ID: 410858
Sample Name: FuiZSHt8Hx
Cookbook: default.jbs
Time: 11:47:22
Date: 11/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

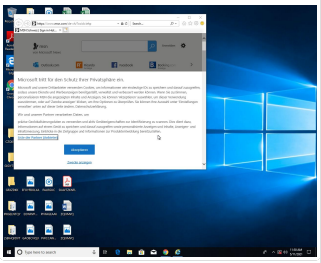
Analysis Report FuiZSHt8Hx

Overview

General Information

Sample Name:	FuiZSHt8Hx (renamed file extension from none to dll)
Analysis ID:	410858
MD5:	c4c0b19091c6ed…
SHA1:	5b1dbdbab64ebc..
SHA256:	821f1b68c207b41.
Tags:	BRT dll gozi isfb unpacked ursnif
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

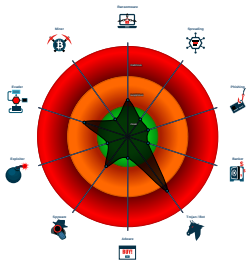
Ursnif

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Machine Learning detection for samp…
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- Connects to many different domains
- Contains functionality to call native f…
- Contains functionality to dynamically…
- Contains functionality to query CPU …
- Creates a process in suspended mo…
- Detected potential crypto function
- IP address seen in connection with o…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 5784 cmdline: loaddll32.exe 'C:\Users\user\Desktop\FuiZSHt8Hx.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 4912 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\FuiZSHt8Hx.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5408 cmdline: rundll32.exe 'C:\Users\user\Desktop\FuiZSHt8Hx.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - regsvr32.exe (PID: 5728 cmdline: regsvr32.exe /s C:\Users\user\Desktop\FuiZSHt8Hx.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - iexplore.exe (PID: 4680 cmdline: C:\Program Files\Internet Explorer\iexplore.exe MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - iexplore.exe (PID: 4456 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 2148 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:17428 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6552 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:17432 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 1148 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:82970 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 3152 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:17448 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6504 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:82976 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 4164 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:82990 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6564 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:17476 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 3264 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:83006 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6576 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:17480 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 5828 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:17492 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6684 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:83014 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - rundll32.exe (PID: 5508 cmdline: rundll32.exe C:\Users\user\Desktop\FuiZSHt8Hx.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
"KujE77ctKyR8x3/dODwZbEsxGmck+FW9384s5u0Kacw8y1gCN+8m2bfjJPovkn+UzufcdfSs+a43eI6oHR1KgWQmvEAO6LK8tJv+Wl7iCBPJP7eef8xKeXht/Mhk1PSj7mHnJ9lcqKMtTteEdSecVvMRtb/WSKVTFfHDva9My7AJ/NbX
qHdzCG7znACswLxD",
  "c2_domain": [
    "outlook.com/login",
    "gmail.com",
    "worunekulo.club",
    "horunekulo.website"
  ],
  "botnet": "8877",
  "server": "12",
  "serpent_key": "30218409ILPAJDUR",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0",
  "DGA_count": "10"
}
```


Yara Overview

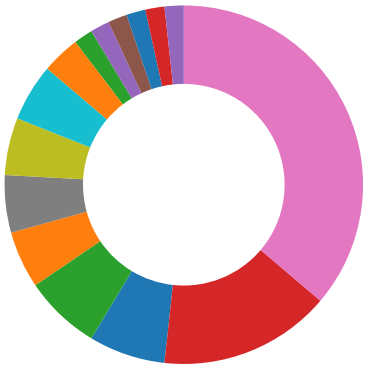
Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.299753602.0000000001C58000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000005.00000003.471813854.0000000004E3B000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.352305744.0000000005B58000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.299604342.0000000001C58000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.505193431.000000000195E000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 35 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 / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

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:

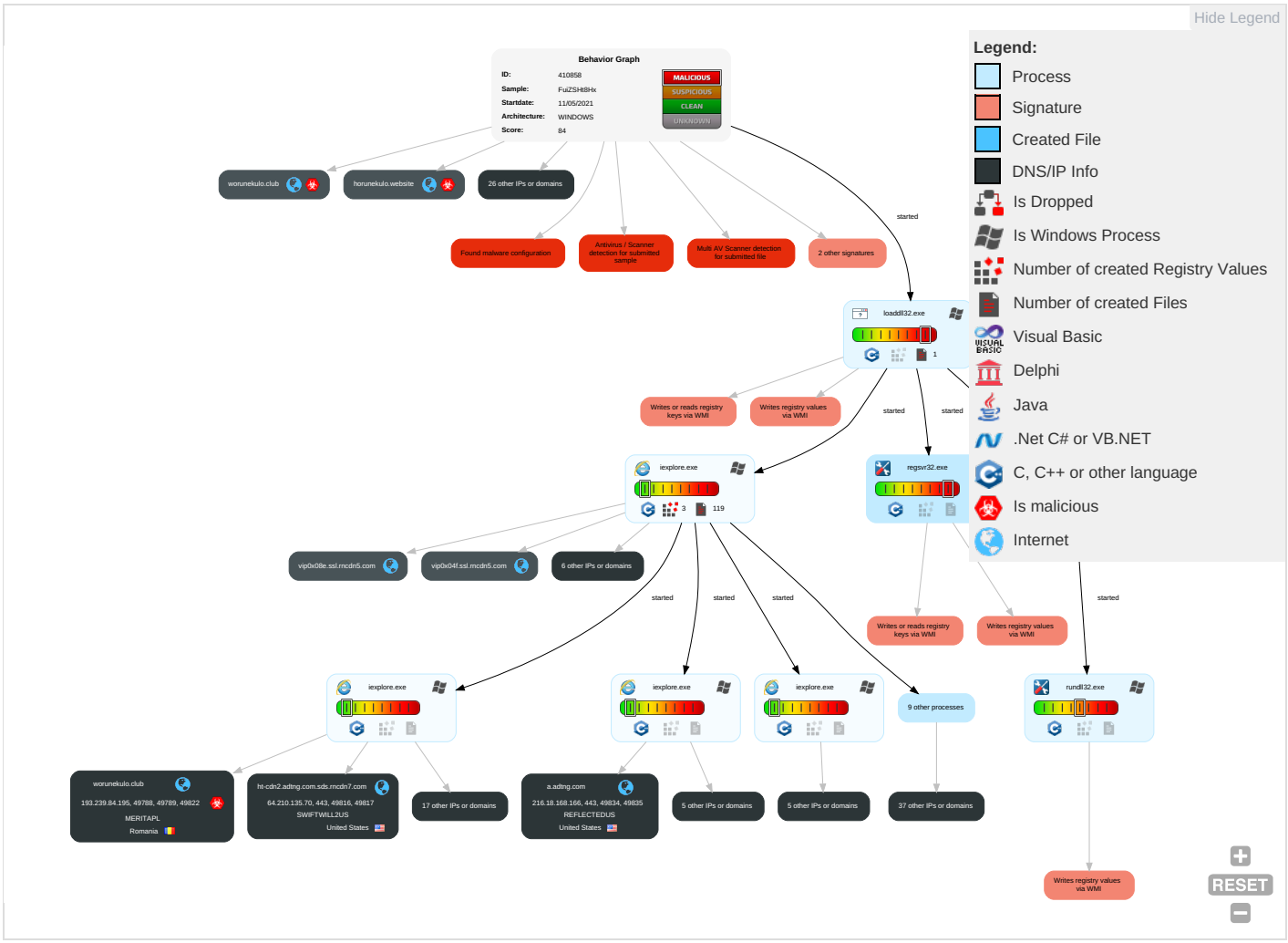
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 2	DLL Side-Loading 1	Process Injection 1 2	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdr Insecure Network Commur
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Virtualization/Sandbox Evasion 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Regsvr32 1	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commur
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rundll32 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial o Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access I

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	System Information Discovery 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocol

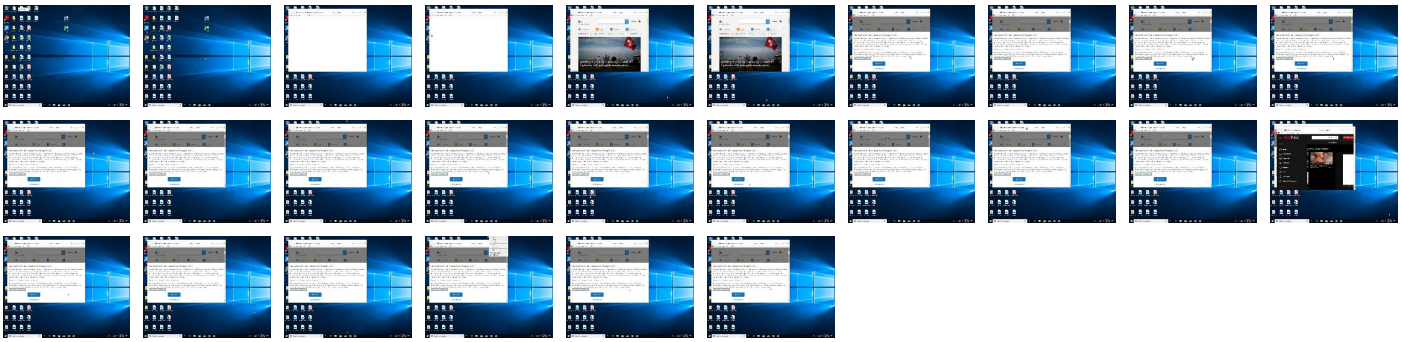
Behavior Graph

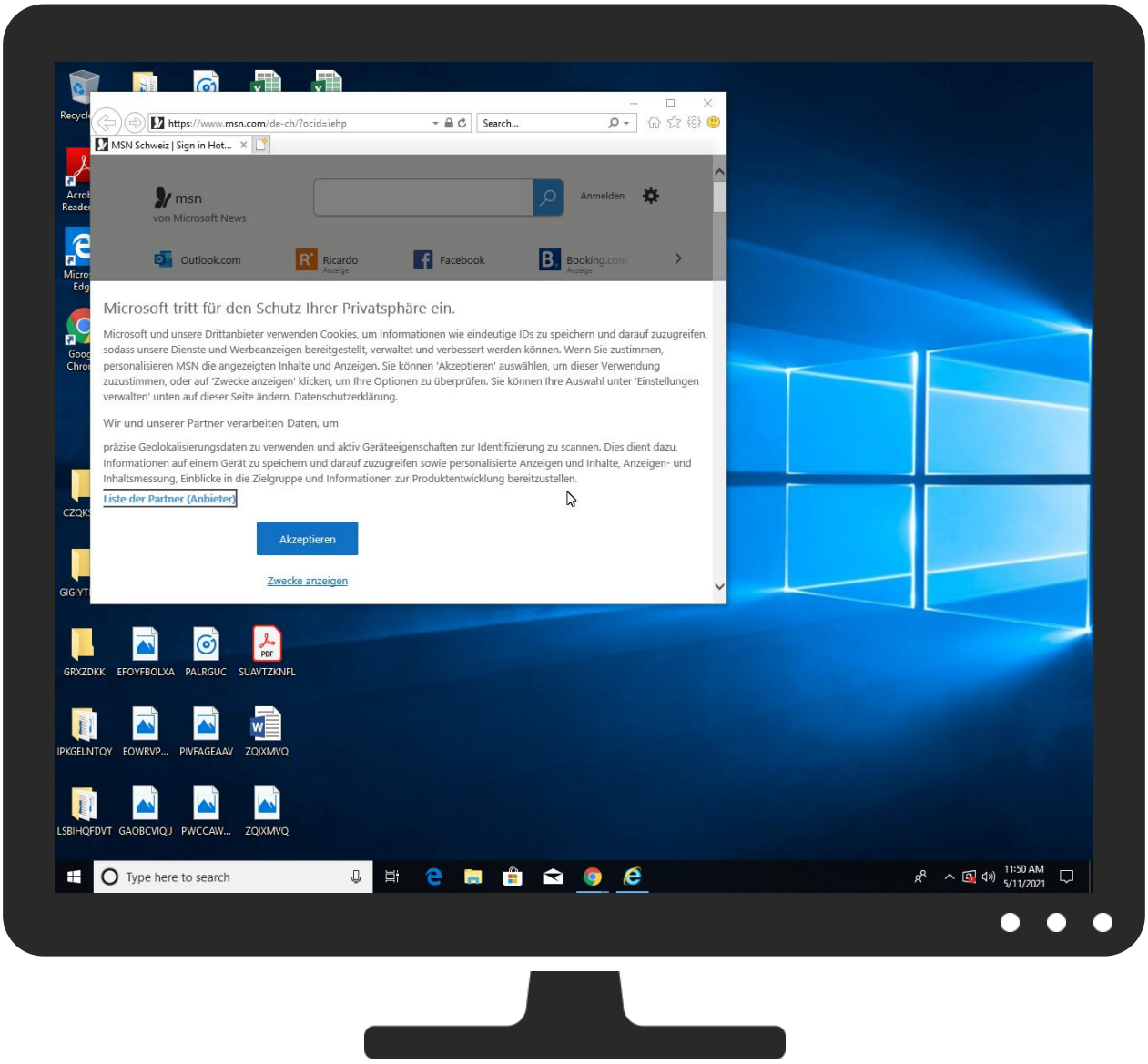


Screenshots

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
FuiZSHt8Hx.dll	49%	Virustotal		Browse
FuiZSHt8Hx.dll	45%	ReversingLabs	Win32.Trojan.Razy	
FuiZSHt8Hx.dll	100%	Avira	TR/Spy.Gen	
FuiZSHt8Hx.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.9e0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
5.2.rundll32.exe.30e0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.2.loaddll32.exe.1200000.0.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
2.2.regsvr32.exe.1000000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

Source	Detection	Scanner	Label	Link
tls13.taboola.map.fastly.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://worunekulo.club/greed/Q7ECAhkT09Dh5Dxzx5NND/wHPvdjMQo9yvTSIz/72Cz1yfrj9oas3F/mlrlmmXnF4mFMyXsRS/lAfcYLSQz/emv5Y2LTHh0gnSKiYnKd/yiqaLkEsaxUTLIXXXkb/fKBJ2kKvoXtzyu88vwhB6r/sfNLlep0RDB8s/ZFdFWunl/pI1RYpuDgoeDLfkKFeCA_2F/BTJiso9B2W/oRKpS4iwlP_2BxR5_/2FtiB90t/R.gfk	0%	Avira URL Cloud	safe	
http://https://www.etahub.com/trackn?app_id=	0%	Avira URL Cloud	safe	
http://https://onedrive.live.com;OneDrive-App	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tls13.taboola.map.fastly.net	151.101.1.44	true	false	• 0%, Virustotal, Browse	unknown
redtube.com	66.254.114.238	true	false		high
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
horunekulo.website	193.239.85.9	true	true		unknown
vip0x08e.ssl.rncdn5.com	205.185.208.142	true	false		unknown
www.google.de	172.217.16.99	true	false		high
ht-cdn.trafficjunky.net.sds.rncdn7.com	64.210.135.70	true	false		unknown
cs742.wpc.rncdn4.com	192.229.221.215	true	false		unknown
stats.l.doubleclick.net	173.194.76.156	true	false		high
cs733.wpc.rncdn4.com	192.229.221.206	true	false		unknown
ht-cdn2.adtng.com.sds.rncdn7.com	64.210.135.70	true	false		unknown
tp-rtb-adserver-eu.eu-west-1.elasticbeanstalk.com	54.247.61.18	true	false		high
HHN-efz.ms-acdc.office.com	52.98.151.242	true	false		high
gmail.com	172.217.19.101	true	false		high
outlook.com	40.97.156.114	true	false		high
worunekulo.club	193.239.84.195	true	true		unknown
hblg.media.net	184.30.24.22	true	false		high
ei.rdtcdn.com.sds.rncdn7.com	64.210.135.72	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
cs2178.wpc.rncdn4.com	152.199.21.187	true	false		unknown
FRA-efz.ms-acdc.office.com	52.97.250.194	true	false		high
geolocation.onetrust.com	104.20.184.68	true	false		high
ht-cdn.trafficjunky.net	unknown	unknown	false		high
srtb.msn.com	unknown	unknown	false		high
hw-cdn2.adtng.com	unknown	unknown	false		unknown
www.redtube.com	unknown	unknown	false		high
img.img-taboola.com	unknown	unknown	false		unknown
eu-adsrv.rtbsuperhub.com	unknown	unknown	false		high
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
bmedia.justservingfiles.net	unknown	unknown	false		high
www.msn.com	unknown	unknown	false		high
vz-cdn2.adtng.com	unknown	unknown	false		unknown
ht-cdn2.adtng.com	unknown	unknown	false		unknown
di.rdtcdn.com	unknown	unknown	false		high
ci.rdtcdn.com	unknown	unknown	false		high
cdn1d-static-shared.phncdn.com	unknown	unknown	false		high
outlook.office365.com	unknown	unknown	false		high
www.outlook.com	unknown	unknown	false		high
ei.rdtcdn.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cvision.media.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://worunekulo.club/greed/Q7ECAhkT09Dh5Dxzx5NND/wHPvdjMQo9yvTSIz/72Cz1yfrj9oas3F/mlrlmmXnF4mFMyXsRS/lAfcYLSQz/emv5Y2LTHh0gnSKiYnKd/yiqaLkEsaxUTLIXXXkb/fKBJ2kKvoXtzyu88vwhB6r/sfNLlep0RDB8s/ZFdFWunl/pI1RYpuDgoeDLfkKFeCA_2F/BTJiso9B2W/oRKpS4iwlP_2BxR5_/2FtiB90t/R.gfk	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

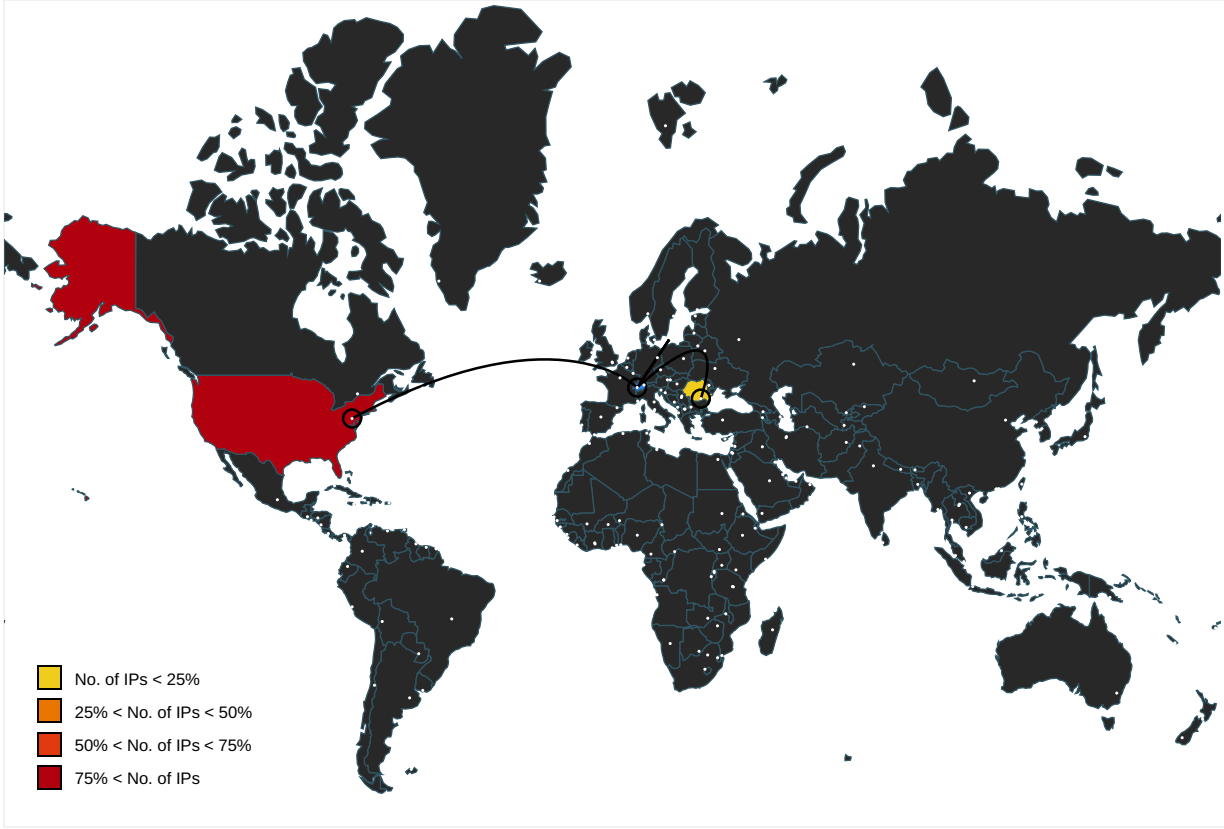
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dw.rdtcdn.com/media/videos/202007/26/34513381/360P_360K_34513381_fb.mp4	22DFL4CR.htm.34.dr	false		high
http://https://ei.rdtcdn.com/m=ejrk8f/media/videos/201408/19/860611/original/15.jpg	TEX0ICSG.htm.36.dr	false		high
http://https://click.linksynergy.com/deeplink?id=xoqYgl4JDe8&mid=46130&u1=dech_promotionalstripe_na	de-ch[1].htm.6.dr	false		high
http://https://ei.rdtcdn.com/m=bIaMwLVg5p/media/videos/202006/12/32620671/original/13.webp	TEX0ICSG.htm.36.dr	false		high
http://https://ew.rdtcdn.com/media/videos/202007/26/34513381/360P_360K_34513381_fb.mp4	TEX0ICSG.htm.36.dr	false		high
http://https://ci-ph.rdtcdn.com/m=bIWpYLVg5p/pics/pornstars/000/273/431/thumb_961012.webp	22DFL4CR.htm.34.dr	false		high
http://https://ei.rdtcdn.com/m=eah-8f/media/videos/201910/14/23039601/original/9.jpg	TEX0ICSG.htm.36.dr	false		high
http://https://ei.rdtcdn.com/m=bIa44NVg5p/media/videos/201909/25/22238621/original/2.webp	TEX0ICSG.htm.36.dr	false		high
http://https://ei.rdtcdn.com/m=eW0Q8f/media/videos/202001/09/26886751/original/12.jpg	TEX0ICSG.htm.36.dr	false		high
http://https://ei-ph.rdtcdn.com/m=bIWpYLVg5p/pics/pornstars/000/004/440/thumb_198761.webp	TEX0ICSG.htm.36.dr	false		high
http://https://www.redtube.com/?page=2	TEX0ICSG.htm.36.dr	false		high
http://https://ei-ph.rdtcdn.com/videos/202101/07/381285532/original/(m=eGJF8f)(mh=nQb4aCoV6ofRuJNn)	TEX0ICSG.htm.36.dr	false		high
http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/images/pc/category/amateur_001.jpg	TEX0ICSG.htm.36.dr	false		high
http://https://ew.rdtcdn.com/media/videos/201908/07/20065021/360P_360K_20065021_fb.mp4	TEX0ICSG.htm.36.dr	false		high
http://https://ci-ph.rdtcdn.com/m=e_rU8f/pics/pornstars/000/006/163/thumb_662761.jpg	22DFL4CR.htm.34.dr	false		high
http://https://dw.rdtcdn.com/media/videos/202009/23/36295991/360P_360K_36295991_fb.mp4	22DFL4CR.htm.34.dr	false		high
http://https://res-a.akamaihd.net/__media__/pics/8000/72/941/fallback1.jpg	{70C8875F-B289-11EB-90E6-ECF4BB82F7E0}.dat.4.dr	false		high
http://https://ei.rdtcdn.com/m=bIaC8JVg5p/media/videos/201611/11/1803966/original/15.webp	TEX0ICSG.htm.36.dr	false		high
http://https://www.onenote.com/notebooks?WT.mc_id=MSN_OneNote_Recent&auth=1&wdorigin=msn	52-478955-68ddb2ab[1].js.6.dr	false		high
http://https://ci.rdtcdn.com/www-static/cdn_files/redtube/fonts/rt_font.woff2?v=c68764eb72df2fd284980d4794d	22DFL4CR.htm.34.dr	false		high
http://https://ei.rdtcdn.com/m=eGJF8f/media/videos/202007/22/34378181/original/	TEX0ICSG.htm.36.dr	false		high
http://https://ei.rdtcdn.com/m=eah-8f/media/videos/202003/13/29344991/original/7.jpg	DTABAP9Y.htm.31.dr	false		high
http://https://outlook.office365.com/login/greed/x8W8BNR9UNCZa/Twkc4UWe/ksrEjoqLIMBWgNaXvBBgZQc/7caPZuKhoQ/	{7FDF5612-B289-11EB-90E6-ECF4BB82F7E0}.dat.4.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ei.rdtcdn.com/m=bIa44NVg5p/media/videos/202006/17/32796601/original/9.webp	TEX0ICSG.htm.36.dr	false		high
http://https://ei-ph.rdtcdn.com/m=bIWpYLVg5p/pics/pornstars/000/146/971/thumb_1175541.webp	TEX0ICSG.htm.36.dr	false		high
http://https://ei.rdtcdn.com/m=eGJF8f/media/videos/202010/01/36578231/original/	TEX0ICSG.htm.36.dr	false		high
http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/images/pc/ads/fallback_pc_top_right.png?v=c68764e	TEX0ICSG.htm.36.dr	false		high
http://https://ei.rdtcdn.com/m=bIijsHVg5p/media/videos/201412/30/998020/original/15.webp	TEX0ICSG.htm.36.dr	false		high
http://https://dw.rdtcdn.com/media/videos/201910/28/23719311/360P_360K_23719311_fb.mp4	22DFL4CR.htm.34.dr	false		high
http://https://ci-ph.rdtcdn.com/videos/201909/10/247562661/thumbs_20/(m=bIa44NVg5p)(mh=1Yaa01-wZF-nhfcu)11.	22DFL4CR.htm.34.dr	false		high
http://https://ei.rdtcdn.com/m=bIa44NVg5p/media/videos/202011/14/37979511/original/10.webp	TEX0ICSG.htm.36.dr	false		high
http://https://ew.rdtcdn.com/media/videos/201909/25/22238621/360P_360K_22238621_fb.mp4	TEX0ICSG.htm.36.dr	false		high
http://https://amzn.to/2TTxhNg	de-ch[1].htm.6.dr	false		high
http://https://static.trafficjunky.com/invocation/embeddedads/	TEX0ICSG.htm.36.dr	false		high
http://https://dw.rdtcdn.com/media/videos/201908/07/20065021/360P_360K_20065021_fb.mp4	22DFL4CR.htm.34.dr	false		high
http://https://ei.rdtcdn.com/m=bIaMwLVg5p/media/videos/202006/17/32796601/original/9.webp	TEX0ICSG.htm.36.dr	false		high
http://https://ci.rdtcdn.com/www-static/cdn_files/redtube/images/pc/network-bar-sprite.png?v=c68764eb72df2f	22DFL4CR.htm.34.dr	false		high
http://https://www.etahub.com/trackn?app_id=	timings-1.0.0[1].js.31.dr	false	• Avira URL Cloud: safe	unknown
http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/fonts/rt_font.woff2?v=c68764eb72df2fd284980d4794d	TEX0ICSG.htm.36.dr	false		high
http://https://ci-ph.rdtcdn.com/videos/202101/07/381285532/original/(m=bIaMwLVg5p)(mh=tImdT2H7gTO9VWG1)0.we	22DFL4CR.htm.34.dr	false		high
http://https://ew.rdtcdn.com/media/videos/202008/12/35041891/360P_360K_35041891_fb.mp4	TEX0ICSG.htm.36.dr	false		high
http://https://ei-ph.rdtcdn.com/m=bIWpYLVg5p/pics/pornstars/000/039/831/thumb_1399282.webp	TEX0ICSG.htm.36.dr	false		high
http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/images/pc/network-bar-sprite.png?v=c68764eb72df2f	TEX0ICSG.htm.36.dr	false		high
http://https://ei.rdtcdn.com/m=bIijsHVg5p/media/videos/201612/17/1871313/original/15.webp	TEX0ICSG.htm.36.dr	false		high
http://https://ei-ph.rdtcdn.com/videos/201909/10/247562661/thumbs_20/(m=bIa44NVg5p)(mh=1Yaa01-wZF-nhfcu)11.	TEX0ICSG.htm.36.dr	false		high
http://https://ei.rdtcdn.com/m=bIa44NVg5p/media/videos/201904/09/15637471/original/7.webp	TEX0ICSG.htm.36.dr	false		high
http://https://ei-ph.rdtcdn.com/m=bIWpYLVg5p/pics/pornstars/000/034/811/thumb_414732.webp	TEX0ICSG.htm.36.dr	false		high
http://https://ei.rdtcdn.com/m=eGJF8f/media/videos/202010/01/36578231/original/3.jpg	TEX0ICSG.htm.36.dr	false		high
http://https://ei.rdtcdn.com/m=bIaMwLVg5p/media/videos/201909/25/22238621/original/2.webp	TEX0ICSG.htm.36.dr	false		high
http://https://ci-ph.rdtcdn.com/videos/201909/10/247562661/thumbs_20/(m=eah-8f)(mh=Ln5T67NuvMOAuIgt)11.jpg	22DFL4CR.htm.34.dr	false		high
http://https://de.redtube.com/	TEX0ICSG.htm.36.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ei.rdtcdn.com/m=bIaMwLVg5p/media/videos/201904/09/15637471/original/7.webp	TEX0ICSG.htm.36.dr	false		high
http://https://cdn1d-static-shared.phncdn.com/timings-1.0.0.js	TEX0ICSG.htm.36.dr	false		high
http://https://gmail.com/greed/lctrLIwgY_2B/TP6odpP7ezu/WCBoLTnqYWdq8j/Q4KzEyzfruaU2o4AYZaBe/eTztEonZ_2FUSm	rundll32.exe, 00000005.00000002.508066657.0000000000DCA000.00000004.00000020.sdmp, ~DFCC2A09043057D1DC.TMP.4.dr, {95A50410-B289-11EB-90E6-ECF4BB82F7E0}.dat.4.dr	false		high
http://https://ei.rdtcdn.com/m=ejrk8f/media/videos/201709/01/241523 8/original/8.jpg	TEX0ICSG.htm.36.dr	false		high
http://https://ei.rdtcdn.com/m=bIaMwLVg5p/media/videos/201908/02/19844991/original/12.webp	TEX0ICSG.htm.36.dr	false		high
http://https://jp.redtube.com/	TEX0ICSG.htm.36.dr	false		high
http://https://ei.rdtcdn.com/m=bIaMwLVg5p/media/videos/201910/14/23039601/original/9.webp	TEX0ICSG.htm.36.dr	false		high
http://https://outlook.office365.com/login/greed/6JA2L69_2BCA0Om9/oYDRb7X4mM7CMUV/GzjWTqcdoobhO1aa1Z/P3XTZR	{7FDF5614-B289-11EB-90E6-ECF4BB82F7E0}.dat.4.dr	false		high
http://https://onedrive.live.com/?wt.mc_id=oo_msn_msnhomepage_header	de-ch[1].htm.6.dr	false		high
http://https://ei.rdtcdn.com/m=bIa44NVg5p/media/videos/201910/14/23039601/original/9.webp	TEX0ICSG.htm.36.dr	false		high
http://https://onedrive.live.com;OneDrive-App	52-478955-68ddb2ab[1].js.6.dr	false	• Avira URL Cloud: safe	low
http://https://ei-ph.rdtcdn.com/m=bIWpYLVg5p/pics/pornstars/000/005/183/thumb_1103531.webp	TEX0ICSG.htm.36.dr	false		high
http://https://ei-ph.rdtcdn.com/videos/202006/03/320302721/original/(m=bIa44NVg5p)(mh=Nf5n1aSFTz4R9-Fi)0.we	TEX0ICSG.htm.36.dr	false		high
http://https://gmail.com/greed/HrSmnFpGUh12/_2FpwPMPFik/bCT3MhW7Qy3fo8/BvutaCWIfwygGzKHyfqWq/gFuvGsw9EwY0E_	{9D8593DD-B289-11EB-90E6-ECF4BB82F7E0}.dat.4.dr, ~DF16D00E5A325F3B1D.TMP.4.dr	false		high
http://www.twitter.com/	msapplication.xml5.4.dr	false		high
http://https://office.live.com/start/Excel.aspx?WT.mc_id=MSN_site;Sway	52-478955-68ddb2ab[1].js.6.dr	false		high
http://https://cv-ph.rdtcdn.com/videos/202006/03/320302721/360P_360K_320302721_fb.mp4?yHlrl6BieqoXxVP-gWPW9	TEX0ICSG.htm.36.dr	false		high
http://https://ei.rdtcdn.com/m=eGJF8f/media/videos/201910/14/23039601/original/9.jpg	TEX0ICSG.htm.36.dr	false		high
http://https://cv-ph.rdtcdn.com/videos/202006/03/320302721/360P_360K_320302721_fb.mp4?k1o3mOF8OYUJh346bmnal	DTABAP9Y.htm.31.dr	false		high
http://https://ei.rdtcdn.com/m=bIaMwLVg5p/media/videos/202011/14/37979511/original/10.webp	TEX0ICSG.htm.36.dr	false		high
http://https://cdn.cookielaw.org/vendorlist/googleData.json	55a804ab-e5c6-4b97-9319-86263d365d28[1].json.6.dr	false		high
http://https://ci-ph.rdtcdn.com/videos/201912/16/269091021/original/(m=bIa44NVg5p)(mh=s8rk-6t3NOgsVKka)0.we	22DFL4CR.htm.34.dr	false		high
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2	{70C8875F-B289-11EB-90E6-ECF4BB82F7E0}.dat.4.dr	false		high
http://https://ei.rdtcdn.com/m=eGJF8f/media/videos/201611/11/1803966/original/15.jpg	TEX0ICSG.htm.36.dr	false		high
http://https://www.msn.com/de-ch/homepage/api/pdp/updatepdpdata"	de-ch[1].htm.6.dr	false		high
http://https://ci.rdtcdn.com/www-static/cdn_files/redtube/images/pc/ads/fallback_pc_top_right.png?v=c68764e	22DFL4CR.htm.34.dr	false		high
http://https://cdn.cookielaw.org/vendorlist/iab2Data.json	55a804ab-e5c6-4b97-9319-86263d365d28[1].json.6.dr	false		high
http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/fonts/rt_font.svg?v=c68764eb72df2fd284980d4794d31	TEX0ICSG.htm.36.dr	false		high
http://https://ei.rdtcdn.com/m=eGJF8f/media/videos/202011/06/377173 71/original/15.jpg	TEX0ICSG.htm.36.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ei-ph.rdtcdn.com/videos/201909/10/247562661/thumbs_20/(m=eW0Q8f)(mh=KdEKWpiDmjWWqhNG)11.jpg	TEX0ICSG.htm.36.dr	false		high
http://https://ei.rdtcdn.com/m=eW0Q8f/media/videos/202008/08/34924331/original/10.jpg	TEX0ICSG.htm.36.dr	false		high
http://https://dw.rdtcdn.com/media/videos/201906/13/17537901/360P_360K_17537901_fb.mp4	22DFL4CR.htm.34.dr	false		high
http://https://dw.rdtcdn.com/media/videos/201909/17/21887251/360P_360K_21887251_fb.mp4	22DFL4CR.htm.34.dr	false		high
http://https://ei.rdtcdn.com/m=bIa44NVg5p/media/videos/201908/02/19844991/original/12.webp	TEX0ICSG.htm.36.dr	false		high
http://https://www.ricardo.ch/?utm_source=msn&utm_medium=affiliate&utm_campaign=msn_mestripe_logo_d	de-ch[1].htm.6.dr	false		high
http://https://ci.rdtcdn.com/www-static/cdn_files/redtube/images/pc/site_sprite.png?v=c68764eb72df2fd284980	22DFL4CR.htm.34.dr	false		high
http://https://ei.rdtcdn.com/m=eW0Q8f/media/videos/202003/13/29344991/original/7.jpg	DTABAP9Y.htm.31.dr	false		high
http://https://ei-ph.rdtcdn.com/m=bIWpYLVg5p/pics/pornstars/000/007/683/thumb_249751.webp	TEX0ICSG.htm.36.dr	false		high
http://https://ev-ph.rdtcdn.com/videos/202006/03/320302721/360P_360K_320302721_fb.mp4?validfrom=1620722976&	22DFL4CR.htm.34.dr	false		high
http://https://outlook.live.com/calendar	52-478955-68ddb2ab[1].js.6.dr	false		high
http://https://ei.rdtcdn.com/m=eah-8f/media/videos/201912/11/25734291/original/8.jpg	TEX0ICSG.htm.36.dr	false		high
http://https://ei.rdtcdn.com/m=eah-8f/media/videos/202007/22/34378181/original/8.jpg	TEX0ICSG.htm.36.dr	false		high
http://api.redtube.com/docs	TEX0ICSG.htm.36.dr	false		high
http://https://ei.rdtcdn.com/m=eGJF8f/media/videos/202004/09/30295811/original/	TEX0ICSG.htm.36.dr	false		high
http://https://www.skyscanner.net/flights?associateid=API_B2B_19305_00001&vertical=custom&pageType=	de-ch[1].htm.6.dr	false		high
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=722878611&size=306x271&https=1	{70C8875F-B289-11EB-90E6-ECF4BB82F7E0}.dat.4.dr	false		high
http://https://ei.rdtcdn.com/m=eW0Q8f/media/videos/202011/14/37979511/original/10.jpg	TEX0ICSG.htm.36.dr	false		high
http://https://clk.tradedoubler.com/click?p=245744&a=3064090&g=21863656	de-ch[1].htm.6.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
173.194.76.156	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
40.97.156.114	outlook.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
172.217.16.99	www.google.de	United States		15169	GOOGLEUS	false
66.254.114.238	redtube.com	United States		29789	REFLECTEDUS	false
52.98.151.242	HHN-efz.ms-acdc.office.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
192.229.221.206	cs733.wpc.rncdn4.com	United States		15133	EDGECASTUS	false
172.217.19.101	gmail.com	United States		15169	GOOGLEUS	false
66.254.114.38	ads.trafficjunky.net	United States		29789	REFLECTEDUS	false
104.20.184.68	geolocation.onetrust.com	United States		13335	CLOUDFLARENETUS	false
52.97.250.194	FRA-efz.ms-acdc.office.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
64.210.135.72	ei.rdtcdn.com.sds.rncdn7.com	United States		30361	SWIFTWILL2US	false
66.254.114.32	hubtraffic.com	United States		29789	REFLECTEDUS	false
64.210.135.70	ht-cdn.trafficjunky.net.sds.rncdn7.com	United States		30361	SWIFTWILL2US	false
40.97.164.146	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.98.152.162	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.97.155.114	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
192.229.221.215	cs742.wpc.rncdn4.com	United States		15133	EDGECASTUS	false
52.97.201.114	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
193.239.84.195	worunekulo.club	Romania		35215	MERITAPL	true
151.101.1.44	tls13.taboola.map.fastly.net	United States		54113	FASTLYUS	false
216.18.168.166	a.adtng.com	United States		29789	REFLECTEDUS	false
40.101.83.18	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.97.201.2	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
205.185.208.79	vip0x04f.ssl.rncdn5.com	United States		20446	HIGHWINDS3US	false
205.185.208.142	vip0x08e.ssl.rncdn5.com	United States		20446	HIGHWINDS3US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
54.247.61.18	tp-rtb-adserver-eu.eu-west-1.elasticbeanstalk.com	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	410858
Start date:	11.05.2021
Start time:	11:47:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	FuiZSHt8Hx (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.troj.winDLL@40/216@116/27
EGA Information:	Failed
HDC Information:	• Successful, ratio: 75.7% (good quality ratio 71.7%) • Quality average: 79.3% • Quality standard deviation: 28.9%
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 20.82.209.183, 52.147.198.201, 92.122.145.220, 104.43.139.144, 88.221.62.148, 131.253.33.203, 92.122.213.187, 92.122.213.231, 65.55.44.109, 184.30.24.22, 104.42.151.234, 184.30.20.56, 152.199.19.161, 92.122.213.194, 92.122.213.247, 13.107.4.50, 172.217.19.100, 216.58.214.238, 20.50.102.62, 209.197.3.25, 69.16.175.42, 69.16.175.10, 205.185.216.10, 205.185.216.42, 52.155.217.156, 20.54.26.129 • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded domains from analysis (whitelisted): cds.g7p6a4c2.hwcdn.net, fs-wildcard.microsoft.com.edgekey.net, e11290.dspg.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, www.google.com, watson.telemetry.microsoft.com, elasticShed.au.au-msedge.net, au-bg-shim.trafficmanager.net, www.google-analytics.com, www.bing.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, cvision.media.net.edgekey.net, ris-prod.trafficmanager.net, skypedataprdcolcus16.cloudapp.net, a1999.dscg2.akamai.net, web.vortex.data.trafficmanager.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, au.au-msedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, cs9.wpc.v0cdn.net, store-images.s-microsoft.com-c.edgekey.net, a-0003.dc-msedge.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, go.microsoft.com, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, vip0x019.map2.ssl.hwcdn.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, Edge-Prod-FRAr4a.env.au.au-msedge.net, www-google-analytics.l.google.com, ie9comview.vo.msecnd.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, cds.e9q5t8x5.hwcdn.net, www-msn-com.a-0003.a-msedge.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, e607.d.akamaiedge.net, afdap.au.au-msedge.net, web.vortex.data.microsoft.com, skypedataprdcoleus16.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, icePrime.a-0003.dc-msedge.net, go.microsoft.com.edgekey.net, static-global-s-msn-com.akamaized.net, au.c-0001.c-msedge.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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

Time	Type	Description
11:48:20	API Interceptor	1x Sleep call for process: loaddll32.exe modified
11:48:26	API Interceptor	1x Sleep call for process: rundll32.exe modified
11:48:51	API Interceptor	1x Sleep call for process: regsvr32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
40.97.156.114	609110f2d14a6.dll	Get hash	malicious	Browse	
	61mamnet@mamnet.com.doc .exe	Get hash	malicious	Browse	
	.exe	Get hash	malicious	Browse	
	32noemai.exe	Get hash	malicious	Browse	
	1attachment.exe	Get hash	malicious	Browse	
	.exe	Get hash	malicious	Browse	
	3messag.exe	Get hash	malicious	Browse	
	1rJ1VNAhR5Z.exe	Get hash	malicious	Browse	
66.254.114.238	609110f2d14a6.dll	Get hash	malicious	Browse	
	PERuTR7vGb.dll	Get hash	malicious	Browse	
	08uyd0CNTM.dll	Get hash	malicious	Browse	
	vbvlCb5GoP.dll	Get hash	malicious	Browse	
	603e0ffd2eeb9.tar.dll	Get hash	malicious	Browse	
	602b97e0b415b.png.dll	Get hash	malicious	Browse	
	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	
192.229.221.206	609110f2d14a6.dll	Get hash	malicious	Browse	
