput_id:"login_password",activeSubMenu_class:"sub_menu_active",login_submit:"js-loginSubmitModal",login_modal:"login_modal"},_.init=function(e){_.params=$.extend(!0,_.defaultSettings,e),_.add_listeners(),_.recaptchaEnable=_.isRecaptchaEnable()},_.add_listeners=function(){$(".login_form_X").click(function(){_.params.disableLogin?$("."+_.params.disableLoginDiv_class).slideUp():$("#"+_.params.mainLoginDiv_id).slideUp(),_.resetErrorMessages(),$('input[name="username"]').val(""),$('input[name="password"]').val("")}),$("#js_loginform").on("submit",function(e){e.preventDefault(),e.stopImmediatePropagation(),_.submitLogin()}),$(".login_rt_premium_btn").click(function(){_.openOauthDialog("/rtplogin")}),$(".js_pornhub_login").click(function(){_.openOauthDialog("/phlogin")}),$("#signup_link_in_modal").on("click"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\generated-service_worker_starter-1.0.0[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):	3420
Entropy (8bit):	5.145089778442548
Encrypted:	false
SSDEEP:	48:7HaIyDwYawCZ6d6g+FYktiFfxf4KIzOPI5DfCjv+eE09ajIGUTVBlBVNvqw2QRyS:7HaDesd6JF94Lf4nx+x9FTLDVNeQM8
MD5:	252268FDAE62AB6C07F60CD8EE76DD25
SHA1:	A2A8B8D71F1EC4A0708DE8AB925E790A16971935
SHA-256:	CECDB8C1DA82E6EED06DB53AD89A6E3C801FA62AFDF08025413A995D68485DBF
SHA-512:	160FA83DA6A17D1220636236DAD668BAC7DBACC0DDB4D7E7E2B6FB8B975A3E4F3F27EFDC8AA686BCAD98A8A97D87CB9BC9AF5BEE15E6A1D68627580B62A20160
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/js/common/common/generated-service_worker_starter-1.0.0.js
Preview:	var SW_Starter=function(){"use strict";var n=this,o=null;n.init=function(e){n.params=e,n.add_listeners()},n.add_listeners=function(){void 0!==page_params.holiday_promo&&page_params.holiday_promo&&"serviceWorker"in navigator?(window.addEventListener("load",function(){navigator.serviceWorker.register(page_params.sw_starter_setup.serviceWorkerPath).then(function(e){o=e,n.manageServiceWorkerVersion(),"PushManager"in window&&page_params.user.isLoggedIn&&n.params.userEnabledNotification?(console.log("Notification Push is supported"),n.askPermission()):console.log("Push messaging is not supported")},function(e){console.log("ServiceWorker registration failed: ",e)})}),window.addEventListener("appinstalled",function(e){console.log("RedTube App Installed"),n.params.isMobile&&ga("send",{hitType:"event",eventCategory:"PWA",eventAction:"Add_to_homescreen",eventLabel:"Mobile"})})):(void 0===page_params.holiday_promo||!page_params.holiday_promo)&&"serviceWorker"in navigator&&navigator.serviceWorker.g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\http___cdn.taboola.com_libtrc_static_thumbnails_831afd7b16ef15301070d350663f9c7a[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):	17922

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\http___cdn.taboola.com_libtrc_static_thumbnails_831afd7b16ef15301070d350663f9c7a[1].jpg	
Entropy (8bit):	7.859255856375248
Encrypted:	false
SSDEEP:	384:OkVCDMrzQUIa36EPUOgrSdPRD2kPJLx25XDenIqTN:OkVCYrzWEPUOgr4h2khLx2XCnXTN
MD5:	CBA5C805BEE81A5DA114F7646613F3FC
SHA1:	587CD288207C2C1F62E43663AD4AC0EAFFF9F87A
SHA-256:	A4A7FD3DA82AD14ED5320348B475C6DF8A3838122CFA1C453FE5D314C32811E9
SHA-512:	1A0F52890E0F0460B460C926A0339B96EB51382475E583759F5DDE694ACF2A57148E8E5F12ED9D0332D45C8FF78E7B27631C4F787EE74A8B715084D09E96101C
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%2F831afd7b16ef15301070d350663f9c7a.jpg
Preview:	.....JFIF.....TICC_PROFILE.....DUCCM.@..mntrRGB XYZ .....acspMSFT....CANOZ009.....-CANO.....rTRC...,....gTRC...,....bTRC...,....rXYZ...8....gXYZ...L....bXYZ...`....chad...t...,cprt.....@dmnd.....|dmdd...\....wtpt.....tech.....desc...\....ucmI.....4curv.....".',.1.6.;.@.E.J.O.T.Y.^.c.h.m.r.v.{.....$.+.1.7.>.D.K.R.Y._.f.m.u.\|.....&./.8.A.J.S.].f.p.z.....!.,.7.C.N.Z.f.q.}.....-.:.G.U.b.p.~.....*.9.H.X.g.v.....&.7.H.X.i.z.....*.<.O.a.s.....2.E.Y.m.....$.9.N.d.y.....'.=.S.j.....!.9.P.h.....*.B.[.t.....&.@.Z.t.....I.d.....%.A.].y.....&.C.`.}.....0.N.m.....%.D.d.....".B.c.....'.H.i.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\load-1.0.3[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	4771
Entropy (8bit):	5.343609788879507
Encrypted:	false
SSDEEP:	96:YqvkALGHRl3Oh3nwy0vwpoH3GMWQlUmYEAYui:YXNr3UdBoH3xVl8Q
MD5:	589EB8DFC8140658A5C4035AD555C34E
SHA1:	0EC7F75B69AC8A674471B2D7BC5636159B673DDF
SHA-256:	876CBB2343AD3050EDE32DB4F222CF1EAEF596ADAC6EFAFE53F235B264AE145A
SHA-512:	483111CCE524C679F1EDA3AE32F1A257BB217EBC5D35130FA619DFA41EC0A956010356EF94129AD639B0FD37D19C54BC852D6D046A7CA14ECBF93EB505127B4
Malicious:	false
IE Cache URL:	http://https://cdn1d-static-shared.phncdn.com/head/load-1.0.3.js
Preview:	/*! head.load - v1.0.3 */.(function(H,t){var l=H.document,F=[],a={},b={},d="async" in l.createElement("script")||"MozAppearance" in l.documentElement.style||H.opera,E,f=H.head_conf&&H.head_conf.head||"head",j=H[f]=(H[f]||function(){j.ready.apply(null,arguments)}),x=1,J=2,z=3,r=4;function L(){}function I(e,P){if(!e){return}if(typeof e==="object"){e=[].slice.call(e)}for(var O=0,N=e.length;O<N;O++){P.call(e,e[O],O)}}function D(e,N){var O=Object.prototype.toString.call(N).slice(8,-1);return N!==t&&N!==null&&O===e}function u(e){return D("Function",e)}function C(e){return D("Array",e)}function m(O){var e=O.split("/"),N=e[e.length-1],P=N.indexOf("?");return P!==-1?N.substring(0,P):N}function q(e){e=e||L;if(e._done){return}e();e._done=1}function y(R,O,e,Q){var N=(typeof R==="object")?R:{test:R,success:!!O?C(O)?O:[O]:false,failure:!!e?C(e)?e:[e]:false,callback:Q||L};var P=!!N.test;if(P&&!!N.success){N.success.push(N.callback);j.load.apply(null,N.success)}else{if(!P&&!!N.failure){N.failure.push(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\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):	384619
Entropy (8bit):	5.4840339551796475
Encrypted:	false
SSDEEP:	6144:4t99Tw5qIZvbzH0m9ZnGQVvgz5RCu1b4xKSv7IW:oIZvvPnGQVvgnxVcK07IW
MD5:	C9DDE414BC967874E3FB6B1457032F31
SHA1:	C46657258A035C1F3FEC4D77F1BA048C27B68D2E
SHA-256:	0C66344911A1192AC3D1A6E6A57F244B91A4C4B79D11CCE1827D866E9E62DA2B
SHA-512:	9B7BFE2B770AC6C68C4B45D0BA8805E0319073C09C14288E401E2E04F5EB66654C9A48AB3B16818288BB9F5C1DA4468668469BC06A52D11C9DD870A6E9177DC
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