	PERuTR7vGb.dll	Get hash	malicious	Browse	
	08uyd0CNTM.dll	Get hash	malicious	Browse	
	vbvlCb5GoP.dll	Get hash	malicious	Browse	
	603e0ffd2eeb9.tar.dll	Get hash	malicious	Browse	
	invoice_order_57832.zip.exe	Get hash	malicious	Browse	
	5f291fa0130fcrar.dll	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
tls13.taboola.map.fastly.net	1.dll	Get hash	malicious	Browse	• 151.101.1.44
	1.dll	Get hash	malicious	Browse	• 151.101.1.44
	9DwsbuAvOT.dll	Get hash	malicious	Browse	• 151.101.1.44
	f6#Uff09.exe	Get hash	malicious	Browse	• 151.101.1.44
	YBGnZblFot.dll	Get hash	malicious	Browse	• 151.101.1.44
	6f57eb37bff30df1a66f848cb648799536dcbc05f6fb3.dll	Get hash	malicious	Browse	• 151.101.1.44
	23cfb512_by_Libranalysis.dll	Get hash	malicious	Browse	• 151.101.1.44
	39bd68d0_by_Libranalysis.dll	Get hash	malicious	Browse	• 151.101.1.44
	4af51e1230519e63f96e7dbbbd8b688575bddd2c33bbf.dll	Get hash	malicious	Browse	• 151.101.1.44
	352fbf0bc54cdd36e9241b632267002e0cb9568505e9e.dll	Get hash	malicious	Browse	• 151.101.1.44
	c6d47c1f4051999dda951902c21130bf7a95982fb9a8e.dll	Get hash	malicious	Browse	• 151.101.1.44
	9beb1b3b4e8b86c245f0088e5aaef7a123650668607ec.dll	Get hash	malicious	Browse	• 151.101.1.44
	344c6aed9945a611ec6e8dba62e7c0c4a0bd8ef573acd.dll	Get hash	malicious	Browse	• 151.101.1.44
	011bc15db92fe83fcbb0904253ef539e88a54d6e6ccef.dll	Get hash	malicious	Browse	• 151.101.1.44
	235b4aef916cfe2b8c63778d22b79340d96bfa09354f6.dll	Get hash	malicious	Browse	• 151.101.1.44
	dd6d136055296abfc6f94c8ae1d039042c603fb1d0938.dll	Get hash	malicious	Browse	• 151.101.1.44
	GC1BuHQFdB.dll	Get hash	malicious	Browse	• 151.101.1.44
	86e010b6_by_Libranalysis.dll	Get hash	malicious	Browse	• 151.101.1.44
	f37daf2f_by_Libranalysis.dll	Get hash	malicious	Browse	• 151.101.1.44
	4663d5c2_by_Libranalysis.dll	Get hash	malicious	Browse	• 151.101.1.44

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
REFLECTEDUS	609110f2d14a6.dll	Get hash	malicious	Browse	• 66.254.114.32

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Four.exe	Get hash	malicious	Browse	• 66.254.114.63
	PERuTR7vGb.dll	Get hash	malicious	Browse	• 67.22.48.100
	08uyd0CNTM.dll	Get hash	malicious	Browse	• 66.254.114.32
	vbvlCb5GoP.dll	Get hash	malicious	Browse	• 216.18.168.166
	603e0ffd2eeb9.tar.dll	Get hash	malicious	Browse	• 66.254.114.32
	602b97e0b415b.png.dll	Get hash	malicious	Browse	• 216.18.168.166
	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
MICROSOFT-CORP-MSN-AS-BLOCKUS	609a460e94791.tiff.dll	Get hash	malicious	Browse	• 40.101.12.82
	iIoO9qC8yj.exe	Get hash	malicious	Browse	• 13.107.4.50
	qLi9sAxeSm.exe	Get hash	malicious	Browse	• 204.95.99.243
	f1a5fbd3e946e8db1c18bd1d30d0f8b41a873cbb76769.exe	Get hash	malicious	Browse	• 20.194.35.6
	tgix.exe	Get hash	malicious	Browse	• 137.117.64.85
	Protiviti.htm	Get hash	malicious	Browse	• 52.240.156.143
	hn80vhR3y1.exe	Get hash	malicious	Browse	• 13.69.222.243
	file.msg.exe	Get hash	malicious	Browse	• 104.47.56.161
	SCB_MT103_31951R2105050031_200505.PDF.exe	Get hash	malicious	Browse	• 157.55.136.23
	Windows_Update.exe	Get hash	malicious	Browse	• 20.52.178.148
	NcLDA3J4Kp.apk	Get hash	malicious	Browse	• 204.79.197.200
	LIau1wwvy5.exe	Get hash	malicious	Browse	• 20.43.33.61
	Update-KB1484-x86.exe	Get hash	malicious	Browse	• 104.47.37.36
	iJdlvBxhYu.dll	Get hash	malicious	Browse	• 52.97.201.82
	2f50000.exe	Get hash	malicious	Browse	• 52.141.33.89
	609110f2d14a6.dll	Get hash	malicious	Browse	• 40.101.137.34
	EBqJhAymeE.rtf	Get hash	malicious	Browse	• 157.55.173.72
	QXfU5ZSUpd.exe	Get hash	malicious	Browse	• 20.194.35.6
	813oo3jeWE.exe	Get hash	malicious	Browse	• 20.184.2.45
	pog.exe	Get hash	malicious	Browse	• 40.124.7.222

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	#Ud83d#Udce9-vesna.starcevic.htm	Get hash	malicious	Browse	• 173.194.76.156 • 172.217.16.99 • 66.254.114.238 • 192.229.221.215 • 192.229.221.206 • 151.101.1.44 • 172.217.19.101 • 66.254.114.38 • 104.20.184.68 • 216.18.168.166 • 205.185.208.79 • 205.185.208.142 • 54.247.61.18 • 64.210.135.72 • 66.254.114.32 • 64.210.135.70

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	sCWXdbS7XR.exe	Get hash	malicious	Browse	• 173.194.76.156 • 172.217.16.99 • 66.254.114.238 • 192.229.221.215 • 192.229.221.206 • 151.101.1.44 • 172.217.19.101 • 66.254.114.38 • 104.20.184.68 • 216.18.168.166 • 205.185.208.79 • 205.185.208.142 • 54.247.61.18 • 64.210.135.72 • 66.254.114.32 • 64.210.135.70
	Ningbo-Bank Details.exe.exe	Get hash	malicious	Browse	• 173.194.76.156 • 172.217.16.99 • 66.254.114.238 • 192.229.221.215 • 192.229.221.206 • 151.101.1.44 • 172.217.19.101 • 66.254.114.38 • 104.20.184.68 • 216.18.168.166 • 205.185.208.79 • 205.185.208.142 • 54.247.61.18 • 64.210.135.72 • 66.254.114.32 • 64.210.135.70
	ATT81583.HTM	Get hash	malicious	Browse	• 173.194.76.156 • 172.217.16.99 • 66.254.114.238 • 192.229.221.215 • 192.229.221.206 • 151.101.1.44 • 172.217.19.101 • 66.254.114.38 • 104.20.184.68 • 216.18.168.166 • 205.185.208.79 • 205.185.208.142 • 54.247.61.18 • 64.210.135.72 • 66.254.114.32 • 64.210.135.70
	receipt748.html	Get hash	malicious	Browse	• 173.194.76.156 • 172.217.16.99 • 66.254.114.238 • 192.229.221.215 • 192.229.221.206 • 151.101.1.44 • 172.217.19.101 • 66.254.114.38 • 104.20.184.68 • 216.18.168.166 • 205.185.208.79 • 205.185.208.142 • 54.247.61.18 • 64.210.135.72 • 66.254.114.32 • 64.210.135.70

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment Report (Mon, 10 May 2021).hTMl	Get hash	malicious	Browse	• 173.194.76.156 • 172.217.16.99 • 66.254.114.238 • 192.229.221.215 • 192.229.221.206 • 151.101.1.44 • 172.217.19.101 • 66.254.114.38 • 104.20.184.68 • 216.18.168.166 • 205.185.208.79 • 205.185.208.142 • 54.247.61.18 • 64.210.135.72 • 66.254.114.32 • 64.210.135.70
	9DwsbuAvOT.dll	Get hash	malicious	Browse	• 173.194.76.156 • 172.217.16.99 • 66.254.114.238 • 192.229.221.215 • 192.229.221.206 • 151.101.1.44 • 172.217.19.101 • 66.254.114.38 • 104.20.184.68 • 216.18.168.166 • 205.185.208.79 • 205.185.208.142 • 54.247.61.18 • 64.210.135.72 • 66.254.114.32 • 64.210.135.70
	receipt156.html	Get hash	malicious	Browse	• 173.194.76.156 • 172.217.16.99 • 66.254.114.238 • 192.229.221.215 • 192.229.221.206 • 151.101.1.44 • 172.217.19.101 • 66.254.114.38 • 104.20.184.68 • 216.18.168.166 • 205.185.208.79 • 205.185.208.142 • 54.247.61.18 • 64.210.135.72 • 66.254.114.32 • 64.210.135.70
	H0kDylXIaQ.exe	Get hash	malicious	Browse	• 173.194.76.156 • 172.217.16.99 • 66.254.114.238 • 192.229.221.215 • 192.229.221.206 • 151.101.1.44 • 172.217.19.101 • 66.254.114.38 • 104.20.184.68 • 216.18.168.166 • 205.185.208.79 • 205.185.208.142 • 54.247.61.18 • 64.210.135.72 • 66.254.114.32 • 64.210.135.70

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	OneDrive digiturk.com.tr.html	Get hash	malicious	Browse	• 173.194.76.156 • 172.217.16.99 • 66.254.114.238 • 192.229.221.215 • 192.229.221.206 • 151.101.1.44 • 172.217.19.101 • 66.254.114.38 • 104.20.184.68 • 216.18.168.166 • 205.185.208.79 • 205.185.208.142 • 54.247.61.18 • 64.210.135.72 • 66.254.114.32 • 64.210.135.70
	f6#Uff09.exe	Get hash	malicious	Browse	• 173.194.76.156 • 172.217.16.99 • 66.254.114.238 • 192.229.221.215 • 192.229.221.206 • 151.101.1.44 • 172.217.19.101 • 66.254.114.38 • 104.20.184.68 • 216.18.168.166 • 205.185.208.79 • 205.185.208.142 • 54.247.61.18 • 64.210.135.72 • 66.254.114.32 • 64.210.135.70
	Y44KdzdByL.exe	Get hash	malicious	Browse	• 173.194.76.156 • 172.217.16.99 • 66.254.114.238 • 192.229.221.215 • 192.229.221.206 • 151.101.1.44 • 172.217.19.101 • 66.254.114.38 • 104.20.184.68 • 216.18.168.166 • 205.185.208.79 • 205.185.208.142 • 54.247.61.18 • 64.210.135.72 • 66.254.114.32 • 64.210.135.70
	YBGnZblFot.dll	Get hash	malicious	Browse	• 173.194.76.156 • 172.217.16.99 • 66.254.114.238 • 192.229.221.215 • 192.229.221.206 • 151.101.1.44 • 172.217.19.101 • 66.254.114.38 • 104.20.184.68 • 216.18.168.166 • 205.185.208.79 • 205.185.208.142 • 54.247.61.18 • 64.210.135.72 • 66.254.114.32 • 64.210.135.70

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	b5lccOmZdI.exe	Get hash	malicious	Browse	• 173.194.76.156 • 172.217.16.99 • 66.254.114.238 • 192.229.221.215 • 192.229.221.206 • 151.101.1.44 • 172.217.19.101 • 66.254.114.38 • 104.20.184.68 • 216.18.168.166 • 205.185.208.79 • 205.185.208.142 • 54.247.61.18 • 64.210.135.72 • 66.254.114.32 • 64.210.135.70
	BasmanF@mashreq.com.htm	Get hash	malicious	Browse	• 173.194.76.156 • 172.217.16.99 • 66.254.114.238 • 192.229.221.215 • 192.229.221.206 • 151.101.1.44 • 172.217.19.101 • 66.254.114.38 • 104.20.184.68 • 216.18.168.166 • 205.185.208.79 • 205.185.208.142 • 54.247.61.18 • 64.210.135.72 • 66.254.114.32 • 64.210.135.70
	New_American_Chamber_commerce 2021..xlsx	Get hash	malicious	Browse	• 173.194.76.156 • 172.217.16.99 • 66.254.114.238 • 192.229.221.215 • 192.229.221.206 • 151.101.1.44 • 172.217.19.101 • 66.254.114.38 • 104.20.184.68 • 216.18.168.166 • 205.185.208.79 • 205.185.208.142 • 54.247.61.18 • 64.210.135.72 • 66.254.114.32 • 64.210.135.70
	GBtiwIB30h.exe	Get hash	malicious	Browse	• 173.194.76.156 • 172.217.16.99 • 66.254.114.238 • 192.229.221.215 • 192.229.221.206 • 151.101.1.44 • 172.217.19.101 • 66.254.114.38 • 104.20.184.68 • 216.18.168.166 • 205.185.208.79 • 205.185.208.142 • 54.247.61.18 • 64.210.135.72 • 66.254.114.32 • 64.210.135.70

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	6f57eb37bff30df1a66f848cb648799536dcbc05f6fb3.dll	Get hash	malicious	Browse	• 173.194.76.156 • 172.217.16.99 • 66.254.114.238 • 192.229.221.215 • 192.229.221.206 • 151.101.1.44 • 172.217.19.101 • 66.254.114.38 • 104.20.184.68 • 216.18.168.166 • 205.185.208.79 • 205.185.208.142 • 54.247.61.18 • 64.210.135.72 • 66.254.114.32 • 64.210.135.70
	23cfb512_by_Libranalysis.dll	Get hash	malicious	Browse	• 173.194.76.156 • 172.217.16.99 • 66.254.114.238 • 192.229.221.215 • 192.229.221.206 • 151.101.1.44 • 172.217.19.101 • 66.254.114.38 • 104.20.184.68 • 216.18.168.166 • 205.185.208.79 • 205.185.208.142 • 54.247.61.18 • 64.210.135.72 • 66.254.114.32 • 64.210.135.70
	39bd68d0_by_Libranalysis.dll	Get hash	malicious	Browse	• 173.194.76.156 • 172.217.16.99 • 66.254.114.238 • 192.229.221.215 • 192.229.221.206 • 151.101.1.44 • 172.217.19.101 • 66.254.114.38 • 104.20.184.68 • 216.18.168.166 • 205.185.208.79 • 205.185.208.142 • 54.247.61.18 • 64.210.135.72 • 66.254.114.32 • 64.210.135.70

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\IUHEMSR9\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):	2897
Entropy (8bit):	4.919943269589007
Encrypted:	false
SSDEEP:	48:Lh7ih7ih7W7ih7ih7ih7ih7ih7ih7D7ih7iN7iN7iN7iN7iN7i7iN7iN7H:F00q0000000f0888888O88Ap0H08Ap0v
MD5:	815B808191BE7556C37A3AE8EC43F57E
SHA1:	51F244A5DC2D6753F49A73F0379848B57DF0C985
SHA-256:	40ADA4A59FDA536B33F473018704A5B3AFC9C20B21C73705B7205A66961E2C68
SHA-512:	DC10544DFE8404C78A4745612E91D4B94FC61484912BA34A104B1A0C01B73335E4D5F3FEB434DD96A9D236AD233722FB9FFEC1D06E16CFCAE987AE02BE2BACB4

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\IUHEMSR9\contextual.media[1].xml	
Malicious:	false
Preview:	<root></root><root><item name="HBCM_BIDS" value="{}" ltime="917552304" htime="30885526" /></root><root><item name="HBCM_BIDS" value="{}" ltime="917552304" htime="30885526" /></root><root><item name="HBCM_BIDS" value="{}" ltime="917552304" htime="30885526" /><item name="mntest" value="mntest" ltime="917552304" htime="30885526" /></root><root><item name="HBCM_BIDS" value="{}" ltime="917552304" htime="30885526" /></root><root><item name="HBCM_BIDS" value="{}" ltime="917552304" htime="30885526" /></root><root><item name="HBCM_BIDS" value="{}" ltime="917552304" htime="30885526" /></root><root><item name="HBCM_BIDS" value="{}" ltime="917552304" htime="30885526" /></root><root><item name="HBCM_BIDS" value="{}" ltime="917552304" htime="30885526" /></root><root><item name="HBCM_BIDS" value="{}" ltime="917552304" htime="30885526" /><item name="mntest" value="mntest" ltime="921552304" htime="30885526" /></root><ro

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\T8DRMTJ1\www.msn[2].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aKb:JFKb
MD5:	C1DDEA3EF6BBEF3E7060A1A9AD89E4C5
SHA1:	35E3224FCBD3E1AF306F2B6A2C6BBEA9B0867966
SHA-256:	B71E4D17274636B97179BA2D97C742735B6510EB54F22893D3A2DAFF2CEB28DB
SHA-512:	6BE8CEC7C862AFAE5B37AA32DC5BB45912881A3276606DA41BF808A4EF92C318B355E616BF45A257B995520D72B7C08752C0BE445DCEADE5CF79F73480910FE D
Malicious:	false
Preview:	<root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{70C8875D-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	478984
Entropy (8bit):	2.6519452029393062
Encrypted:	false
SSDEEP:	384:rmXo/MmcNHLzFZHlyEOc68+pq1y77OqzkUW8k8cV9cJDjF62i7Ya8u7TLIdYfBgd:B
MD5:	FDCE9F17C08230B1FB8E6F9282BCEE98
SHA1:	99BC6605A44871C8B513A636FF1B0257CA27671B
SHA-256:	CECE83C5EE59BBB37E2F18759622D0B2CA7C82FA61A21E9BAC84C3777DF11A24
SHA-512:	EEF829F7272581028978737F8052E717B77474902FB47899FF4894B20A7134B2C3B24F63FA4679933D3B71209AC42057BEA52DFE655846CA5B5D72D9B6506B27
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{70C8875F-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	197126
Entropy (8bit):	3.582860337163241
Encrypted:	false
SSDEEP:	3072:NZ/2BfcYmu5kLTzGtxZ/2Bfc/mu5kLTzGtO:Ugt
MD5:	560BBB41451B79C12B707C9B6F26CFB6
SHA1:	56C163FA0F69AE9DBA7A6EF3F0A6D78F82CFCE35
SHA-256:	DBFFB522F29D04C62CBA0BF0BF1167B4BA0B42FA54FC54869DE750589E084479
SHA-512:	3685E12C7DB3640FB4083CDA4B185444A2D2B137ED3B23269D317C618E828981BCD1906B21880996928C8A8142573C18EE7A1A59FEC9537F7B732CA96932A714
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7FDF5612-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7FDF5612-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Size (bytes):	27388
Entropy (8bit):	1.8479239720873024
Encrypted:	false
SSDEEP:	96:rIZDQ361BSJj0E21WpMFOdQ0KtRdQ0KZA:rIZDQ361kJjp21WpMFOdxcRdxcA
MD5:	F085A6F3DC4E0B7C7E09C241403848B8
SHA1:	C9F111C7A7390A0A4EC59558CF18EAD4D2D5F784
SHA-256:	AE44BA85968B539982967706327D6C8168801A0901EA14CBED8C4094301A1CC0
SHA-512:	425D1C29252A69B6CA5D7DCA7CD51C5D10136F699A1176783C67521CB73E0681837666F4A92097389F6E9E13EE1D4C8DB2EEC99764D7B7B152F7AE36C7C0065
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7FDF5614-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27432
Entropy (8bit):	1.86396063759608
Encrypted:	false
SSDEEP:	192:rBZyQS6Iknjh2VW4MQGiUUl3xUUlPlFVA:rHf9VjQsdE/B/dU
MD5:	D9FED4F373C9209367DCDC11D1C084B9
SHA1:	025A22B92B824C83A67FEA5FA9F53C159DE71360
SHA-256:	3331AE619146921735E440FDB4710290728F02A1C2321F40FBD6C212624949BF
SHA-512:	79D87C5BBA0DE931B56C38528FE1A67E56B5373A435C714213973409BA41503AB4CD2D60284603C0CCAE8E5F25A405F8F88415CB4027DC75591F2A6D02F12306
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{879BFBC6-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27384
Entropy (8bit):	1.8475415579762864
Encrypted:	false
SSDEEP:	96:rvZwQA6SBSyjjF2dWHMTyXNM8ipRXNM8itMzA:rvZwQA6Skyjp2dWHMTyXNkpRXNktUA
MD5:	769CB762CF1203FA913232E4C197D828
SHA1:	66D9C9864603330BBA389C7BD75576AAA51C826F
SHA-256:	B79454E55DD4304AF8CCA437EC4AFFD48309CB8192589C899B7D6C8450D89D93
SHA-512:	B0E5C539A2C5292F1D13BDACC022938A19BDC2015611078EE1F8DD6BE2ECDCF939C05878D7407007F4F6343960FDF14037242D0F5B58BF1714D4E714759EB11
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{8EF8C44C-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27864
Entropy (8bit):	1.8264495577100925
Encrypted:	false
SSDEEP:	96:rOZtQV6DBStjjF24EW47M4vSy5KMAbHRy5KMAbzKpr:rOZtQV6DktjZ24EW47M4vSytmRytnr
MD5:	A786DF32C5862E1DC2B797CA06A95DE5
SHA1:	94E703BA3DB752FC10F174CD822D24B4B1807516
SHA-256:	172ED36796B8839A771C1E80DC02FDFC399D417C0D8C80CC2E8F70AD0152879E
SHA-512:	C59983F8C35F335D8636353B2DC2F3A05F1BCD25E3D00ED88B24DF63ECEA2C69F93C8F54EDBB4DA4361F85329443C57DAAE95055A089AEBF2CD66FA09181B7A
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{8EF8C44C-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{8EF8C44E-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27448
Entropy (8bit):	1.8699677625650784
Encrypted:	false
SSDEEP:	192:rVZ+Qd6bkljF/2FDWFVMFJyXwSEAlW7NgRXwSEAlW7N4EANA:rb7IgBFuFaFWFsXKAlWJ4XKAlWJ5Ae
MD5:	67763E6B42A81566778C05DD57876882
SHA1:	32D653485FEE1D701B1DD32C175B8DD00B3812B6
SHA-256:	3B9623658AD08DDA5D86B27452E9626D62D7A27810313CA82EC53E6CDBFD5F9E
SHA-512:	1DAC00BB13AC4AC23FA4782361A7F29281722AEC4B76B39ACF3399EF9F1BE5D2967263F855202A3806FF41C63EC9A1E4B52751898DF0278B92BCAEF6BE268DC2
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{8EF8C450-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27384
Entropy (8bit):	1.845905842989005
Encrypted:	false
SSDEEP:	96:rIZTQv6NBSjjVP25WZMhykQpUxfkRkQpUxfqpA:rIZTQv6NkjjF25WZMhyk9x8Rk9xCpA
MD5:	2BA23CED2270E9964CBB9776BFB18FF1
SHA1:	50E9FE52AC2FB01D28E82B4E6D4B7B0ADC43977A
SHA-256:	BE49EA93C03A710BEB52F56001FAB9B678265BFEC8F64F21D072752D327F6F93
SHA-512:	94D38C19365EE2A0EA917FF2AAA33DDF2629B0458D0BF341D6423EA1FEAA34D6D8A8DAB759F2E7835F186F772790B1A30977540C501B0A74D3919959F911B109
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{95A50410-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27404
Entropy (8bit):	1.8533835031710497
Encrypted:	false
SSDEEP:	96:rPZ0QA6WBSuj+W29W3Mjeu41uSxu41uZ1dA:rPZ0QA6Wkujx29W3Mjeu4ESxu4EZ3A
MD5:	9789CF7820B42D767BB5A3260B28CAAA
SHA1:	C8C9CA582BA82256D50D3482AE54C19C535D67D9
SHA-256:	5DF7D851B61F5FB8556DE362B4BFC7B64D88AEAB653AAE6CEB32AB6BA0B5D37C
SHA-512:	8856C3A0ADDAFF7EE98ACDB28D124BDC14B07DE571C180946DE747A16858A175490B7046A971DA2F40B0B3B945DA5F0A9C4BC78A03AC534716459E5437C1E48
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9D8593DB-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	31344

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9D8593DB-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Entropy (8bit):	1.6737114284448087
Encrypted:	false
SSDEEP:	48:IwRGcpr8Gwpa8G4pQUGrapbSdhGQpBe3GHHpcUiTGUp87GzYpmfAWGopGlfaxGyN:rnZ0Qc6iBSdjei2ZWBM5s6/b24F4A
MD5:	38A4C152D9EA504E38819F3D33256EB8
SHA1:	5924FA5428EAAB8844B467B0E5713EAB53305F84
SHA-256:	8D07548C2CAC01DDD2982D518829C7C46481C3805110D98D399EEAE21D7EC8F6
SHA-512:	A2E17309823E4C045EF78A548095AFB706731B4454CF10E5A46EB6D8F588332A504F3ECFEC5DF044572DF22AAC3E2D9A807AAFABB37E1FA5FBEA7C1E4409986
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9D8593DD-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27088
Entropy (8bit):	1.8358770461973293
Encrypted:	false
SSDEEP:	96:rWZJQ96HBS5jHd2NWuM+TmXcni7LZxWxXcnqcni7LZxeA:rWZJQ96Hk5j92NWuM+TmM+dgxMx+dAA
MD5:	AE799D4FD313906938FE6E202793E932
SHA1:	CE03AB7649706BB1A96DE8979E698AAF0E25DDD4
SHA-256:	DC4372E01C5B2194CB63162806F158DE7F5288BC17D2960EE6E0BF6866672E1B
SHA-512:	6193D00BAA0CBCF954DE01D295E587B39307BBFDD8904B89DD0463E0B171471D16F98A2E100E3DB25EE1C267E44F376EAAD91300BE336D09D4A9C8E61C8358 A
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9D8593DF-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	31344
Entropy (8bit):	1.674520722496874
Encrypted:	false
SSDEEP:	48:IwLGcpruGwpaSG4pQ6GrapbSkGQpB23GHHpcsTGUp8DGzYpm37GopGNfaZGyXpda:rRZGQi6sBS8j2i2kWZMNsC/m28FeA
MD5:	0A83A35E1F86E7AA2B94909C1F373379
SHA1:	6D109E16D1DA9619E0533E6861904C57666E2B7F
SHA-256:	04E84898E823DE81764EFA34E0E42519D0D3B56AC92BE27B86BA1BAA6B9B4D5B
SHA-512:	EF83F84EC00C17B0E797D2FAE3E9514C26F25FE7AF346246AF6CCE6D839F6E9CA3688B08AFFD7AE07369B91D69987A9D7FFCE00D956DB6E10A2E0AE0C567B8 4E
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9D8593E1-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	31344
Entropy (8bit):	1.6748536154450628
Encrypted:	false
SSDEEP:	48:IwpGcprkGwpaMG4pQ0GrapbSzGQpB7+GHHpcUTGUp8dGzYpmyUGopGMfalGyXpdv:rvZcQM6CBSNj7N2MWjMzsZ/7x2sF0A
MD5:	C43E6BEE06FFD9DB8EA3816512B9E7CF
SHA1:	54A16C8708E3EA1A4FFBDC9CF3594B6270B96F01
SHA-256:	7510E3731361EA60A5282CD9E8F7AF52C1DB778B9B756CAEFBBC0D18E39B585A
SHA-512:	5087714A4DC6D3FA1DE93850473BF8604BBBCDA7962B6C4CCBE4B6B438BAE7BBA7C3AB717E90CE6A780A4899775D9608CCAAB2755FFDAAD125DDB92468F32 877
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{9D8593E1-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{AB2EED2E-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	31344
Entropy (8bit):	1.674859591192103
Encrypted:	false
SSDEEP:	48:IwxgGcprPLGwpawgG4pQqSGrapbSRcGQpBNIGHHpcPTGUp8gGzYpm0/GopGmfaEL:reZNQ16jBSR0jNH2ZWUMUsA/32wFqA
MD5:	34FB83980508254E65E3AD95FA16AE23
SHA1:	BE347D15296A66313A86D63DCB25204C8AD87390
SHA-256:	BF04B208EB6298DEDBE757EE9A8D036BBD1247A9CC9436A68F7F15FE93A1EFDC
SHA-512:	DBCC48B8F9812830851A1131BB72131EF8978DE4C93064056626E9BFA2309D5EC975EBD04A30B7B93FFB5C25D89F9219C38B81A4D513366AE3CFB107AEBA39C A
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{AB2EED30-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	31344
Entropy (8bit):	1.674638601524446
Encrypted:	false
SSDEEP:	48:IwsGcprxGwpaxG4pQdGrapbSu7GQpBvlgGHHpcXTGUp8XGzYpmkMGopGGfanGyX5:rwZrQj69BSSj9P2hWVMhsh/K2gF5A
MD5:	ADE77570A3A99726D15F3ECF62EADD4A
SHA1:	641AC68F748C150A8EAA7C5627300B5EEAF55ECA
SHA-256:	0AC5CFF11DC850B54C825682CAB762FDC2B17A38D3669B42E791B98852E2514F
SHA-512:	4E6E60A75D65E709EE4483BD5C132BD9368C54ABD70268E6A32771986CA920395254F0437FDC925448B2C0066CE5303AB8D73029660A0EFAF182A4F6E4D15A88
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{AB2EED32-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	31344
Entropy (8bit):	1.672332681084016
Encrypted:	false
SSDEEP:	96:r+Z1QB6nBSYXjAtvs2AnWWAYMAss6y/6Y26AF62A:r+Z1QB6nkgjJ2tWzM3sT/J2dF3A
MD5:	74F13E23B08EB6F0776D47628DDCF6C1
SHA1:	79243F0D498856CA6A0777344654B67D1483AB8A
SHA-256:	56996DCB613157A50B1095EEEDBADD116C371B6CEC542E54451D0E3366FFAAE6
SHA-512:	B480E7A42109A3D2AD66B663A2026CB0CE9F4CDB678E907352F5731007B6639695B7CFC94EA5366645548D038C57F8E5F3A76E3EDD0C3BF83B2BE807DAF3D91
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B1478A0B-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	31344

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B1478A0B-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Entropy (8bit):	1.6739848268004556
Encrypted:	false
SSDEEP:	48:Iwl1Gcpr3OGwpak1G4pQanGrapbSdGQpBFgGHHpc/TGUp8XGzYpmskGopG+fabGa:rpZ2QG6wBSnjFP2JWVMJsV/a2ZFqA
MD5:	DDC69128A6EBE277DB8B9DF8C042BD18
SHA1:	25AC2F888F02FD9BA70E88CBC3098DB1CDBEB32E
SHA-256:	C7E7658D66100F7F889BF2A6234B7A5319B13C23B390A30BF8F7E802135C65BD
SHA-512:	C3DFEDA0A58C0C7EB48ADA14072F6071288B45D1D59A4DD3F1B3985F8E0F7E7A8BD2AE90F085AEF56A37AC12C4373E2D1348F59C2611E446537E73A9F22A7F4
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B8EF06FD-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	31344
Entropy (8bit):	1.6767422365900713
Encrypted:	false
SSDEEP:	192:rJZ2QW6wkbjV2HlWHYMHUstR/tl2tOFtzA:r/Dh9HMcdhndg2
MD5:	518E91E777E27469122513693F479DBB
SHA1:	8AF7FBB4308657594E1306356D6416408A613EE2
SHA-256:	062CEF428296391AF963DF7374141281BC48A8DFCBB96722CEE1FBEF0F1D6B09
SHA-512:	A05A3CD86B84BC9DEAB2C73C5EE48374BB9B8AF9F2BA589648F2C65F4557E29AB6DCB8763AC01AFA7FA10D710DB6D8EC45E260B0F10186E9BC4A22BC307DE F6E
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B8EF06FF-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27396
Entropy (8bit):	1.855236539152366
Encrypted:	false
SSDEEP:	48:IwIGcprRGwpalG4pQeGrapbSUGQpB81GHHpcUTGUp8hGzYpmNbGop0bTCKMdquTT:r8ZLQ36QBSMj842MWPMrmvp0FRvp0BA
MD5:	B187A995C7FE737CA40725E92711A1BC
SHA1:	593B1BBDF9138B537391721987903E0B0D1D9CD6
SHA-256:	CDE483053F79303F7F16FEB58904029B17A0968FF9E11F348D2FD274779ED6B0
SHA-512:	6A8B53734C0ED0FC1CD28917E1278F8BE36A8EDB2B668014A55FC5C89C2FFFED63549F96B5FB1494ED0CDC262357EA9CECEF4844AC45819003D0912FB08435 E
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B8EF0701-B289-11EB-90E6-ECF4BB82F7E0}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	16984
Entropy (8bit):	1.5738002706448162
Encrypted:	false
SSDEEP:	48:IwMGcprtGwpaaG4pQSGrapbSCGQpBq/GHHpcgTGUpG:rQZ3Qa6UBSKjqa2oA
MD5:	43F406C1C34BB964E9D145F0509A4429
SHA1:	17335CBACD6BFBBE982A2717632FFD8B6E05D47F
SHA-256:	92F097B73EF8C5F358B687251C80E64DA93652E6A6E49955A6202FEE2C1F670F
SHA-512:	92E3C7D04317D4A536BEA49FAF14BE554DF8E733D4A952CC5466A4ACA9EDE5FEDDABB2B66D6C7BB00CE1710ADFA47FC04423F0D967A85647457FC077DE3A7 1B5
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B8EF0701-B289-11EB-90E6-ECF4BB82F7E0}.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):	660
Entropy (8bit):	5.133134879161687
Encrypted:	false
SSDEEP:	12:TMHdNMNxOE6TsTzNnWimI002EtM3MHdNMNxOE6TsTzNnWimI00OYVbkEtMb:2d6NxOiNSZHKd6NxOiNSZ7xb
MD5:	79940B1246C49B315D97AAF888D2EA09
SHA1:	AD410D45AB47C316D928C30BE263E548AF92EF08
SHA-256:	E259DFC0744C3F2D453F2870FE18AE4C4962B8435FC42F6C051BE16FAF0BA7BA
SHA-512:	A9C30B11DE4C947652177334624C5B7A73CF25B0B0E15803C8A63AD2AE1E14E3535F28CA8996FDCAD0F705D8CFA952F806DFE2E38BA7CE1E14D2EFA1DE7AAB4
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0x672135c1,0x01d74696</date><accdate>0x672135c1,0x01d74696</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>0x672135c1,0x01d74696</date><accdate>0x672135c1,0x01d74696</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):	657
Entropy (8bit):	5.150102989205941
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kvNnWimI002EtM3MHdNMNxe2kvNnWimI00OYkak6EtMb:2d6Nxr6NSZHKd6Nxr6NSZ7Ja7b
MD5:	A74D88A082041D4C5A1FCE99C6170E9F
SHA1:	AE252BE4D467A9A1A24644EF9BEFFF91BCE26DAE
SHA-256:	8B97EDA36AE1F50BFB802DD74BD4D6BF74295253F9458B9573C1F4E3C5BE1425
SHA-512:	C952E5AFE45AC26F1AD199F0EEFE2C8E0E8E526B002CFC73550ACE4B8599997927B96736C935527D3D68F86A3369104B543AF8C660D0E90FCE2F612D6A34F87
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0x671946be,0x01d74696</date><accdate>0x671946be,0x01d74696</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>0x671946be,0x01d74696</date><accdate>0x671946be,0x01d74696</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):	666
Entropy (8bit):	5.148679831442917
Encrypted:	false
SSDEEP:	12:TMHdNMNxvL6TsTzNnWimI002EtM3MHdNMNxvL6TsTzNnWimI00OYmZEtMb:2d6NxvPNSZHKd6NxvPNSZ7Zb
MD5:	6DB84ED6FCE065AE6641157D90E03FAA
SHA1:	D26525A1DA0D8F42D68F75051FE760890E86D80C
SHA-256:	818E294EE12AFF049F06604625649992C77EFD3D3A05D28D50FF147832EB3C55
SHA-512:	EC576D1CB4BBD804FEB087EEDF8BB2D23033D046FC6CC735F7F08957227D22EA4667C26002976C0E34AEE91725154D506BB36A6AAA61AD595D35E1095561803
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0x672135c1,0x01d74696</date><accdate>0x672135c1,0x01d74696</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>0x672135c1,0x01d74696</date><accdate>0x672135c1,0x01d74696</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Category:	dropped
Size (bytes):	651
Entropy (8bit):	5.149796038895868
Encrypted:	false
SSDEEP:	12:TMHdNMNxi6TsTzNnWimI002EtM3MHdNMNxi6TsTzNnWimI00OYd5EtMb:2d6NxUNSZHKd6NxUNSZ7qjb
MD5:	3FE696B9181CB17081D73CBF32E2B6CC
SHA1:	2F4978FBDE83EFCBB371BB52D747636AB8C9CEB0
SHA-256:	E5AC78C667DE6B1EED7A641D4AC75BEF6F19F5DE252C208D6918D5AFA479C833
SHA-512:	404F634F87B2CCF9BDA19C40501039963D79EF9714FD28EE5C8EDA0023C14DF81F752FE9B01F8B227875E0332924A3762C30A512BF8F11EB8BB31B7EA52BF218
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0x672135c1,0x01d74696</date><acc date>0x672135c1,0x01d74696</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>0x672135c1,0x01d74696</date><accdate>0x672135c1,0x01d74696</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):	660
Entropy (8bit):	5.1552198683192465
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwoEtNnWimI002EtM3MHdNMNxhGwoEtNnWimI00OY8K075EtMb:2d6NxQLEtNSZHKd6NxQLEtNSZ7RKajb
MD5:	747B3BC425778AA76A83B82566C668F8
SHA1:	3596614C87FC15AA14D849C2195B619EEF07C422
SHA-256:	E3F5B991F3FD86F6A1B7AB4539F267EAF64B9144478D400537C3A6850874830F
SHA-512:	283A506C515B3D8946D17A5DCE472B8AAF4D65490D25A76F7189587C8A6DC0918F19B467265F1785913DF776781DEFD366B5D6B6AC2E5CAAA5677AE5EE1A2B4
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0x672a64e7,0x01d74696</date><accdate>0x672a64e7,0x01d74696</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>0x672a64e7,0x01d74696</date><accdate>0x672a64e7,0x01d74696</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):	657
Entropy (8bit):	5.136767221713154
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n6TsTzNnWimI002EtM3MHdNMNx0n6TsTzNnWimI00OYxEtMb:2d6Nx0zNSZHKd6Nx0zNSZ7+b
MD5:	CD1FB6A5E583480DAD92413FF86B33D6
SHA1:	6C29557504FFDA036CCB0AA4FB70C5FF9F7F9270
SHA-256:	2CD957715395E92D546079EC6FDE5F2B74D4B392EB2C685958FF6791FD424A65
SHA-512:	58A1B91F76FFEE7819B76D2D265D8B7F242342E2C7D5D5FC97BC0207A84C271BB1D8C7A297639D2A72DE3A13AE380F9ACBF04DC6C4BFCA65A50CB19272F7F4F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0x672135c1,0x01d74696</date><accdate>0x672135c1,0x01d74696</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>0x672135c1,0x01d74696</date><accdate>0x672135c1,0x01d74696</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin202591677780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	660
Entropy (8bit):	5.173233176410025
Encrypted:	false
SSDEEP:	12:TMHdNMNxx6TsTzNnWimI002EtM3MHdNMNxx6TsTzNnWimI00OY6Kq5EtMb:2d6NxZNSZHKd6NxZNSZ7Xb
MD5:	C19440F1AF524DFA7A5040D7B8D0399A
SHA1:	6AF9E500717A33929B9342D43A72A94C8565D9FA
SHA-256:	F5044774ED4D07D3C081718E224636B1EBCD48AD9706426F4042837D038A0F66

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
SHA-512:	E6E694D6902B933F2C32B344DDF28ADB5C36833BD268FB15EB01528BEAE0E422A9712941556AF3C02281EAEB42C2B289403F4E25EAFF25D2556EEB3D9A169A28
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0x672135c1,0x01d74696</date><accdate>0x672135c1,0x01d74696</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>0x672135c1,0x01d74696</date><accdate>0x672135c1,0x01d74696</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):	663
Entropy (8bit):	5.148871285698569
Encrypted:	false
SSDEEP:	12:TMHdNMNxc6TsTzNnWimI002EtM3MHdNMNxc6TsTzNnWimI00OYVEtMb:2d6NxqNSZHKd6NxqNSZ7Gb
MD5:	8DA7ABE77AC7E2E318C48AD6377AB250
SHA1:	4E6602B3CA86E0A8BE27FA5635F2729CFCFCA78D
SHA-256:	46CD221E9DCBBBC91FFDEF037E861DC1E18CBC7A792766EE83644D5A7529D3FC
SHA-512:	46ADA9D041912EE886AAE696AB9C324DF514E8EA1D24D2D37702CBEE0ADAA9EC88B9BA3BA32EED024E72795EF39D690A070C7215C78A52EB03AD56DB6E361E64
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0x672135c1,0x01d74696</date><accdate>0x672135c1,0x01d74696</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>0x672135c1,0x01d74696</date><accdate>0x672135c1,0x01d74696</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):	657
Entropy (8bit):	5.134940334463526
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn6TsTzNnWimI002EtM3MHdNMNxfn6TsTzNnWimI00OYe5EtMb:2d6NxbNSZHKd6NxbNSZ7Fjb
MD5:	2CE1D56EEC317EE366426E1830D0D040
SHA1:	71FC5E54919D0C3709808D4F706CAB904908F629
SHA-256:	9BE4E7A9B9E8F2C0479D6F05BBBA456ED6DEE41ADED933B4701BD028515D1202
SHA-512:	103489DFA30DA30487C2AA7588A11F104420C88EDB18C36F9AF61E5913721A941952DD0981B5728DAB6C6E8F160FB59C0DD9172A943067ADD5E4740AE7428F0D
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0x672135c1,0x01d74696</date><accdate>0x672135c1,0x01d74696</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>0x672135c1,0x01d74696</date><accdate>0x672135c1,0x01d74696</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\po60zt0\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	7372
Entropy (8bit):	7.8826218687505625
Encrypted:	false
SSDEEP:	96:T/fStNJlGUv9aiNwBMZSs4f44FmuT7e9hP0xspI6VQQozqUSiLn3QmMsPK1sBZBH:bfSy3NwU5TIm/ZppBpo2UesiW7xLoo6G
MD5:	1047130163DC8E9F3335F6C335910681
SHA1:	17A59E65C79D457AE2CB1D5C6F40797E0E5E4F99
SHA-256:	D960F61F044BF1E9EFCC4310A33D3A912DD11EEFA1C99D9C3FDA6652614CF63A
SHA-512:	B92594958EB80468F0C40795D0E8112DF7CD8559D63353439032B5565CDD1099CB2022A2175A3CB7ECEC38DCE8D8235A6274F85A4F12AE95234348EDA9166DC
Malicious:	false
Preview:	o.h.t.t.p.s.:././.c.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.=.c.6.8.7.6.4.e.b.7.2.d.f.2.f.d.2.8.4.9.8.0.d.4.7.9.4.d.3.1.c.9.1.9.4.1.b.1.8.3.c.....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\INetCache\IE\0MX4YUS9\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):	11769
Entropy (8bit):	7.940924515668722
Encrypted:	false
SSDEEP:	192:Z86qVucPa8YRH0Xcm8hImCWoYkKWypvqR4pL7ge6xdM7JlBWZtjzaoiwWQJ:ZZnNRHwckYM4pADduWtjOo/
MD5:	A8947168B5A76BE27C4ADCA5B19FC946
SHA1:	F2F6B9C3A971F80AD772C9718E4C7C19C632C47E
SHA-256:	B7A90CF060E0EF272E3FFC4C3C108735811995177B4A6499E071AFA2D050CF2B
SHA-512:	F7D49890056B61986C6E82313E922935FE614D697019CF4C04D7D0406D52EC38FE17224334552CB75C3E2B0B09B9E19C5D21E8569EF392DE880B5DD5972C4B33
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/m=eW0Q8f/media/videos/202003/10/29214321/original/13.jpg
Preview:	......JFIF.....C.....!......"$".$.....C.....0..".....80 .OE...Qi.....Y<....7.I..B.....g?s.{....2N.;....v.....+.k....5xS.kiJr.z.5|.....>mX*.g...f..>Rm..Q..m(..O.....m.).E.$W..X.y.T.<.p...\.$..0eV..i.8F.....VU.6En...l6...sz.....ec..|...2t.c.... . .#_.Y.o..%..2r.s$..=u.s.....YF.ea{k..9....A...M.....<..._5.T..G../...-.....w[.iK0e.IK~b...=:...g...~.. d{...6...d.coa8VY]...8....s.`...p.\|.6..i%.e....J.$..g.tS..s.A..C....8.....Z..l .T.d.... .tA9.au...].\c]5h.:...t.S>.....,..\9.^3.....[.7...q...<6.b...E.|tkJ...Co.J~...3.....Z.....4.t.RN..0..`...6...V.-^.f.,..9.1...+.!T.a...S~... B..C..K.....Sw.]sT.W.....T.4b...IL.j"..Y.....k.f. ..'G..qf+....I#._....ttv....V..}K.....'U..E...J..t`..[2..a.^..''W-.%%D.K.pI.fm...V.F..Zc(....j.+..&+.pJ..8..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\14[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):	10334
Entropy (8bit):	7.9296764071809775
Encrypted:	false
SSDEEP:	192:10613h3J6JOsKopSPSLqs8ZbZCkfE57hqebWYwofQI7ANT+dxwZM:e61R34AstOSGfOkfEjWYJoRNadxwG
MD5:	F69B1B8C9D89F299709BC3386757C686
SHA1:	60A231E8FC8610080BADB790D922EA3012CDE758
SHA-256:	6767A3DBF271E6FC42CA20C12752362585F04E0F8A04618B92F2F3C5A6CDAEB6
SHA-512:	15FCEB96959173D60739F5648CB8AD1F99413A63CAE09344EB552D6621F892200F82556FDB8FE7B7D16698BCCF2984B66D524216AE303AD223031070D3E3FEB2
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/m=eW0Q8f/media/videos/201907/09/18708901/original/14.jpg
Preview:	......JFIF.....C.....!......"$".$.....C.....0.."..... .@)..:.8./..^*.Hv.u...S.zu.x..P.....V.^....k4..u..:..U..S5....S.y.%.p+a>5.z!.L-..s.f....9~...7....=,,rE.k6..e>..>.:.....3."Z..d.....td.=.V;q.....".!5O.....:0.h.W.#q.YIB.=:f.b....r/N.:.... .7.:9..!ul.2.l..X..|7....>d*m:...,E..c...j.5.P...{...Z)....E.{kc....5.y's..#s..+y...|.m..#WQg.,V=.IY.d.P...L....v.Y..V..2..\EE.....!.7i.@ZR.=....7.Z.K.Ye..m...~..~.p.....A..uL.A%..;. rQ...TzviQT.V.K.s.....J...)P.}pi.,.<.ds.p.0....I.{.D%...Nz[^...\.k....r6.N...0.Z.6.p..e^sf.,i.R.,.....n6.....h...|...hTf..z.B..>.....UE(..f.].LG.JA..''.....\,...l..*.z~.>.C.....~.G.R.. ..g.9....].r.z(...m.U.....I,..o...8..54..:.>.....'.....c..g.w.ok.p6....G_.U..tW.`ZM.bZ.u..z.Z.1S..WVmB.n..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\22DFL4CR.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):	442430
Entropy (8bit):	4.934263869753209
Encrypted:	false
SSDEEP:	6144:kFEBDSK/cnXOwkW7W5Mboiy71WbP7m2HkWTAj5Qc/a+Syi9ubULfZ4W0m3bMVMna:kFWWdstk+
MD5:	47F6727A6D1BB268E33D449B34C24089
SHA1:	C2D614A6124CC2D97AD807CE08EB43F3030A5BBB
SHA-256:	F89680E53AE75FB40B3D42B7BF0239941B61067753263B5D29B2C33470AF5D4F
SHA-512:	91BFE1E5CCE911187EAB0858E33A553D68ADA4A6F23AAA3800DD50B38790125D9943604FB96379EB50F22CD0C8BD60906F747F1AA850AFB53FE1826AFE5B77E 9
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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\2d-0e97d4-185735b[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	249857
Entropy (8bit):	5.295039902555087

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\2d-0e97d4-185735b[1].css	
Encrypted:	false
SSDEEP:	3072:jaPMUzTAHEkm8OUdvUvOZkru/rpjp4tQH:ja0UzTAHLOUdv1Zkru/rpjp4tQH
MD5:	B16073A9EC93B3B478EC2D5305BAB0E8
SHA1:	446E73EF46D83EE7BE6AFC3F7707D409DFE3FFF3
SHA-256:	6561EBD5D1938217C45AD793DA4DCF4772B5B6E339C2B4A1086AB273EBB0865A
SHA-512:	19B2F38AF4AD3DB28F1823D94928DEABEF5FC5D1B61EF7E4DAE5E242ADB7403C0BE7F30BFAF07A259DB31C35ED9A9A043928FB3655F47D9C063B38E5C3FD9CEF
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\0MX4YUS9\52-478955-68ddb2ab[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):	394417
Entropy (8bit):	5.3247938581106515
Encrypted:	false
SSDEEP:	6144:08w9z/hSg/jgyYdw4467hmnid1WPqIjHSja4CWJSgxO0Dvq4FcG6IuNK:mJ/Scnid1WPqIjHdQrtHcGBt
MD5:	52E2B5A497C99DF1EE81C53C7281504D
SHA1:	74558D022C0E67E5D1873CF678EE1B072B064CEF
SHA-256:	AC5C2D695CC38D282BA01BC6BF7AE5382F7288DF1F20109AA6CC4B9884F8A1B9
SHA-512:	02CF68C169D44EA3AB623E44264329AD1A2C6724F31C881857C54882375F994C3E1287EB06FEAC94D580D2458318D716CA7FFBDE6E7FBF19B76C70F1A56816F1
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\0MX4YUS9\55a804ab-e5c6-4b97-9319-86263d365d28[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2939
Entropy (8bit):	4.794189660497687
Encrypted:	false
SSDEEP:	48:Y9vlgmDHF6Bjb40UMRBrvdiZv5Gh8aZa6AyYAcHHPk5JKIcFerZjSaSZjfumjVT4:OymDwb40zrvdip5GHZa6AymshjUjVjx4
MD5:	B2B036D0AFB84E48CDB782A34C34B9D5
SHA1:	DFC7C8BA62D71767F2A60AED568D915D1C9F82D6
SHA-256:	DC51F0A9F93038659B0DB1B69B69FCFB00FB5911805F8B1E40591F9867FD566F
SHA-512:	C2AAAF7BC1DF73018D92ABD994AF3C0041DCCE883C10F4F4E17685CD349B3AF320BBA29718F98CFF6CC24BE4BDD5360E1D3327AFFBF0C87622AE7CBAB677CF22
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/9c38ab9f/webcore/externalscripts/oneTrustV2/consent/55a804ab-e5c6-4b97-9319-86263d365d28/55a804ab-e5c6-4b97-9319-86263d365d28.json
Preview:	{"CookieSPAEnabled":false,"MultiVariantTestingEnabled":false,"UseV2":true,"MobileSDK":false,"SkipGeolocation":false,"ScriptType":"LOCAL","Version":"6.4.0","OptanonDataJSON":"55a804ab-e5c6-4b97-9319-86263d365d28","GeolocationUrl":"https://geolocation.onetrust.com/cookieconsentpub/v1/geo/location","RuleSet":[{"Id":"6f0cca92-2dda-4588-a757-0e009f333603","Name":"Global","Countries":["pr","ps","pw","py","qa","ad","ae","af","ag","ai","al","am","ao","aq","ar","as","au","aw","az","ba","bb","rs","bd","ru","bf","rw","bh","bi","bj","bl","bm","bn","bo","sa","bq","sb","sc","br","bs","sd","bt","sg","bv","sh","bw","by","sj","bz","sl","sn","so","ca","sr","ss","cc","st","cd","sv","cf","cg","sx","ch","sy","ci","sz","ck","cl","cm","cn","co","tc","cr","td","cu","tf","tg","cv","th","cw","cx","tj","tk","tl","tm","tn","to","tr","tt","tv","tw","dj","tz","dm","do","ua","ug","dz","um","us","ec","eg","eh","uy","uz","va","er","vc","et","ve","vg","vi","vn","vu","fj","fk","fm","fo","wf","ga","ws","gd","ge","gg","gh

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\AA6wTdK[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):	543
Entropy (8bit):	7.422513046358932
Encrypted:	false
SSDEEP:	12:6v/78/kFBVoROFJeVmDZFr3iR4f85jaSirm4VFF9LW+etOdx1Y0:+Vom4cfU4mGmab9L7dg0
MD5:	91EE9ECB5C9196CBD18EE4E9C41F94B5

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\AA6wTdK[1].png	
SHA1:	F829201477F63B908789BB895823E5A4D16ABBD7
SHA-256:	2BA5AC02E5C6AE8D5BBD3D8C0CD5603A02A67E192394813514D151AE1D6988B6
SHA-512:	A30B7F28E690DE2B8AB0E413861E4B6ED0BD7CEB0695A93526620E44F20011905FD72A6F489C62EE1753235F063188156D50BBE44F5588250EA9395942505134
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AA6wTdK.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.S=,CQ.....E..... ..F..`0.....?.``..&D"."......Q.!.OK...S.D.../.....|.....Y.T!.aA.R..P.HJ ....O..sM....rE%.|><o...C.{L0.....i(.m..>....`\.qt.....>..J.G. *.W..l..~=.cN.{.K[.@..W...zeM...@y`..T....O7.....u...F0U. v{..2....!..T.B.=.<v@....W..ax.+P.81...<....]{....f...E..5... ...6v.;8...2.h..%7...)...|;2....t..,....!.fY.:>.....:.R..(B.s...M&.F.R..Z$.....B.e.w.....N.....AM....O.d.?....>.g...Z&.@....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB15AQNm[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 192x192, segment length 16, baseline, precision 8, 622x368, frames 3
Category:	downloaded
Size (bytes):	23518
Entropy (8bit):	7.93794948271159
Encrypted:	false
SSDEEP:	384:7XNEQW4OGoP8X397crjXt1/v2032/EcJ+eGovCO2+m5fC/lWL2ZSwdeL5HER4ycP:7uf4ik390Xt1vP2/RVCqm5foMyDdeiRU
MD5:	C701BB9A16E05B549DA89DF384ED874D
SHA1:	61F7574575B318BDBE0BADB5942387A65CAB213C
SHA-256:	445339480FB2AE6C73FF3A11F9F9F3902588BFB8093D5CC8EF60AF8EF9C43B35
SHA-512:	AD226B2FE4FF44BBBA00DFA6A7C572BD2433C3821161F03A811847B822BA4FC9F311AD1A16C5304ABE868B0FA1F548B8AEF988D87345AEB579B9F31A74D5BF3C
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB15AQNm.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg&x=868&y=379
Preview:	......JFIF.....C..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO...C.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijs tuvwxyz.....?...(...CKHh.....i.@.....i..lR2...MpR..^E....&EYv..N.j...e..j..U,..*..BZ...qQM.dT....@..8..s..i..}....n..D...i..... VC.HK"..T.iX.f.v&.}.v..7..jV.....jF.c..NhS.L.b>x".D...,..G.Z..!.i..VO..._4.@X.].p..].5b+...Uk...((@.s'..?Hv.....\z.z.JGih..}*S.....T..WBZ...'.T?6..j.H"....*..%p3.YnEc.W.f.^. .....Q.....#..k..Z.....I:..MC..H.S..#..Y ..A.Zr...T..H..P..[..b.C.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB170q7z[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):	428
Entropy (8bit):	7.343532010599778
Encrypted:	false
SSDEEP:	12:6v/7AU9LXfExBOtdb/qYwgkOok6r5bfjGEQz/X6/CGRNqfu0fnN4:DU9LvBdLHwg4pbGJ/X8q20vq
MD5:	BD7AB09D738CCFDE1542F5E564EA71C2
SHA1:	6E1EC3A0DB0A02C40C5D74342502C6EF24A5F4F8
SHA-256:	C1008C0363E859A70508CEBFBBD6735A5C26E47DFD8FBAC25DFB6538AA74A10A
SHA-512:	CEA71979D29896FB646B25202B00C2F27BD9CBB05689FB2EC1BEEBF6651F76AB4F993E6D1F1F361F544CF0E0886F2826CB885B22CF0AAF64B27F9886D120D4D
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB170q7z.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....^IDATx....KBa..#..B-. ...8EK(.$.6..^.....-E.."...4i..N..".../.~.....s.9.\...g..-2..2..t..S...d.....C.ba...."..d.....'....[..&u..#.[..WB.V_ .....QO....-.....af...,Iw..b.m.....X..#.....=E.!....}q:..8.....[.....A=.e.....z...]{...f.=....!..}5....d.A.....u.t.....W!Nef..v~.VCk.g.Z...r".B...+{....?....G.....P.....^w.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB1gABgY[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	13604
Entropy (8bit):	7.86809066900137
Encrypted:	false
SSDEEP:	384:N6ElcXwszIX0MCWWdxi2SvXMKao36thFQ3Emet4C:N62cXwsQd8xi2qaa6thFb
MD5:	35E8E7F2D69C997BCB0CE293FD8DCC06
SHA1:	4707671C86A3217A40FD41111973D6C52FF796EC
SHA-256:	B8392322E2B2848EAE5FFB0D452AAD29E543C7C9581174A2C54B2C70E24D7564
SHA-512:	3E66780973CE6E4EA9F07B29656620AF8B7E8215F5A6A957C28EB01A638E3AF52F0F030C456888F4F1C1E3EB00C071841B75D5849A7F7ADFA03F25CCED4249B2
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1gABgY.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB1gABgY[1].jpg</th></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......M.7...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?.....f......3@.h......4.f......f.._+A.l.So.qS-.h+.G...W).!q. .q@..c$Q. #q....?....6..U6..`.<\B.Fjf..3@.h......4.f...3@.....4.f......(......4...b
...n..u.....@...3@.h...G-.p.ep....in4..uX...#~B..".35..Q....(....0>..+.j..|.....O.h......=8T..L..R4..........B...".~..g.l......cci.t..C.3@.h......u....4.f...........3@...3@.h.........7P....u.....@...
7P...*j..YC...L...n.A;.!.G,...;w..I%.n...</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB1gANz4[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 100x75, frames 3</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>3218</td></tr>
<tr><td>Entropy (8bit):</td><td>7.872378359673003</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>96:Qf7ENIlZlkP1eJGjRuK33teMyPt9SQg3uQKKj3:QjUIlkPU8jRuK33UMyvg+XKj3</td></tr>
<tr><td>MD5:</td><td>06C195A6435970CEB135AEC822409253</td></tr>
<tr><td>SHA1:</td><td>21B49001B9E799E5013C11EC33B57E9168AB7468</td></tr>
<tr><td>SHA-256:</td><td>D3A39616315D30D47666CEA5E7358D86EC52A44D983FB334E5CB3BC17E6F5ED1</td></tr>
<tr><td>SHA-512:</td><td>AB06AFCDE8E64F99F7505CF85072FB5C1710AD87CC078680F09D63A54398AC1A8369966F9C10386E006F0ABCC1C99917476237EA4CC8EB535E2D4574C76C6BD</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1gANz4.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f&f=jpg</td></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......K.d...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?..U...vXb.;...lRD..f.|L..@....hrf.(..z....[81J..p...I..FT.o.V.t......,@9.[1..i.p...Ca..;..=..J..6...t......9...g9....t.,..{o,.l...d.}.j........\
..C8f.H.$..{ksn...!$..Lt.?.zJH9].P8..8..W...g..e...sK.../%..5d.Z.......I-NU.92..N...5..MX....8..v*.....8'.B..l.=>....r.....u*...#.L..GB...r..T...|.N.KYK..r.=N..tCr.k......4v..a...c.^)K..}?.]
.$...ksn.w)(.....6y..zR....d..</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB1gAV1d[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>7305</td></tr>
<tr><td>Entropy (8bit):</td><td>7.870294318591518</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>96:QfQEe8wStlEqZaNiZ64r7UHrWfHzPoEbJWxTPhdBYR6LM1kCto0rMYEpo3crxKx:QoMl9l8Lohb8xrhdBS6LWVtX6D2</td></tr>
<tr><td>MD5:</td><td>26C97B5C8F5851746E73C69D0EC46BAB</td></tr>
<tr><td>SHA1:</td><td>530302314F9020A221EE286A57B7E34E37E9AAFD</td></tr>
<tr><td>SHA-256:</td><td>4B255E98778FCE1D905CE88CA3EFBD227F5AA452F6C74647DE37E76AA733425B</td></tr>
<tr><td>SHA-512:</td><td>D027AB078EFA10D96EE4E16684525B7FF4F36B169CA63E493BF0854D219070E0D43C4E136C774093DF0D72235A45F2A6290767D2A51AB6E18B5AD452587FF2D6</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1gAV1d.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg</td></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?..B......P#..._g..%9.wT...\....)..tt..uU.C4...~.<,...&6.$.=GA..V...I.fG7...pZ......'..........+..J.+..U..B1...v....k.>.GV5...g..J...*.
9..~..]u..v<....j.,(.P.P ......`..P.@....P0.A@.@.B......_E.i....!R....).p8.._K{..N..v.....R...H..KbSct.8...[.R...G.|)..y......R.....-.=.v.[..`HAV..=.......^.[A.u1...q.j..........`..U..RO.W.z
."......@....g..dIR0....@........1@....P.@...............8</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB1gAY0y[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>9460</td></tr>
<tr><td>Entropy (8bit):</td><td>7.935651364743537</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>192:QouFZndjJEfreBXbmS9NJwKWstKK/Z6e4Zfuoer5+WMEjT0s1:buFZn1JwqBSS9NiRNfTe+D2T0c</td></tr>
<tr><td>MD5:</td><td>2BD3498797D3DD6D4C1030B242C1F184</td></tr>
<tr><td>SHA1:</td><td>AD5CED3AE31C5FB58167F7707A69D94857F2AAEF</td></tr>
<tr><td>SHA-256:</td><td>9EDA6ACA212CE74B551D166066BD3B8D59CABDE390551E6C31B645ECFEED21E3</td></tr>
<tr><td>SHA-512:</td><td>833833C5DBC50DF0FAA1E7831E5C9C24C91F47DA8CFA4A385A7BB739C8E0FD9AC424AB7B7DDD8D1D38840E7CE1E2C6CF28DD758143BF3082A30FFB32B0B65
DC</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1gAY0y.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=292&y=133</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB1gAY0y[1].jpg	
Preview:	......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?.....p82.'.)r..$_Zj.W../.>F..e_Z9..L.;..ap....|..O....W.F..2....U...]@.7_.]0VB.\\37...U..>..L.4.!..b.....iJ..?p.P#..ki.IZG.0...+.....t .W*.LNU..=k..hw#2...F..._Z\.p..F....V....G#...}h.....Z\.q...K..(.}h....;.....G..=ir ...Zj..?.|u...M....Ar6..Z\.w.\?.5.+...."..3?.>D.....$.?...qHkP.........9-.+95.\#......w... r..k..H..q*]....t....u... K....v...04..hud..0....3=.-..'R.J.T.g:}.z;...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB1gB50w[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	19162
Entropy (8bit):	7.945549041258211
Encrypted:	false
SSDEEP:	384:Nqzu8Nm8er+1R1V45r0Ef+O5uZEvG7eezfXLeO7/+IjKVjbRoDuCj3V3V:NgNMkR1ef+O5memXv+rRRo1bpV
MD5:	C5FBE46385D37A9E8F1F50863E9D1644
SHA1:	9106034A2B8B84A26967FD1D93E87A1D20A63DC9
SHA-256:	558C26674794A1D39AA27E9832CA8C9850829E08ABDF37ADA8DD765F0EBF9395
SHA-512:	BFCAA6FEA9A1AF95A62951EF6D54802F6AB61110AB038FE7591BBAAE6A5CE8827E83C4C1E475581D73C91F8895845137AC7A0C4F976F41DC9D973220611A49F
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1gB50w.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO......M.7...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?......@...\....4.f........f......(.h.....4\,...a(....E.G.+...tB7 ..k.u........].w9g.P........Ke$&jYHCJ....Y.D...4.C@.4..@.4..y..W. .4.......4... ....3@.h.3@.h.s@...\.....Hc..g)..0...3.j&S.bD|...I..Dc...D.q&..*.C..3....\t.uIhZ....M...if..9.$Y(. z..Hv.....S.>P.(.....dI..J..SL...i....a4...C*.1wP!wP....@....u.....@....u....s@....h.s@. O..4.N.S..s.....e..k.-...D.4........E.....V

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB1gBb9f[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	6459
Entropy (8bit):	7.854682213199596
Encrypted:	false
SSDEEP:	192:QoKS7oQBj5HrQkHl/MpDOHt0ojZWB4R7IQJahIdEPJ/:bKS71Bj5HjHl/KDCt0zW+wEx
MD5:	3228E4B35A5727B172510F6F06F8F4A6
SHA1:	EF90CA8036997A5CF7D1FB7249F8963664D618B5
SHA-256:	06BE1F33A728FF16EFB6D870B3A05B1F7AF6737F25AC553EE23264CBF22A9AC2
SHA-512:	9BC66F9B4E47E966C0B9D63AD4BE604A8D01E24AA8E2E16AC2C3042A90D716DA6D33D5BE7D8281E68DE2EDEE5A8C9AEEF65D7CD499B207423A72D0DDCFE7 D6ED
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1gBb9f.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=471&y=314
Preview:	......JFIF.....`.`...................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO OOOOOOOOOOOOOO...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........ ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz......... ....?..k.p...h..h.h.X.q.....X.."....c\\|..%..U........@.(...`8u.E..L...C.P.m.bm...S...J@..)...P..V&..1A...@....n.aM..f...K5Pg.d.b........"O. .X.MN...r.4\vfY.]..V;y..I...h\|...\|L$?..eOPs.9..6n.]Ct..p.;...a..LDy.1..LA@.@....P.@.-Y..!.@.@.).,g.......4...........5.PF.H.Uz.8..Z...sw.l.d..._....r..H...9...i ....$@.3..b..#...Z0xY.....y.H. (#i.z.C.X.3[..zu.zjM.QL...F=B .F..V........%........

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB1gBiTM[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	23096
Entropy (8bit):	7.942141574344352
Encrypted:	false
SSDEEP:	384:NPY/BVjckFnQ+9Fx7SKYBsWGhmCaL8lTZxOOaRWfOK3MuL6dExiJWNNTa1xoMZZJ:NPYLjpQ8dYyzhoLaT7OOaqCuUExikN9+
MD5:	E26816C584842AA9EDE68F5FED41F9B7
SHA1:	9B6CE100D84C1E954D2EAFDF21916AA32D8CF3BD
SHA-256:	A2A6274BCE985AB12B2E1FAE1FB0AD742D01214FE2A3F69EA315369ABEEAF59F
SHA-512:	4656A8A81ACD6F491486AE6B19D38359B389957BE8B1243FF9BBD7A83F88739638D28F8CEC2BC9970FC6D04A88BB58ECA99099C14187A47C2901BF9CA1FC2C2
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1gBiTM.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB1gBiTM[1].jpg</th></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......M.7...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?.w.$.W../....]&!.......?...|..Qq......?...|..Qp...+.....o.C....~[.~...@.[.V.[..C..0F(.R...n...........I..r1{m.o.B.L.....8.@<..B....1L.P... +..D?
.7.4..HO...1X(.....L.~..s..B...W...t.*.....v...62B\D...g....sZHr\..94.Ps._.1..*y,W8..QH%.......7....$p $U(...]..~M.$.....+._.v0......(b=h..X.,H...|Qi.#..z.?..X.#.............J......|7.P!..4........
(.....x._......|..Z...........5"_ .S.b.</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB1gBjEO[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>23539</td></tr>
<tr><td>Entropy (8bit):</td><td>7.9664067827580585</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>384:NwgXjyJEXCFn1+gu3u4c4SPeykKjfZKZCqM7SMuRXI5e1hU3LDhhcnDA4:NwqyqXCF1+zMe8yM7NA4gDU3LDoP</td></tr>
<tr><td>MD5:</td><td>970F476CC5E82496769F715CA79C5BF4</td></tr>
<tr><td>SHA1:</td><td>0D2F11D5A64442DDA2254404744584871DB0A20F</td></tr>
<tr><td>SHA-256:</td><td>EC7574AD747391E27978CCD177D131A7F3BE14C57A95309C4120DA7683F64453</td></tr>
<tr><td>SHA-512:</td><td>31E9A437DC1EE101D8B8D39AC537B37C2C320FB688B42046958F2A856061CD1B31D0E2083922F461444C3672A9C2025DDA07B0CE79E04A8053B3E99FEDDC2D
A</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1gBjEO.img?h=333&w=311&m=6&q=60&u=t&o=t&l=f&f=jpg&x=1500&y=677</td></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......M.7...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?.......S.".?x..J@=I...2c..x.J.Vf...P.'i.E.#`..J`0..r..8a..z...U.........#<}(....h.@x\.`D.rh.Q...47`5.."[..."S..9$\cr..x..mo.(Wfq....'c
.l$.Y."...X..=kk$BM.!X..C._.[=(.v.{...#.1.+.......iN.\..........7.L..d..... ...Z.-.m...Z.;..eQ...(..y..4..P.0".t..A........X|....L.4...<.[..d.M..L.<.q.....o.....,..:VM...5...A....B....^.%~ul.8...RK..4
.rk........ .....j.5........i.I!..~ws.}(cF</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB1gqLTH[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>31022</td></tr>
<tr><td>Entropy (8bit):</td><td>7.848014730846984</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>768:IlQ2jsa7fWcqHXadq9bIb0A+zqt5yeDqLhWGc:IlVjvm32+bW+u7b0/c</td></tr>
<tr><td>MD5:</td><td>231F085871C9F1A5C5F78E7DFF9E46B3</td></tr>
<tr><td>SHA1:</td><td>D74981CA122ECB9C79C74E854DC5E585201DCE4E</td></tr>
<tr><td>SHA-256:</td><td>2B280F39377EF2577EC93772E5AFCDF9AD67480F885D89B7E437E6A8CB580B05</td></tr>
<tr><td>SHA-512:</td><td>ADDA409DCE6659E32DC20B37562602C9501FA6D4777F29E1312E4798A6198260C79DA5906BEF8BA0A3D7DD9341E4741A34071DB76937719FADF89878A0B190A</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1gqLTH.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg</td></tr>
<tr><td>Preview:</td><td>......JFIF.....`.`..................... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.......&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO
OOOOOOOOOOOOOO......p.n...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz........