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.96470149693475
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:	602b97e0b415b.png.dll
File size:	343552
MD5:	262590037c93a5496b38565c9dfc85d8
SHA1:	29616a643f896d6ab55d7129a813fa4056400c0e
SHA256:	eaeb42576fb19b866abdc99b5b8f867f3c69d8da9e941f2ca5af1f0e3e342a6c
SHA512:	c566f68a5d8b6769595836bffdf7e05b439a9a26ed7a500348a6ca4dea3effbdf0db1da64d219b7c6ac35143604782d5ffd47633a6297e3191224210d4de0bee
SSDEEP:	3072:lYEuU/HsL0icNk2S/G7xBYT147Q1zzWpYnJw19qVFXEqnQvSoLRRybz5m76nf7fF:ypGHq8ujuVeZWQ1WmnaHqrCybs+fbpC
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T...5...5...5...g2..5...z7..5...g4..5...g"..5...g%..5.....5...5..N5...g+..5...g3..5...g5..5...g0..5..Rich.5.....PE..L..

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x100272a5
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE
Time Stamp:	0x4B71D781 [Tue Feb 9 21:45:37 2010 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	68b46a79797ab738bab23808c616c230

Entrypoint Preview

Instruction
mov edi, edi
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007F796C97D3D7h
call 00007F796C9842BCh
push dword ptr [ebp+08h]
mov ecx, dword ptr [ebp+10h]
mov edx, dword ptr [ebp+0Ch]
call 00007F796C97D2C1h
pop ecx

Instruction
pop ebp
retn 000Ch
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
xor ecx, ecx
cmp eax, dword ptr [1004F310h+ecx*8]
je 00007F796C97D3E5h
inc ecx
cmp ecx, 2Dh
jc 00007F796C97D3C3h
lea ecx, dword ptr [eax-13h]
cmp ecx, 11h
jnbe 00007F796C97D3E0h
push 0000000Dh
pop eax
pop ebp
ret
mov eax, dword ptr [1004F314h+ecx*8]
pop ebp
ret
add eax, FFFFFF44h
push 0000000Eh
pop ecx
cmp ecx, eax
sbb eax, eax
and eax, ecx
add eax, 08h
pop ebp
ret
call 00007F796C982E3Fh
test eax, eax
jne 00007F796C97D3D8h
mov eax, 1004F478h
ret
add eax, 08h
ret
call 00007F796C982E2Ch
test eax, eax
jne 00007F796C97D3D8h
mov eax, 1004F47Ch
ret
add eax, 0Ch
ret
mov edi, edi
push ebp
mov ebp, esp
push esi
call 00007F796C97D3B7h
mov ecx, dword ptr [ebp+08h]
push ecx
mov dword ptr [eax], ecx
call 00007F796C97D357h
pop ecx
mov esi, eax
call 00007F796C97D391h
mov dword ptr [eax], esi
pop esi
pop ebp
ret
mov edi, edi
push ebp
mov ebp, esp

Instruction
sub esp, 4Ch
mov eax, dword ptr [1004F72Ch]
xor eax, ebp
mov dword ptr [ebp-04h], eax
push ebx
xor ebx, ebx
push esi
mov esi, dword ptr [ebp+08h]

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x4e2f0	0x8b	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4da4c	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb0000	0x4c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb1000	0x1bcc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x3c1f0	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x4c070	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x3c000	0x188	.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	0x3a9fc	0x3aa00	False	0.716355443763	data	6.9097618053	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x3c000	0x1237b	0x12400	False	0.713011023116	data	6.58294971291	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x4f000	0x60828	0x3a00	False	0.617120150862	data	5.87627574056	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xb0000	0x4c8	0x600	False	0.391927083333	data	3.58188077568	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb1000	0x2b38	0x2c00	False	0.519797585227	data	5.07362748368	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xb00a0	0x2a4	data	English	United States
RT_MANIFEST	0xb0348	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import

DLL	Import
KERNEL32.dll	ExitProcess, TlsSetValue, CreateProcessA, FindFirstFileA, RemoveDirectoryA, FindClose, LoadLibraryA, GetModuleFileNameA, FindNextFileA, VirtualProtect, GetFileTime, GetCurrentThreadId, TlsAlloc, GetTempPathA, SetEnvironmentVariableA, CompareStringW, CompareStringA, CreateFileA, SetStdHandle, WriteConsoleW, GetConsoleOutputCP, WriteConsoleA, WideCharToMultiByte, InterlockedIncrement, InterlockedDecrement, InterlockedExchange, MultiByteToWideChar, Sleep, InitializeCriticalSection, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, GetSystemTimeAsFileTime, GetCommandLineA, GetCPInfo, RaiseException, GetLastError, HeapFree, RtlUnwind, LCMapStringA, LCMapStringW, GetTimeZoneInformation, HeapAlloc, GetModuleHandleW, GetProcAddress, TlsGetValue, TlsFree, SetLastError, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, HeapCreate, HeapDestroy, VirtualFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetStringTypeA, GetStringTypeW, VirtualAlloc, HeapReAlloc, WriteFile, GetConsoleCP, GetConsoleMode, FlushFileBuffers, ReadFile, SetFilePointer, CloseHandle, HeapSize, GetACP, GetOEMCP, IsValidCodePage, GetUserDefaultLCID, GetLocaleInfoA, EnumSystemLocalesA, IsValidLocale, InitializeCriticalSectionAndSpinCount, GetLocaleInfoW, GetModuleHandleA
WS2_32.dll	WSACloseEvent, WSAStartup, WSAConnect, WSACleanup, WSASocketA, WSAAddressToStringA, WSAWaitForMultipleEvents

Exports

Name	Ordinal	Address
Crossput	1	0x10020e90
Directclear	2	0x10021420
DllRegisterServer	3	0x10020f70
Summerwind	4	0x10021340