....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........
....?..#.u.b.:P.w.@.Q.@........`..J...&;...J.n._z.1L..84....h.GLf....@.u.)......z..O...h.8.. .ph...).f..4.2...).....OZ.>.S....#.4......@..x<br>..W..;.8..1..0.c..4.H.>..L.(..i.nG.@.j..`.qLA.H..E.7....`..!<......:..BN@....<...C.sL.>.L..:R....F4..c&..#.......J.bD6&.1.'..!.q@...A.....h......=(..G8..........!..v^....<_V.f...tS.NS.Z...@<br>.@.@....v.^.......J.P.H..j.Bz.4........).... ..`9H.3@... .</td></tr>
</table>

<table>
<tr><th colspan="2">C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB1gySTO[1].jpg</th></tr>
<tr><td>Process:</td><td>C:\Program Files (x86)\Internet Explorer\iexplore.exe</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 622x368, frames 3</td></tr>
<tr><td>Category:</td><td>downloaded</td></tr>
<tr><td>Size (bytes):</td><td>39915</td></tr>
<tr><td>Entropy (8bit):</td><td>7.947025708066676</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>768:IAoGnvPp3E4h4cq+9G/ckbWhzU0DFQjauAsp4mr1Bgl91v5:IAjnvPOHcq+GckblIQja+r1B091x</td></tr>
<tr><td>MD5:</td><td>746D72022FB5E32D9F8A5EF327DAF8B7</td></tr>
<tr><td>SHA1:</td><td>BF649090A1378A991BE799CC86CCEF279448E9B3</td></tr>
<tr><td>SHA-256:</td><td>3F850D3776EBC9FF43DE4EDE3671366953521271EF3666BD4914B8232B0E084E</td></tr>
<tr><td>SHA-512:</td><td>FBACA7B753209BF7C2573A7FBAC130B69B70A7B72D7E6532AA61F5A6AFDEBE8A67553B987EFA5F0BBCB482C6BB5C93FAB24C2B6B68154AF1FB467DA07A206
F13</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>IE Cache URL:</td><td>http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1gySTO.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB1gySTO[1].jpg	
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....t....r;.`....4..(.j....~S.P..W.#_1w!....U....'...-.....3.2.o..c..X7F..e*..5.7k2...qL..r;m..nM.(.ZMj.p...G9....M.,.....;..i..A....B. .....c....9....L..4..'.1E..^.jE.0p.q.O..}I..18o.."..%.R..S.W:.%..`.@.Si.Q.-O.;a!9#..J....v+.{#...\U8$.Sm.]...$.....'..d....q...*G.h..y....1.0s.?..N!..p.....a.@.....\.i.Ei.....*.+.sUa\.X. .. oJ...H.=..*9Gq..m..V..[.x$Q`.Ir..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\BB1gzyNY[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):	2767
Entropy (8bit):	7.835483910527824
Encrypted:	false
SSDEEP:	48:QfAuETAZhSimqBk+CoaBf7zxlQ0aZ4QMFrsgQloT5xQ:Qf7Eai3DlBf7HQgGac
MD5:	0A320B72A45E644B83A7B3D00C3443F3
SHA1:	08BA4AC4D37572B86F3B1CE4760543A4A9AA4FB3
SHA-256:	9D4CE7085429EEC1A2348291D27ACA7A588940D7E4BC654963D3EF6078DC731A
SHA-512:	E462E604BB8121EDF6CB9655894D0230A1F8257054770795DE1AC9EA8FFE12E074BB9B98A67D546C382C4D1D1D72085F971BB84A5358DBE2581D55ED230906B
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1gzyNY.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f&f=jpg&x=408&y=357
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....Z.(.9...I.*(.'..&.s7.:. .m.g....~5\..d.g.4.....A)....:9{......).dR.r.k9MCr.F..3m.3.q.Y,D..71...8...B.B.`[.....#R2.....U.Z.(.....w}z.m .Yd..I.....SN.....?....."...Q..}...j...@W*2.nj..p-.{T....A...+..=.+.:nB.....<..m..Tz.U.... f.H.N.....j..s.eh.....=i.X=.i5..n.Q.@...S.Z.5....5~..F...+...I....('.'..f....yc.'..o.k.;...q....[.0.[..G. .59.J..t1Z,..)..s...XU..u.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\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.....$1I.%.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\0MX4YUS9\BBkwUr[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	431
Entropy (8bit):	7.092776502566883
Encrypted:	false
SSDEEP:	12:6v/78/kFkUgT6V0UnwQYst4azG487XqYsT:YgTA0UnwMM487XqZT
MD5:	D59ADB8423B8A56097C2AE6CBEDBEC57
SHA1:	CAFB3A8ABA2423C99C218C298C28774857BEBB46
SHA-256:	4CC08B49D22AF4993F4B43FD05DE6E1E98451A83B3C09198F58D1BAFD0B1BFC3
SHA-512:	34001CBE0731E45FB000E31E45C7D7FEE039548B3EA91EBE05156A4040FA45BC75062A0077BF15E0D5255C37FE30F5AE3D7F64FDD10386FFBB8FDB35ED8145FC
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBkwUr.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J....DIDAT8O..M.EA...sad&V l.o.b.X.....O,.+..D....8_u.N.y.$.....5.E..D.....@...A.2.....!..7.X.w..H... /..W2....."....c.Q.....x+f..w.H.`...1...J.....~'.{z)fj...`I.W.M..(.!..&E..b...8.1w.U...K.O,.....1...D.C..J....a..2P.9.j.@.....4l....Kg6.....#.....g....n.>.p.....Q.....h1.g .qA\..A..L .|ED. ..>h....#....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\a5ea21[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\a5ea21[1].ico	
File Type:	PNG image data, 32 x 32, 8-bit/color RGB, non-interlaced
Category:	downloaded
Size (bytes):	758
Entropy (8bit):	7.432323547387593
Encrypted:	false
SSDEEP:	12:6v/792/6TCfasyRmQ/iyzH48qyNkWCj7ev50C5qABOTo+CGB++yg43qX4b9uTmMI:F/6easyD/iCHLSWWqyCoTTdTc+yhaX4v
MD5:	84CC977D0EB148166481B01D8418E375
SHA1:	00E2461BCD67D7BA511DB230415000AEFBD30D2D
SHA-256:	BBF8DA37D92138CC08FFEEC8E3379C334988D5AE99F4415579999BFBBB57A66C
SHA-512:	F47A507077F9173FB07EC200C2677BA5F783D645BE100F12EFE71F701A74272A98E853C4FAB63740D685853935D545730992D0004C9D2FE8E1965445CAB509C3
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/hp-neu/sc/2b/a5ea21.ico
Preview:	.PNG.....IHDR... ... .pHYs.....vpAg... ... .eIDATH...o.@../..MT..KY..P!9^....:UjS..T."P.(R.PZ.KQZ.S. ....,v2.^.....9/t....K..;_ }'.....~..qK..i.;.B..2.`.C...B.....<...CB.....).....;..Bx..2.}.. ._>w!..%B..{.d...LCgz..j/.7D.*.M.*.....'.HK..j%.!DOf7.....C.]._Z.f+..1.I+.;.Mf....L:Vhg..[.. ..O:..1.a....F..S.D...8<n.V.7M.....cY@.....4.D..kn%.e.A.@ lA.,>\.Q|.N.P.....<.!....ip...y..U....J...9...R..mgp}vvn.f4$..X.E.1.T...?.....'.wz..U...../[...z..(DB.B(....-.....B.=m.3.....X...p...Y.....w..<.....8...3.;.0....(..I...A..6f.g.xF..7h.Gmq |....gz_Z...x..0F'.....x..=Y}.,jT..R.....72w/...Bh..5..C...2.06`.....8@A..."zTXtSoftware..x.sL.OJU..MLO.JML.../.....M....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\ad7e2b59-d67f-4c69-8b14-45547302a263[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	[TIFF image data, little-endian, direntries=0], baseline, precision 8, 950x250, frames 3
Category:	downloaded
Size (bytes):	123908
Entropy (8bit):	7.976407168770927
Encrypted:	false
SSDEEP:	3072:R7w9/zYqkCq+Ox6MA9xdySKpe2Hbv6RG0FQqKwRNGCqqN7:dw9UqdOmRuHD6hFyen9
MD5:	49B3853117559FE0D410F565948881E8
SHA1:	3A499086DD35078778C6584E2FFFD789B4949B43
SHA-256:	120E6494A7CCDE78476AC75AB5794131DE95103ADD000A5FAAC267FFE3704D5B
SHA-512:	35A2252D52E9E911E548BC9C8A27AFEE74B82AC0F951CA4FC60C5BE09A087F2A9F9D51B40B838277626CC144AA5C7F7CABA92710554F837B9179EEA18973758
Malicious:	false
IE Cache URL:	http://https://bmedia.justservingfiles.net/ad7e2b59-d67f-4c69-8b14-45547302a263.jpg
Preview:	.....Exif..II*.....Ducky.....d.....http://ns.adobe.com/xap/1.0/.<?xpacket begin="." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c132 79.159284, 2016/04/19-13:13:40 "> <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:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:b981f470-1576-7c4e-9d22-fad2e84e73c3" xmpMM:DocumentID="xmp.did:289FF8D65B3311EB8CC986F9BDFD8418" xmpMM:InstanceID="xmp.iid:289FF8D55B3311EB8CC986F9BDFD8418" xmp:CreatorTool="Adobe Photoshop CC 2015.5 (Windows)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:1bae8a93-001a-4341-b4df-80d45fd30cbb" stRef:documentID="adobe:docid:photoshop:15b5afc7-5b33-11eb-8371-fa814c4cf6c7"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>....Adobe.d.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\analytics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	49153
Entropy (8bit):	5.520906949461031
Encrypted:	false
SSDEEP:	768:/yR3fYFBLbfs5sP5XqY3TyPnHpl1WY3SoavFVv6PU+CgYUD0lgEw0stZM:/y9gZfl5h3UHpaY3SoRCw0sk
MD5:	6DF1787C4BE82D1BB24F8BFFA10C7738
SHA1:	3634E839429E462E49C5F42B75FBFB4BA318AF6D
SHA-256:	2CB09C7B3E19BFC41743CA3624EF81C3258D56525647FEAC76AA757E0292627A
SHA-512:	CB3CE2BCEB61F390298C21E470423CCEB6DD93E648A7DD0467195B11FEF30BF7A086DFF47C4494E2533498D1448C1A22AAB1414C14FD73278F1C92E0F7BC3F54
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 n=this||self,p=function(a,b){a=a.split(".");var c=n;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={},r=function(){q.TAGGING=q.TAGGING||[];q.TAGGING[1]=!0};var t=function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},v=function(a){for(var b in a)if(a.hasOwnProperty(b))return!0;return!1};var x=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?:[/?#]|$))/i;var y=window,z=document,A=function(a,b){z.addEventListener?z.addEventListener(a,b,!1):z.attachEvent&&z.attachEvent("on"+a,b)};var B=/:[0-9]+$/,C=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," ")}},F=function(a,b){b&&(b=String(b).toLowerCase());if("p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\auction[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	25403

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\auction[1].htm	
Entropy (8bit):	5.699690173038996
Encrypted:	false
SSDEEP:	384:z9h7oUiYDwPApMHZELeToV53Zbc5iHpREY+jbWJPpfBkLaA3R6PmoLbA4EYP5+W:zzousze1kkIpjqlk2dPWiV
MD5:	BAF6E28C51FCDB267840BE9FE1270A60
SHA1:	448CC2B0B51EC7660A8630860ADD78D322AB2C72
SHA-256:	7F695B3780FA6F560F142685AB7B122C530967946DA5548DCA03C615F67A334F
SHA-512:	7A8C98832A7A6D27395FAD7980864F3070F95768763EA85BB3502DE3BB13FDA675FAA731DDEEA349C1A2850DD8E89070C808331745881652EF72F20E91F0241F
Malicious:	false
IE Cache URL:	http://https://srtb.msn.com/auction?a=de-ch&b=39a87478674e4640b1efffea733128ec&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=&_=1620758898931
Preview:	..<script id="sam-metadata" type="text/html" data-json="{"optout":{"msaOptOut":false,"browserOptOut":false},"taboola":{"sessionId":"v2_71ae373ced9c5b0579f92d8b370d4082_ed4414b3-a4c9-4b7e-8bec-9d6a3bf48921-tuct793d868_1620726504_1620726504_CIi3jgYQr4c_GPWKu67GstHVASABKAEwKziy0A1A0IgQSN7Y2QNQ_____AVgAYABoopyqvanCqcmOAQ"},"tbsessionid":"v2_71ae373ced9c5b0579f92d8b370d4082_ed4414b3-a4c9-4b7e-8bec-9d6a3bf48921-tuct793d868_1620726504_1620726504_CIi3jgYQr4c_GPWKu67GstHVASABKAEwKziy0A1A0IgQSN7Y2QNQ_____AVgAYABoopyqvanCqcmOAQ","pageViewId":"39a87478674e4640b1efffea733128ec","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\0MX4YUS9\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):	424038
Entropy (8bit):	5.433066424896135
Encrypted:	false
SSDEEP:	3072:Lf0JUKxx+lPkf8h3yTfj6wgrWMO+4spQp04saWhogLt2loNF2sZkWf10a6OAIb7q:Lf07OluMAp04gLLNRHzCMe7j
MD5:	EBB3EB0FBCBFA9373D13012928952A8D
SHA1:	8194F0185B7C8E297DF6F7359307D9C4AE440723
SHA-256:	2B90606F846BD4FCE75DEB252CC2B33931525C160F19540BAEF791CBE9396E0D
SHA-512:	ECA62FCDF48B13238F384D75403A0945D6A57A2866BDE8BB86BC5F5D7B7A9B5307A55D216A7432A4CEFAE013F4ECB314B74C9E06C10EE47535C5EF1F1B047AD9
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:20210504_20729690;a:39a87478-674e-4640-b1ef-ffea733128ec;cn:8;az:{did:951b20c4cd6d42d29795c846b4755d88, rid: 8, sn: neurope-prod-hp, dt: 2021-04-27T01:24:28.8067137Z, bt: 2021-05-04T00:18:30.3694362Z};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:2021-05-05 17:29:43Z;xdmap:2021-05-11 09:48:04Z;axd:;f:msnallexpusers,muidflt259cf,muidflt312cf,startedge3cf,bingcollabedge2cf,starthp3cf,moneyhp1cf,artgly2cf,gallery2cf,onetrustpoplive,1s-bing-news,vebudumu04302020,bbh20200521msncf,msnsports2cf,weather4cf,prg-adspeek;userOptOut:false;userOptOutOptions:" data-js="{"dpi":1.0,"ddpi":1.0,"dpio":null,"forcedpi":null,"dms":6000,"ps":1000,"bds":7,"dg":"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\default-redtube[1].css	
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):	81298
Entropy (8bit):	5.122579161600824
Encrypted:	false
SSDEEP:	1536:1VXorGHaV610Ax2/jr/CU/13/OI6AS/rMD76obNMh5fIlxVoQrv5gk:grG61
MD5:	E60E5077AB4E088ECD09F178CD1393CE
SHA1:	9FAF3FA6BD588D99803FFFDEFD156D97CC92E2AF
SHA-256:	4E836A3B177FBCD04B5B4CDDE6F16832ECF6AAAF02C1AFE2101F9CF059FC62CB
SHA-512:	AAB9A02F96D70A6CE5D5AD184A5AA830C4E33300EC7947F4D76006E695E00098124A7FC6440BBD1DAEC52E13734C3928E49258D3B6B0F804CAF6C9C3C1F5FFB
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/css/generated/pc/default-redtube.css?v=c68764eb72df2fd284980d4794d31c91941b183c
Preview:	.rt_icon{font-family:rt_font!important;speak:never;font-style:normal;font-weight:400;font-variant:normal;text-transform:none;line-height:1;letter-spacing:0;-webkit-font-feature-settings:"liga";-moz-font-feature-settings:"liga=1";-moz-font-feature-settings:"liga";-ms-font-feature-settings:"liga" 1;font-feature-settings:"liga";-webkit-font-variant-ligatures:discretionary-ligatures;font-variant-ligatures:discretionary-ligatures;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.rt_warning:before{content:"\e96a"}.rt_Channels_Active:before{content:"\e965"}.rt_Gay_PS_Active:before{content:"\e966"}.rt_Home_Active:before{content:"\e967"}.rt_PS_Active:before{content:"\e968"}.rt_Search_Active:before{content:"\e969"}.rt_gay_icon:before{content:"\e964"}.rt_shop:before{content:"\e963"}.rt_Seek_To:before{content:"\e960"}.rt_Seek_To_Small:before{content:"\e962"}.rt_library:before{content:"\e961"}.rt_Send_Message:before{content:"\e95f"}.rt_save:before{content:"\e95e"}.rt_Trending:be

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\default-redtube_logged_out[1].css	
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):	5933

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\default-redtube_logged_out[1].css	
Entropy (8bit):	4.978970495241967
Encrypted:	false
SSDEEP:	96:og06cSF9meBQgOhMk/UWMQbyNPKVhe+UlFPAVZzVINZO:o96cYm4BDZQONSDe17bO
MD5:	A2ABE3C0AC7D20144C90610C73121137
SHA1:	BB46952BA96BD8062D4AFFD57FC5BB53DBA2C13F
SHA-256:	329BE541A2F6C615EDD88631A58814EF29BE02BF8B571B305F0F5BB02E830854
SHA-512:	3469D45A06E7CB96315457D8AF8575FD1F8FF86D5DD5EA2D6FBA53E6DC6A21CAF559C504735DD74D85D4AF922B6198B8DAE200BAAF0CFAB793A18A179F95BE 44
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/css/generated/pc/default-redtube_logged_out.css?v=c68764eb72df2fd284980d4794d31c91941b183c
Preview:	#login_form_container .main_heading{color:#fff;text-align:center;font-weight:700;margin:0 0 20px;font-size:2.5em;letter-spacing:1px}#login_form_container .login_or_delimiter{text-transform:uppercase;text-align:center;margin-top:25px;font-size:1em;font-weight:700;color:#999}#login_form_container .sign_up_text{clear:both;display:block;overflow:hidden;margin:10px 0 0;padding:25px 0 0;border-top:solid 1px #444}#login_form_container .sign_up_text .sign_up_title{display:block;overflow:hidden;margin-bottom:20px;text-align:center;font-size:1.65em;font-weight:700;color:#999}#login_form_container .sign_up_text .sign_up_btn{display:block;width:100%;height:40px;overflow:hidden;line-height:38px;color:#fff;font-size:1.166em;text-align:center;text-transform:uppercase;font-weight:700;letter-spacing:.5px;background-color:#3c3c3c;border:none;border-radius:4px}#login_form_container .sign_up_text .sign_up_btn:hover{background-color:#505050}#login_form_container{overflow:hidden;width:93%;padding:0}#login_f

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\favicon[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 192 x 192, 8-bit/color RGBA, interlaced
Category:	downloaded
Size (bytes):	7112
Entropy (8bit):	7.929079219699957
Encrypted:	false
SSDEEP:	96:1StNJIGUv9aiNwBMZSs4f44FmuT7e9hP0xspI6VQQozqUSiLn3QmMsPK1sBZBwMy:1Sy3NwU5TIm/ZppBpo2UesiW7xLoo6x
MD5:	D905EA6840CBC5953D204FB40F87C828
SHA1:	2B018A12DB88B7C4549297901C04F6E33E8FB171
SHA-256:	FFA6FAF1AFDA6C294B589EFDF15D2F9EDF285A5FEFA78F11A5F6E8690BEDFDA0
SHA-512:	24D8415BA26BACC508A38F9969F723E91E3B0B5DDB02CEC30EC0D86B9E47D597DF22CCDD674CC7A6F8D5436E2FDF2BD24F1821B4410865F5BC54478BEC175 AA
Malicious:	false
IE Cache URL:	http://https://ci.rdtcdn.com/www-static/cdn_files/redtube/icons/favicon.png?v=c68764eb72df2fd284980d4794d31c91941b183c
Preview:	.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 *.m|.. ..li.l=@.9.p.....9 Z..t.X-vgY..O%..e.&C..9.V.A....a.H.....Z.].Q.....s&.$O...$V...h.e.p..].@f%.W..(...<....R./..a<.3.V'"#.....3a.#.v...(".X1..w.g.....>..}3....Z.y..gx..',q.-...J.{#....~..0.4*..bky..v.;`6...x

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\http___cdn.taboola.com_libtrc_static_thumbnails_15494c1f83f34b45710c6136bc079606[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):	22047
Entropy (8bit):	7.977959608000999
Encrypted:	false
SSDEEP:	384:kLgzRy3iHRapYmihTnbRsD5Y2j5h8xrfOjxfwN9bjnUW/ASfbCi3ZpJKf:kLggCo+miREYchurfOjxIPbjUWXfb5pa
MD5:	6A517E1FB2F8A4ABD2084A8C8F83567A
SHA1:	43B2814FC4DF2A5750FF1C97B45069B99D213643
SHA-256:	EBCEF6D364D208293A38ABB72652A85103F1EA756B32F4622AEF762947B29377
SHA-512:	E9BF85C945EC5D89C0A3EF351090402BB6398817D71F324D6D9F68021C55C8D83FD5B50A8A479A36068DF8376AC46B4CF439CDA576EC4D8DA0034D995216254
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%2F15494c1f83f34b45710c6136bc079606.png
Preview:	......JFIF.....&""&0-0>>T.....!..!..)1(%(1)!9339ITGCGTf[[f.z.....7.....5..... ...5....@....#..H....G.'.A..c<....w..<x.}>...I..x.....1...a.....A`.....0H.>..g..~...O...0<\y...3..!.J0!.04..[.j.....>...G....T)P-O.g. .... ...dZ'..>.Es..q?.....>.!..s.....I.e[].E..}A...:dHS20 ....DA.5"....].....G.V..I/.{<.".+A.&L.>.vx=....}.H.zU?..Sy.....B.....y.....;..Z..h2J.h! ..C.RS....u.:.....7..Sg.....h..?.....{<.@...`....L.....>?.@...~.....q.l.rz....O.|..k^..H..<LI2.....slD# ...}>H...k..o.....;.+?Lk..q...7.. ..._UM.v].=Nc.!.....1...j.8c.o.qU_G.}. ^G..xX..>.....y.M{<)b.....n`.N.x=o\....>.kvU....!=..h...../..wFw..LG.I<(?g.<'.;.j.R~..-..t.|.z.b.9..^.i[...y..1..... .8).Z...+.(6.R.h+.Lu.9.....;.Iv....zpn.,.....]..Y^gT_:....|N..,.....7t....z.<o@Vd....g6efQ..Z.Vx.Z'.."]z+..... :....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\http___cdn.taboola.com_libtrc_static_thumbnails_45a5849d6cc96ef07d2370f20bfea334[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):	21914

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\http___cdn.taboola.com_libtrc_static_thumbnails_45a5849d6cc96ef07d2370f20bfea334[1].jpg	
Entropy (8bit):	7.96678358003523
Encrypted:	false
SSDEEP:	384:IWI9pPWRh0tivEL2kW4haqgs1r8eRHO3MCP5S1dGjOQJ9xS4er2W+rrQXAq4HRjM:o9Eh0e7Og84eRucCQGjOOC2pmf4HRje/
MD5:	12F7320E70E6B06E100A461406088D7E
SHA1:	94AECC8F83B3BD012046292F542661975D7F5E97
SHA-256:	2A37FE97E2E5DE08274CB4013ADD44DCCECAE9E5889F9E0BBED75B7C6B9E0D6A
SHA-512:	F7A602DD76984335A0CB5C9FFAF3600331DCD299E68552C650A75A3AF02CA25D3134B677186E51AA80F6E04F4C9BA38D743647DB0A19354DA75451E990964BB6
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%2F45a5849d6cc96ef07d2370f20bfea334.jpg
Preview:	......JFIF.....,. .. .,'/&$&/'F7117FQD@DQbXXb\|v\|.....- " " -D*2**2*D<I;7;I<IUKKUI}ici}.....7.....4.....7.....<...r....kA..... .b"6..`.Q.s.3..w..7...=.+..{...I.!...W].....L.O_.^.....)W/;.~u.fz.C.t..}.;..;.....y....Ay....H....Y.....R..y..H....-d.Pr.hjy.....;..k.....5.4....u.).PVBW...5 Ac1...r..QR.\|..R.H504OG..{..7..7...v..8.Mh..X.0Z).A.hNO-..=.1.ke.t...e..3.oJ..;U.6....;..m..oI.bs..(...g*...A....&..".d,i...8.+..M_r1;.....h..Z..... ..M4..^47.&.<+).*M.b.M_....w.....Q /..c.?..o>P=rj{..Y...y..Q.FnK!..J5.:..U....b.S".V.._.<..Q...\|&.Vb...E..$tJ:.er.-...[..7....Yj..d....R.4gT.TK&.....lW.;...K..e.....{WF.....K...9.7.VH...J.;C!..h...(\.....{f.T.w0.KL..g..#.T iTO@.B.*e.....A..6.V.F....$.:..f....lw!..p..K...yV.(h.....By...S...l.-/...F....e.D...cU(.a.....^.;uH.rz....&.>c.k..5...@Ku.k.5.KV.....J.Y.....`.<

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\http___cdn.taboola.com_libtrc_static_thumbnails_7d4a1914f83988c0cb22d7e32e5e29d7[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):	3769
Entropy (8bit):	7.732834519465285
Encrypted:	false
SSDEEP:	96:ZvXh3HRTtmISwjqVZKFX7fSary/wdxWOHAZ+Gjwi:Zvx/3rOPsy/exWOHAwi
MD5:	84ABD66DD18293042CC61F8483A463C3
SHA1:	4239DBBF0C563E43B7B93ADDBD78ED374E779F34
SHA-256:	BD37370480091C892DB40B7850354FAD5D1915CC810E54989D62AC48958F348C
SHA-512:	14DE5327B50DF28BE7C999F0961CC533E0B1A0BB9BB4BB283222D00A8ABCD16CE9D8865E84878A9FB9E7D356CA01F67D154C4CFF0C14C926D20E206A9873C9F
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%2F7d4a1914f83988c0cb22d7e32e5e29d7.jpg
Preview:	......JFIF.....+"..."+2*(*2<66<LHLdd.....+"..."+2*(*2<66<LHLdd.....7...."..... .....6 ..b.....3..b.....J.d%X.=X.D@h..lC`.x.'....X'...W..Xe&.)G=.H.(..Ph.V.)f.$..9=.g'....E1,..K$r.....Q....#U.....K..%...Y.X.&...^..$.A.+....@...A<S..r[..%...e.bY...H.$.7.+*.G....* .J....n....O.jx....;'.....y...u?|.....w.q+...v....gI.....A).JD..a!.....V.....B..!yi0.ZM/../.{.E....au).t...at..R.....kAAM.....O...)..Z..N..q.R.T-..]...R.....+TYcx.....zS..@.W|.X...DN&!Ia..B.fy. .i...F#.&>/...O..y.WG.N>....07..S.8Ab..W....A.9.QSI3.P.SU.O5d.q.&S.92..vS..f....i.p].84..q.Lf.a.t....$..t..\t...t...t...]..W.S.^mN....^p9...h1k..9.....W...yU:....^IN.y.....hvk.jq a..z.F..D..V.V[.V,.r.W,.b.W,.rp.. 'C...T.D3.AL.....D3...4C8...D3...4P.4C^....AL..S8...D3...4C8...D3...M$3...4B.....h...P[.g...h.y...g.....h!A4...R.t).T..B.x(..]R.t).B

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\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):	390978
Entropy (8bit):	5.484753185037266
Encrypted:	false
SSDEEP:	6144:zNv9Tu0WIqvbpDnmPlnGZUvgz5MCu1bdaZ+pv9lIq:4Iqv1DwnGZUvgKxV6E1lIq
MD5:	3B968DA735104DBAA4F70E2922223994
SHA1:	9A4ED0A838DD95243B02C763A054D77047D009E8
SHA-256:	B9A5438B84576BC17E94D6E00D876DCC4932545430506A3A02A1BA65AB4CF46E
SHA-512:	5FFA42D500C0F0A30988C80D3A3CB5F192A728A9166CBC6840C812CCB8A76D7D84AA78B518538153FD6D2800C865AEB0295F89EE5390DC39967854858815AAA
Malicious:	false
IE Cache URL:	http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=722878611&size=306x271&https=1
Preview:	<html>.<head></head>.<body style="margin: 0px; padding: 0px; background-color: transparent;">.<script language="javascript" type="text/javascript" >window.mnjs=window.mnjs||{},window.mnjs.ERP=window.mnjs.ERP||function(){"use strict";for(var l="",s="",c="",f={},u=encodeURIComponent(navigator.userAgent),g=[] ,e=0;e<3;e++)g[e]=[];function d(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(a=0;a<3;a++) e+=g[a].length;if(0!==e){for(var n,r=new Image,o=f.lurl||"https://lg3-a.akamaihd.net/nerrping.php",t="",i=0,a=2;0<=a;a--){for(e=g[a].length,0;0<e;){if(n=1===a?g[a][0]:{lo gLevel:g[a][0].logLevel,errorVal:{name:g[a][0].errorVal.name,type:l,svr:s,servname:c,errId:g[a][0].errId,message:g[a][0].errorVal.message,line:g[a][0].errorVal.lineNumber ,description:g[a][0].errorVal.description,stack:g[a][0].errorVal.stack}},n=n,!((n="object"!=typeof JSON||"function"!=typeof JSON.stringify?"JSON IS NOT SUPPORTE D":JSON.stringify(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\medianet[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\medianet[2].htm	
Size (bytes):	390978
Entropy (8bit):	5.4847803039135785
Encrypted:	false
SSDEEP:	6144:zNv9Tu0WIqvbpDnmPlnGZUvgz5MCu1bgaZ+pv9llq:4Iqv1DwnGZUvgKxVZE1llq
MD5:	12F335BF7CA5671A961A0A6FDBB8BE79
SHA1:	1FBED8F3CC00229166515DE176AE28A4DA354230
SHA-256:	F30E0905E45F0569B9C8AA51439D7D905E8B6B649422DBB4F1B4696C502CC449
SHA-512:	029075AA69BDB1E45F47F17C14577910DBB3D207DA48688DB8472ED126A10CB19893059B34ECBCD94263BBA3224E750F30DAC4D5699E3649BA77BB9D0314DD4
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 l="",s="",c="",f={},u=encodeURIComponent(navigator.userAgent),g=[] ,e=0;e<3;e++)g[e]=[];function d(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(a=0;a<3;a++) e+=g[a].length;if(0!==e){for(var n,r=new Image,o=f.lurl||"https://lg3-a.akamaihd.net/nerrping.php",t="",i=0,a=2;0<=a;a--){for(e=g[a].length,0;0<e;){if(n=1===a?g[a][0]:{lo gLevel:g[a][0].logLevel,errorVal:{name:g[a][0].errorVal.name,type:l,svr:s,servname:c,errId:g[a][0].errId,message:g[a][0].errorVal.message,line:g[a][0].errorVal.lineNumber ,description:g[a][0].errorVal.description,stack:g[a][0].errorVal.stack}},n=n,!((n="object"!=typeof JSON||"function"!=typeof JSON.stringify?"JSON IS NOT SUPPORTE D":JSON.stringify(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\modernizr[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	8104
Entropy (8bit):	5.298807633749026
Encrypted:	false
SSDEEP:	96:7pNcA1YAbyKMaruPiTepmNWb14ANxYPeqdqPqyPC01XlgovyO41Cgth7tYwpGljk:F/M2XKQob1dHYPeIny6ZLDDhWwpy8b7z
MD5:	7EA3C79E9B0A5589AFF8FDD72660D81A
SHA1:	A9CDDB1407CBCB97D5BE32F03594B53BECFFF8AE
SHA-256:	61AB308003A3D546EA9F191CBB44AD21A8C81FE98B536037B6C570DCF16FD2E7
SHA-512:	E1C86B7E4DC06653B63C32A125EB69FA7FFF2EEF72544D692FE91EC16BB3D85BEDC37E3666756D82F95DF73E8C469FF0F3B64DA1259D4B9DF0E9A6AD17BA34 C9
Malicious:	false
IE Cache URL:	http://https://ht-cdn.trafficjunky.net/html5video/modernizr.js
Preview:	/* Modernizr 2.8.3 (Custom Build) | MIT & BSD. * Build: http://modernizr.com/download/#-video-shiv-cssclasses-load. */.;window.Modernizr=function(a,b,c){function u(a){j.c ssText=a}function v(a,b){return u(prefixes.join(a+";")+(b||""))}function w(a,b){return typeof a===b}function x(a,b){return!!~(""+a).indexOf(b)}function y(a,b,d){for(var e in a) {var f=b[a[e]];if(f!==c)return d===!1?a[e]:w(f,"function")?f.bind(d||b):f}return!1}var d="2.8.3",e={},f=!0,g=b.documentElement,h="modernizr",i=b.createElement(h),j=i.style,k, l={}.toString,m={},n={},o={},p=[],q=p.slice,r,s={}.hasOwnProperty,t;!w(s,"undefined")&&!w(s.call,"undefined")?t=function(a,b){return s.call(a,b)}:t=function(a,b){return b in a&&w(a.constructor.prototype[b],"undefined")},Function.prototype.bind||(Function.prototype.bind=function(b){var c=this;if(typeof c!="function")throw new TypeError;var d=q.call(arguments,1),e=function(){if(this instanceof e){var a=function(){};a.prototype=c.prototype;var f=new a,g=c.apply(f,d.concat(q.call

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\otBannerSdk[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	374818
Entropy (8bit):	5.338137698375348
Encrypted:	false
SSDEEP:	3072:axBt4stoUf3MiPnDxOFvxYyTcwY+OiHeNUQW2SzDZTpl1L:NUfbPnDxOFvxYyY+Oi+yQW2CDZTn1L
MD5:	2E5F92E8C8983AA13AA99F443965BB7D
SHA1:	D80209C734F458ABA811737C49E0A1EAF75F9BCA
SHA-256:	11D9CC951D602A168BD260809B0FA200D645409B6250BD8E8996882EBE3F5A9D
SHA-512:	A699BEC040B1089286F9F258343E012EC2466877CC3C9D3DFEF9D00591C88F976B44D9795E243C7804B62FDC431267E1117C2D42D4B73B7E879AEFB1256C644E
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/9c38ab9f/webcore/externalscripts/oneTrustV2/scripttemplates/6.4.0/otBannerSdk.js
Preview:	/** .. * onetrust-banner-sdk.. * v6.13.0.. * by OneTrust LLC.. * Copyright 2021 .. */..!function(){"use strict";var o=function(e,t){return(o=Object.setPrototypeOf||{__proto__:[]}in stanceof Array&&function(e,t){e.__proto__=t}||function(e,t){for(var o in t)t.hasOwnProperty(o)&&(e[o]=t[o])})(e,t)};var r=function(){return(r=Object.assign||function(e){for(var t,o=1,n=arguments.length;o<n;o++)for(var r in t=arguments[o])Object.prototype.hasOwnProperty.call(t,r)&&(e[r]=t[r]);return e}).apply(this,arguments)};function a(s,i,l,a){ret urn new(l=l||Promise)(function(e,t){function o(e){try{r(a.next(e))}catch(e){t(e)}}function n(e){try{r(a.throw(e))}catch(e){t(e)}}function r(t){t.done?e(t.value):new l(function(e){e (t.value)}).then(o,n)}r((a=a.apply(s,i||[]).next())}))}function d(o,n){var r,s,i,e,l={label:0,sent:function(){if(1&i[0])throw i[1];return i[1]},trys:[],ops:[]};return e={next:t(0),throw:t(1) ,return:t(2)},"function"==typeof Symbol&&(e[Symbol.iterator]=function(){return this}),e;function t(t

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\otSDKStub[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	16853
Entropy (8bit):	5.393243893610489

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\otSDKStub[1].js	
Encrypted:	false
SSDEEP:	192:2Qp/7PwSgaXIXbci91iEBadZH8fKR9OcmIQMYOYS7uzdwnBZv7iIHXF2FsT:FRr14FLMdZH8f4wOjawnTvuIHVh
MD5:	82566994A83436F3BDD00843109068A7
SHA1:	6D28B53651DA278FAE9CFBCEE1B93506A4BCD4A4
SHA-256:	450CFBC8F3F760485FBF12B16C2E4E1E9617F5A22354337968DD661D11FFAD1D
SHA-512:	1513DCF79F9CD8318109BDFD8BE1AEA4D2AEB4B9C869DAFF135173CC1C4C552C4C50C494088B0CA04B6FB6C208AA323BFE89E9B9DED57083F0E8954970EF822
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/9c38ab9f/webcore/externalscripts/oneTrustV2/scripttemplates/otSDKStub.js
Preview:	var OneTrustStub=function(e){"use strict";var t,o,n,i,a,r,s,l,c,p,u,d,m,h,f,g,b,A,C,v,y,I,S,w,T,L,R,B,D,G,E,P,_,U,k,O,F,V,x,N,H,M,j,K=new function(){this.optanonCookieName="OptanonConsent",this.optanonHtmlGroupData=[],this.optanonHostData=[],this.genVendorsData=[],this.IABCookieValue="",this.oneTrustIABCookieName="eupubconsent",this.oneTrustIsIABCrossConsentEnableParam="isIABGlobal",this.isStubReady=!0,this.geolocationCookiesParam="geolocation",this.EUCOUNTRIES=["BE","BG","CZ","DK","DE","EE","IE","GR","ES","FR","IT","CY","LV","LT","LU","HU","MT","NL","AT","PL","PT","RO","SI","SK","FI","SE","GB","HR","LI","NO","IS"],this.stubFileName="otSDKStub",this.DATAFILEATTRIBUTE="data-domain-script",this.bannerScriptName="otBannerSdk.js",this.mobileOnlineURL=[],this.isMigratedURL=!1,this.migratedCCTID="[[OldCCTID]]",this.migratedDomainId="[[NewDomainId]]",this.userLocation={country:"",state:""}};(o=t=t||{})[o.Unknown=0]="Unknown",o[o.BannerCloseButton=1]="BannerCloseButton",o[o.ConfirmChoiceButton

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\rt_font[1].eot	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	Embedded OpenType (EOT), rt_font family
Category:	downloaded
Size (bytes):	50508
Entropy (8bit):	6.241740550675033
Encrypted:	false
SSDEEP:	1536:pKhMTynpoy+Y31ecBtVPOMDXlFwyyE4JkYzHRU:ohMTynp3+YvBtVzD1RyE4CYO
MD5:	31AC50F85D54C33FFDBA0EA5F035FDB8
SHA1:	EE335815F28A058C2F240FD58FF886B8578DD71F
SHA-256:	64699F58282DB926AAFE33D32526C26661ED22CBD17CC87C1C1DB6BFFEADFC21
SHA-512:	0DA254888FD66C1D2CD1EAAA1E318A75A2BF31050648E363802D8D184534BAC80706D080B33AB53869585F8322918F4C779164230FAD61D21A3A989407C94924
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/fonts/rt_font.eot?v=c68764eb72df2fd284980d4794d31c91941b183c
Preview:	L.....LP.....W.....r.t._.f.o.n.t.....R.e.g.u.l.a.r.....V.e.r.s.i.o.n. .1...6.....r.t._.f.o.n.t.....@GSUB.....~OS/2.....L...`cmapL.Q..... ..gasp.....glyf.....head.~.....d...6hhea.C.....$hmtx...]....loca2.b.....maxp..... name.`.....post..... .....,..latn.....liga.....:..... .....3.....@...;.....@...@..... ....-.2.a.p.r.u.w...P.l.|.....j.;..... .-.2.a.o .r.u.w...P.l.|.....:..... .....l.....79.....79.....79.....79.....79.....79 .....79.....79.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\rt_utils-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):	6211
Entropy (8bit):	5.30892710774022
Encrypted:	false
SSDEEP:	192:F2+YwSvZvZ8SyxTREaQYCLD+ozJ41Mw6OzWD:FrYwSvZiHRKtLD+71M46
MD5:	57374E105B2BAF9DEDA055250C7B726B
SHA1:	9A0AF064EEB3B31394BF51295C6B6FCB5BC7DF2F
SHA-256:	C9EE853B1CB3CC13C13D87F5F06781F9E1A78107A8785029596FFAD720DB39FE
SHA-512:	249C2E7B1FC90B2594F520B8191116731C27B65B664E61107FB16C31A35558BA9C4FF8326AAF93B8916BEA6F33A7C9BC464BA647EF56279D6576AA7C992723DC
Malicious:	false
IE Cache URL:	http://https://ci.rdtcdn.com/www-static/cdn_files/redtube/js/generated/common/rt_utils-1.0.0.js
Preview:	var RT_Utils={browser:{hasTouchSupport:"createTouch"in document,version:(navigator.userAgent.toLowerCase().match(/.+(?:rv|it|ra|ie)[\/:]([\d.]+)/)||[])[1],androidversion:function androidversion(){var e=navigator.userAgent.match(/\s*Android\s*([0-9]+)\.?([0-9]+)?\.?([0-9]+)?\s*/);return e&&e[1]&&e[2]?parseFloat(e[1]+"."+e[2]):!(!e||!e[1])&&parseFloat(e[1])},isWebkit:navigator.userAgent.indexOf("AppleWebKit/")>-1,isMobileSafari:/(ipad|iphone|ipod|android).*apple.*mobile.*safari/.test(navigator.userAgent.toLowerCase()),isAppleChrome:/crios/.test(navigator.userAgent.toLowerCase()),isAppleMobileDevice:/(ipad|iphone|ipod)/.test(navigator.userAgent.toLowerCase()),isAndroidMobileDevice:/android/.test(navigator.userAgent.toLowerCase()),isTansoDl:navigator.userAgent.toLowerCase().match(/TansoDL/i),isWindowsPhone:function isWindowsPhone(){return!(!navigator.userAgent.toLowerCase().match(/Windows CE|IEMobile|Windows Phone OS/i)&&!("XDomainRequest"in window))},highPixelDensityDisplay:window.device

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\video-index[1].css	
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):	28636
Entropy (8bit):	5.053776024229463
Encrypted:	false
SSDEEP:	384:l27q9HpmR7R76KMsuyMBqzIOcuVTBVYGuJs+c4Xb+zO:YRQulBVYGubcHO

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0MX4YUS9\video-index[1].css	
MD5:	C9B739D7AE9BEC31FE3FC38450F378A4
SHA1:	336F19A35FB16DA32020E3E68C78B1C370D0432C
SHA-256:	31DE15F0F44952E901F8D42D4B02DFCD03925A5EFA75BBD9467AFB75E945AC32
SHA-512:	43056D72CE171C79E056F7270A2BD376DD3E0A384E1B527BCD35437AC5AC6ABC03139AAAC226703F36F35E6DB4D11BD7DA8859912F4AF6F3B8B241EDB05291A
Malicious:	false
IE Cache URL:	http://https://ci.rdtcdn.com/www-static/cdn_files/redtube/css/generated/pc/video-index.css?v=c68764eb72df2fd284980d4794d31c91941b183c
Preview:	@supports (display:grid){.channels_grid,.galleries_grid,.members_grid,.ps_grid,.streamate_grid,.videos_grid{display:grid}.channels_grid li,.galleries_grid li,.members_grid li,.ps_grid li,.streamate_grid li,.videos_grid li{min-width:0}.one_row_grid{grid-template-rows:1fr;overflow-y:hidden;grid-auto-rows:0;grid-row-gap:0!important}.wideGrid .title_filter_wrapper.is_sticky{width:973px;padding:20px 0;margin:0 auto}@media only screen and (min-width:1324px){.wideGrid .title_filter_wrapper.is_sticky{max-width:none;padding:20px 30px;right:0;left:300px;width:auto}.wideGrid.menu_hide .title_filter_wrapper.is_sticky{left:66px}}@media only screen and (min-width:1980px){.wideGrid .title_filter_wrapper.is_sticky{max-width:1980px;padding:20px 30px;right:0}}@media only screen and (min-width:1324px){#content_container{width:100%}}@media only screen and (min-width:1324px) and (max-width:1630px){.wideGrid .content_limit{width:100%;padding:0 30px}.wideGrid .ps_grid{grid-template-columns:repeat(8,1fr)}.wid

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\1018263891[1].gif	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 950 x 250
Category:	modified
Size (bytes):	3954
Entropy (8bit):	7.866064568149102
Encrypted:	false
SSDEEP:	96:lBlLtplsUP9lUNrWtbM98rWQPxeMsOzrzbU:xLtPj9lAg881PQMsOjbU
MD5:	00512C36B5B14E1CBCE65670C164C477
SHA1:	F58A3EDF7D008703837B298F2BCD0591A67FF06C
SHA-256:	893771F299B56351FFCD9BFBD8046881CF1892B12051F2F330E64759F0D1B21F
SHA-512:	DD0AE24FC25F459A0FDB3B9F6DF9FC02145D7B6D90083E39448FDDB3FEDBADA361A409720A3BEF92D552AE634EC49D6C8EAC5490A6BED76A2199751BD7C1C52D
Malicious:	false
Preview:	GIF89a.....}..S4.....Qk.....eE...uT.....k4U.M&."....`8....Z@m6$.zd..h.rI.bD.....fv^E..t.tUvD(.y..z.....w.{c.tX...yS4.kH\|l0....E.zX.kV..uS2!...pI....YhB'5S..iQ.jQb,.....hS9W@,eI3...A.....vQ(.uK....i<....pJ..._....~`6..l.lZ...eA.kP)-L.<2.]M.....l.....]<....6V.$g{...fR.Y.Z%H....i...D....b.a..!.!...L....+T.....;v.A....+.*.-.x..6..Z...&,E.D.C..tA.P.?...0K.....z.~.....!..NETSCAPE2.0.....!..Optimized using ezgif.com.!.....},.....@.....<."D.?NN%I.D.....D./D././F.1....S.....%%.....5/.*.*1,.....L$$7CA..A....7A..A.CWC..W.WWGG....)....0....aC&.H..GQ.E}..%..#...Cz.I2...'!)R.h.../c.I...8s.....@...J...H.*]...P.....C."D.d...'9r....&N..nJ.i.....X....].L..U.WF*..P.C..M&(.....[4..82...3WV.X...'v$. !...S!..E.....Q.;r.....].#C.V<.....0.#.....<.....C.Jj..;K..[..)....._.....<x...@…I$..&?`...:8.X.'.....vZ.&T...j....R...&..B/h.u.'?4...M.%Y.0. c..80.8....6x.2.]..\oM..j.....O....8@.N.T.P.D.Q

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\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):	10089
Entropy (8bit):	7.9226684555886635
Encrypted:	false
SSDEEP:	192:eP3tRcmkRhtlpeojd13EVh+Q/ZpWBDYbdehWGP3Q2p2Qb0uFzCyMNo3:ePdRARSojnEjx/D68b0R3QVluFzCyMN8
MD5:	B670C3F13CC66B985817B9D4EE82F8A4
SHA1:	531F55DD7C31571EDBD01B39CDFEAC9E1221C293
SHA-256:	56E7E424D5948D8C5D31A1E9D51EC4C12274BC378098775395A3D4924EBF8914
SHA-512:	D5C998A6FF622755B9E09D6C5DB11DF2CE6D862A59FA480E2F0657D949DB47C064071339CA4F72C30190E2957BA7A300DF6F3A38C96F8A4ED7518AAF707A716
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/m=eW0Q8f/media/videos/201907/30/19703412/original/12.jpg
Preview:	......JFIF.....C.....!......"$".$.....C.....0..".....3~.Kw.D...NAH..o.[.....U...B.r.KV.4.Ob.....E...VI.9..m.F.3//R.1.iC.....*...(.y|.t...f,..].3rb...5.g.fC...M....z.....ej.W.>.3.....3..<3}.;....lK.Q....<...4..=4.;..".V...c..<...D.<..%$Ok.g.l.2.(.....<...9.(..*.R0..5#N`G.....z...._/P..S...v.^'..g...!<.....0.I..>..GBx..x..KV_y....`.u.iR..L.#.2....?N...(H0.t<..o....T.....".Y...=s.P.4.pS.X..pJ..-..i....Y.t..U6..fM.Y..... ...{..'..%>.u&{.(..[.....=..F..i'=+}&j6H"..=.C.l:...D....$xt..P..^.._....xs..Wl.(....V..c?S...$....&.2.j.O...lZ$.....rq)I+..t.8(..8.....4.....p....s.2..[g.$..H6..~...x+..*..WP....GE.....'@...`..G8;..\.....,-...,(.f8.C..'C.....:.....A0..+.%xE@]8U.](..3l.....o.....G...1.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\12[2].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):	11596
Entropy (8bit):	7.943737682772087
Encrypted:	false
SSDEEP:	192:eX+wQMCwYw6UqGEDUENI7vhl26uI+0Kp7syUrYh1QAxQZ7Q9OFOT/NULFTUKE:bxDGEDUVwRN+Y1f6ROtv
MD5:	E95AC97D6F7AA912978E78E2CEFCE92E
SHA1:	B3000EA02EB929C5B2E0D20046886AE1D5AB048E
SHA-256:	4975E09023FFC9556F4C888C75BD9AC46E0427E7AB40FB521306CD48D2737C69
SHA-512:	9FDA7B833B6EDF2BE2381618D7F728B4528AA415D35611DD4B61C98CB23AA01F3EBA803249BE01E05746B97FB79782A22F236E61CFDC198EA31EC0132982C47

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\12[2].jpg	
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/m=eW0Q8f/media/videos/201910/28/23719311/original/12.jpg
Preview:	......JFIF.....C.....!....."$".$.....C.....0.."....w .....F...Y-..^..%V..#.7g.8._...c}u.F...q."!..g+.(..i.6.{....l<.H%a5.i{.....-.ke.uY.....Q.F7...+.....;..3.b^...V.W.....fs.....d.....(.a'/....wq=..{...V.U..M....~{.e.%....[.../_u.97..H.,..},.. .PR04..Z/=U..J..}.{.>.....R=..#...~m?.P.o.c:/X .K~..w.m..GbD....F.l.dka`.th.luv...!]....Cn[.fa..6.....$A..V.+:.}....j...&...../jg.h.{e.0..*cW?T.uB.1..\...^H....CL..'.'...4.f>..,kH.lv.q....- ...T...8...)..Kj_.d.&..M...R.Y.d...k..#!'..+....._K.e.[.*..H.....$r...Ker.B.i.*.z.{Q4YY.[<.... ....E.N....).G?}OVm.l.....g.t.....lv.\..p.#EeS.....-.jH...P..J..q54iQa2..<BJ.5.w.k&.....u.K ..3.t.:9c:..MU..]...,2.%w..}5q.0.!..VG.$B.p..>.Ux[O...Y].....Xa..e#..d.....W...^...-..zEU.`.K..N..(v..hGB.#T..h.)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\AA7XCQ3[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	667
Entropy (8bit):	7.561736401445472
Encrypted:	false
SSDEEP:	12:6v/7TUYRk5V6RwLzZvLk519s0/tWnssyQSKZLsLO7qcNrXlUA3YUz1oK9:STuzZc19skWssyQ5ZsO7qc1Vdf9
MD5:	C9E843CDDAD2F56F8F88B8D6A937B602
SHA1:	EE3382E8031321B266BA31CA47D0667F03C469F8
SHA-256:	D0A577DFBCF142D19E89E5ABC3EEC3020AD0C3A65B9BA6F6534097D0806B2100
SHA-512:	677CDE3738656508AEDBE2DA698B21B5AA15EBA8EDECE60192A5B61004E6CB6A1F718A02066AFF367021C31B9B13D2DDD703976E8F26C22272AE8AADBECC5 ED
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/AA7XCQ3.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....MIDATx...]HSa...n.l;.d..a-HK)..6....."..... ..Gn...E.Q&.EA.y.T....25.K..UT8...M.....>.[u.=.;.y_..../....#.z..w.....6.....n!(.k{<... .K..dv..Fm..Ro.NT..Y.N....;....$x.....d....p:.?^LR.8k.....7...9.....S<....)...B..#.5:uck...0..0 d..=V.T..ad.{[Z.?.026<..@...R..@.....}.p-..:.....Qlo....5$.D.....,..Q".x...c.....+./` .f<...._F.&2q.8E.....(...%T.}8...=.:...[[...@ ..e...6....Q...?..".q.....p.....j.f.....4H\#j.i"@|6_..2.i-.>.j.....)..'*]..r9.[.T5...$l.A.wa-<#.Dt]sPnc9F..Q.8...].....D...f._S...0WG.>b.....t. ~j>.K.h]4~.....Q....BA..?.}.s..;.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\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):	936
Entropy (8bit):	7.711185429072882
Encrypted:	false
SSDEEP:	24:IJJuYNKuGlZLocJZlxAgAbiuoSrZzi1g3+:IJn94F/IxAZiuoSNYgO
MD5:	19B9391F3CA20AA5671834C668105A22
SHA1:	81C2522FC7C808683191D2469426DFC06100F574
SHA-256:	3557A603145306F90828FF3EA70902A1822E8B117F4BDF39933A2A413A79399F
SHA-512:	0E4BA430498B10CE0622FF745A4AE352FDA75E44C50C7D5EBBC270E68D56D8750CE89435AE3819ACA7C2DD709264E71CE7415B7EBAB24704B83380A5B99C66 C
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....pHYs.....+.....ZIDATx.m._hSW....?....E...U.Z.M..a.1.}P..6+.....l.....LDA.....u.a.U..P..&k..Iz...&....R_.q.=p8....~.'...5..}....._.I$FS.\.c][4#... .....+...U@fZz.Y.....|.7....r.x..S.?.ws....B9.P.-Yt*..N.}.'V.....G...5....uc....XV.=.{..ai.pw.v)...(.9.z\|.3:Q..,qr.es...ZTp..Mt.iB.2.{w.C*WB..F...b../.H..\..*.).0l.R.....c.....@S5.? 3...q..:...8.?....p.=6`..T...5.nn.....].b.j.,..pf.....8...".M..?.@K...L.='.1.O.2Kb.p..(..\.D.....n..._.....0.....w^bR....v\..)..I..f..I..M.m.6t.7....U.Y3?.h=..!.<.._.....pL..V"[..... {[P....e07...Wc....IH.T@...*..A@.....;....>Gt&...}...o...KP...7W1.sm~...&.....00.....>/....I.#.t.....2.....L_Owu.*.A)...-.w.*.1/+.)....XR.A#;..X...p..3!...H.....f.ok;..|x..1.R.\W.H\...<.. <&.M!mk:|....%.<..,.%.g..g..G@z^Q..I...T.D^..G.&v6$.J.2J....~..Y\kX.j.....c.&.>.3.....ek..+..~B.\.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\BB14hq0P[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):	19135
Entropy (8bit):	7.696449301996147
Encrypted:	false
SSDEEP:	384:IHtFIzAsGkT2tP9ah048vTWjczBRfCghSyOaWLxyAy3FN5GU643lb1y6N0:INFIFTsEG46SjcbmaWLsR3FNY/Ayz
MD5:	01269B6BB16F7D4753894C9DC4E35D8C
SHA1:	B3EBFE430E1BBC0C951F6B7FB5662FEB69F53DEE
SHA-256:	D3E92DB7FBE8DF1B9EA32892AD81853065AD2A68C80C50FB335363A5F24D227D
SHA-512:	0AF92FBC8D3E06C3F82C6BA1DE0652706CA977ED10EEB664AE49DD4ADA3063119D194146F2B6D643F633D48AE7A841A14751F56CC41755B813B9C4A33B82E45 C
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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\BB14hq0P[1].jpg	
Preview:	......JFIF.....``.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..h.h.....(.h.....(.h.....Z.(.....(.h.....TNY...W....q@..~..<..h.....dG.@.....F....L.@%}.....-K.F.9...c..O.7X9u,%.k.4..4..c.<p"...cp.-...U.J.n2..9.b.d.SphR.\V.5Q-./.LV.6...HM.V.d^E...F.q.*+7..a.m..VOA..qR.X.rx5&.(..Q..P.R..x..WM-.?.....V..GTi.(.(.....(.....J.(.(.....J.(.....Z.(.....Z.(.....Z.(.....(.h.....i..H.@...;..Y...q...0.<e+.B...[.v..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\BB1aXITZ[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):	1149
Entropy (8bit):	7.791975792327417
Encrypted:	false
SSDEEP:	24:hhxlcJrB6QJ0CXhyPAGQ3QgLEvDsLyW3ZXr4X6HpEv7V8F+:hSrFkoGGVLE7lW9rjE58F+
MD5:	F43DDA08A617022485897A32BA92626B
SHA1:	BB8D872DFF74D6ADBB7C670B9A5530400D54DCAB
SHA-256:	88961720A724D8CE8C455B1A2A85AE64952816CE480956BFE4ACEF400EBD7A93
SHA-512:	B87F90B283922333C56422EF5083BE9B82A7C4F2215595C2A674B8A813C12FF0D3A4B84DE6C96C110CC7C3A8A8F50AEAE74F24EB045809B5283875071670740E
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1aXITZ.img?h=27&w=27&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....U....pHYs.....+...../IDATx...}..c...SN$..@.e.Y..<.f...y.X.0.j..Z...T...)5..h.s.l..0.8gSh*l.T.l)..r.>?....Q.k{..}...~.VVta...V}.F.R...l.X.....AbD..].)8..`....{p/..;.`..Q[.....u..<.o."..u....u.Ge%1.....`.F..J1Y..u....k..sew.bf....E.o....+.GPU..\..u.?(*....j.>.B3.Da/K.QLo~'...]...go.k[+.@..K..U.\.....zInT....^..N.k.....M.."V..J.".i.-q.r=.....}.L]?..].#..'..g..q"?l.....^.O .i.,.,|.v\...,...Y.;.....J.Rd.s...N{.e*l.d.....=.h....X.k.....^..N.....,v...Kt...b_...bx.w.....^1....|...p.l#....}QXNd.9..~$.f....<'p.n..Pr..m5.@t;_.J.?4.\.[.,U1.....L.....g.Ky...?...c.....|F.....2... w.i.>.rRs.K0._..0....v.&..s.r.v...u.Kbf."..rc=.....R,.V".#.....r.,.../.|..$v..GX.|}1...y."2..".....X.*6.g"..dP.....a.....q.b. ...s4..y.B....6og.D.@.ATa.....FE.n>H,Q..p.....(...c...|.R..<_Kq.i?ME}.....h.?)...:....x.P^.?.=x.x|...0.30...'v+..0.p.D...p.....`m.y-....*. ..Gb:.>....[.....0..Y..\..n..-..a.%.H..O...#1.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\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\2K7JPOQS\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):	1131
Entropy (8bit):	7.767634475904567
Encrypted:	false
SSDEEP:	24:lGH0pUewXx5mbpLxMkes8rZDN+HFlCwUntvB:JCY9xr4rZDEFC
MD5:	D1495662336B0F1575134D32AF5D670A
SHA1:	EF841C80BB68056D4EF872C3815B33F147CA31A8
SHA-256:	8AD6ADB61B38AFF497F2EEB25D22DB30F25DE67D97A61DC6B050BB40A09ACD76
SHA-512:	964EE15CDC096A75B03F04E532F3AA5DCBCB622DE5E4B7E765FB4DE58FF93F12C1B49A647DA945B38A647233256F90FB71E699F65EE289C8B5857A73A7E6AA06
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1cG73h.img?h=27&w=27&m=6&q=60&u=t&o=t&l=f&f=png

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\BB1cG73h[1].png	
Preview:	.PNG.....IHDR.....U....pHYs.....+.....IDATx..U=l.E.~3;w{..#].Dg!.SD...p...E....PEJ.....B4.RE. :h..B.0.-$.D"Q 8.(.;.r.{3...d...G.....7o..9....vQ.+...Q....."!#I.....x\|...\...& .T6..~.....Mr.d.....K..&..}.m.c....`.`....AAA..,F.?.v..Zk;...G...r7!..z.....^K...z.....y...._..E..S....!$...0...u.-.Yp...@;;;%BQa.j..A.<)..k..N.....9.?..]t.Y.`....o....[.~~..u.sX.L..tN..m1...u .....Ic....,7..(..&...t.Ka.]..,.T..g..".'...W.....q....:+t.?6....A..}...3h.BM/.....*..<.~..A.`m...:.....H...7.....{.....$... AL..^-...?5FA7'q..8jue...*.....?A...v..0...aS.*:.0.%.%"......[.=a.....X..j.. <725.C..@.\. ..`..._....'...=....+.Sz.{.....JK.A...C\{.\|r.$.=Y.#5.K6.!.....d.G...{.....$.-D*.z..{...@.!d.e...&..o...$Y...v.1.....w..(U...iyWg.$...\>..].N...L.n=.[.....QeVe..&h...`;=.w.e9..} a=.....(.A&..#.jM~4.1.sH.%...h...Z2".....RP....&.3.....a..&.I...y.m...XJK..'...a.....!.d.....Tf.yLo8.+.+...KcZ.....|K..T....vd....cH.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\BB1gALGD[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	9614
Entropy (8bit):	7.931405010713805
Encrypted:	false
SSDEEP:	192:Qo1YgupHoWpmuNmuCamC+x/IRTOodWXehE+:bHkHoWp7/5mC+1qxCU
MD5:	9B8B918F7B52DEE51A31F654634A7D0F
SHA1:	EE0BE74032433075B14C1ACD6D9CBE1AE0E0EC66
SHA-256:	2E07D45DE122788C2293FEAC29B025A1024C3559FFDF389A8263FD5C888F922F
SHA-512:	E1750FF23B33458F74F08AF95551E598581863832CAF6B1DC854B4AF0EE5E95FF217F7B7311F411ACB1A116777C1117B861A0B5F67F0274815386AFDE79B37D9
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1gALGD.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=535&y=265
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...fc.$.z`6..@.@....P...wj` ...q.,.@.0..@zT.54KU.....H.:..!.ljp;..1...-.....n.Y..Rv9..#9..&.D.40.6.C..... ...Q@.....H..... (.h.....Fo.&..0L...@...8...Y..Eq..M1.f^.\cs.. .....[W...'..S..&..R....o...D.rMM.*6MTX.*..s..i~j@M..d...E0.>..2=h.....L.....n...d.i....1....d..4.....h...V7.../U|.....OBi....u....a..`..v.....)(....J. X...1....*..40..*@k5!..H.74....CKb.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\BB1gBirh[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 206x250, frames 3
Category:	downloaded
Size (bytes):	8091
Entropy (8bit):	7.909776950175143
Encrypted:	false
SSDEEP:	192:QoT5UfTLN8VuF+n9fKqrCYxqkZN9dcyTI+lEdmB6:byf3mT9fDhLhk+lhU
MD5:	FF32BE9DE438EB84D185586FAFD4E875
SHA1:	8E3C078A4B47BC1E09EC2900DCE8EE7828AFA39F
SHA-256:	21A2415EB246A875CA7838F79B6617046D4DC0C2409CE8CDCFFDD820826A43E1
SHA-512:	3B9BF727908F0689A1FF866BFDD3D0D37CEB14E2DB8ABAFA68421FDEB5D7B90CF37EF93E96AAD07BD4C51FFD09863ACB0895E24EFDFED1F6A292EA22E3FCF 391
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1gBirh.img?h=250&w=206&m=6&q=60&u=t&o=t&l=f&f=jpg&x=458&y=252
Preview:	......JFIF.....`.`..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....v.p.....(.....u...(..).W..\.e...+L...d..g#...(.....b..(.1@...1@.....b...S..EY.....@....H...p....u.-0...,..i..c...P...#%.....(.....(.).P.h..... .....8P.. .(.....(...)..a...KA..:.?....r.T...,..zW..{.$C..R.]..r.8.zQ..%.*...(..A@.@.i.....q[...@....@...<P..!....L..E....Zl.{.P.!..!..u.9(..c.7dg.w.K!X`(...*.{.....u(.Eze.....Vm.vo...,D...H.}T ..q.}<R.w,...v..$i..,...#8=Ek

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\BB1gBjOT[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 311x333, frames 3
Category:	downloaded
Size (bytes):	14673
Entropy (8bit):	7.813570703195593
Encrypted:	false
SSDEEP:	384:NAnXwOWEtz7KWTUd6NEz6RvCOfmFH9YZD/FuY:N8XZWEtzRTUIEORvKywY
MD5:	D672D00AA568398073E487A9963BA33A
SHA1:	2AB4E3B71E1271D2291D22873425B037D1FAB005
SHA-256:	76417781A14BF70F3672C22A67E232E979BC17A23CC0EFFA2EB282EE4F6B7921
SHA-512:	F8F11DDCD50B47C8ED8B42636FE4F6C3E91CB8DDE07A59140853A3C79F6E63EB6703D4AD7CC48BDF9BF9367D8B5510C3E80971978C007AAB67C1FEF7ABD92 CF
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1gBjOT.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\2K7JPOQS\BB1gBjOT[1].jpg	
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....M.7.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..L.@....&(.q@...Z.Q@.@.....(.....4....4...J.(...4.....P...3@.h.h.h.....G..b..P.@.@.@..(....P.@.@.@..-.....4. 3@...3@X3@..`..&h.f...3@.h.....P...<P.@....b....P.@.@.@.@.....Z.3@.@..%...P.@.....@.@....(.h.h.E.-.(....Z..@.....Z.(..a@.@..-...P.....&h.....(.....(.. .@.@....P.....,W.A@.@.@.....(....@.....4.f..4.P.P.....@....P.@....P.@.@...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\BB1gvzoE[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):	68603
Entropy (8bit):	7.970500497235454
Encrypted:	false
SSDEEP:	1536:IQAhU/zNTmplmsfhcP8Hm/+JA/z23SMy6Hkls0dK:tAC/5mXmsJ4X/zedrHkrE
MD5:	D4C1DFF9112E9F21C2810B7ADA52131D
SHA1:	738FF1AE0DA7FFE0C10ABA04D4963B268C1A9036
SHA-256:	AC36D93E1348B4299AAB021DF06B7BEFDD954FC512BD633CB10B7EE98DA1E445
SHA-512:	386B2538507E32200012606CA9F6EBFBC3004A100DB430D3B4C5E2834FE304D4DED53BC9672F302D8D0D6AF60216E1F6BAA7D823708D43B42EE6D27D967A34B
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1gvzoE.img?h=368&w=622&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....p.n.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?...).*....0....#....2..w.2.%6..Z..p...e...;.2ih.Mwss!V.V5.....@.N;....B.N.k."....*...'...BMGQ.\...xdVQ._..I..C.I.:.....#....)E...-J [Y..$...F#..t...4_..k....>.".Kyp..y`t.z.jd..b..E.y.c.BK.q.(.3.....u$;.6..U..... .H..]U[K.....).V.....^.)s.I...{..1.J.^.:~TYE..<._|HK9..1.8.+...G-..C.....8.v.v.Y}....2E...p!s.....t.....v.c.....>YA. ..t...#;P..]>...\...}.k.)..8....AO..1Q+.lj-

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\BB1gzKxK[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):	2266
Entropy (8bit):	7.810577731541967
Encrypted:	false
SSDEEP:	48:QfAuETAFY+Hexi7y2wV7nTd4q7v4q8r4E1Ru/:Qf7EB+y2WTd98r4Cg/
MD5:	2C98FA94D5E5D5E2ACC3447D502487A4
SHA1:	FCE7A1949FE292162880EC0DB14F27CB844EB50A
SHA-256:	1E00D66BC4C9A4643C532F74AE4E53705568885013D2864C6BE4D2D05BE2D0D3
SHA-512:	82F2D534D00C09CBF41C436C1057004272D6773FDAF42D4D5B57B1526A2B9B4145B38E83A4DD40AE6C3541F28ED1DFF1439E154C38616DC8668E5E68E315AD7
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB1gzKxK.img?h=75&w=100&m=6&q=60&u=t&o=t&l=f&f=jpg
Preview:	......JFIF.....``..... .....'... .)10.)-,3:J>36F7,-@WAFLNRSR2>ZaZP`JQRO.....&..&O5-5OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO.....K.d.....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.../c....:U4.+....|...E..yyr~P2hz2..`.....-..a.....&..R...m8.....Y.....w}."KY.}J.?:v-.Gc.w.'..>^qL.Rrz.I ..A.c.....sV@.<\..+J ...u<..Zb;.K...A.G9.k..n.r..7.z..3...|.V..X..L..#.]NHa.Se.=.H.2[o..*|....O2%_..I;7.3.9.....H.....!...V.X.....3..._QJpK.1...,x=Ni.....3..a....#...B.....q.)..U.....]..\.&..{...:g.....q...w..H.#[.k. ..*....3...WYJ.9..)XW!...2..{.o.e.G.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\BB7gRE[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	482
Entropy (8bit):	7.256101581196474
Encrypted:	false
SSDEEP:	12:6v/78/kFLsiHAnE3oWxYZOjNO/wpc433jHgbc:zLeO/wc433Cc
MD5:	307888C0F03ED874ED5C1D0988888311
SHA1:	D6FB271D70665455A0928A93D2ABD9D9C0F4E309
SHA-256:	D59C8ADBE1776B26EB3A85630198D841F1A1B813D02A6D458AF19E9AAD07B29F
SHA-512:	6856C3AA0849E585954C3C30B4C9C992493F4E28E41D247C061264F1D1363C9D48DB2B9FA1319EA77204F55ADBD383EFEE7CF1DA97D5CBEAC27EC3EF36DEF 8E
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BB7gRE.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....sRGB.....gAMA.....a.....pHYs.....(J....wIDAT8O.RKN.0.}v\....U....-.. .....8..{$...z..@.....+.....K...%)...I.....C4.../XD].Y..:.w.....B9..7..Y.. (.m.*3. .!..p...,c.>.\<H.0.*...,w:.F..m...8c,.^.....E.....S...G.%.y.b....Ab.V.-.}.=..."m.O..!...q.....]N.)..w..\..v^.^...u...k..0.....R.....c!.N...DN`)x..:.."*Brg.0avY.>.h...C.S...Fqv._.].... ..E.h.|Wg..l.....@.$.Z.]....i8.$).t..y.W..H..H.W.8..B...'.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\BBPfCZL[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	GIF image data, version 89a, 50 x 50
Category:	downloaded
Size (bytes):	2313
Entropy (8bit):	7.594679301225926
Encrypted:	false
SSDEEP:	48:5Zvh21Zt5SkY33fS+PuSsgSrrVi7X3ZgMjkCqBn9VKg3dPnRd:vkrrS333q+PagKk7X3ZgaI9kMpRd
MD5:	59DAB7927838DE6A39856EED1495701B
SHA1:	A80734C857BFF8FF159C1879A041C6EA2329A1FA
SHA-256:	544BA9B5585B12B62B01C095633EFC953A7732A29CB1E941FDE5AD62AD462D57
SHA-512:	7D3FB1A5CC782E3C5047A6C5F14BF26DD39B8974962550193464B84A9B83B4C42FB38B19BD0CEF8247B78E3674F0C26F499DAFCF9AF780710221259D2625DB86
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBPfCZL.img?h=27&w=27&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	GIF89a2.2.....7..;..?..C..I..H..<..9.....8..F..7..E..@..C..@..6..9..8..J..*z.G..>..?..A..6..>..8..:..A..=..B..4..B..D..=..K..=..@..<..:..3~.B..D.....,|.4..2..6..:..J..;..G....Fl..1}.4..R.... .Y..E..>..9..5..X..A..2..P..J../|.9....T.+Z.....+..<.Fq.Gn..V..;..7.Lr..W..C..<.Fp.]......A.....0{.L..E..H..@.....3..3..O..M..K....#[.3i..D..>.....I....<n..;..Z..1..G..8..E....Hu..1..>.. T..a.Fs..C..8..0}...;..6..t.Ft..5.Bi..:.x...E.....'z^~.....[....8`.....;..@..B.....7.....<.....F.....6.....>..?.n.....g.....s...)a.Cm....'a.0Z..7....3f..<.:e.....@.q.....Ds..B....!P .n...J.....Li..=.....F.....B.....:r....w..|.....`..[}.g...J.Ms..K.Ft....'..>.....Ry.Nv.n..]..Bl.....S..;....Dj.....=.....O.y.....6..J.....)V..g..5.....!..NETSCAPE2.0.....!...d...,....2.2..... ..3.`..9.(|.d.C .wH.(."D...(D.....d.Y.....<.(PP.F...dL.@.&.28..$1S....*TP.....>...L..!T.X!.(..@a..IsgM..|..Jc(Q.+.....2.:.)y2.J.....W,..eW2.!....!....C.....d...zeh....P.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\BBRUB0d[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	489
Entropy (8bit):	7.208309014650151
Encrypted:	false
SSDEEP:	12:6v/7wmcW0JYErMXrLYTh/BBoqavcAccySLY:jmx0aaM7LYtTpaWcy4Y
MD5:	C090E4C7C513884E6B10030FCE2F2B37
SHA1:	2BE9AD7D8CE94A585F0EA58DBC0B0A9A9933E854
SHA-256:	C18187F3EF7089F6EA948C35797228FC4DFD3F90DBD2E78E531C6D2A92740471
SHA-512:	DA9A5F97B70845AECD6BA20F87DA7FC2D6947AC9E2CFBA299B402459CE5ED8A1AA918A140B11879038961A3FA6B986736813CD1707D05B4A1BB9C195F52005C E
Malicious:	false
IE Cache URL:	http://https://static-global-s-msn-com.akamaized.net/img-resizer/tenant/amp/entityid/BBRUB0d.img?h=16&w=16&m=6&q=60&u=t&o=t&l=f&f=png
Preview:	.PNG.....IHDR.....a....pHYs.....+.....IDATx.c.....B.^.V..0..2..D0...3.J.1|\w....].L.....Km...M...|gx^<.....7.5.....k.1(n.f.v...}.....3.1|.w.....%@gr2..Y.....0...? Q.Q\ ....m.....W./..(.q....D5 ..,.e.Y..?.aj..(.p.+...;u.....A..n.FFF0...;.wLRQ.D1...?...w .....p5..a.n.. .....=c.4Vg.q..\!..&...._.....a...>....?/.....lP..y....c...v.:..T_.69q..k..Y.x...jA...@ 1../.wm...&.....&..}.x..~.0.....j.....Bb.._.\.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\BBX2afX[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 27 x 27, 8-bit/color RGBA, non-interlaced
Category:	downloaded
Size (bytes):	879
Entropy (8bit):	7.684764008510229
Encrypted:	false
SSDEEP:	24:nbwTOG/D9S9kmVgvOc0WL9P9juX7wlA3lrvfFRNa:bwTOk5S96vBB1jGwO3lzfxa
MD5:	4AAAEC9CA6F651BE6C54B005E92EA928
SHA1:	7296EC91AC01A8C127CD5B032A26BBC0B64E1451
SHA-256:	90396DF05C94DD44E772B064FF77BC1E27B5025AB9C21CE748A717380D4620DD
SHA-512:	09E0DE84657F2E520645C6BE20452C1779F6B492F67F88ABC7AB062D563C060AE51FC1E99579184C274AC3805214B6061AEC1730F72A6445AEBDB7E9F255755F
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....pHYs.....+.....!IDATx...K.Q..wfv.u.....*.,I"...)...z.....>.OVObQ.....d?|.....F.QI$....qf.s.....">y`.....{~.6.Z.`.D[&.cV`..-8i...J.S.N..xf.6@.v.(E..S. ....&...T...?.X)${.....s.l."V..r...PJ*!..p.4b}.=2...[.....:.....LW3...A.eB.;...2...~...s_z.x|..o....+..x....KW.G2..9.....<.\....gv...n..1..0...1}....Ht_A.x...D..5.H.....W..$_\G.e;./.1R+v....j.6v... .....z.k.....&..(....,F.u8^..v...d-.j?.w..;..O.<9$..A..f.k.Kq9..N..p.rP2K.0.).X.4..Uh[..8..h....O..V.%.f.....G..U.m.6$.....X...../.=....f:.....\|c(,.....l.\..<./..6...!...z(.....# "S..f .Q.N=.0VQ._..\|....>@....P.7T.$./)s....Wy..8..xV.....D....8r."b@....:.E.E....._(....4w....Ir..e-5..zjg...e?./...|X..."!..'*/.....OI..J"I.MP....#...G.Vc..E..m.....wS.&.K<...K*q..\...A..$.K .....,...[..D...8.?..)..3....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\BBnYSFZ[1].png	
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\2K7JPOQS\DTABAP9Y.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):	440327
Entropy (8bit):	4.930628163442562
Encrypted:	false
SSDEEP:	6144:W7bopSwHnEOdznvGBeBotHUUlmzhy8a59CxmgfrSTtrft27sJCuZqOUNuYVEHnBQ:W7MO3qtk4
MD5:	4FEC052ECA7508D36DBDD2A294F831F8
SHA1:	E8BE268FD7C382B59F160C07EC933D490D9F7467
SHA-256:	02D40365F87238B669496FC7FCD0C2BC83A8CFA477B7C4EC66AF2674773CDB8E
SHA-512:	A6CC47E975A4DE5CD7AE7971B2E7BB9E3EE42FC4405EBD5D2B8C790745887372293908 0FCB6BB7EC8EEF85902D6125167D3BB92C5A028A0BF5CFC23568108B 1
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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\TEX0ICSG.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):	440971
Entropy (8bit):	4.927535027743115
Encrypted:	false
SSDEEP:	6144:uWdoFSwbnEOdznvGBeBotzq6WUUlmzSd59CxmgfrSTtrftA7sJC7ZqCUmuYVE/nB:uWxCeRtk4
MD5:	8B0F5BB8C0498C7A64CAABE36CD5B132
SHA1:	1E9F840FF6DB275BEF4DC229AE0FB3E8E8F7BB3D
SHA-256:	963E0F6E016BC687FAAC4A2B52685B4FBDB07A80F625AD84E58FA79F568267E2
SHA-512:	AB07D06D7930844EFCEBF45DE0A35B08CFCC75734260D714C07EA561D39092CDC0202D2072A3C70BC4FE6BF6664C44199F8F6D7F253250E7546F2416D329AFB
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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\ads_batch[1].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):	2524
Entropy (8bit):	5.969628867331106
Encrypted:	false
SSDEEP:	48:+AZCWgMHvLSbm4Ne+lvfyjE7pItDg7MWM/Mx7RN5O8yjE7pItDg9mqB:+HMPLWW+d6MItDg7WoU86MItDg9x
MD5:	3260F13B521939CF2757332F7A9398A5
SHA1:	8D22F4396FBBCFA2A33804C5F1CCE5D189F79087
SHA-256:	FC3E5D073F897812678F157AC53D7C0B71F999334BBF8D439C112C46F3BDF274
SHA-512:	2C63489E9F1081258086E273EF53564CE6885B3A5ED8B56214DE6D948ECB83BB31EE9EEE8C45333CE781CA015F603DE3B707AF3FAE229C0577ACB663698A573
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\ads_batch[1].json	
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=9ABD720B-760B-4B95-A7BB-3C7EF0B667B9&data=%5B%7B%22spots%22%3A%5B%7B%22zone%22%3A11531%7D%5D%7D%5D
Preview:	[{"ad_id":1042289131,"member_id":1001938571,"campaign_id":1005453111,"zone_id":11531,"media_type":"image","html":"","full_html":"<!DOCTYPE html>\n<html>\n\t<head>\n\t\t c_id=1005453111 z_id=\"11531\" ad_id=\"1491393291\"-->\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--></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=NVOaYAAAAACLXrg7EAAAAAstAAALLQAAAAAADf_7TsL2-RY6xEgPgvb5FgAAAAAWP58W7BUFz8AAAAA&cmp_id=1005453111&ct=wifi&geo=CH%257C%253A%257CZH%257C%253A%257CZurich&info=CiQyYjZjMDdhMi0yNmVmLTRjM2ItYWY1Ny1mYmYxNmU2NWE0MzUQtabphAYaJjQwMzMyNDlhLWI4NjktNDI0ZC1iZTYyLTQyZTM5OTcwOWI0ZC0xMItaOItaSLf%2Bt98DUgIxNliLveHdA2Dro4DxA3ITNzkxMTEzNzMyMzQ2OTI2NTM5MoEBW

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\ads_batch[2].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):	10487
Entropy (8bit):	5.458610180127543
Encrypted:	false
SSDEEP:	192:1xGNR/ruINPgy4QHnqpG2iNxPgy4QHnqpG2eyFruINPgy4QHnqpG2iNx3:1xuRj/YaqeyR/Yal
MD5:	642FB54BF958F93AFC5D9963DE7FCE73
SHA1:	337669829813FA6C7CEFE7D9C55B0648FC00CEB5
SHA-256:	F33C071155375143CD44A2D8047A0C6104D54406F1A13485EF80DBD918101CAD
SHA-512:	61C6F40FA5B1CC9292AAA636BF9E0920167A933E441BAFE7B54A4510F443B0ABB350A32AE4DEF3D4EC0683072925AECDD8A0A082A66CF77FE4A0D58AB681F51B
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=9ABD720B-760B-4B95-A7BB-3C7EF0B667B9&data=%5B%7B%22spots%22%3A%5B%7B%22zone%22%3A11571%7D%5D%7D%5D
Preview:	[{"ad_id":1418981851,"member_id":6766,"campaign_id":1003862321,"country_code":"CH","zone_id":"11571","link":"https://ads.trafficjunky.net/click?url=\u0026amp;click_data=QAAAAG4aAAA1U5pgAAAAAAAAAAAzLQAAMy0AAAAAAAAxudU72_GTVEH4wD1rr4JAAAAAAAEAAAAAAAAAAAAAAAA==\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=52_162072658156138646 4_10725_9316\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=0f9421342e82edf9969cc6252f52f23fdb407ae0","img_url":"https://eu-adsrv.rtbsuperhub.com/ir/?placement=1631_banner_950x250_DACH_desktop_Foot_RT_Flat","isdefault":0,"html":"\u003cHTML\u003e\u003cHEAD\u003e\u003cTITLE\u003eAd delivery system\u003c/TITLE\u003e\u003cmeta name=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\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):	21265
Entropy (8bit):	5.302037526120113
Encrypted:	false
SSDEEP:	384:2YAGcVXlblcqnzleZSweg2f5ngB/LkPF3OZOZQWwY4RXrqt:l86qhbS2RxF3OsZQWwY4RXrqt
MD5:	C89F7744ECC865A513D728318C7D58FA
SHA1:	985304188B0D17829D0BED5B5CA103D79CFFED37
SHA-256:	76E861943FC9EAC1B8C0892FBE5905DBE308BD9D7D2920CCE853FC63A393697E
SHA-512:	7CF7B34FB3B241E740D3904917F6B7D4EC857C4D44A92F2A8EF4314AD0341615BF17598FE8C6C0B8E7FA6B8EFB76D03AB8106756AF39C9821D2AB590F9CA17A
Malicious:	false
Preview:	<html> <head></head> <body> <script type="text/javascript">try{.var cookieSyncConfig = {"datalen":74,"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\2K7JPOQS\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):	79096
Entropy (8bit):	5.33782687971214
Encrypted:	false
SSDEEP:	768:olAy9XsiItnuy5zIux1whjCU7kJB1C54AYtiQzNEJEWlCxP5HVN/QZYUmftKCB:olLEJxa4CmdiuWlcxHga7B
MD5:	15BCB7BBE03E5ABCE3162F71DADD8D63
SHA1:	2EF0AB2CC332049F5C79A7E088BD877759E93993
SHA-256:	5004E4E24FE7DCD410FE6274C514A5E49984353512A1FB0F962812065C6A381B
SHA-512:	FBAE0225579AEAF527F22914C6AC758D2D70A7870F167142D5B004A018CC454FFFDB9B2001181429FEE24012553177D929DC3FDA0CB7BB870F649DCF75561333

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\de-ch[1].json	
Malicious:	false
IE Cache URL:	http://https://www.msn.com/_h/9c38ab9f/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\2K7JPOQS\default-redtube[1].css	
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):	81298
Entropy (8bit):	5.122579161600824
Encrypted:	false
SSDEEP:	1536:1VXorGHaV610Ax2/jr/CU/13/OI6AS/rMD76obNMh5fIlxVoQrv5gk:grG61
MD5:	E60E5077AB4E088ECD09F178CD1393CE
SHA1:	9FAF3FA6BD588D99803FFFDEFD156D97CC92E2AF
SHA-256:	4E836A3B177FBCD04B5B4CDDE6F16832ECF6AAAF02C1AFE2101F9CF059FC62CB
SHA-512:	AAB9A02F96D70A6CE5D5AD184A5AA830C4E33300EC7947F4D76006E695E00098124A7FC6440BBD1DAEC52E13734C3928E49258D3B6B0F804CAF6C9C3C1F5FFB
Malicious:	false