Version Infos

Description	Data
LegalCopyright	Copyright Goodsure 1998-2014
FileVersion	4.0.4.690
CompanyName	Goodsure
ProductName	Give make
ProductVersion	4.0.4.690
FileDescription	Give make
OriginalFilename	Mine.dll Choosegroup
Translation	0x0409 0x04e4

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 151

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 17:13:40.502978086 CET	49730	443	192.168.2.6	104.20.185.68
Feb 16, 2021 17:13:40.525497913 CET	49731	443	192.168.2.6	104.20.185.68
Feb 16, 2021 17:13:40.555852890 CET	443	49730	104.20.185.68	192.168.2.6
Feb 16, 2021 17:13:40.556010962 CET	49730	443	192.168.2.6	104.20.185.68
Feb 16, 2021 17:13:40.558958054 CET	49730	443	192.168.2.6	104.20.185.68
Feb 16, 2021 17:13:40.578548908 CET	443	49731	104.20.185.68	192.168.2.6
Feb 16, 2021 17:13:40.578684092 CET	49731	443	192.168.2.6	104.20.185.68
Feb 16, 2021 17:13:40.579349995 CET	49731	443	192.168.2.6	104.20.185.68
Feb 16, 2021 17:13:40.611844063 CET	443	49730	104.20.185.68	192.168.2.6
Feb 16, 2021 17:13:40.614324093 CET	443	49730	104.20.185.68	192.168.2.6
Feb 16, 2021 17:13:40.614352942 CET	443	49730	104.20.185.68	192.168.2.6
Feb 16, 2021 17:13:40.614428043 CET	49730	443	192.168.2.6	104.20.185.68
Feb 16, 2021 17:13:40.614448071 CET	49730	443	192.168.2.6	104.20.185.68
Feb 16, 2021 17:13:40.632158041 CET	49730	443	192.168.2.6	104.20.185.68
Feb 16, 2021 17:13:40.632299900 CET	443	49731	104.20.185.68	192.168.2.6
Feb 16, 2021 17:13:40.632580042 CET	49730	443	192.168.2.6	104.20.185.68
Feb 16, 2021 17:13:40.632780075 CET	49730	443	192.168.2.6	104.20.185.68
Feb 16, 2021 17:13:40.633495092 CET	443	49731	104.20.185.68	192.168.2.6
Feb 16, 2021 17:13:40.633526087 CET	443	49731	104.20.185.68	192.168.2.6
Feb 16, 2021 17:13:40.633594036 CET	49731	443	192.168.2.6	104.20.185.68
Feb 16, 2021 17:13:40.633624077 CET	49731	443	192.168.2.6	104.20.185.68
Feb 16, 2021 17:13:40.637988091 CET	49731	443	192.168.2.6	104.20.185.68
Feb 16, 2021 17:13:40.638376951 CET	49731	443	192.168.2.6	104.20.185.68
Feb 16, 2021 17:13:40.684895992 CET	443	49730	104.20.185.68	192.168.2.6
Feb 16, 2021 17:13:40.685218096 CET	443	49730	104.20.185.68	192.168.2.6
Feb 16, 2021 17:13:40.685568094 CET	443	49730	104.20.185.68	192.168.2.6
Feb 16, 2021 17:13:40.687402964 CET	443	49730	104.20.185.68	192.168.2.6
Feb 16, 2021 17:13:40.687488079 CET	49730	443	192.168.2.6	104.20.185.68
Feb 16, 2021 17:13:40.687982082 CET	443	49730	104.20.185.68	192.168.2.6
Feb 16, 2021 17:13:40.688045979 CET	49730	443	192.168.2.6	104.20.185.68
Feb 16, 2021 17:13:40.688268900 CET	49730	443	192.168.2.6	104.20.185.68
Feb 16, 2021 17:13:40.690998077 CET	443	49731	104.20.185.68	192.168.2.6
Feb 16, 2021 17:13:40.691303015 CET	443	49731	104.20.185.68	192.168.2.6
Feb 16, 2021 17:13:40.691322088 CET	443	49731	104.20.185.68	192.168.2.6
Feb 16, 2021 17:13:40.691420078 CET	49731	443	192.168.2.6	104.20.185.68
Feb 16, 2021 17:13:40.691553116 CET	443	49731	104.20.185.68	192.168.2.6
Feb 16, 2021 17:13:40.691634893 CET	49731	443	192.168.2.6	104.20.185.68
Feb 16, 2021 17:13:40.695820093 CET	49731	443	192.168.2.6	104.20.185.68
Feb 16, 2021 17:13:40.706650972 CET	443	49730	104.20.185.68	192.168.2.6
Feb 16, 2021 17:13:40.706773996 CET	443	49730	104.20.185.68	192.168.2.6
Feb 16, 2021 17:13:40.706824064 CET	49730	443	192.168.2.6	104.20.185.68
Feb 16, 2021 17:13:40.707855940 CET	49730	443	192.168.2.6	104.20.185.68
Feb 16, 2021 17:13:40.740942955 CET	443	49730	104.20.185.68	192.168.2.6
Feb 16, 2021 17:13:40.748871088 CET	443	49731	104.20.185.68	192.168.2.6
Feb 16, 2021 17:13:45.842786074 CET	49742	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.842822075 CET	49741	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.842888117 CET	49743	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.842927933 CET	49740	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.847037077 CET	49744	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.847135067 CET	49745	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.886302948 CET	443	49742	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.886326075 CET	443	49740	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.886339903 CET	443	49743	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.886352062 CET	443	49741	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.886506081 CET	49742	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.886534929 CET	49741	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.886554003 CET	49743	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.886564970 CET	49740	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.887330055 CET	49740	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.887384892 CET	49741	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.888086081 CET	49743	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.888796091 CET	49742	443	192.168.2.6	151.101.1.44

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 17:13:45.890460014 CET	443	49745	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.890486956 CET	443	49744	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.890597105 CET	49745	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.890638113 CET	49744	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.891359091 CET	49744	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.909225941 CET	49745	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.930746078 CET	443	49740	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.930784941 CET	443	49741	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.931432009 CET	443	49743	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.931921959 CET	443	49741	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.931965113 CET	443	49741	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.932018042 CET	443	49741	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.932035923 CET	49741	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.932053089 CET	49741	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.932063103 CET	443	49740	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.932075977 CET	49741	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.932106972 CET	443	49740	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.932142019 CET	443	49740	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.932157993 CET	49740	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.932216883 CET	49740	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.932224989 CET	49740	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.932389021 CET	443	49742	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.932462931 CET	443	49743	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.932506084 CET	443	49743	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.932528973 CET	443	49743	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.932552099 CET	49743	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.932585001 CET	49743	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.932604074 CET	49743	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.933723927 CET	443	49742	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.933772087 CET	443	49742	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.933805943 CET	443	49742	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.933834076 CET	49742	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.933866024 CET	49742	443	192.168.2.6	151.101.1.44
Feb 16, 2021 17:13:45.934763908 CET	443	49744	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.944025040 CET	443	49744	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.944067001 CET	443	49744	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.944122076 CET	443	49744	151.101.1.44	192.168.2.6
Feb 16, 2021 17:13:45.944122076 CET	49744	443	192.168.2.6	151.101.1.44