IE Cache URL:	http://https://ci.rdtcdn.com/www-static/cdn_files/redtube/css/generated/pc/default-redtube.css?v=c68764eb72df2fd284980d4794d31c91941b183c
Preview:	.rt_icon{font-family:rt_font!important;speak:never;font-style:normal;font-weight:400;font-variant:normal;text-transform:none;line-height:1;letter-spacing:0;-webkit-font-feature-settings:"liga";-moz-font-feature-settings:"liga=1";-moz-font-feature-settings:"liga";-ms-font-feature-settings:"liga" 1;font-feature-settings:"liga";-webkit-font-variant-ligatures:discretionary-ligatures;font-variant-ligatures:discretionary-ligatures;-webkit-font-smoothing:antialiased;-moz-osx-font-smoothing:grayscale}.rt_warning:before{content:"\e96a"}.rt_Channels_Active:before{content:"\e965"}.rt_Gay_PS_Active:before{content:"\e966"}.rt_Home_Active:before{content:"\e967"}.rt_PS_Active:before{content:"\e968"}.rt_Search_Active:before{content:"\e969"}.rt_gay_icon:before{content:"\e964"}.rt_shop:before{content:"\e963"}.rt_Seek_To:before{content:"\e960"}.rt_Seek_To_Small:before{content:"\e962"}.rt_library:before{content:"\e961"}.rt_Send_Message:before{content:"\e95f"}.rt_save:before{content:"\e95e"}.rt_Trending:be

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2K7JPOQS\default-redtube_logged_out[1].css	
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):	5933
Entropy (8bit):	4.978970495241967
Encrypted:	false
SSDEEP:	96:og06cSF9meBQgOhMk/UWMQbyNPKVhe+UlFPAVZzVINZO:o96cYm4BDZQONSDe17bO
MD5:	A2ABE3C0AC7D20144C90610C73121137
SHA1:	BB46952BA96BD8062D4AFFD57FC5BB53DBA2C13F
SHA-256:	329BE541A2F6C615EDD88631A58814EF29BE02BF8B571B305F0F5BB02E830854
SHA-512:	3469D45A06E7CB96315457D8AF8575FD1F8FF86D5DD5EA2D6FBA53E6DC6A21CAF559C504735DD74D85D4AF922B6198B8DAE200BAAF0CFAB793A18A179F95BB44
Malicious:	false
IE Cache URL:	http://https://ci.rdtcdn.com/www-static/cdn_files/redtube/css/generated/pc/default-redtube_logged_out.css?v=c68764eb72df2fd284980d4794d31c91941b183c
Preview:	#login_form_container .main_heading{color:#fff;text-align:center;font-weight:700;margin:0 0 20px;font-size:2.5em;letter-spacing:1px}#login_form_container .login_or_delimiter{text-transform:uppercase;text-align:center;margin-top:25px;font-size:1em;font-weight:700;color:#999}#login_form_container .sign_up_text{clear:both;display:block;overflow:hidden;margin:10px 0 0;padding:25px 0 0;border-top:solid 1px #444}#login_form_container .sign_up_text .sign_up_title{display:block;overflow:hidden;margin-bottom:20px;text-align:center;font-size:1.65em;font-weight:700;color:#999}#login_form_container .sign_up_text .sign_up_btn{display:block;width:100%;height:40px;overflow:hidden;line-height:38px;color:#fff;font-size:1.166em;text-align:center;text-transform:uppercase;font-weight:700;letter-spacing:.5px;background-color:#3c3c3c;border:none;border-radius:4px}#login_form_container .sign_up_text .sign_up_btn:hover{background-color:#505050}#login_form_container{overflow:hidden;width:93%;padding:0}#login_f

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.080434293790918

General

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:	FuiZSHt8Hx.dll
File size:	61440
MD5:	c4c0b19091c6edd5fd46867caf99026d
SHA1:	5b1dbdbab64ebcb665e91d442a847cc3a9552a38
SHA256:	821f1b68c207b41e21b519610931ce46719307d99e3e8a eb397ac720d870b476
SHA512:	3d017883a412f3e813b3c83d1acc326c6bb598b7b87604 368ad3e651909a1de4391b458021e342c630802774cce9 3907d61bedd9f092d0dea8b212fdb1371e41
SSDEEP:	768:JmKbkq07vrxPpdGvmlwblv4NZx+ab03qTwlVaj1eY qFN35zLRUfAf:JmKbn0vJpdUmwb+NfwrIcYqFJ5zLRU o
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....S>.n._.= ._.=._.='.=._.='.=._.=._.=f_.=.P.=._.=.P.=._.=.P.=._.='.= ._.='.=._.='.=._.=Rich._.=.....PE..L.....`.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x70991f56
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x70990000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x6092DEFF [Wed May 5 18:07:59 2021 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:	6e9163c62b29a1ccabed40ce8621a95a

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
push ecx
mov eax, dword ptr [ebp+0Ch]
push ebx
push esi
push edi
xor edi, edi
inc edi
xor ebx, ebx
sub eax, ebx
mov dword ptr [ebp-04h], edi
je 00007FEF1C875F51h
dec eax

Instruction
jne 00007FEF1C875F9Bh
push 70994108h
call dword ptr [7099304Ch]
cmp eax, edi
jne 00007FEF1C875F88h
push ebx
push 00400000h
push ebx
call dword ptr [70993034h]
mov dword ptr [70994110h], eax
cmp eax, ebx
je 00007FEF1C875F1Ch
mov eax, dword ptr [ebp+08h]
mov esi, 70994118h
mov dword ptr [70994130h], eax
mov eax, esi
lock xadd dword ptr [eax], edi
mov ecx, dword ptr [ebp+10h]
lea eax, dword ptr [ebp+0Ch]
push eax
call 00007FEF1C875B98h
push eax
push 7099173Dh
call 00007FEF1C8756BBh
mov dword ptr [7099410Ch], eax
cmp eax, ebx
jne 00007FEF1C875F3Bh
or eax, FFFFFFFFh
lock xadd dword ptr [esi], eax
mov dword ptr [ebp-04h], ebx
jmp 00007FEF1C875F2Fh
push 70994108h
call dword ptr [70993048h]
test eax, eax
jne 00007FEF1C875F20h
cmp dword ptr [7099410Ch], ebx
je 00007FEF1C875F0Ch
mov esi, 00002328h
push edi
push 00000064h
call dword ptr [70993040h]
mov eax, dword ptr [70994118h]
test eax, eax
je 00007FEF1C875EE9h
sub esi, 64h
cmp esi, ebx
jnle 00007FEF1C875EC9h
push dword ptr [7099410Ch]
call dword ptr [70993018h]
push dword ptr [00000000h]

Rich Headers

Programming Language:	• [ASM] VS2008 SP1 build 30729 • [LNK] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729 • [EXP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x3570	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x311c	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6000	0x150	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x3000	0xc0	.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	0x15c7	0x1600	False	0.733309659091	data	6.60256403131	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x3000	0x5c0	0x600	False	0.634765625	data	5.46311630617	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x4000	0x1dc	0x200	False	0.091796875	data	0.420971943134	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.bss	0x5000	0x2dc	0x400	False	0.759765625	data	6.299194261	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0x6000	0x9000	0x8400	False	0.975497159091	data	7.88576942103	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Imports

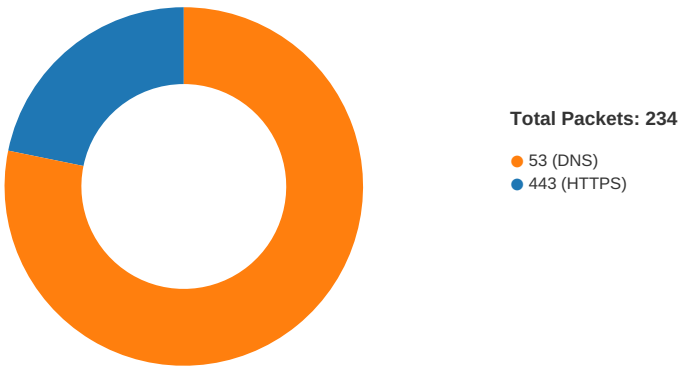
DLL	Import
KERNEL32.dll	HeapAlloc, HeapFree, Sleep, ExitThread, CloseHandle, GetLastError, GetExitCodeThread, GetSystemTime, SwitchToThread, SetThreadAffinityMask, SetThreadPriority, HeapCreate, HeapDestroy, GetCurrentThread, SleepEx, WaitForSingleObject, InterlockedDecrement, InterlockedIncrement, lstrlenW, VirtualProtect, GetModuleFileNameW, SetLastError, GetModuleHandleA, OpenProcess, CreateEventA, GetLongPathNameW, GetVersion, GetCurrentProcessId, TerminateThread, QueueUserAPC, CreateThread, GetProcAddress, LoadLibraryA, VirtualFree, VirtualAlloc, MapViewOfFile, GetSystemTimeAsFileTime, CreateFileMappingW
ntdll.dll	_snwprintf, memset, memcpy, _aulldiv, RtlUnwind, NtQueryVirtualMemory
ADVAPI32.dll	ConvertStringSecurityDescriptorToSecurityDescriptorA

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x70991787

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 11:48:19.900818110 CEST	49718	443	192.168.2.7	104.20.184.68
May 11, 2021 11:48:19.901153088 CEST	49719	443	192.168.2.7	104.20.184.68
May 11, 2021 11:48:19.942512989 CEST	443	49718	104.20.184.68	192.168.2.7
May 11, 2021 11:48:19.942641973 CEST	443	49719	104.20.184.68	192.168.2.7
May 11, 2021 11:48:19.942660093 CEST	49718	443	192.168.2.7	104.20.184.68
May 11, 2021 11:48:19.942727089 CEST	49719	443	192.168.2.7	104.20.184.68
May 11, 2021 11:48:19.950500965 CEST	49718	443	192.168.2.7	104.20.184.68
May 11, 2021 11:48:19.951575041 CEST	49719	443	192.168.2.7	104.20.184.68
May 11, 2021 11:48:19.992058992 CEST	443	49718	104.20.184.68	192.168.2.7
May 11, 2021 11:48:19.992790937 CEST	443	49718	104.20.184.68	192.168.2.7
May 11, 2021 11:48:19.992811918 CEST	443	49718	104.20.184.68	192.168.2.7
May 11, 2021 11:48:19.992896080 CEST	49718	443	192.168.2.7	104.20.184.68
May 11, 2021 11:48:19.992933035 CEST	49718	443	192.168.2.7	104.20.184.68
May 11, 2021 11:48:19.993127108 CEST	443	49719	104.20.184.68	192.168.2.7
May 11, 2021 11:48:19.994163990 CEST	443	49719	104.20.184.68	192.168.2.7
May 11, 2021 11:48:19.994271994 CEST	49719	443	192.168.2.7	104.20.184.68
May 11, 2021 11:48:19.994335890 CEST	443	49719	104.20.184.68	192.168.2.7
May 11, 2021 11:48:19.994469881 CEST	49719	443	192.168.2.7	104.20.184.68
May 11, 2021 11:48:20.004066944 CEST	49718	443	192.168.2.7	104.20.184.68
May 11, 2021 11:48:20.004523039 CEST	49718	443	192.168.2.7	104.20.184.68
May 11, 2021 11:48:20.004762888 CEST	49718	443	192.168.2.7	104.20.184.68
May 11, 2021 11:48:20.010907888 CEST	49719	443	192.168.2.7	104.20.184.68
May 11, 2021 11:48:20.011524916 CEST	49719	443	192.168.2.7	104.20.184.68
May 11, 2021 11:48:20.047487020 CEST	443	49718	104.20.184.68	192.168.2.7
May 11, 2021 11:48:20.047516108 CEST	443	49718	104.20.184.68	192.168.2.7
May 11, 2021 11:48:20.047528028 CEST	443	49718	104.20.184.68	192.168.2.7
May 11, 2021 11:48:20.047544003 CEST	443	49718	104.20.184.68	192.168.2.7
May 11, 2021 11:48:20.047559023 CEST	443	49718	104.20.184.68	192.168.2.7
May 11, 2021 11:48:20.047574997 CEST	443	49718	104.20.184.68	192.168.2.7
May 11, 2021 11:48:20.047630072 CEST	49718	443	192.168.2.7	104.20.184.68
May 11, 2021 11:48:20.047692060 CEST	49718	443	192.168.2.7	104.20.184.68
May 11, 2021 11:48:20.049963951 CEST	49718	443	192.168.2.7	104.20.184.68
May 11, 2021 11:48:20.052037954 CEST	443	49719	104.20.184.68	192.168.2.7
May 11, 2021 11:48:20.053337097 CEST	443	49719	104.20.184.68	192.168.2.7
May 11, 2021 11:48:20.053361893 CEST	443	49719	104.20.184.68	192.168.2.7
May 11, 2021 11:48:20.053379059 CEST	443	49719	104.20.184.68	192.168.2.7
May 11, 2021 11:48:20.053476095 CEST	49719	443	192.168.2.7	104.20.184.68
May 11, 2021 11:48:20.053582907 CEST	443	49719	104.20.184.68	192.168.2.7
May 11, 2021 11:48:20.053646088 CEST	49719	443	192.168.2.7	104.20.184.68
May 11, 2021 11:48:20.054609060 CEST	49719	443	192.168.2.7	104.20.184.68
May 11, 2021 11:48:20.061202049 CEST	443	49718	104.20.184.68	192.168.2.7
May 11, 2021 11:48:20.061223984 CEST	443	49718	104.20.184.68	192.168.2.7
May 11, 2021 11:48:20.061326981 CEST	49718	443	192.168.2.7	104.20.184.68
May 11, 2021 11:48:20.091568947 CEST	443	49718	104.20.184.68	192.168.2.7
May 11, 2021 11:48:20.098798037 CEST	443	49719	104.20.184.68	192.168.2.7
May 11, 2021 11:48:24.945503950 CEST	49734	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:24.947627068 CEST	49735	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:24.955146074 CEST	49736	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:24.955924034 CEST	49738	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:24.955971956 CEST	49739	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:24.956782103 CEST	49737	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:24.989047050 CEST	443	49734	151.101.1.44	192.168.2.7
May 11, 2021 11:48:24.989154100 CEST	49734	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:24.991137028 CEST	443	49735	151.101.1.44	192.168.2.7
May 11, 2021 11:48:24.991305113 CEST	49735	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:24.998559952 CEST	49735	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:24.998594999 CEST	443	49736	151.101.1.44	192.168.2.7
May 11, 2021 11:48:24.999190092 CEST	443	49738	151.101.1.44	192.168.2.7
May 11, 2021 11:48:24.999208927 CEST	443	49739	151.101.1.44	192.168.2.7
May 11, 2021 11:48:24.999320984 CEST	49738	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:24.999466896 CEST	49736	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:24.999471903 CEST	49739	443	192.168.2.7	151.101.1.44

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 11:48:24.999491930 CEST	49736	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:25.000143051 CEST	443	49737	151.101.1.44	192.168.2.7
May 11, 2021 11:48:25.000308037 CEST	49734	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:25.001029015 CEST	49737	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:25.003592014 CEST	49738	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:25.004776955 CEST	49739	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:25.007494926 CEST	49737	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:25.042047977 CEST	443	49735	151.101.1.44	192.168.2.7
May 11, 2021 11:48:25.042646885 CEST	443	49736	151.101.1.44	192.168.2.7
May 11, 2021 11:48:25.043327093 CEST	443	49735	151.101.1.44	192.168.2.7
May 11, 2021 11:48:25.043363094 CEST	443	49735	151.101.1.44	192.168.2.7
May 11, 2021 11:48:25.043406963 CEST	443	49735	151.101.1.44	192.168.2.7
May 11, 2021 11:48:25.043426037 CEST	49735	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:25.043482065 CEST	49735	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:25.043570042 CEST	443	49734	151.101.1.44	192.168.2.7
May 11, 2021 11:48:25.045162916 CEST	443	49736	151.101.1.44	192.168.2.7
May 11, 2021 11:48:25.045197964 CEST	443	49736	151.101.1.44	192.168.2.7
May 11, 2021 11:48:25.045233965 CEST	443	49736	151.101.1.44	192.168.2.7
May 11, 2021 11:48:25.045310020 CEST	49736	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:25.045439959 CEST	49736	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:25.045680046 CEST	443	49734	151.101.1.44	192.168.2.7
May 11, 2021 11:48:25.045705080 CEST	443	49734	151.101.1.44	192.168.2.7
May 11, 2021 11:48:25.045738935 CEST	443	49734	151.101.1.44	192.168.2.7
May 11, 2021 11:48:25.045780897 CEST	49734	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:25.045804024 CEST	49734	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:25.046879053 CEST	443	49738	151.101.1.44	192.168.2.7
May 11, 2021 11:48:25.048006058 CEST	443	49739	151.101.1.44	192.168.2.7
May 11, 2021 11:48:25.048281908 CEST	443	49738	151.101.1.44	192.168.2.7
May 11, 2021 11:48:25.048913956 CEST	49738	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:25.048948050 CEST	443	49738	151.101.1.44	192.168.2.7
May 11, 2021 11:48:25.048978090 CEST	443	49738	151.101.1.44	192.168.2.7
May 11, 2021 11:48:25.049009085 CEST	49738	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:25.049038887 CEST	49738	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:25.049583912 CEST	443	49739	151.101.1.44	192.168.2.7
May 11, 2021 11:48:25.049614906 CEST	443	49739	151.101.1.44	192.168.2.7
May 11, 2021 11:48:25.049635887 CEST	443	49739	151.101.1.44	192.168.2.7
May 11, 2021 11:48:25.049679041 CEST	49739	443	192.168.2.7	151.101.1.44
May 11, 2021 11:48:25.049717903 CEST	49739	443	192.168.2.7	151.101.1.44

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 11:48:05.515767097 CEST	57820	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:05.575767994 CEST	53	57820	8.8.8.8	192.168.2.7
May 11, 2021 11:48:06.042366982 CEST	50848	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:06.099658012 CEST	53	50848	8.8.8.8	192.168.2.7
May 11, 2021 11:48:06.128201962 CEST	61242	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:06.200606108 CEST	53	61242	8.8.8.8	192.168.2.7
May 11, 2021 11:48:07.469295979 CEST	58562	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:07.518060923 CEST	53	58562	8.8.8.8	192.168.2.7
May 11, 2021 11:48:08.462354898 CEST	56590	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:08.511287928 CEST	53	56590	8.8.8.8	192.168.2.7
May 11, 2021 11:48:09.283772945 CEST	60501	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:09.335341930 CEST	53	60501	8.8.8.8	192.168.2.7
May 11, 2021 11:48:09.785077095 CEST	53775	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:09.846678019 CEST	53	53775	8.8.8.8	192.168.2.7
May 11, 2021 11:48:10.122539043 CEST	51837	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:10.175800085 CEST	53	51837	8.8.8.8	192.168.2.7
May 11, 2021 11:48:11.188945055 CEST	55411	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:11.239289045 CEST	53	55411	8.8.8.8	192.168.2.7
May 11, 2021 11:48:12.312479019 CEST	63668	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:12.362396955 CEST	53	63668	8.8.8.8	192.168.2.7
May 11, 2021 11:48:13.179302931 CEST	54640	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:14.186292887 CEST	54640	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 11:48:14.234968901 CEST	53	54640	8.8.8.8	192.168.2.7
May 11, 2021 11:48:15.274317980 CEST	58739	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:15.336442947 CEST	53	58739	8.8.8.8	192.168.2.7
May 11, 2021 11:48:15.898458958 CEST	60338	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:15.948545933 CEST	53	60338	8.8.8.8	192.168.2.7
May 11, 2021 11:48:16.697977066 CEST	58717	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:16.765043974 CEST	53	58717	8.8.8.8	192.168.2.7
May 11, 2021 11:48:16.971445084 CEST	59762	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:17.022883892 CEST	53	59762	8.8.8.8	192.168.2.7
May 11, 2021 11:48:17.500029087 CEST	54329	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:17.524149895 CEST	58052	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:17.550086975 CEST	53	54329	8.8.8.8	192.168.2.7
May 11, 2021 11:48:17.590352058 CEST	53	58052	8.8.8.8	192.168.2.7
May 11, 2021 11:48:18.589284897 CEST	54008	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:18.638115883 CEST	53	54008	8.8.8.8	192.168.2.7
May 11, 2021 11:48:19.431925058 CEST	59451	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:19.502326965 CEST	53	59451	8.8.8.8	192.168.2.7
May 11, 2021 11:48:19.835427046 CEST	52914	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:19.888895035 CEST	53	52914	8.8.8.8	192.168.2.7
May 11, 2021 11:48:19.948782921 CEST	64569	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:20.020838022 CEST	53	64569	8.8.8.8	192.168.2.7
May 11, 2021 11:48:20.053296089 CEST	52816	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:20.102035046 CEST	53	52816	8.8.8.8	192.168.2.7
May 11, 2021 11:48:21.093310118 CEST	50781	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:21.143675089 CEST	53	50781	8.8.8.8	192.168.2.7
May 11, 2021 11:48:21.594712019 CEST	54230	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:21.662158966 CEST	53	54230	8.8.8.8	192.168.2.7
May 11, 2021 11:48:21.674173117 CEST	54911	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:21.747256041 CEST	53	54911	8.8.8.8	192.168.2.7
May 11, 2021 11:48:22.661957979 CEST	49958	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:22.713418961 CEST	53	49958	8.8.8.8	192.168.2.7
May 11, 2021 11:48:22.737883091 CEST	50860	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:22.796694040 CEST	53	50860	8.8.8.8	192.168.2.7
May 11, 2021 11:48:23.424263954 CEST	50452	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:23.477477074 CEST	53	50452	8.8.8.8	192.168.2.7
May 11, 2021 11:48:23.770593882 CEST	59730	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:23.819427013 CEST	53	59730	8.8.8.8	192.168.2.7
May 11, 2021 11:48:24.890393972 CEST	59310	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:24.943361044 CEST	53	59310	8.8.8.8	192.168.2.7
May 11, 2021 11:48:25.302781105 CEST	51919	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:25.354232073 CEST	53	51919	8.8.8.8	192.168.2.7
May 11, 2021 11:48:26.477257967 CEST	64296	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:26.525897026 CEST	53	64296	8.8.8.8	192.168.2.7
May 11, 2021 11:48:27.716655016 CEST	56680	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:27.765460014 CEST	53	56680	8.8.8.8	192.168.2.7
May 11, 2021 11:48:29.071470022 CEST	58820	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:29.137907982 CEST	53	58820	8.8.8.8	192.168.2.7
May 11, 2021 11:48:29.570048094 CEST	60983	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:29.620920897 CEST	53	60983	8.8.8.8	192.168.2.7
May 11, 2021 11:48:31.540412903 CEST	49247	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:31.589129925 CEST	53	49247	8.8.8.8	192.168.2.7
May 11, 2021 11:48:33.114415884 CEST	52286	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:33.176116943 CEST	53	52286	8.8.8.8	192.168.2.7
May 11, 2021 11:48:33.992742062 CEST	56064	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:34.049751043 CEST	53	56064	8.8.8.8	192.168.2.7
May 11, 2021 11:48:41.288872004 CEST	63744	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:41.340394974 CEST	53	63744	8.8.8.8	192.168.2.7
May 11, 2021 11:48:42.302978039 CEST	61457	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:42.362421036 CEST	53	61457	8.8.8.8	192.168.2.7
May 11, 2021 11:48:43.895694971 CEST	58367	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:43.947530985 CEST	53	58367	8.8.8.8	192.168.2.7
May 11, 2021 11:48:45.297282934 CEST	60599	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:45.347635984 CEST	53	60599	8.8.8.8	192.168.2.7
May 11, 2021 11:48:46.130197048 CEST	59571	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 11:48:46.197737932 CEST	53	59571	8.8.8.8	192.168.2.7
May 11, 2021 11:48:46.298028946 CEST	60599	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:46.346760988 CEST	53	60599	8.8.8.8	192.168.2.7
May 11, 2021 11:48:46.462778091 CEST	52689	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:46.511580944 CEST	53	52689	8.8.8.8	192.168.2.7
May 11, 2021 11:48:47.346554995 CEST	60599	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:47.397449970 CEST	53	60599	8.8.8.8	192.168.2.7
May 11, 2021 11:48:47.728918076 CEST	52689	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:47.786602020 CEST	53	52689	8.8.8.8	192.168.2.7
May 11, 2021 11:48:48.738404036 CEST	52689	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:48.787695885 CEST	53	52689	8.8.8.8	192.168.2.7
May 11, 2021 11:48:49.220812082 CEST	50290	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:49.272397041 CEST	53	50290	8.8.8.8	192.168.2.7
May 11, 2021 11:48:49.392168999 CEST	60599	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:49.440896034 CEST	53	60599	8.8.8.8	192.168.2.7
May 11, 2021 11:48:49.819717884 CEST	60427	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:49.881705046 CEST	53	60427	8.8.8.8	192.168.2.7
May 11, 2021 11:48:50.094355106 CEST	56209	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:50.143126011 CEST	53	56209	8.8.8.8	192.168.2.7
May 11, 2021 11:48:50.782052040 CEST	52689	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:50.830884933 CEST	53	52689	8.8.8.8	192.168.2.7
May 11, 2021 11:48:53.442481995 CEST	60599	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:53.491590977 CEST	53	60599	8.8.8.8	192.168.2.7
May 11, 2021 11:48:54.213079929 CEST	59582	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:54.261889935 CEST	53	59582	8.8.8.8	192.168.2.7
May 11, 2021 11:48:54.793625116 CEST	60949	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:54.829313993 CEST	52689	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:54.842464924 CEST	53	60949	8.8.8.8	192.168.2.7
May 11, 2021 11:48:54.878185034 CEST	53	52689	8.8.8.8	192.168.2.7
May 11, 2021 11:48:55.045588970 CEST	58542	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:55.094230890 CEST	53	58542	8.8.8.8	192.168.2.7
May 11, 2021 11:48:57.040481091 CEST	59179	53	192.168.2.7	8.8.8.8
May 11, 2021 11:48:57.092089891 CEST	53	59179	8.8.8.8	192.168.2.7
May 11, 2021 11:49:00.815654039 CEST	60927	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:00.873512983 CEST	53	60927	8.8.8.8	192.168.2.7
May 11, 2021 11:49:00.959832907 CEST	57854	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:01.017492056 CEST	53	57854	8.8.8.8	192.168.2.7
May 11, 2021 11:49:07.444122076 CEST	62026	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:07.465312004 CEST	59453	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:07.514158964 CEST	53	59453	8.8.8.8	192.168.2.7
May 11, 2021 11:49:07.517314911 CEST	53	62026	8.8.8.8	192.168.2.7
May 11, 2021 11:49:08.104397058 CEST	62468	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:08.171678066 CEST	53	62468	8.8.8.8	192.168.2.7
May 11, 2021 11:49:08.190121889 CEST	52563	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:08.247298956 CEST	53	52563	8.8.8.8	192.168.2.7
May 11, 2021 11:49:08.375240088 CEST	54721	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:08.424179077 CEST	53	54721	8.8.8.8	192.168.2.7
May 11, 2021 11:49:12.645114899 CEST	62826	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:12.718048096 CEST	53	62826	8.8.8.8	192.168.2.7
May 11, 2021 11:49:17.592077017 CEST	62046	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:17.649398088 CEST	53	62046	8.8.8.8	192.168.2.7
May 11, 2021 11:49:31.200529099 CEST	51223	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:31.211865902 CEST	63908	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:31.261517048 CEST	53	51223	8.8.8.8	192.168.2.7
May 11, 2021 11:49:31.281362057 CEST	53	63908	8.8.8.8	192.168.2.7
May 11, 2021 11:49:31.436405897 CEST	49226	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:31.486903906 CEST	53	49226	8.8.8.8	192.168.2.7
May 11, 2021 11:49:31.986469030 CEST	60212	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:31.989778996 CEST	50864	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:31.991530895 CEST	58867	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:31.992479086 CEST	61504	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:32.007776976 CEST	60231	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:32.038800001 CEST	53	50864	8.8.8.8	192.168.2.7
May 11, 2021 11:49:32.041726112 CEST	53	61504	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 11:49:32.056627035 CEST	53	60231	8.8.8.8	192.168.2.7
May 11, 2021 11:49:32.109338045 CEST	50095	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:32.158049107 CEST	53	50095	8.8.8.8	192.168.2.7
May 11, 2021 11:49:32.277290106 CEST	53	58867	8.8.8.8	192.168.2.7
May 11, 2021 11:49:32.278726101 CEST	53	60212	8.8.8.8	192.168.2.7
May 11, 2021 11:49:32.622436047 CEST	59654	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:32.694293022 CEST	53	59654	8.8.8.8	192.168.2.7
May 11, 2021 11:49:32.770766020 CEST	58233	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:32.819425106 CEST	53	58233	8.8.8.8	192.168.2.7
May 11, 2021 11:49:33.401367903 CEST	56822	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:33.449980021 CEST	53	56822	8.8.8.8	192.168.2.7
May 11, 2021 11:49:33.752947092 CEST	62572	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:33.755048037 CEST	57179	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:33.761636972 CEST	56124	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:33.772862911 CEST	62287	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:33.822824001 CEST	53	62572	8.8.8.8	192.168.2.7
May 11, 2021 11:49:33.823712111 CEST	53	62287	8.8.8.8	192.168.2.7
May 11, 2021 11:49:33.831100941 CEST	53	57179	8.8.8.8	192.168.2.7
May 11, 2021 11:49:34.049549103 CEST	53	56124	8.8.8.8	192.168.2.7
May 11, 2021 11:49:35.399615049 CEST	54644	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:35.467108011 CEST	53	54644	8.8.8.8	192.168.2.7
May 11, 2021 11:49:35.720659018 CEST	59159	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:35.784024954 CEST	53	59159	8.8.8.8	192.168.2.7
May 11, 2021 11:49:35.966732025 CEST	57924	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:36.019480944 CEST	53	57924	8.8.8.8	192.168.2.7
May 11, 2021 11:49:36.889739037 CEST	51712	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:36.894444942 CEST	58865	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:36.908502102 CEST	64337	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:36.938515902 CEST	53	51712	8.8.8.8	192.168.2.7
May 11, 2021 11:49:36.957369089 CEST	53	64337	8.8.8.8	192.168.2.7
May 11, 2021 11:49:36.962465048 CEST	53	58865	8.8.8.8	192.168.2.7
May 11, 2021 11:49:37.049813032 CEST	50407	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:37.111428022 CEST	53	50407	8.8.8.8	192.168.2.7
May 11, 2021 11:49:37.717082024 CEST	61075	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:37.777355909 CEST	53	61075	8.8.8.8	192.168.2.7
May 11, 2021 11:49:38.487852097 CEST	54952	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:38.504393101 CEST	59186	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:38.536997080 CEST	53	54952	8.8.8.8	192.168.2.7
May 11, 2021 11:49:38.553560972 CEST	53	59186	8.8.8.8	192.168.2.7
May 11, 2021 11:49:38.752567053 CEST	52280	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:38.768923044 CEST	51794	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:38.801434040 CEST	53	52280	8.8.8.8	192.168.2.7
May 11, 2021 11:49:39.054255009 CEST	53	51794	8.8.8.8	192.168.2.7
May 11, 2021 11:49:40.683099985 CEST	50815	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:40.743920088 CEST	53	50815	8.8.8.8	192.168.2.7
May 11, 2021 11:49:40.926469088 CEST	58498	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:40.975166082 CEST	53	58498	8.8.8.8	192.168.2.7
May 11, 2021 11:49:41.519208908 CEST	56862	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:41.521142960 CEST	61807	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:41.521658897 CEST	52009	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:41.573271990 CEST	53	56862	8.8.8.8	192.168.2.7
May 11, 2021 11:49:41.573431969 CEST	53	52009	8.8.8.8	192.168.2.7
May 11, 2021 11:49:41.581955910 CEST	53	61807	8.8.8.8	192.168.2.7
May 11, 2021 11:49:41.730592012 CEST	58648	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:41.796046019 CEST	53	58648	8.8.8.8	192.168.2.7
May 11, 2021 11:49:42.406912088 CEST	59337	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:42.455703020 CEST	53	59337	8.8.8.8	192.168.2.7
May 11, 2021 11:49:42.460452080 CEST	59269	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:42.490129948 CEST	49802	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:42.509357929 CEST	53	59269	8.8.8.8	192.168.2.7
May 11, 2021 11:49:42.553545952 CEST	53	49802	8.8.8.8	192.168.2.7
May 11, 2021 11:49:42.704149961 CEST	50706	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:42.757795095 CEST	53	50706	8.8.8.8	192.168.2.7
May 11, 2021 11:49:45.295389891 CEST	55153	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 11:49:45.354449987 CEST	53	55153	8.8.8.8	192.168.2.7
May 11, 2021 11:49:53.374280930 CEST	59744	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:53.432423115 CEST	53	59744	8.8.8.8	192.168.2.7
May 11, 2021 11:49:53.587825060 CEST	59987	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:53.639441967 CEST	53	59987	8.8.8.8	192.168.2.7
May 11, 2021 11:49:54.066752911 CEST	61272	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:54.067255020 CEST	54352	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:54.069013119 CEST	60696	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:54.116395950 CEST	53	54352	8.8.8.8	192.168.2.7
May 11, 2021 11:49:54.116430998 CEST	53	61272	8.8.8.8	192.168.2.7
May 11, 2021 11:49:54.120568037 CEST	53	60696	8.8.8.8	192.168.2.7
May 11, 2021 11:49:54.172590017 CEST	59139	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:54.229785919 CEST	53	59139	8.8.8.8	192.168.2.7
May 11, 2021 11:49:54.718347073 CEST	59565	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:54.775541067 CEST	56397	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:54.775674105 CEST	53	59565	8.8.8.8	192.168.2.7
May 11, 2021 11:49:54.825416088 CEST	53	56397	8.8.8.8	192.168.2.7
May 11, 2021 11:49:54.956393003 CEST	52818	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:54.992247105 CEST	54236	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:55.004951954 CEST	53	52818	8.8.8.8	192.168.2.7
May 11, 2021 11:49:55.015211105 CEST	54698	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:55.058893919 CEST	53	54236	8.8.8.8	192.168.2.7
May 11, 2021 11:49:55.064198017 CEST	53	54698	8.8.8.8	192.168.2.7
May 11, 2021 11:49:55.231564999 CEST	58468	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:55.233953953 CEST	58290	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:55.266335964 CEST	54102	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:55.283153057 CEST	53	58468	8.8.8.8	192.168.2.7
May 11, 2021 11:49:55.285373926 CEST	53	58290	8.8.8.8	192.168.2.7
May 11, 2021 11:49:55.318046093 CEST	53	54102	8.8.8.8	192.168.2.7
May 11, 2021 11:49:55.721441031 CEST	55822	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:55.726994991 CEST	64562	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:55.742913008 CEST	61557	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:55.772910118 CEST	53	55822	8.8.8.8	192.168.2.7
May 11, 2021 11:49:55.784446955 CEST	53	64562	8.8.8.8	192.168.2.7
May 11, 2021 11:49:55.791635990 CEST	53	61557	8.8.8.8	192.168.2.7
May 11, 2021 11:49:55.831645012 CEST	54375	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:55.891700029 CEST	53	54375	8.8.8.8	192.168.2.7
May 11, 2021 11:49:56.166451931 CEST	49821	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:56.216947079 CEST	53	49821	8.8.8.8	192.168.2.7
May 11, 2021 11:49:56.250067949 CEST	54012	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:56.253499985 CEST	63684	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:56.270965099 CEST	62912	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:56.300575972 CEST	53	54012	8.8.8.8	192.168.2.7
May 11, 2021 11:49:56.305774927 CEST	53	63684	8.8.8.8	192.168.2.7
May 11, 2021 11:49:56.322490931 CEST	53	62912	8.8.8.8	192.168.2.7
May 11, 2021 11:49:56.494143009 CEST	60804	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:56.511223078 CEST	60139	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:56.559899092 CEST	53	60139	8.8.8.8	192.168.2.7
May 11, 2021 11:49:56.780894041 CEST	53	60804	8.8.8.8	192.168.2.7
May 11, 2021 11:49:57.140531063 CEST	59140	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:57.145548105 CEST	50905	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:57.198756933 CEST	53	50905	8.8.8.8	192.168.2.7
May 11, 2021 11:49:57.201684952 CEST	53	59140	8.8.8.8	192.168.2.7
May 11, 2021 11:49:59.300059080 CEST	53381	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:59.359657049 CEST	53	53381	8.8.8.8	192.168.2.7
May 11, 2021 11:49:59.525960922 CEST	54390	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:59.577655077 CEST	53	54390	8.8.8.8	192.168.2.7
May 11, 2021 11:49:59.992141008 CEST	63514	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:59.993017912 CEST	50578	53	192.168.2.7	8.8.8.8
May 11, 2021 11:49:59.996596098 CEST	63554	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:00.044786930 CEST	53	50578	8.8.8.8	192.168.2.7
May 11, 2021 11:50:00.048291922 CEST	53	63554	8.8.8.8	192.168.2.7
May 11, 2021 11:50:00.059436083 CEST	53	63514	8.8.8.8	192.168.2.7
May 11, 2021 11:50:00.121139050 CEST	63878	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 11:50:00.178607941 CEST	53	63878	8.8.8.8	192.168.2.7
May 11, 2021 11:50:00.518558025 CEST	53792	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:00.527606010 CEST	65280	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:00.567159891 CEST	55890	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:00.570705891 CEST	53	53792	8.8.8.8	192.168.2.7
May 11, 2021 11:50:00.580288887 CEST	53	65280	8.8.8.8	192.168.2.7
May 11, 2021 11:50:00.855999947 CEST	53	55890	8.8.8.8	192.168.2.7
May 11, 2021 11:50:01.357070923 CEST	57082	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:01.427908897 CEST	53	57082	8.8.8.8	192.168.2.7
May 11, 2021 11:50:03.599823952 CEST	64328	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:03.660826921 CEST	53	64328	8.8.8.8	192.168.2.7
May 11, 2021 11:50:03.824548960 CEST	54400	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:03.877849102 CEST	53	54400	8.8.8.8	192.168.2.7
May 11, 2021 11:50:04.286372900 CEST	52514	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:04.286813021 CEST	53104	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:04.296497107 CEST	54367	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:04.335633993 CEST	53	53104	8.8.8.8	192.168.2.7
May 11, 2021 11:50:04.346385002 CEST	64202	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:04.348226070 CEST	53	54367	8.8.8.8	192.168.2.7
May 11, 2021 11:50:04.352222919 CEST	53	52514	8.8.8.8	192.168.2.7
May 11, 2021 11:50:04.406579018 CEST	53	64202	8.8.8.8	192.168.2.7
May 11, 2021 11:50:04.717170954 CEST	62171	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:04.724883080 CEST	50672	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:04.765985012 CEST	53	62171	8.8.8.8	192.168.2.7
May 11, 2021 11:50:04.773502111 CEST	53	50672	8.8.8.8	192.168.2.7
May 11, 2021 11:50:04.948400974 CEST	63565	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:04.997364044 CEST	53	63565	8.8.8.8	192.168.2.7
May 11, 2021 11:50:11.599478006 CEST	62121	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:11.774121046 CEST	53	62121	8.8.8.8	192.168.2.7
May 11, 2021 11:50:12.304141998 CEST	59330	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:12.481300116 CEST	53	59330	8.8.8.8	192.168.2.7
May 11, 2021 11:50:13.331486940 CEST	51378	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:13.380732059 CEST	53	51378	8.8.8.8	192.168.2.7
May 11, 2021 11:50:13.816967964 CEST	58418	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:13.881798029 CEST	53	58418	8.8.8.8	192.168.2.7
May 11, 2021 11:50:14.322616100 CEST	63211	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:14.379796982 CEST	53	63211	8.8.8.8	192.168.2.7
May 11, 2021 11:50:14.740293026 CEST	57515	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:14.812777996 CEST	53	57515	8.8.8.8	192.168.2.7
May 11, 2021 11:50:14.836473942 CEST	56381	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:14.896657944 CEST	53	56381	8.8.8.8	192.168.2.7
May 11, 2021 11:50:15.308917999 CEST	58367	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:15.369173050 CEST	53	58367	8.8.8.8	192.168.2.7
May 11, 2021 11:50:16.050564051 CEST	56096	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:16.114617109 CEST	53	56096	8.8.8.8	192.168.2.7
May 11, 2021 11:50:16.418128967 CEST	60044	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:16.475475073 CEST	53	60044	8.8.8.8	192.168.2.7
May 11, 2021 11:50:16.640779972 CEST	61775	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:16.692681074 CEST	53	61775	8.8.8.8	192.168.2.7
May 11, 2021 11:50:16.777905941 CEST	50813	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:16.893085957 CEST	53	50813	8.8.8.8	192.168.2.7
May 11, 2021 11:50:17.117862940 CEST	65173	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:17.119951010 CEST	51307	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:17.120474100 CEST	51248	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:17.170727015 CEST	53	51307	8.8.8.8	192.168.2.7
May 11, 2021 11:50:17.171204090 CEST	53	51248	8.8.8.8	192.168.2.7
May 11, 2021 11:50:17.177534103 CEST	53	65173	8.8.8.8	192.168.2.7
May 11, 2021 11:50:17.268577099 CEST	50476	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:17.330157995 CEST	53	50476	8.8.8.8	192.168.2.7
May 11, 2021 11:50:17.359464884 CEST	63168	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:17.413256884 CEST	53	63168	8.8.8.8	192.168.2.7
May 11, 2021 11:50:17.615936041 CEST	62993	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:17.622018099 CEST	56452	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:17.654922962 CEST	54547	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 11:50:17.664822102 CEST	53	62993	8.8.8.8	192.168.2.7
May 11, 2021 11:50:17.673472881 CEST	53	56452	8.8.8.8	192.168.2.7
May 11, 2021 11:50:17.703572989 CEST	53	54547	8.8.8.8	192.168.2.7
May 11, 2021 11:50:17.869446039 CEST	49886	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:18.153424978 CEST	53	49886	8.8.8.8	192.168.2.7
May 11, 2021 11:50:18.943317890 CEST	56647	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:18.995031118 CEST	53	56647	8.8.8.8	192.168.2.7
May 11, 2021 11:50:19.607700109 CEST	58845	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:19.665263891 CEST	53	58845	8.8.8.8	192.168.2.7
May 11, 2021 11:50:19.830272913 CEST	59815	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:19.879065990 CEST	53	59815	8.8.8.8	192.168.2.7
May 11, 2021 11:50:21.879597902 CEST	59847	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:21.931201935 CEST	53	59847	8.8.8.8	192.168.2.7
May 11, 2021 11:50:22.511796951 CEST	57749	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:22.572264910 CEST	53	57749	8.8.8.8	192.168.2.7
May 11, 2021 11:50:22.749667883 CEST	64554	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:22.798465967 CEST	53	64554	8.8.8.8	192.168.2.7
May 11, 2021 11:50:26.270045996 CEST	61143	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:26.324234962 CEST	53	61143	8.8.8.8	192.168.2.7
May 11, 2021 11:50:26.925851107 CEST	60842	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:26.987087011 CEST	53	60842	8.8.8.8	192.168.2.7
May 11, 2021 11:50:27.147394896 CEST	54779	53	192.168.2.7	8.8.8.8
May 11, 2021 11:50:27.200872898 CEST	53	54779	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 11, 2021 11:48:16.971445084 CEST	192.168.2.7	8.8.8.8	0x84c6	Standard query (0)	www.msn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:48:19.431925058 CEST	192.168.2.7	8.8.8.8	0x4561	Standard query (0)	web.vortex .data.msn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:48:19.835427046 CEST	192.168.2.7	8.8.8.8	0x98a3	Standard query (0)	geolocatio n.onetrust.com	A (IP address)	IN (0x0001)
May 11, 2021 11:48:19.948782921 CEST	192.168.2.7	8.8.8.8	0xd1ff	Standard query (0)	contextual .media.net	A (IP address)	IN (0x0001)
May 11, 2021 11:48:21.594712019 CEST	192.168.2.7	8.8.8.8	0xc17a	Standard query (0)	lg3.media.net	A (IP address)	IN (0x0001)
May 11, 2021 11:48:21.674173117 CEST	192.168.2.7	8.8.8.8	0xc145	Standard query (0)	hblg.media.net	A (IP address)	IN (0x0001)
May 11, 2021 11:48:22.737883091 CEST	192.168.2.7	8.8.8.8	0x431	Standard query (0)	cvision.media.net	A (IP address)	IN (0x0001)
May 11, 2021 11:48:23.424263954 CEST	192.168.2.7	8.8.8.8	0xca81	Standard query (0)	srtb.msn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:48:24.890393972 CEST	192.168.2.7	8.8.8.8	0xc484	Standard query (0)	img.img-ta boola.com	A (IP address)	IN (0x0001)
May 11, 2021 11:48:41.288872004 CEST	192.168.2.7	8.8.8.8	0x2a96	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
May 11, 2021 11:48:42.302978039 CEST	192.168.2.7	8.8.8.8	0x3e64	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
May 11, 2021 11:48:43.895694971 CEST	192.168.2.7	8.8.8.8	0x9cf5	Standard query (0)	outlook.of fice365.com	A (IP address)	IN (0x0001)
May 11, 2021 11:48:49.220812082 CEST	192.168.2.7	8.8.8.8	0x5164	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
May 11, 2021 11:48:49.819717884 CEST	192.168.2.7	8.8.8.8	0xb0a7	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
May 11, 2021 11:48:50.094355106 CEST	192.168.2.7	8.8.8.8	0x8b3a	Standard query (0)	outlook.of fice365.com	A (IP address)	IN (0x0001)
May 11, 2021 11:48:54.213079929 CEST	192.168.2.7	8.8.8.8	0x5342	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
May 11, 2021 11:48:54.793625116 CEST	192.168.2.7	8.8.8.8	0x3966	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
May 11, 2021 11:48:55.045588970 CEST	192.168.2.7	8.8.8.8	0x7fd4	Standard query (0)	outlook.of fice365.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:07.444122076 CEST	192.168.2.7	8.8.8.8	0x6d3c	Standard query (0)	gmail.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:07.465312004 CEST	192.168.2.7	8.8.8.8	0xc716	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:08.104397058 CEST	192.168.2.7	8.8.8.8	0xff67	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 11, 2021 11:49:08.375240088 CEST	192.168.2.7	8.8.8.8	0xdcfa	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:12.645114899 CEST	192.168.2.7	8.8.8.8	0x19f	Standard query (0)	gmail.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:17.592077017 CEST	192.168.2.7	8.8.8.8	0xd1c	Standard query (0)	gmail.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:31.200529099 CEST	192.168.2.7	8.8.8.8	0x8bd7	Standard query (0)	worunekulo.club	A (IP address)	IN (0x0001)
May 11, 2021 11:49:31.211865902 CEST	192.168.2.7	8.8.8.8	0x7a92	Standard query (0)	gmail.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:31.436405897 CEST	192.168.2.7	8.8.8.8	0x9b13	Standard query (0)	www.redtube.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:31.986469030 CEST	192.168.2.7	8.8.8.8	0x8cc6	Standard query (0)	ei.rdtcdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:31.989778996 CEST	192.168.2.7	8.8.8.8	0x9779	Standard query (0)	static.trafficjunky.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:31.991530895 CEST	192.168.2.7	8.8.8.8	0x8402	Standard query (0)	ei.rdtcdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:31.992479086 CEST	192.168.2.7	8.8.8.8	0xc52f	Standard query (0)	cdn1d-static-shared.phncdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:32.007776976 CEST	192.168.2.7	8.8.8.8	0xb1f5	Standard query (0)	ht.redtube.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:32.109338045 CEST	192.168.2.7	8.8.8.8	0x36fb	Standard query (0)	static.trafficjunky.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:32.770766020 CEST	192.168.2.7	8.8.8.8	0xcfc6	Standard query (0)	cdn1d-static-shared.phncdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:33.401367903 CEST	192.168.2.7	8.8.8.8	0x98ce	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
May 11, 2021 11:49:33.755048037 CEST	192.168.2.7	8.8.8.8	0x1963	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)
May 11, 2021 11:49:33.761636972 CEST	192.168.2.7	8.8.8.8	0xaeb3	Standard query (0)	ht-cdn.trafficjunky.net	A (IP address)	IN (0x0001)
May 11, 2021 11:49:33.772862911 CEST	192.168.2.7	8.8.8.8	0x6fe	Standard query (0)	ads.trafficjunky.net	A (IP address)	IN (0x0001)
May 11, 2021 11:49:35.720659018 CEST	192.168.2.7	8.8.8.8	0xf17f	Standard query (0)	worunekulo.club	A (IP address)	IN (0x0001)
May 11, 2021 11:49:35.966732025 CEST	192.168.2.7	8.8.8.8	0xa5f4	Standard query (0)	www.redtube.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:36.889739037 CEST	192.168.2.7	8.8.8.8	0x3691	Standard query (0)	cdn1d-static-shared.phncdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:36.894444942 CEST	192.168.2.7	8.8.8.8	0x4917	Standard query (0)	ci.rdtcdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:36.908502102 CEST	192.168.2.7	8.8.8.8	0x22ee	Standard query (0)	static.trafficjunky.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:37.049813032 CEST	192.168.2.7	8.8.8.8	0x619f	Standard query (0)	ci.rdtcdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:38.487852097 CEST	192.168.2.7	8.8.8.8	0xd721	Standard query (0)	a.adtng.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:38.504393101 CEST	192.168.2.7	8.8.8.8	0x85e	Standard query (0)	ads.trafficjunky.net	A (IP address)	IN (0x0001)
May 11, 2021 11:49:38.752567053 CEST	192.168.2.7	8.8.8.8	0xc8d6	Standard query (0)	hw-cdn2.adtng.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:38.768923044 CEST	192.168.2.7	8.8.8.8	0x96f1	Standard query (0)	ht-cdn2.adtng.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:40.683099985 CEST	192.168.2.7	8.8.8.8	0x9d71	Standard query (0)	worunekulo.club	A (IP address)	IN (0x0001)
May 11, 2021 11:49:40.926469088 CEST	192.168.2.7	8.8.8.8	0x6077	Standard query (0)	www.redtube.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:41.519208908 CEST	192.168.2.7	8.8.8.8	0x1a96	Standard query (0)	cdn1d-static-shared.phncdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:41.521142960 CEST	192.168.2.7	8.8.8.8	0xdfa9	Standard query (0)	ei.rdtcdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:41.521658897 CEST	192.168.2.7	8.8.8.8	0x2fb1	Standard query (0)	static.trafficjunky.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:42.406912088 CEST	192.168.2.7	8.8.8.8	0x1eaa	Standard query (0)	eu-adsrv.rtbsuperhub.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:42.460452080 CEST	192.168.2.7	8.8.8.8	0xd191	Standard query (0)	ads.trafficjunky.net	A (IP address)	IN (0x0001)
May 11, 2021 11:49:42.490129948 CEST	192.168.2.7	8.8.8.8	0x1e0d	Standard query (0)	vz-cdn.trafficjunky.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 11, 2021 11:49:42.704149961 CEST	192.168.2.7	8.8.8.8	0x660e	Standard query (0)	bmedia.jus tservingfiles.net	A (IP address)	IN (0x0001)
May 11, 2021 11:49:53.374280930 CEST	192.168.2.7	8.8.8.8	0x7e57	Standard query (0)	worunekulo.club	A (IP address)	IN (0x0001)
May 11, 2021 11:49:53.587825060 CEST	192.168.2.7	8.8.8.8	0x3a8d	Standard query (0)	www.redtub e.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:54.066752911 CEST	192.168.2.7	8.8.8.8	0xe578	Standard query (0)	ei.rdtcdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:54.067255020 CEST	192.168.2.7	8.8.8.8	0x3b20	Standard query (0)	static.trafficjunky. com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:54.069013119 CEST	192.168.2.7	8.8.8.8	0x55a6	Standard query (0)	cdn1d-static- shared. phncdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:54.718347073 CEST	192.168.2.7	8.8.8.8	0x16bc	Standard query (0)	ci.rdtcdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:54.775541067 CEST	192.168.2.7	8.8.8.8	0xbf86	Standard query (0)	eu-adsrv.r tbsuperhub.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:54.956393003 CEST	192.168.2.7	8.8.8.8	0xe638	Standard query (0)	ads.traffi cjunky.net	A (IP address)	IN (0x0001)
May 11, 2021 11:49:54.992247105 CEST	192.168.2.7	8.8.8.8	0xc9ed	Standard query (0)	horunekulo .website	A (IP address)	IN (0x0001)
May 11, 2021 11:49:55.015211105 CEST	192.168.2.7	8.8.8.8	0x5990	Standard query (0)	a.adtng.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:55.231564999 CEST	192.168.2.7	8.8.8.8	0x8153	Standard query (0)	hw-cdn2.ad tng.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:55.233953953 CEST	192.168.2.7	8.8.8.8	0xd783	Standard query (0)	vz-cdn2.ad tng.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:55.266335964 CEST	192.168.2.7	8.8.8.8	0xbeda	Standard query (0)	www.redtub e.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:55.721441031 CEST	192.168.2.7	8.8.8.8	0xee13	Standard query (0)	cdn1d-static- shared. phncdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:55.726994991 CEST	192.168.2.7	8.8.8.8	0xd925	Standard query (0)	ei.rdtcdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:55.742913008 CEST	192.168.2.7	8.8.8.8	0x7eb8	Standard query (0)	static.trafficjunky. com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:56.166451931 CEST	192.168.2.7	8.8.8.8	0xb253	Standard query (0)	di.rdtcdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:56.250067949 CEST	192.168.2.7	8.8.8.8	0x1de7	Standard query (0)	eu-adsrv.r tbsuperhub.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:56.253499985 CEST	192.168.2.7	8.8.8.8	0xa2bb	Standard query (0)	ads.traffi cjunky.net	A (IP address)	IN (0x0001)
May 11, 2021 11:49:56.270965099 CEST	192.168.2.7	8.8.8.8	0x9732	Standard query (0)	a.adtng.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:56.494143009 CEST	192.168.2.7	8.8.8.8	0xf5c8	Standard query (0)	ht-cdn2.ad tng.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:56.511223078 CEST	192.168.2.7	8.8.8.8	0x43e9	Standard query (0)	hw-cdn2.ad tng.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:57.140531063 CEST	192.168.2.7	8.8.8.8	0x7dc4	Standard query (0)	ei.rdtcdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:57.145548105 CEST	192.168.2.7	8.8.8.8	0x3b65	Standard query (0)	cdn1d-static- shared. phncdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:59.300059080 CEST	192.168.2.7	8.8.8.8	0xea25	Standard query (0)	horunekulo .website	A (IP address)	IN (0x0001)
May 11, 2021 11:49:59.525960922 CEST	192.168.2.7	8.8.8.8	0xb2a0	Standard query (0)	www.redtub e.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:59.992141008 CEST	192.168.2.7	8.8.8.8	0xe56f	Standard query (0)	ci.rdtcdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:59.993017912 CEST	192.168.2.7	8.8.8.8	0x679e	Standard query (0)	cdn1d-static- shared. phncdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:49:59.996596098 CEST	192.168.2.7	8.8.8.8	0xa212	Standard query (0)	static.trafficjunky. com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:00.518558025 CEST	192.168.2.7	8.8.8.8	0x9c50	Standard query (0)	eu-adsrv.r tbsuperhub.com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:00.527606010 CEST	192.168.2.7	8.8.8.8	0xb4c1	Standard query (0)	ads.traffi cjunky.net	A (IP address)	IN (0x0001)
May 11, 2021 11:50:00.567159891 CEST	192.168.2.7	8.8.8.8	0xabaf	Standard query (0)	ht-cdn.tra fficjunky.net	A (IP address)	IN (0x0001)
May 11, 2021 11:50:01.357070923 CEST	192.168.2.7	8.8.8.8	0x242d	Standard query (0)	ci.rdtcdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:03.599823952 CEST	192.168.2.7	8.8.8.8	0x99eb	Standard query (0)	horunekulo .website	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 11, 2021 11:50:03.824548960 CEST	192.168.2.7	8.8.8.8	0x2517	Standard query (0)	www.redtube.com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:04.286372900 CEST	192.168.2.7	8.8.8.8	0xf7af	Standard query (0)	ei.rdtcdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:04.286813021 CEST	192.168.2.7	8.8.8.8	0x5024	Standard query (0)	cdn1d-static-shared.phncdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:04.296497107 CEST	192.168.2.7	8.8.8.8	0x2d41	Standard query (0)	static.trafficjunky.com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:04.717170954 CEST	192.168.2.7	8.8.8.8	0x2637	Standard query (0)	a.adtng.com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:04.724883080 CEST	192.168.2.7	8.8.8.8	0x28d5	Standard query (0)	ads.trafficjunky.net	A (IP address)	IN (0x0001)
May 11, 2021 11:50:04.948400974 CEST	192.168.2.7	8.8.8.8	0x979f	Standard query (0)	hw-cdn2.adtng.com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:16.418128967 CEST	192.168.2.7	8.8.8.8	0xf0a1	Standard query (0)	horunekulo.website	A (IP address)	IN (0x0001)
May 11, 2021 11:50:16.640779972 CEST	192.168.2.7	8.8.8.8	0x9794	Standard query (0)	www.redtube.com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:17.117862940 CEST	192.168.2.7	8.8.8.8	0x1ef9	Standard query (0)	ei.rdtcdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:17.119951010 CEST	192.168.2.7	8.8.8.8	0x5df9	Standard query (0)	static.trafficjunky.com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:17.120474100 CEST	192.168.2.7	8.8.8.8	0xfeb8	Standard query (0)	cdn1d-static-shared.phncdn.com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:17.615936041 CEST	192.168.2.7	8.8.8.8	0xb81b	Standard query (0)	eu-adsrv.rtbsuperhub.com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:17.622018099 CEST	192.168.2.7	8.8.8.8	0x510a	Standard query (0)	ads.trafficjunky.net	A (IP address)	IN (0x0001)
May 11, 2021 11:50:17.654922962 CEST	192.168.2.7	8.8.8.8	0xde5f	Standard query (0)	a.adtng.com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:17.869446039 CEST	192.168.2.7	8.8.8.8	0xe7bc	Standard query (0)	ht-cdn2.adtng.com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:18.943317890 CEST	192.168.2.7	8.8.8.8	0x744d	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:19.607700109 CEST	192.168.2.7	8.8.8.8	0x7462	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:19.830272913 CEST	192.168.2.7	8.8.8.8	0x6b6f	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:21.879597902 CEST	192.168.2.7	8.8.8.8	0xb30f	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:22.511796951 CEST	192.168.2.7	8.8.8.8	0x2e80	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:22.749667883 CEST	192.168.2.7	8.8.8.8	0x3d8c	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:26.270045996 CEST	192.168.2.7	8.8.8.8	0x610c	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:26.925851107 CEST	192.168.2.7	8.8.8.8	0x80e0	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
May 11, 2021 11:50:27.147394896 CEST	192.168.2.7	8.8.8.8	0x6b73	Standard query (0)	outlook.office365.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2021 11:48:17.022883892 CEST	8.8.8.8	192.168.2.7	0x84c6	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:19.502326965 CEST	8.8.8.8	192.168.2.7	0x4561	No error (0)	web.vortex.data.msn.com	web.vortex.data.microsoft.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:19.888895035 CEST	8.8.8.8	192.168.2.7	0x98a3	No error (0)	geolocation.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
May 11, 2021 11:48:19.888895035 CEST	8.8.8.8	192.168.2.7	0x98a3	No error (0)	geolocation.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
May 11, 2021 11:48:20.020838022 CEST	8.8.8.8	192.168.2.7	0xd1ff	No error (0)	contextual.media.net		184.30.24.22	A (IP address)	IN (0x0001)
May 11, 2021 11:48:21.662158966 CEST	8.8.8.8	192.168.2.7	0xc17a	No error (0)	lg3.media.net		184.30.24.22	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2021 11:48:21.747256041 CEST	8.8.8.8	192.168.2.7	0xc145	No error (0)	hblg.media.net		184.30.24.22	A (IP address)	IN (0x0001)
May 11, 2021 11:48:22.796694040 CEST	8.8.8.8	192.168.2.7	0x431	No error (0)	cvision.media.net	cvision.media.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:23.477477074 CEST	8.8.8.8	192.168.2.7	0xca81	No error (0)	srtb.msn.com	www.msn.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:23.477477074 CEST	8.8.8.8	192.168.2.7	0xca81	No error (0)	www.msn.com	www-msn-com.a-0003.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:24.943361044 CEST	8.8.8.8	192.168.2.7	0xc484	No error (0)	img.img-taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:24.943361044 CEST	8.8.8.8	192.168.2.7	0xc484	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
May 11, 2021 11:48:24.943361044 CEST	8.8.8.8	192.168.2.7	0xc484	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
May 11, 2021 11:48:24.943361044 CEST	8.8.8.8	192.168.2.7	0xc484	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
May 11, 2021 11:48:24.943361044 CEST	8.8.8.8	192.168.2.7	0xc484	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)
May 11, 2021 11:48:41.340394974 CEST	8.8.8.8	192.168.2.7	0x2a96	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
May 11, 2021 11:48:41.340394974 CEST	8.8.8.8	192.168.2.7	0x2a96	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
May 11, 2021 11:48:41.340394974 CEST	8.8.8.8	192.168.2.7	0x2a96	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
May 11, 2021 11:48:41.340394974 CEST	8.8.8.8	192.168.2.7	0x2a96	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
May 11, 2021 11:48:41.340394974 CEST	8.8.8.8	192.168.2.7	0x2a96	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
May 11, 2021 11:48:41.340394974 CEST	8.8.8.8	192.168.2.7	0x2a96	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
May 11, 2021 11:48:41.340394974 CEST	8.8.8.8	192.168.2.7	0x2a96	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
May 11, 2021 11:48:41.340394974 CEST	8.8.8.8	192.168.2.7	0x2a96	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
May 11, 2021 11:48:42.362421036 CEST	8.8.8.8	192.168.2.7	0x3e64	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:42.362421036 CEST	8.8.8.8	192.168.2.7	0x3e64	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:42.362421036 CEST	8.8.8.8	192.168.2.7	0x3e64	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:42.362421036 CEST	8.8.8.8	192.168.2.7	0x3e64	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:42.362421036 CEST	8.8.8.8	192.168.2.7	0x3e64	No error (0)	HHN-efz.ms-acdc.office.com		52.98.151.242	A (IP address)	IN (0x0001)
May 11, 2021 11:48:42.362421036 CEST	8.8.8.8	192.168.2.7	0x3e64	No error (0)	HHN-efz.ms-acdc.office.com		52.98.171.242	A (IP address)	IN (0x0001)
May 11, 2021 11:48:42.362421036 CEST	8.8.8.8	192.168.2.7	0x3e64	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.66	A (IP address)	IN (0x0001)
May 11, 2021 11:48:42.362421036 CEST	8.8.8.8	192.168.2.7	0x3e64	No error (0)	HHN-efz.ms-acdc.office.com		40.101.138.2	A (IP address)	IN (0x0001)
May 11, 2021 11:48:43.947530985 CEST	8.8.8.8	192.168.2.7	0x9cf5	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2021 11:48:43.947530985 CEST	8.8.8.8	192.168.2.7	0x9cf5	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:43.947530985 CEST	8.8.8.8	192.168.2.7	0x9cf5	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:43.947530985 CEST	8.8.8.8	192.168.2.7	0x9cf5	No error (0)	FRA-efz.ms-acdc.office.com		52.97.250.194	A (IP address)	IN (0x0001)
May 11, 2021 11:48:43.947530985 CEST	8.8.8.8	192.168.2.7	0x9cf5	No error (0)	FRA-efz.ms-acdc.office.com		40.101.19.162	A (IP address)	IN (0x0001)
May 11, 2021 11:48:43.947530985 CEST	8.8.8.8	192.168.2.7	0x9cf5	No error (0)	FRA-efz.ms-acdc.office.com		52.97.135.114	A (IP address)	IN (0x0001)
May 11, 2021 11:48:49.272397041 CEST	8.8.8.8	192.168.2.7	0x5164	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
May 11, 2021 11:48:49.272397041 CEST	8.8.8.8	192.168.2.7	0x5164	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
May 11, 2021 11:48:49.272397041 CEST	8.8.8.8	192.168.2.7	0x5164	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
May 11, 2021 11:48:49.272397041 CEST	8.8.8.8	192.168.2.7	0x5164	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
May 11, 2021 11:48:49.272397041 CEST	8.8.8.8	192.168.2.7	0x5164	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
May 11, 2021 11:48:49.272397041 CEST	8.8.8.8	192.168.2.7	0x5164	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
May 11, 2021 11:48:49.272397041 CEST	8.8.8.8	192.168.2.7	0x5164	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
May 11, 2021 11:48:49.272397041 CEST	8.8.8.8	192.168.2.7	0x5164	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
May 11, 2021 11:48:49.881705046 CEST	8.8.8.8	192.168.2.7	0xb0a7	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:49.881705046 CEST	8.8.8.8	192.168.2.7	0xb0a7	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:49.881705046 CEST	8.8.8.8	192.168.2.7	0xb0a7	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:49.881705046 CEST	8.8.8.8	192.168.2.7	0xb0a7	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:49.881705046 CEST	8.8.8.8	192.168.2.7	0xb0a7	No error (0)	HHN-efz.ms-acdc.office.com		52.98.151.242	A (IP address)	IN (0x0001)