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 17:13:26.530545950 CET	58377	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:26.535639048 CET	55074	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:26.579559088 CET	53	58377	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:26.584583998 CET	53	55074	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:26.708318949 CET	54513	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:26.757041931 CET	53	54513	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:27.547569990 CET	62044	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:27.596282005 CET	53	62044	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:28.818286896 CET	63791	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:28.869812012 CET	53	63791	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:30.161295891 CET	64267	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:30.219795942 CET	53	64267	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:30.445797920 CET	49448	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:30.497364044 CET	53	49448	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:31.710880041 CET	60342	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:31.762528896 CET	53	60342	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:32.519153118 CET	61346	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:32.567919970 CET	53	61346	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:33.760020971 CET	51774	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:33.808804035 CET	53	51774	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:35.362014055 CET	56023	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:35.410820961 CET	53	56023	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 17:13:36.044239044 CET	58384	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:36.114939928 CET	53	58384	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:37.039403915 CET	60261	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:37.100712061 CET	53	60261	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:37.368771076 CET	56061	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:37.417718887 CET	53	56061	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:37.947057962 CET	58336	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:37.991230011 CET	53781	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:37.998528004 CET	53	58336	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:38.051165104 CET	53	53781	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:39.869321108 CET	54064	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:39.935137987 CET	53	54064	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:40.383327007 CET	52811	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:40.448982954 CET	55299	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:40.450809002 CET	53	52811	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:40.500674963 CET	53	55299	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:42.637480974 CET	63745	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:42.705665112 CET	53	63745	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:43.583009958 CET	50055	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:43.652962923 CET	53	50055	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:43.815963984 CET	61374	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:43.877336025 CET	53	61374	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:44.347043991 CET	50339	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:44.398403883 CET	53	50339	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:45.669475079 CET	63307	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:45.718072891 CET	53	63307	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:48.200419903 CET	49694	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:48.252028942 CET	53	49694	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:52.783543110 CET	54982	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:52.832423925 CET	53	54982	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:53.607100964 CET	50010	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:53.656021118 CET	53	50010	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:55.081032991 CET	63718	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:55.130105972 CET	53	63718	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:56.300245047 CET	62116	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:56.349039078 CET	53	62116	8.8.8.8	192.168.2.6
Feb 16, 2021 17:13:57.501789093 CET	63816	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:13:57.550452948 CET	53	63816	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:00.811645985 CET	55014	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:00.860160112 CET	53	55014	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:02.397031069 CET	62208	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:02.448510885 CET	53	62208	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:03.578452110 CET	57574	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:03.629976034 CET	53	57574	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:04.493519068 CET	51818	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:04.542546034 CET	53	51818	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:04.731441021 CET	56628	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:04.783229113 CET	53	56628	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:05.964128971 CET	60778	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:06.013076067 CET	53	60778	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:06.784733057 CET	53799	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:06.833520889 CET	53	53799	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:06.958748102 CET	60778	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:07.007462025 CET	53	60778	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:08.064853907 CET	60778	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:08.064970970 CET	53799	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:08.113487959 CET	53	60778	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:08.113524914 CET	53	53799	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:09.068564892 CET	53799	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:09.117319107 CET	53	53799	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:10.069426060 CET	60778	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:10.118012905 CET	53	60778	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:11.096093893 CET	53799	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:11.144737959 CET	53	53799	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 17:14:13.671142101 CET	54683	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:13.732573032 CET	53	54683	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:14.080821991 CET	60778	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:14.130069017 CET	53	60778	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:15.102526903 CET	53799	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:15.151210070 CET	53	53799	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:21.848594904 CET	59329	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:21.907783985 CET	53	59329	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:22.024662971 CET	64021	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:22.082923889 CET	53	64021	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:25.267642975 CET	56129	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:25.317719936 CET	53	56129	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:28.114837885 CET	58177	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:28.166294098 CET	53	58177	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:37.543057919 CET	50700	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:37.601921082 CET	53	50700	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:54.376358032 CET	54069	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:54.436547041 CET	53	54069	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:55.067223072 CET	61178	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:55.116126060 CET	53	61178	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:55.659739971 CET	57017	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:55.711196899 CET	53	57017	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:56.153168917 CET	56327	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:56.240741014 CET	53	56327	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:56.322215080 CET	50243	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:56.384284973 CET	53	50243	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:56.719775915 CET	62055	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:56.781913042 CET	53	62055	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:57.387100935 CET	61249	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:57.444214106 CET	53	61249	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:58.162694931 CET	65252	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:58.235793114 CET	53	65252	8.8.8.8	192.168.2.6