May 11, 2021 11:48:49.881705046 CEST	8.8.8.8	192.168.2.7	0xb0a7	No error (0)	HHN-efz.ms-acdc.office.com		52.98.171.242	A (IP address)	IN (0x0001)
May 11, 2021 11:48:49.881705046 CEST	8.8.8.8	192.168.2.7	0xb0a7	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.66	A (IP address)	IN (0x0001)
May 11, 2021 11:48:49.881705046 CEST	8.8.8.8	192.168.2.7	0xb0a7	No error (0)	HHN-efz.ms-acdc.office.com		40.101.138.2	A (IP address)	IN (0x0001)
May 11, 2021 11:48:50.143126011 CEST	8.8.8.8	192.168.2.7	0x8b3a	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:50.143126011 CEST	8.8.8.8	192.168.2.7	0x8b3a	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:50.143126011 CEST	8.8.8.8	192.168.2.7	0x8b3a	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:50.143126011 CEST	8.8.8.8	192.168.2.7	0x8b3a	No error (0)	FRA-efz.ms-acdc.office.com		40.101.83.18	A (IP address)	IN (0x0001)
May 11, 2021 11:48:50.143126011 CEST	8.8.8.8	192.168.2.7	0x8b3a	No error (0)	FRA-efz.ms-acdc.office.com		52.97.189.66	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2021 11:48:50.143126011 CEST	8.8.8.8	192.168.2.7	0x8b3a	No error (0)	FRA-efz.ms-acdc.office.com		52.97.176.2	A (IP address)	IN (0x0001)
May 11, 2021 11:48:54.261889935 CEST	8.8.8.8	192.168.2.7	0x5342	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
May 11, 2021 11:48:54.261889935 CEST	8.8.8.8	192.168.2.7	0x5342	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
May 11, 2021 11:48:54.261889935 CEST	8.8.8.8	192.168.2.7	0x5342	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
May 11, 2021 11:48:54.261889935 CEST	8.8.8.8	192.168.2.7	0x5342	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
May 11, 2021 11:48:54.261889935 CEST	8.8.8.8	192.168.2.7	0x5342	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
May 11, 2021 11:48:54.261889935 CEST	8.8.8.8	192.168.2.7	0x5342	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
May 11, 2021 11:48:54.261889935 CEST	8.8.8.8	192.168.2.7	0x5342	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
May 11, 2021 11:48:54.261889935 CEST	8.8.8.8	192.168.2.7	0x5342	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
May 11, 2021 11:48:54.842464924 CEST	8.8.8.8	192.168.2.7	0x3966	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:54.842464924 CEST	8.8.8.8	192.168.2.7	0x3966	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:54.842464924 CEST	8.8.8.8	192.168.2.7	0x3966	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:54.842464924 CEST	8.8.8.8	192.168.2.7	0x3966	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:54.842464924 CEST	8.8.8.8	192.168.2.7	0x3966	No error (0)	HHN-efz.ms-acdc.office.com		52.97.201.2	A (IP address)	IN (0x0001)
May 11, 2021 11:48:54.842464924 CEST	8.8.8.8	192.168.2.7	0x3966	No error (0)	HHN-efz.ms-acdc.office.com		40.101.136.242	A (IP address)	IN (0x0001)
May 11, 2021 11:48:54.842464924 CEST	8.8.8.8	192.168.2.7	0x3966	No error (0)	HHN-efz.ms-acdc.office.com		52.97.233.82	A (IP address)	IN (0x0001)
May 11, 2021 11:48:54.842464924 CEST	8.8.8.8	192.168.2.7	0x3966	No error (0)	HHN-efz.ms-acdc.office.com		52.97.201.50	A (IP address)	IN (0x0001)
May 11, 2021 11:48:55.094230890 CEST	8.8.8.8	192.168.2.7	0x7fd4	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:55.094230890 CEST	8.8.8.8	192.168.2.7	0x7fd4	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:55.094230890 CEST	8.8.8.8	192.168.2.7	0x7fd4	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:48:55.094230890 CEST	8.8.8.8	192.168.2.7	0x7fd4	No error (0)	HHN-efz.ms-acdc.office.com		52.98.152.162	A (IP address)	IN (0x0001)
May 11, 2021 11:48:55.094230890 CEST	8.8.8.8	192.168.2.7	0x7fd4	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.34	A (IP address)	IN (0x0001)
May 11, 2021 11:48:55.094230890 CEST	8.8.8.8	192.168.2.7	0x7fd4	No error (0)	HHN-efz.ms-acdc.office.com		52.97.201.50	A (IP address)	IN (0x0001)
May 11, 2021 11:48:55.094230890 CEST	8.8.8.8	192.168.2.7	0x7fd4	No error (0)	HHN-efz.ms-acdc.office.com		52.98.171.242	A (IP address)	IN (0x0001)
May 11, 2021 11:49:07.514158964 CEST	8.8.8.8	192.168.2.7	0xc716	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
May 11, 2021 11:49:07.514158964 CEST	8.8.8.8	192.168.2.7	0xc716	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2021 11:49:07.514158964 CEST	8.8.8.8	192.168.2.7	0xc716	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
May 11, 2021 11:49:07.514158964 CEST	8.8.8.8	192.168.2.7	0xc716	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
May 11, 2021 11:49:07.514158964 CEST	8.8.8.8	192.168.2.7	0xc716	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
May 11, 2021 11:49:07.514158964 CEST	8.8.8.8	192.168.2.7	0xc716	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
May 11, 2021 11:49:07.514158964 CEST	8.8.8.8	192.168.2.7	0xc716	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
May 11, 2021 11:49:07.514158964 CEST	8.8.8.8	192.168.2.7	0xc716	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
May 11, 2021 11:49:07.517314911 CEST	8.8.8.8	192.168.2.7	0x6d3c	No error (0)	gmail.com		172.217.19.101	A (IP address)	IN (0x0001)
May 11, 2021 11:49:08.171678066 CEST	8.8.8.8	192.168.2.7	0xff67	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:08.171678066 CEST	8.8.8.8	192.168.2.7	0xff67	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:08.171678066 CEST	8.8.8.8	192.168.2.7	0xff67	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:08.171678066 CEST	8.8.8.8	192.168.2.7	0xff67	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:08.171678066 CEST	8.8.8.8	192.168.2.7	0xff67	No error (0)	FRA-efz.ms-acdc.office.com		52.97.155.114	A (IP address)	IN (0x0001)
May 11, 2021 11:49:08.171678066 CEST	8.8.8.8	192.168.2.7	0xff67	No error (0)	FRA-efz.ms-acdc.office.com		52.97.183.194	A (IP address)	IN (0x0001)
May 11, 2021 11:49:08.171678066 CEST	8.8.8.8	192.168.2.7	0xff67	No error (0)	FRA-efz.ms-acdc.office.com		40.101.12.50	A (IP address)	IN (0x0001)
May 11, 2021 11:49:08.424179077 CEST	8.8.8.8	192.168.2.7	0xdcfa	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:08.424179077 CEST	8.8.8.8	192.168.2.7	0xdcfa	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:08.424179077 CEST	8.8.8.8	192.168.2.7	0xdcfa	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:08.424179077 CEST	8.8.8.8	192.168.2.7	0xdcfa	No error (0)	FRA-efz.ms-acdc.office.com		52.97.201.114	A (IP address)	IN (0x0001)
May 11, 2021 11:49:08.424179077 CEST	8.8.8.8	192.168.2.7	0xdcfa	No error (0)	FRA-efz.ms-acdc.office.com		40.101.18.34	A (IP address)	IN (0x0001)
May 11, 2021 11:49:08.424179077 CEST	8.8.8.8	192.168.2.7	0xdcfa	No error (0)	FRA-efz.ms-acdc.office.com		52.97.188.66	A (IP address)	IN (0x0001)
May 11, 2021 11:49:12.718048096 CEST	8.8.8.8	192.168.2.7	0x19f	No error (0)	gmail.com		172.217.19.101	A (IP address)	IN (0x0001)
May 11, 2021 11:49:17.649398088 CEST	8.8.8.8	192.168.2.7	0xd1c	No error (0)	gmail.com		172.217.19.101	A (IP address)	IN (0x0001)
May 11, 2021 11:49:31.261517048 CEST	8.8.8.8	192.168.2.7	0x8bd7	No error (0)	worunekulo.club		193.239.84.195	A (IP address)	IN (0x0001)
May 11, 2021 11:49:31.281362057 CEST	8.8.8.8	192.168.2.7	0x7a92	No error (0)	gmail.com		172.217.19.101	A (IP address)	IN (0x0001)
May 11, 2021 11:49:31.486903906 CEST	8.8.8.8	192.168.2.7	0x9b13	No error (0)	www.redtube.com	redtube.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:31.486903906 CEST	8.8.8.8	192.168.2.7	0x9b13	No error (0)	redtube.com		66.254.114.238	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2021 11:49:32.038800001 CEST	8.8.8.8	192.168.2.7	0x9779	No error (0)	static.trafficjunky.com	vip0x04f.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:32.038800001 CEST	8.8.8.8	192.168.2.7	0x9779	No error (0)	vip0x04f.ssl.rncdn5.com		205.185.208.79	A (IP address)	IN (0x0001)
May 11, 2021 11:49:32.041726112 CEST	8.8.8.8	192.168.2.7	0xc52f	No error (0)	cdn1d-static-shared.phncdn.com	vip0x08e.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:32.041726112 CEST	8.8.8.8	192.168.2.7	0xc52f	No error (0)	vip0x08e.ssl.rncdn5.com		205.185.208.142	A (IP address)	IN (0x0001)
May 11, 2021 11:49:32.056627035 CEST	8.8.8.8	192.168.2.7	0xb1f5	No error (0)	ht.redtube.com	hubtraffic.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:32.056627035 CEST	8.8.8.8	192.168.2.7	0xb1f5	No error (0)	hubtraffic.com		66.254.114.32	A (IP address)	IN (0x0001)
May 11, 2021 11:49:32.158049107 CEST	8.8.8.8	192.168.2.7	0x36fb	No error (0)	static.trafficjunky.com	vip0x04f.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:32.158049107 CEST	8.8.8.8	192.168.2.7	0x36fb	No error (0)	vip0x04f.ssl.rncdn5.com		205.185.208.79	A (IP address)	IN (0x0001)
May 11, 2021 11:49:32.277290106 CEST	8.8.8.8	192.168.2.7	0x8402	No error (0)	ei.rdtcdn.com	ei.rdtcdn.com.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:32.277290106 CEST	8.8.8.8	192.168.2.7	0x8402	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.72	A (IP address)	IN (0x0001)
May 11, 2021 11:49:32.277290106 CEST	8.8.8.8	192.168.2.7	0x8402	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.68	A (IP address)	IN (0x0001)
May 11, 2021 11:49:32.277290106 CEST	8.8.8.8	192.168.2.7	0x8402	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.70	A (IP address)	IN (0x0001)
May 11, 2021 11:49:32.278726101 CEST	8.8.8.8	192.168.2.7	0x8cc6	No error (0)	ei.rdtcdn.com	ei.rdtcdn.com.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:32.278726101 CEST	8.8.8.8	192.168.2.7	0x8cc6	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.68	A (IP address)	IN (0x0001)
May 11, 2021 11:49:32.278726101 CEST	8.8.8.8	192.168.2.7	0x8cc6	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.70	A (IP address)	IN (0x0001)
May 11, 2021 11:49:32.278726101 CEST	8.8.8.8	192.168.2.7	0x8cc6	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.72	A (IP address)	IN (0x0001)
May 11, 2021 11:49:32.819425106 CEST	8.8.8.8	192.168.2.7	0xcfc6	No error (0)	cdn1d-static-shared.phncdn.com	vip0x08e.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:32.819425106 CEST	8.8.8.8	192.168.2.7	0xcfc6	No error (0)	vip0x08e.ssl.rncdn5.com		205.185.208.142	A (IP address)	IN (0x0001)
May 11, 2021 11:49:33.449980021 CEST	8.8.8.8	192.168.2.7	0x98ce	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:33.449980021 CEST	8.8.8.8	192.168.2.7	0x98ce	No error (0)	stats.l.doubleclick.net		173.194.76.156	A (IP address)	IN (0x0001)
May 11, 2021 11:49:33.449980021 CEST	8.8.8.8	192.168.2.7	0x98ce	No error (0)	stats.l.doubleclick.net		173.194.76.157	A (IP address)	IN (0x0001)
May 11, 2021 11:49:33.449980021 CEST	8.8.8.8	192.168.2.7	0x98ce	No error (0)	stats.l.doubleclick.net		173.194.76.154	A (IP address)	IN (0x0001)
May 11, 2021 11:49:33.449980021 CEST	8.8.8.8	192.168.2.7	0x98ce	No error (0)	stats.l.doubleclick.net		173.194.76.155	A (IP address)	IN (0x0001)
May 11, 2021 11:49:33.823712111 CEST	8.8.8.8	192.168.2.7	0x6fe	No error (0)	ads.trafficjunky.net		66.254.114.38	A (IP address)	IN (0x0001)
May 11, 2021 11:49:33.831100941 CEST	8.8.8.8	192.168.2.7	0x1963	No error (0)	www.google.de		172.217.16.99	A (IP address)	IN (0x0001)
May 11, 2021 11:49:34.049549103 CEST	8.8.8.8	192.168.2.7	0xaeb3	No error (0)	ht-cdn.trafficjunky.net	ht-cdn.trafficjunky.net.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2021 11:49:34.049549103 CEST	8.8.8.8	192.168.2.7	0xaeb3	No error (0)	ht-cdn.trafficjunky.net.sds.rncdn7.com		64.210.135.70	A (IP address)	IN (0x0001)
May 11, 2021 11:49:34.049549103 CEST	8.8.8.8	192.168.2.7	0xaeb3	No error (0)	ht-cdn.trafficjunky.net.sds.rncdn7.com		64.210.135.72	A (IP address)	IN (0x0001)
May 11, 2021 11:49:34.049549103 CEST	8.8.8.8	192.168.2.7	0xaeb3	No error (0)	ht-cdn.trafficjunky.net.sds.rncdn7.com		64.210.135.68	A (IP address)	IN (0x0001)
May 11, 2021 11:49:35.784024954 CEST	8.8.8.8	192.168.2.7	0xf17f	No error (0)	worunekulo.club		193.239.84.195	A (IP address)	IN (0x0001)
May 11, 2021 11:49:36.019480944 CEST	8.8.8.8	192.168.2.7	0xa5f4	No error (0)	www.redtube.com	redtube.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:36.019480944 CEST	8.8.8.8	192.168.2.7	0xa5f4	No error (0)	redtube.com		66.254.114.238	A (IP address)	IN (0x0001)
May 11, 2021 11:49:36.938515902 CEST	8.8.8.8	192.168.2.7	0x3691	No error (0)	cdn1d-static-shared.phncdn.com	vip0x08e.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:36.938515902 CEST	8.8.8.8	192.168.2.7	0x3691	No error (0)	vip0x08e.ssl.rncdn5.com		205.185.208.142	A (IP address)	IN (0x0001)
May 11, 2021 11:49:36.957369089 CEST	8.8.8.8	192.168.2.7	0x22ee	No error (0)	static.trafficjunky.com	vip0x04f.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:36.957369089 CEST	8.8.8.8	192.168.2.7	0x22ee	No error (0)	vip0x04f.ssl.rncdn5.com		205.185.208.79	A (IP address)	IN (0x0001)
May 11, 2021 11:49:36.962465048 CEST	8.8.8.8	192.168.2.7	0x4917	No error (0)	ci.rdtcdn.com	cs733.wpc.rncdn4.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:36.962465048 CEST	8.8.8.8	192.168.2.7	0x4917	No error (0)	cs733.wpc.rncdn4.com		192.229.221.206	A (IP address)	IN (0x0001)
May 11, 2021 11:49:37.111428022 CEST	8.8.8.8	192.168.2.7	0x619f	No error (0)	ci.rdtcdn.com	cs733.wpc.rncdn4.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:37.111428022 CEST	8.8.8.8	192.168.2.7	0x619f	No error (0)	cs733.wpc.rncdn4.com		192.229.221.206	A (IP address)	IN (0x0001)
May 11, 2021 11:49:38.536997080 CEST	8.8.8.8	192.168.2.7	0xd721	No error (0)	a.adtng.com		216.18.168.166	A (IP address)	IN (0x0001)
May 11, 2021 11:49:38.553560972 CEST	8.8.8.8	192.168.2.7	0x85e	No error (0)	ads.trafficjunky.net		66.254.114.38	A (IP address)	IN (0x0001)
May 11, 2021 11:49:38.801434040 CEST	8.8.8.8	192.168.2.7	0xc8d6	No error (0)	hw-cdn2.adtng.com	vip0x019.map2.ssl.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:39.054255009 CEST	8.8.8.8	192.168.2.7	0x96f1	No error (0)	ht-cdn2.adtng.com	ht-cdn2.adtng.com.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:39.054255009 CEST	8.8.8.8	192.168.2.7	0x96f1	No error (0)	ht-cdn2.adtng.com.sds.rncdn7.com		64.210.135.70	A (IP address)	IN (0x0001)
May 11, 2021 11:49:39.054255009 CEST	8.8.8.8	192.168.2.7	0x96f1	No error (0)	ht-cdn2.adtng.com.sds.rncdn7.com		64.210.135.72	A (IP address)	IN (0x0001)
May 11, 2021 11:49:39.054255009 CEST	8.8.8.8	192.168.2.7	0x96f1	No error (0)	ht-cdn2.adtng.com.sds.rncdn7.com		64.210.135.68	A (IP address)	IN (0x0001)
May 11, 2021 11:49:40.743920088 CEST	8.8.8.8	192.168.2.7	0x9d71	No error (0)	worunekulo.club		193.239.84.195	A (IP address)	IN (0x0001)
May 11, 2021 11:49:40.975166082 CEST	8.8.8.8	192.168.2.7	0x6077	No error (0)	www.redtube.com	redtube.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:40.975166082 CEST	8.8.8.8	192.168.2.7	0x6077	No error (0)	redtube.com		66.254.114.238	A (IP address)	IN (0x0001)
May 11, 2021 11:49:41.573271990 CEST	8.8.8.8	192.168.2.7	0x1a96	No error (0)	cdn1d-static-shared.phncdn.com	vip0x08e.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2021 11:49:41.573271990 CEST	8.8.8.8	192.168.2.7	0x1a96	No error (0)	vip0x08e.ssl.rncdn5.com		205.185.208.142	A (IP address)	IN (0x0001)
May 11, 2021 11:49:41.573431969 CEST	8.8.8.8	192.168.2.7	0x2fb1	No error (0)	static.trafficjunky.com	vip0x04f.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:41.573431969 CEST	8.8.8.8	192.168.2.7	0x2fb1	No error (0)	vip0x04f.ssl.rncdn5.com		205.185.208.79	A (IP address)	IN (0x0001)
May 11, 2021 11:49:41.581955910 CEST	8.8.8.8	192.168.2.7	0xdfa9	No error (0)	ei.rdtcdn.com	ei.rdtcdn.com.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:41.581955910 CEST	8.8.8.8	192.168.2.7	0xdfa9	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.68	A (IP address)	IN (0x0001)
May 11, 2021 11:49:41.581955910 CEST	8.8.8.8	192.168.2.7	0xdfa9	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.70	A (IP address)	IN (0x0001)
May 11, 2021 11:49:41.581955910 CEST	8.8.8.8	192.168.2.7	0xdfa9	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.72	A (IP address)	IN (0x0001)
May 11, 2021 11:49:42.455703020 CEST	8.8.8.8	192.168.2.7	0x1eaa	No error (0)	eu-adsrv.rtbsuperhub.com	tp-rtb-adserver-eu.eu-west-1.elasticbeanstalk.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:42.455703020 CEST	8.8.8.8	192.168.2.7	0x1eaa	No error (0)	tp-rtb-adserver-eu.eu-west-1.elasticbeanstalk.com		54.247.61.18	A (IP address)	IN (0x0001)
May 11, 2021 11:49:42.455703020 CEST	8.8.8.8	192.168.2.7	0x1eaa	No error (0)	tp-rtb-adserver-eu.eu-west-1.elasticbeanstalk.com		54.72.255.40	A (IP address)	IN (0x0001)
May 11, 2021 11:49:42.509357929 CEST	8.8.8.8	192.168.2.7	0xd191	No error (0)	ads.trafficjunky.net		66.254.114.38	A (IP address)	IN (0x0001)
May 11, 2021 11:49:42.553545952 CEST	8.8.8.8	192.168.2.7	0x1e0d	No error (0)	vz-cdn.trafficjunky.net	cs742.wpc.rncdn4.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:42.553545952 CEST	8.8.8.8	192.168.2.7	0x1e0d	No error (0)	cs742.wpc.rncdn4.com		192.229.221.215	A (IP address)	IN (0x0001)
May 11, 2021 11:49:42.757795095 CEST	8.8.8.8	192.168.2.7	0x660e	No error (0)	bmedia.justservingfiles.net	cds.g7p6a4c2.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:53.432423115 CEST	8.8.8.8	192.168.2.7	0x7e57	No error (0)	worunekulo.club		193.239.84.195	A (IP address)	IN (0x0001)
May 11, 2021 11:49:53.639441967 CEST	8.8.8.8	192.168.2.7	0x3a8d	No error (0)	www.redtube.com	redtube.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:53.639441967 CEST	8.8.8.8	192.168.2.7	0x3a8d	No error (0)	redtube.com		66.254.114.238	A (IP address)	IN (0x0001)
May 11, 2021 11:49:54.116395950 CEST	8.8.8.8	192.168.2.7	0x3b20	No error (0)	static.trafficjunky.com	vip0x04f.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:54.116395950 CEST	8.8.8.8	192.168.2.7	0x3b20	No error (0)	vip0x04f.ssl.rncdn5.com		205.185.208.79	A (IP address)	IN (0x0001)
May 11, 2021 11:49:54.116430998 CEST	8.8.8.8	192.168.2.7	0xe578	No error (0)	ei.rdtcdn.com	ei.rdtcdn.com.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:54.116430998 CEST	8.8.8.8	192.168.2.7	0xe578	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.68	A (IP address)	IN (0x0001)
May 11, 2021 11:49:54.116430998 CEST	8.8.8.8	192.168.2.7	0xe578	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.70	A (IP address)	IN (0x0001)
May 11, 2021 11:49:54.116430998 CEST	8.8.8.8	192.168.2.7	0xe578	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.72	A (IP address)	IN (0x0001)
May 11, 2021 11:49:54.120568037 CEST	8.8.8.8	192.168.2.7	0x55a6	No error (0)	cdn1d-static-shared.phncdn.com	vip0x08e.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:54.120568037 CEST	8.8.8.8	192.168.2.7	0x55a6	No error (0)	vip0x08e.ssl.rncdn5.com		205.185.208.142	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2021 11:49:54.775674105 CEST	8.8.8.8	192.168.2.7	0x16bc	No error (0)	ci.rdtcdn.com	cs733.wpc.rncdn4.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:54.775674105 CEST	8.8.8.8	192.168.2.7	0x16bc	No error (0)	cs733.wpc.rncdn4.com		192.229.221.206	A (IP address)	IN (0x0001)
May 11, 2021 11:49:54.825416088 CEST	8.8.8.8	192.168.2.7	0xbf86	No error (0)	eu-adsrv.rtbsuperhub.com	tp-rtb-adserver-eu.eu-west-1.elasticbeanstalk.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:54.825416088 CEST	8.8.8.8	192.168.2.7	0xbf86	No error (0)	tp-rtb-adserver-eu.eu-west-1.elasticbeanstalk.com		54.247.61.18	A (IP address)	IN (0x0001)
May 11, 2021 11:49:54.825416088 CEST	8.8.8.8	192.168.2.7	0xbf86	No error (0)	tp-rtb-adserver-eu.eu-west-1.elasticbeanstalk.com		54.72.255.40	A (IP address)	IN (0x0001)
May 11, 2021 11:49:55.004951954 CEST	8.8.8.8	192.168.2.7	0xe638	No error (0)	ads.trafficjunky.net		66.254.114.38	A (IP address)	IN (0x0001)
May 11, 2021 11:49:55.058893919 CEST	8.8.8.8	192.168.2.7	0xc9ed	No error (0)	horunekulo.website		193.239.85.9	A (IP address)	IN (0x0001)
May 11, 2021 11:49:55.064198017 CEST	8.8.8.8	192.168.2.7	0x5990	No error (0)	a.adtng.com		216.18.168.166	A (IP address)	IN (0x0001)
May 11, 2021 11:49:55.283153057 CEST	8.8.8.8	192.168.2.7	0x8153	No error (0)	hw-cdn2.adtng.com	vip0x019.map2.ssl.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:55.285373926 CEST	8.8.8.8	192.168.2.7	0xd783	No error (0)	vz-cdn2.adtng.com	cs2178.wpc.rncdn4.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:55.285373926 CEST	8.8.8.8	192.168.2.7	0xd783	No error (0)	cs2178.wpc.rncdn4.com		152.199.21.187	A (IP address)	IN (0x0001)
May 11, 2021 11:49:55.318046093 CEST	8.8.8.8	192.168.2.7	0xbeda	No error (0)	www.redtube.com	redtube.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:55.318046093 CEST	8.8.8.8	192.168.2.7	0xbeda	No error (0)	redtube.com		66.254.114.238	A (IP address)	IN (0x0001)
May 11, 2021 11:49:55.772910118 CEST	8.8.8.8	192.168.2.7	0xee13	No error (0)	cdn1d-static-shared.phncdn.com	vip0x08e.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:55.772910118 CEST	8.8.8.8	192.168.2.7	0xee13	No error (0)	vip0x08e.ssl.rncdn5.com		205.185.208.142	A (IP address)	IN (0x0001)
May 11, 2021 11:49:55.784446955 CEST	8.8.8.8	192.168.2.7	0xd925	No error (0)	ei.rdtcdn.com	ei.rdtcdn.com.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:55.784446955 CEST	8.8.8.8	192.168.2.7	0xd925	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.68	A (IP address)	IN (0x0001)
May 11, 2021 11:49:55.784446955 CEST	8.8.8.8	192.168.2.7	0xd925	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.70	A (IP address)	IN (0x0001)
May 11, 2021 11:49:55.784446955 CEST	8.8.8.8	192.168.2.7	0xd925	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.72	A (IP address)	IN (0x0001)
May 11, 2021 11:49:55.791635990 CEST	8.8.8.8	192.168.2.7	0x7eb8	No error (0)	static.trafficjunky.com	vip0x04f.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:55.791635990 CEST	8.8.8.8	192.168.2.7	0x7eb8	No error (0)	vip0x04f.ssl.rncdn5.com		205.185.208.79	A (IP address)	IN (0x0001)
May 11, 2021 11:49:56.216947079 CEST	8.8.8.8	192.168.2.7	0xb253	No error (0)	di.rdtcdn.com	cds.e9q5t8x5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:56.300575972 CEST	8.8.8.8	192.168.2.7	0x1de7	No error (0)	eu-adsrv.rtbsuperhub.com	tp-rtb-adserver-eu.eu-west-1.elasticbeanstalk.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:56.300575972 CEST	8.8.8.8	192.168.2.7	0x1de7	No error (0)	tp-rtb-adserver-eu.eu-west-1.elasticbeanstalk.com		54.72.255.40	A (IP address)	IN (0x0001)
May 11, 2021 11:49:56.300575972 CEST	8.8.8.8	192.168.2.7	0x1de7	No error (0)	tp-rtb-adserver-eu.eu-west-1.elasticbeanstalk.com		54.247.61.18	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2021 11:49:56.305774927 CEST	8.8.8.8	192.168.2.7	0xa2bb	No error (0)	ads.trafficjunky.net		66.254.114.38	A (IP address)	IN (0x0001)
May 11, 2021 11:49:56.322490931 CEST	8.8.8.8	192.168.2.7	0x9732	No error (0)	a.adtng.com		216.18.168.166	A (IP address)	IN (0x0001)
May 11, 2021 11:49:56.559899092 CEST	8.8.8.8	192.168.2.7	0x43e9	No error (0)	hw-cdn2.adtng.com	vip0x019.map2.ssl.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:56.780894041 CEST	8.8.8.8	192.168.2.7	0xf5c8	No error (0)	ht-cdn2.adtng.com	ht-cdn2.adtng.com.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:56.780894041 CEST	8.8.8.8	192.168.2.7	0xf5c8	No error (0)	ht-cdn2.adtng.com.sds.rncdn7.com		64.210.135.70	A (IP address)	IN (0x0001)
May 11, 2021 11:49:56.780894041 CEST	8.8.8.8	192.168.2.7	0xf5c8	No error (0)	ht-cdn2.adtng.com.sds.rncdn7.com		64.210.135.72	A (IP address)	IN (0x0001)
May 11, 2021 11:49:56.780894041 CEST	8.8.8.8	192.168.2.7	0xf5c8	No error (0)	ht-cdn2.adtng.com.sds.rncdn7.com		64.210.135.68	A (IP address)	IN (0x0001)
May 11, 2021 11:49:57.198756933 CEST	8.8.8.8	192.168.2.7	0x3b65	No error (0)	cdn1d-static-shared.phncdn.com	vip0x08e.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:57.198756933 CEST	8.8.8.8	192.168.2.7	0x3b65	No error (0)	vip0x08e.ssl.rncdn5.com		205.185.208.142	A (IP address)	IN (0x0001)
May 11, 2021 11:49:57.201684952 CEST	8.8.8.8	192.168.2.7	0x7dc4	No error (0)	ei.rdtcdn.com	ei.rdtcdn.com.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:57.201684952 CEST	8.8.8.8	192.168.2.7	0x7dc4	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.72	A (IP address)	IN (0x0001)
May 11, 2021 11:49:57.201684952 CEST	8.8.8.8	192.168.2.7	0x7dc4	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.68	A (IP address)	IN (0x0001)
May 11, 2021 11:49:57.201684952 CEST	8.8.8.8	192.168.2.7	0x7dc4	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.70	A (IP address)	IN (0x0001)
May 11, 2021 11:49:59.359657049 CEST	8.8.8.8	192.168.2.7	0xea25	No error (0)	horunekulo.website		193.239.85.9	A (IP address)	IN (0x0001)
May 11, 2021 11:49:59.577655077 CEST	8.8.8.8	192.168.2.7	0xb2a0	No error (0)	www.redtube.com	redtube.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:49:59.577655077 CEST	8.8.8.8	192.168.2.7	0xb2a0	No error (0)	redtube.com		66.254.114.238	A (IP address)	IN (0x0001)
May 11, 2021 11:50:00.044786930 CEST	8.8.8.8	192.168.2.7	0x679e	No error (0)	cdn1d-static-shared.phncdn.com	vip0x08e.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:00.044786930 CEST	8.8.8.8	192.168.2.7	0x679e	No error (0)	vip0x08e.ssl.rncdn5.com		205.185.208.142	A (IP address)	IN (0x0001)
May 11, 2021 11:50:00.048291922 CEST	8.8.8.8	192.168.2.7	0xa212	No error (0)	static.trafficjunky.com	vip0x04f.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:00.048291922 CEST	8.8.8.8	192.168.2.7	0xa212	No error (0)	vip0x04f.ssl.rncdn5.com		205.185.208.79	A (IP address)	IN (0x0001)
May 11, 2021 11:50:00.059436083 CEST	8.8.8.8	192.168.2.7	0xe56f	No error (0)	ci.rdtcdn.com	cs733.wpc.rncdn4.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:00.059436083 CEST	8.8.8.8	192.168.2.7	0xe56f	No error (0)	cs733.wpc.rncdn4.com		192.229.221.206	A (IP address)	IN (0x0001)
May 11, 2021 11:50:00.570705891 CEST	8.8.8.8	192.168.2.7	0x9c50	No error (0)	eu-adsrv.rtbsuperhub.com	tp-rtb-adserver-eu.eu-west-1.elasticbeanstalk.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:00.570705891 CEST	8.8.8.8	192.168.2.7	0x9c50	No error (0)	tp-rtb-adserver-eu.eu-west-1.elasticbeanstalk.com		54.72.255.40	A (IP address)	IN (0x0001)
May 11, 2021 11:50:00.570705891 CEST	8.8.8.8	192.168.2.7	0x9c50	No error (0)	tp-rtb-adserver-eu.eu-west-1.elasticbeanstalk.com		54.247.61.18	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2021 11:50:00.580288887 CEST	8.8.8.8	192.168.2.7	0xb4c1	No error (0)	ads.traffi cjunky.net		66.254.114.38	A (IP address)	IN (0x0001)
May 11, 2021 11:50:00.855999947 CEST	8.8.8.8	192.168.2.7	0xabaf	No error (0)	ht-cdn.tra fficjunky.net	ht-cdn.trafficjunky.net.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:00.855999947 CEST	8.8.8.8	192.168.2.7	0xabaf	No error (0)	ht-cdn.tra fficjunky. net.sds.rn cdn7.com		64.210.135.70	A (IP address)	IN (0x0001)
May 11, 2021 11:50:00.855999947 CEST	8.8.8.8	192.168.2.7	0xabaf	No error (0)	ht-cdn.tra fficjunky. net.sds.rn cdn7.com		64.210.135.72	A (IP address)	IN (0x0001)
May 11, 2021 11:50:00.855999947 CEST	8.8.8.8	192.168.2.7	0xabaf	No error (0)	ht-cdn.tra fficjunky. net.sds.rn cdn7.com		64.210.135.68	A (IP address)	IN (0x0001)
May 11, 2021 11:50:01.427908897 CEST	8.8.8.8	192.168.2.7	0x242d	No error (0)	ci.rdtcdn.com	cs733.wpc.rncdn4.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:01.427908897 CEST	8.8.8.8	192.168.2.7	0x242d	No error (0)	cs733.wpc. rncdn4.com		192.229.221.206	A (IP address)	IN (0x0001)
May 11, 2021 11:50:03.660826921 CEST	8.8.8.8	192.168.2.7	0x99eb	No error (0)	horunekulo .website		193.239.85.9	A (IP address)	IN (0x0001)
May 11, 2021 11:50:03.877849102 CEST	8.8.8.8	192.168.2.7	0x2517	No error (0)	www.redtub e.com	redtube.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:03.877849102 CEST	8.8.8.8	192.168.2.7	0x2517	No error (0)	redtube.com		66.254.114.238	A (IP address)	IN (0x0001)
May 11, 2021 11:50:04.335633993 CEST	8.8.8.8	192.168.2.7	0x5024	No error (0)	cdn1d-static-shared. phncdn.com	vip0x08e.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:04.335633993 CEST	8.8.8.8	192.168.2.7	0x5024	No error (0)	vip0x08e.s sl.rncdn5.com		205.185.208.142	A (IP address)	IN (0x0001)
May 11, 2021 11:50:04.348226070 CEST	8.8.8.8	192.168.2.7	0x2d41	No error (0)	static.tra fficjunky.com	vip0x04f.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:04.348226070 CEST	8.8.8.8	192.168.2.7	0x2d41	No error (0)	vip0x04f.s sl.rncdn5.com		205.185.208.79	A (IP address)	IN (0x0001)
May 11, 2021 11:50:04.352222919 CEST	8.8.8.8	192.168.2.7	0xf7af	No error (0)	ei.rdtcdn.com	ei.rdtcdn.com.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:04.352222919 CEST	8.8.8.8	192.168.2.7	0xf7af	No error (0)	ei.rdtcdn. com.sds.rn cdn7.com		64.210.135.68	A (IP address)	IN (0x0001)
May 11, 2021 11:50:04.352222919 CEST	8.8.8.8	192.168.2.7	0xf7af	No error (0)	ei.rdtcdn. com.sds.rn cdn7.com		64.210.135.70	A (IP address)	IN (0x0001)
May 11, 2021 11:50:04.352222919 CEST	8.8.8.8	192.168.2.7	0xf7af	No error (0)	ei.rdtcdn. com.sds.rn cdn7.com		64.210.135.72	A (IP address)	IN (0x0001)
May 11, 2021 11:50:04.765985012 CEST	8.8.8.8	192.168.2.7	0x2637	No error (0)	a.adtng.com		216.18.168.166	A (IP address)	IN (0x0001)
May 11, 2021 11:50:04.773502111 CEST	8.8.8.8	192.168.2.7	0x28d5	No error (0)	ads.traffi cjunky.net		66.254.114.38	A (IP address)	IN (0x0001)
May 11, 2021 11:50:04.997364044 CEST	8.8.8.8	192.168.2.7	0x979f	No error (0)	hw-cdn2.ad tng.com	vip0x019.map2.ssl.hwcdn .net		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:16.475475073 CEST	8.8.8.8	192.168.2.7	0xf0a1	No error (0)	horunekulo .website		193.239.85.9	A (IP address)	IN (0x0001)
May 11, 2021 11:50:16.692681074 CEST	8.8.8.8	192.168.2.7	0x9794	No error (0)	www.redtub e.com	redtube.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:16.692681074 CEST	8.8.8.8	192.168.2.7	0x9794	No error (0)	redtube.com		66.254.114.238	A (IP address)	IN (0x0001)
May 11, 2021 11:50:17.170727015 CEST	8.8.8.8	192.168.2.7	0x5df9	No error (0)	static.tra fficjunky.com	vip0x04f.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2021 11:50:17.170727015 CEST	8.8.8.8	192.168.2.7	0x5df9	No error (0)	vip0x04f.ssl.rncdn5.com		205.185.208.79	A (IP address)	IN (0x0001)
May 11, 2021 11:50:17.171204090 CEST	8.8.8.8	192.168.2.7	0xfeb8	No error (0)	cdn1d-static-shared.phncdn.com	vip0x08e.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:17.171204090 CEST	8.8.8.8	192.168.2.7	0xfeb8	No error (0)	vip0x08e.ssl.rncdn5.com		205.185.208.142	A (IP address)	IN (0x0001)
May 11, 2021 11:50:17.177534103 CEST	8.8.8.8	192.168.2.7	0x1ef9	No error (0)	ei.rdtcdn.com	ei.rdtcdn.com.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:17.177534103 CEST	8.8.8.8	192.168.2.7	0x1ef9	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.72	A (IP address)	IN (0x0001)
May 11, 2021 11:50:17.177534103 CEST	8.8.8.8	192.168.2.7	0x1ef9	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.68	A (IP address)	IN (0x0001)
May 11, 2021 11:50:17.177534103 CEST	8.8.8.8	192.168.2.7	0x1ef9	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		64.210.135.70	A (IP address)	IN (0x0001)
May 11, 2021 11:50:17.664822102 CEST