Feb 16, 2021 17:14:58.996501923 CET	64367	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:14:59.056776047 CET	53	64367	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:00.019397974 CET	55066	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:00.079957008 CET	53	55066	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:00.123913050 CET	60211	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:00.241168022 CET	53	60211	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:00.247208118 CET	56570	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:00.326212883 CET	53	56570	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:00.338891029 CET	58454	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:00.398833990 CET	53	58454	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:00.631527901 CET	55180	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:00.680180073 CET	53	55180	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:09.519328117 CET	58721	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:09.578227997 CET	53	58721	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:22.572022915 CET	57691	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:22.638927937 CET	53	57691	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:22.847590923 CET	52943	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:22.897663116 CET	53	52943	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:23.404803991 CET	59489	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:23.405369997 CET	60023	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:23.405513048 CET	64022	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:23.406085014 CET	57193	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:23.433617115 CET	50248	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:23.453891039 CET	53	60023	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:23.457439899 CET	53	57193	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:23.470242023 CET	53	59489	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:23.470624924 CET	53	64022	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:23.473663092 CET	64413	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:23.485039949 CET	53	50248	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:23.525218010 CET	53	64413	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:23.549473047 CET	60429	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:23.552031040 CET	60345	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 16, 2021 17:15:23.603444099 CET	53	60345	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:23.609720945 CET	53	60429	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:23.885423899 CET	58730	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:23.934315920 CET	53	58730	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:24.519809008 CET	53830	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:24.571234941 CET	53	53830	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:24.763607025 CET	57226	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:24.820764065 CET	53	57226	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:24.851691008 CET	57880	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:24.907445908 CET	60850	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:24.910298109 CET	53	57880	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:24.920401096 CET	53187	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:24.946161032 CET	55830	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:24.948985100 CET	55145	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:24.958975077 CET	53	60850	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:24.977679014 CET	53	53187	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:24.994849920 CET	53	55830	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:25.016117096 CET	53	55145	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:27.158277035 CET	64091	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:27.206814051 CET	53	64091	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:47.259238005 CET	55728	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:47.324301958 CET	53	55728	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:47.704771042 CET	55694	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:47.756269932 CET	53	55694	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:48.223407984 CET	53926	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:48.227658033 CET	65531	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:48.230021954 CET	65437	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:48.278681993 CET	53	65437	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:48.279166937 CET	53	65531	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:48.288739920 CET	53	53926	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:48.506725073 CET	54590	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:48.571563959 CET	53	54590	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:49.207015038 CET	51318	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:49.225625038 CET	60888	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:49.250071049 CET	58474	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:49.258469105 CET	53	51318	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:49.277272940 CET	53	60888	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:49.298603058 CET	53	58474	8.8.8.8	192.168.2.6
Feb 16, 2021 17:15:49.545567989 CET	64575	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:15:49.611587048 CET	53	64575	8.8.8.8	192.168.2.6
Feb 16, 2021 17:16:11.542444944 CET	59092	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:16:11.600228071 CET	53	59092	8.8.8.8	192.168.2.6
Feb 16, 2021 17:16:11.616204023 CET	57483	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:16:11.667637110 CET	53	57483	8.8.8.8	192.168.2.6
Feb 16, 2021 17:16:11.676063061 CET	53830	53	192.168.2.6	8.8.8.8
Feb 16, 2021 17:16:11.735893965 CET	53	53830	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 16, 2021 17:13:37.368771076 CET	192.168.2.6	8.8.8.8	0x5ca8	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
Feb 16, 2021 17:13:39.869321108 CET	192.168.2.6	8.8.8.8	0x8a16	Standard query (0)	web.vortex .data.msn.com	A (IP address)	IN (0x0001)
Feb 16, 2021 17:13:40.383327007 CET	192.168.2.6	8.8.8.8	0x8a56	Standard query (0)	contextual .media.net	A (IP address)	IN (0x0001)
Feb 16, 2021 17:13:40.448982954 CET	192.168.2.6	8.8.8.8	0x9c6b	Standard query (0)	geolocatio n.onetrust.com	A (IP address)	IN (0x0001)
Feb 16, 2021 17:13:42.637480974 CET	192.168.2.6	8.8.8.8	0xdafe	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
Feb 16, 2021 17:13:43.583009958 CET	192.168.2.6	8.8.8.8	0xa605	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
Feb 16, 2021 17:13:43.815963984 CET	192.168.2.6	8.8.8.8	0x3d83	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
Feb 16, 2021 17:13:44.347043991 CET	192.168.2.6	8.8.8.8	0x6ce9	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 16, 2021 17:13:45.669475079 CET	192.168.2.6	8.8.8.8	0x9053	Standard query (0)	img.img-taboola.com	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:22.572022915 CET	192.168.2.6	8.8.8.8	0xfb6	Standard query (0)	haloopolikosul.xyz	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:22.847590923 CET	192.168.2.6	8.8.8.8	0x37a9	Standard query (0)	www.redtube.com	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:23.404803991 CET	192.168.2.6	8.8.8.8	0x9110	Standard query (0)	ei.rdtcdn.com	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:23.405369997 CET	192.168.2.6	8.8.8.8	0xb062	Standard query (0)	static.trafficjunky.com	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:23.405513048 CET	192.168.2.6	8.8.8.8	0x60b	Standard query (0)	ei.rdtcdn.com	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:23.406085014 CET	192.168.2.6	8.8.8.8	0xd8f4	Standard query (0)	cdn1d-static-shared.phncdn.com	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:23.433617115 CET	192.168.2.6	8.8.8.8	0xf68b	Standard query (0)	ht.redtube.com	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:23.473663092 CET	192.168.2.6	8.8.8.8	0xf3ff	Standard query (0)	cdn1d-static-shared.phncdn.com	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:23.549473047 CET	192.168.2.6	8.8.8.8	0x8a40	Standard query (0)	cdn.speedcurve.com	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:23.552031040 CET	192.168.2.6	8.8.8.8	0x2ee8	Standard query (0)	static.trafficjunky.com	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:24.519809008 CET	192.168.2.6	8.8.8.8	0x873d	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:24.763607025 CET	192.168.2.6	8.8.8.8	0xdde9	Standard query (0)	di.rdtcdn.com	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:24.851691008 CET	192.168.2.6	8.8.8.8	0xc724	Standard query (0)	vz-cdn.trafficjunky.net	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:24.907445908 CET	192.168.2.6	8.8.8.8	0xedf2	Standard query (0)	ads.trafficjunky.net	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:24.920401096 CET	192.168.2.6	8.8.8.8	0xe588	Standard query (0)	hw-cdn-ap.trafficjunky.net	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:24.948985100 CET	192.168.2.6	8.8.8.8	0xd4bf	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:47.259238005 CET	192.168.2.6	8.8.8.8	0x73d5	Standard query (0)	trapolikoliosilios.xyz	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:47.704771042 CET	192.168.2.6	8.8.8.8	0xdf59	Standard query (0)	www.redtube.com	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:48.223407984 CET	192.168.2.6	8.8.8.8	0x2087	Standard query (0)	ei.rdtcdn.com	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:48.227658033 CET	192.168.2.6	8.8.8.8	0x6c7e	Standard query (0)	static.trafficjunky.com	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:48.230021954 CET	192.168.2.6	8.8.8.8	0xe2c5	Standard query (0)	cdn1d-static-shared.phncdn.com	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:49.207015038 CET	192.168.2.6	8.8.8.8	0xf807	Standard query (0)	hw-cdn-ap.trafficjunky.net	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:49.225625038 CET	192.168.2.6	8.8.8.8	0x4f76	Standard query (0)	ads.trafficjunky.net	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:49.250071049 CET	192.168.2.6	8.8.8.8	0x669d	Standard query (0)	a.adtng.com	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:49.545567989 CET	192.168.2.6	8.8.8.8	0x1ba4	Standard query (0)	ht-cdn2.adtng.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 16, 2021 17:13:37.417718887 CET	8.8.8.8	192.168.2.6	0x5ca8	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:13:39.935137987 CET	8.8.8.8	192.168.2.6	0x8a16	No error (0)	web.vortex.data.msn.com	web.vortex.data.microsoft.com		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:13:40.450809002 CET	8.8.8.8	192.168.2.6	0x8a56	No error (0)	contextual.media.net		184.30.24.22	A (IP address)	IN (0x0001)
Feb 16, 2021 17:13:40.500674963 CET	8.8.8.8	192.168.2.6	0x9c6b	No error (0)	geolocation.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
Feb 16, 2021 17:13:40.500674963 CET	8.8.8.8	192.168.2.6	0x9c6b	No error (0)	geolocation.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 16, 2021 17:13:42.705665112 CET	8.8.8.8	192.168.2.6	0xdafe	No error (0)	hblg.media.net		184.30.24.22	A (IP address)	IN (0x0001)
Feb 16, 2021 17:13:43.652962923 CET	8.8.8.8	192.168.2.6	0xa605	No error (0)	lg3.media.net		184.30.24.22	A (IP address)	IN (0x0001)
Feb 16, 2021 17:13:43.877336025 CET	8.8.8.8	192.168.2.6	0x3d83	No error (0)	cvision.media.net	cvision.media.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:13:44.398403883 CET	8.8.8.8	192.168.2.6	0x6ce9	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:13:44.398403883 CET	8.8.8.8	192.168.2.6	0x6ce9	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:13:45.718072891 CET	8.8.8.8	192.168.2.6	0x9053	No error (0)	img.img-taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:13:45.718072891 CET	8.8.8.8	192.168.2.6	0x9053	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
Feb 16, 2021 17:13:45.718072891 CET	8.8.8.8	192.168.2.6	0x9053	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Feb 16, 2021 17:13:45.718072891 CET	8.8.8.8	192.168.2.6	0x9053	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Feb 16, 2021 17:13:45.718072891 CET	8.8.8.8	192.168.2.6	0x9053	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:22.638927937 CET	8.8.8.8	192.168.2.6	0xfb6	No error (0)	haloopolikosul.xyz		185.186.246.166	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:22.897663116 CET	8.8.8.8	192.168.2.6	0x37a9	No error (0)	www.redtube.com	redtube.com		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:15:22.897663116 CET	8.8.8.8	192.168.2.6	0x37a9	No error (0)	redtube.com		66.254.114.238	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:23.453891039 CET	8.8.8.8	192.168.2.6	0xb062	No error (0)	static.trafficjunky.com	vip0x04f.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:15:23.453891039 CET	8.8.8.8	192.168.2.6	0xb062	No error (0)	vip0x04f.ssl.rncdn5.com		205.185.208.79	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:23.457439899 CET	8.8.8.8	192.168.2.6	0xd8f4	No error (0)	cdn1d-static-shared.phncdn.com	vip0x08e.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:15:23.457439899 CET	8.8.8.8	192.168.2.6	0xd8f4	No error (0)	vip0x08e.ssl.rncdn5.com		205.185.208.142	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:23.470242023 CET	8.8.8.8	192.168.2.6	0x9110	No error (0)	ei.rdtcdn.com	ei.rdtcdn.com.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:15:23.470242023 CET	8.8.8.8	192.168.2.6	0x9110	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		67.22.48.100	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:23.470242023 CET	8.8.8.8	192.168.2.6	0x9110	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		67.22.48.102	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:23.470242023 CET	8.8.8.8	192.168.2.6	0x9110	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		67.22.48.104	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:23.470624924 CET	8.8.8.8	192.168.2.6	0x60b	No error (0)	ei.rdtcdn.com	ei.rdtcdn.com.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:15:23.470624924 CET	8.8.8.8	192.168.2.6	0x60b	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		67.22.48.100	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:23.470624924 CET	8.8.8.8	192.168.2.6	0x60b	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		67.22.48.102	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:23.470624924 CET	8.8.8.8	192.168.2.6	0x60b	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		67.22.48.104	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:23.485039949 CET	8.8.8.8	192.168.2.6	0xf68b	No error (0)	ht.redtube.com	hubtraffic.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 16, 2021 17:15:23.485039949 CET	8.8.8.8	192.168.2.6	0xf68b	No error (0)	hubtraffic.com		66.254.114.32	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:23.525218010 CET	8.8.8.8	192.168.2.6	0xf3ff	No error (0)	cdn1d-static-shared.phncdn.com	vip0x08e.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:15:23.525218010 CET	8.8.8.8	192.168.2.6	0xf3ff	No error (0)	vip0x08e.ssl.rncdn5.com		205.185.208.142	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:23.603444099 CET	8.8.8.8	192.168.2.6	0x2ee8	No error (0)	static.trafficjunky.com	vip0x04f.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:15:23.603444099 CET	8.8.8.8	192.168.2.6	0x2ee8	No error (0)	vip0x04f.ssl.rncdn5.com		205.185.208.79	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:23.609720945 CET	8.8.8.8	192.168.2.6	0x8a40	No error (0)	cdn.speedcurve.com	a3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:15:24.571234941 CET	8.8.8.8	192.168.2.6	0x873d	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:15:24.571234941 CET	8.8.8.8	192.168.2.6	0x873d	No error (0)	stats.l.doubleclick.net		74.125.206.156	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:24.571234941 CET	8.8.8.8	192.168.2.6	0x873d	No error (0)	stats.l.doubleclick.net		74.125.206.157	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:24.571234941 CET	8.8.8.8	192.168.2.6	0x873d	No error (0)	stats.l.doubleclick.net		74.125.206.154	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:24.571234941 CET	8.8.8.8	192.168.2.6	0x873d	No error (0)	stats.l.doubleclick.net		74.125.206.155	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:24.820764065 CET	8.8.8.8	192.168.2.6	0xdde9	No error (0)	di.rdtcdn.com	cds.e9q5t8x5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:15:24.910298109 CET	8.8.8.8	192.168.2.6	0xc724	No error (0)	vz-cdn.trafficjunky.net	cs742.wpc.rncdn4.com		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:15:24.910298109 CET	8.8.8.8	192.168.2.6	0xc724	No error (0)	cs742.wpc.rncdn4.com		192.229.221.215	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:24.958975077 CET	8.8.8.8	192.168.2.6	0xedf2	No error (0)	ads.trafficjunky.net		66.254.114.38	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:24.977679014 CET	8.8.8.8	192.168.2.6	0xe588	No error (0)	hw-cdn-ap.trafficjunky.net	cds.q7x2a8v5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:15:25.016117096 CET	8.8.8.8	192.168.2.6	0xd4bf	No error (0)	www.google.co.uk		216.58.208.131	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:47.324301958 CET	8.8.8.8	192.168.2.6	0x73d5	No error (0)	trapolikoliosilios.xyz		185.186.245.78	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:47.756269932 CET	8.8.8.8	192.168.2.6	0xdf59	No error (0)	www.redtube.com	redtube.com		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:15:47.756269932 CET	8.8.8.8	192.168.2.6	0xdf59	No error (0)	redtube.com		66.254.114.238	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:48.278681993 CET	8.8.8.8	192.168.2.6	0xe2c5	No error (0)	cdn1d-static-shared.phncdn.com	vip0x08e.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:15:48.278681993 CET	8.8.8.8	192.168.2.6	0xe2c5	No error (0)	vip0x08e.ssl.rncdn5.com		205.185.208.142	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:48.279166937 CET	8.8.8.8	192.168.2.6	0x6c7e	No error (0)	static.trafficjunky.com	vip0x04f.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:15:48.279166937 CET	8.8.8.8	192.168.2.6	0x6c7e	No error (0)	vip0x04f.ssl.rncdn5.com		205.185.208.79	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:48.288739920 CET	8.8.8.8	192.168.2.6	0x2087	No error (0)	ei.rdtcdn.com	ei.rdtcdn.com.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:15:48.288739920 CET	8.8.8.8	192.168.2.6	0x2087	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		67.22.48.104	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 16, 2021 17:15:48.288739920 CET	8.8.8.8	192.168.2.6	0x2087	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		67.22.48.100	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:48.288739920 CET	8.8.8.8	192.168.2.6	0x2087	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		67.22.48.102	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:49.258469105 CET	8.8.8.8	192.168.2.6	0xf807	No error (0)	hw-cdn-ap.trafficjunky.net	cds.q7x2a8v5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:15:49.277272940 CET	8.8.8.8	192.168.2.6	0x4f76	No error (0)	ads.trafficjunky.net		66.254.114.38	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:49.298603058 CET	8.8.8.8	192.168.2.6	0x669d	No error (0)	a.adtng.com		216.18.168.166	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:49.611587048 CET	8.8.8.8	192.168.2.6	0x1ba4	No error (0)	ht-cdn2.adtng.com	ht-cdn2.adtng.com.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)
Feb 16, 2021 17:15:49.611587048 CET	8.8.8.8	192.168.2.6	0x1ba4	No error (0)	ht-cdn2.adtng.com.sds.rncdn7.com		67.22.48.100	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:49.611587048 CET	8.8.8.8	192.168.2.6	0x1ba4	No error (0)	ht-cdn2.adtng.com.sds.rncdn7.com		67.22.48.102	A (IP address)	IN (0x0001)
Feb 16, 2021 17:15:49.611587048 CET	8.8.8.8	192.168.2.6	0x1ba4	No error (0)	ht-cdn2.adtng.com.sds.rncdn7.com		67.22.48.104	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- haloopolikosul.xyz
- trapolikoliosilios.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49785	185.186.246.166	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2021 17:15:22.714082956 CET	7623	OUT	GET /manifest/YcHhvzqnGV3dy_2/FvEnS_2F9p1dXR5ImF/Zp9nA6_2B/trDvtMc01BMk6W10nS4b/nBY6Ro9NIY ZgB4PdSB2/i1mhjy8xHpcjAa_2BlE3Kc/q_2FYOvC1J7aP/FNI18_2F/AG7vxeQbhoSEjouJBbqlUsR/JPS1_2BPEm /2lxmo_2BYnZJRzpXG/9_2FrnCKa8_2/B0uAY1BCgPp/SFeeWzcA5y/ICN_2FD.cnx 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: haloopolikosul.xyz Connection: Keep-Alive
Feb 16, 2021 17:15:22.799535036 CET	7624	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 16 Feb 2021 16:15:22 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=g5ac9844mmcie5f608h8640981; path=/; domain=.haloopolikosul.xyz Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: lang=en; expires=Thu, 18-Mar-2021 16:15:22 GMT; path=/; domain=.haloopolikosul.xyz Location: https://www.redtube.com/ Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49824	185.186.245.78	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 16, 2021 17:15:47.501647949 CET	9689	OUT	GET /manifest/6RdkLdcwvw_2FaqHQmLpM4K/xGxqXBd9cs/4qTL6qYc4ErNURqkt/XUq53JLMr1fD/RtNeBJnMak A/x3ecxxT0_2FZo4/viq_2FU3gJRlWwreK7Aro/xONAtX4tjMzUOqke/ZVsOFfFPnv3v7Yl/RAyVT9rsvo9A_2FB_2/BG4jenq1F /zEAUnyy5QmhMnaXqJirl/_2B75bS5kThvkB9AKZc/Wf0DyNgBKbqHX1zjWouA/W.cnx 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: trapolikoliosilios.xyz Connection: Keep-Alive
Feb 16, 2021 17:15:47.681173086 CET	9690	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 16 Feb 2021 16:15:47 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=va812k09o89ib13pkgscr3t0l6; path=/; domain=.trapolikoliosilios.xyz Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: lang=en; expires=Thu, 18-Mar-2021 16:15:47 GMT; path=/; domain=.trapolikoliosilios.xyz Location: https://www.redtube.com/ Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8

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 17:13:40.614352942 CET	104.20.185.68	443	192.168.2.6	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 17:13:40.633526087 CET	104.20.185.68	443	192.168.2.6	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		
Feb 16, 2021 17:13:45.932018042 CET	151.101.1.44	443	192.168.2.6	49741	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 16, 2021 17:13:45.932142019 CET	151.101.1.44	443	192.168.2.6	49740	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	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 17:13:45.932528973 CET	151.101.1.44	443	192.168.2.6	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 17:13:45.933805943 CET	151.101.1.44	443	192.168.2.6	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	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 17:13:45.944122076 CET	151.101.1.44	443	192.168.2.6	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 17:13:45.953866005 CET	151.101.1.44	443	192.168.2.6	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		

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 17:15:23.001105070 CET	66.254.114.238	443	192.168.2.6	49786	CN=*.redtube.com, O=MG Freesites Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jun 18 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Tue Jun 22 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 16, 2021 17:15:23.001317024 CET	66.254.114.238	443	192.168.2.6	49787	CN=*.redtube.com, O=MG Freesites Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jun 18 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Tue Jun 22 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 16, 2021 17:15:23.599070072 CET	66.254.114.32	443	192.168.2.6	49789	CN=*.redtube.com, O=MG Freesites Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jun 17 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Tue Jun 22 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 16, 2021 17:15:23.599451065 CET	66.254.114.32	443	192.168.2.6	49788	CN=*.redtube.com, O=MG Freesites Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jun 17 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Tue Jun 22 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 16, 2021 17:15:23.627243996 CET	67.22.48.100	443	192.168.2.6	49790	CN=*.rdtcdn.com, O=MG Freesites Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Oct 26 02:00:00 CEST 2019 Tue Oct 22 14:00:00 CEST 2013 Fri Nov 10 01:00:00 CET 2006	Fri Oct 29 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028 Mon Nov 10 01:00:00 CET 2031	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 SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Feb 16, 2021 17:15:23.649874926 CET	205.185.208.142	443	192.168.2.6	49796	CN=*.phncdn.com, O=MG Freesites Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Feb 20 01:00:00 CET 2020 Tue Oct 22 14:00:00 CEST 2013	Thu Feb 24 13:00:00 CET 2022 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 16, 2021 17:15:23.650523901 CET	67.22.48.100	443	192.168.2.6	49792	CN=*.rdtcdn.com, O=MG Freesites Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Oct 26 02:00:00 CEST 2019 Tue Oct 22 14:00:00 CEST 2013 Fri Nov 10 01:00:00 CET 2006	Fri Oct 29 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028 Mon Nov 10 01:00:00 CET 2031	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 SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
					CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Feb 16, 2021 17:15:23.651369095 CET	67.22.48.100	443	192.168.2.6	49794	CN=*.rdtcdn.com, O=MG Freesites Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Oct 26 02:00:00 CEST 2019 Tue Oct 22 14:00:00 CEST 2013 Fri Nov 10 01:00:00 CET 2006	Fri Oct 29 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028 Mon Nov 10 01:00:00 CET 2031	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 SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
					CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Feb 16, 2021 17:15:23.651462078 CET	205.185.208.142	443	192.168.2.6	49797	CN=*.phncdn.com, O=MG Freesites Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Feb 20 01:00:00 CET 2020 Tue Oct 22 14:00:00 CEST 2013	Thu Feb 24 13:00:00 CET 2022 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 16, 2021 17:15:23.651541948 CET	67.22.48.100	443	192.168.2.6	49791	CN=*.rdtcdn.com, O=MG Freesites Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Oct 26 02:00:00 CEST 2019 Tue Oct 22 14:00:00 CEST 2013 Fri Nov 10 01:00:00 CET 2006	Fri Oct 29 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028 Mon Nov 10 01:00:00 CET 2031	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 SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
					CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Feb 16, 2021 17:15:23.651859999 CET	67.22.48.100	443	192.168.2.6	49795	CN=*.rdtcdn.com, O=MG Freesites Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Oct 26 02:00:00 CEST 2019 Tue Oct 22 14:00:00 CEST 2013 Fri Nov 10 01:00:00 CET 2006	Fri Oct 29 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028 Mon Nov 10 01:00:00 CET 2031	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 SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
					CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Feb 16, 2021 17:15:23.652602911 CET	67.22.48.100	443	192.168.2.6	49793	CN=*.rdtcdn.com, O=MG Freesites Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Oct 26 02:00:00 CEST 2019 Tue Oct 22 14:00:00 CEST 2013 Fri Nov 10 01:00:00 CET 2006	Fri Oct 29 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028 Mon Nov 10 01:00:00 CET 2031	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 SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
					CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

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 17:15:23.727394104 CET	205.185.208.79	443	192.168.2.6	49799	CN=*.trafficjunky.com, O=MG Freesites Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Oct 15 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Wed Oct 20 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 16, 2021 17:15:23.729065895 CET	205.185.208.79	443	192.168.2.6	49798	CN=*.trafficjunky.com, O=MG Freesites Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Oct 15 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Wed Oct 20 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 16, 2021 17:15:24.710983038 CET	74.125.206.156	443	192.168.2.6	49804	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 26 10:00:56 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:00:55 CEST 2021 Wed Dec 15 01:00:42 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Feb 16, 2021 17:15:24.711992025 CET	74.125.206.156	443	192.168.2.6	49805	CN=*.g.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 26 10:00:56 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:00:55 CEST 2021 Wed Dec 15 01:00:42 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Feb 16, 2021 17:15:24.997162104 CET	192.229.221.215	443	192.168.2.6	49812	CN=*.trafficjunky.net, O=MG Freesites Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jan 28 01:00:00 CET 2020 Tue Oct 22 14:00:00 CEST 2013	Tue Feb 01 13:00:00 CET 2022 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

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 17:15:24.997282982 CET	192.229.221.215	443	192.168.2.6	49813	CN=*.trafficjunky.net, O=MG Freesites Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jan 28 01:00:00 CET 2020 Tue Oct 22 14:00:00 CEST 2013	Tue Feb 01 13:00:00 CET 2022 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 16, 2021 17:15:25.058177948 CET	66.254.114.38	443	192.168.2.6	49814	CN=*.trafficjunky.net, O=MG Freesites Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jan 28 01:00:00 CET 2020 Tue Oct 22 14:00:00 CEST 2013	Tue Feb 01 13:00:00 CET 2022 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 16, 2021 17:15:25.058245897 CET	66.254.114.38	443	192.168.2.6	49815	CN=*.trafficjunky.net, O=MG Freesites Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jan 28 01:00:00 CET 2020 Tue Oct 22 14:00:00 CEST 2013	Tue Feb 01 13:00:00 CET 2022 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 16, 2021 17:15:25.167211056 CET	216.58.208.131	443	192.168.2.6	49821	CN=www.google.co.uk, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 19 09:02:47 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 13 10:02:46 CEST 2021 Wed Dec 15 01:00:42 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		
Feb 16, 2021 17:15:25.168116093 CET	216.58.208.131	443	192.168.2.6	49820	CN=www.google.co.uk, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 19 09:02:47 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 13 10:02:46 CEST 2021 Wed Dec 15 01:00:42 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=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 16, 2021 17:15:47.861464024 CET	66.254.114.238	443	192.168.2.6	49826	CN=*.redtube.com, O=MG Freesites Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jun 18 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Tue Jun 22 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 16, 2021 17:15:47.861519098 CET	66.254.114.238	443	192.168.2.6	49825	CN=*.redtube.com, O=MG Freesites Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jun 18 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Tue Jun 22 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 16, 2021 17:15:49.393207073 CET	66.254.114.38	443	192.168.2.6	49829	CN=*.trafficjunky.net, O=MG Freesites Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jan 28 01:00:00 CET 2020 Tue Oct 22 14:00:00 CEST 2013	Tue Feb 01 13:00:00 CET 2022 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 16, 2021 17:15:49.417000055 CET	66.254.114.38	443	192.168.2.6	49830	CN=*.trafficjunky.net, O=MG Freesites Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jan 28 01:00:00 CET 2020 Tue Oct 22 14:00:00 CEST 2013	Tue Feb 01 13:00:00 CET 2022 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 16, 2021 17:15:49.439841986 CET	216.18.168.166	443	192.168.2.6	49833	CN=*.adtng.com, O=MG Premium Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jun 16 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Wed Sep 01 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

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 17:15:49.442832947 CET	216.18.168.166	443	192.168.2.6	49834	CN=*.adtng.com, O=MG Premium Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jun 16 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Wed Sep 01 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 16, 2021 17:15:49.730521917 CET	67.22.48.100	443	192.168.2.6	49835	CN=*.adtng.com, O=MG Premium Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jun 16 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Wed Sep 01 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 16, 2021 17:15:49.732184887 CET	67.22.48.100	443	192.168.2.6	49836	CN=*.adtng.com, O=MG Premium Ltd, L=Nicosia, C=CY CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jun 16 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Wed Sep 01 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6928 Parent PID: 5804

General

Start time:	17:13:34
Start date:	16/02/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\602b97e0b415b.png.dll'
Imagebase:	0xff0000
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: 6936 Parent PID: 6928

General

Start time:	17:13:34
Start date:	16/02/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\602b97e0b415b.png.dll
Imagebase:	0xc10000
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: 00000001.00000003.504046984.0000000005048000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.503943251.0000000005048000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.504289437.0000000005048000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.504009334.0000000005048000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.656990122.0000000004D4E000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.608771986.0000000004ECB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.504205344.0000000005048000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.504140362.0000000005048000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.503904598.0000000005048000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.503972106.0000000005048000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6944 Parent PID: 6928

General

Start time:	17:13:34
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:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6964 Parent PID: 6944

General

Start time:	17:13:35
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:	0x7ff721e20000

File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File 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: 7028 Parent PID: 6964

General

Start time:	17:13:36
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:6964 CREDAT:17410 /prefetch:2
Imagebase:	0xe20000
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: 5456 Parent PID: 6964

General

Start time:	17:14:58
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:6964 CREDAT:17428 /prefetch:2
Imagebase:	0xe20000
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: 1916 Parent PID: 6964

General

Start time:	17:15:21
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:6964 CREDAT:82958 /prefetch:2
Imagebase:	0xe20000
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	Completion	Count	Source Address	Symbol

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: 3132 Parent PID: 6964

General

Start time:	17:15:45
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:6964 CREDAT:17436 /prefetch:2
Imagebase:	0xe20000
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: 5456 Parent PID: 6964

General

Start time:	17:16:10
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:6964 CREDAT:82964 /prefetch:2
Imagebase:	0xe20000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis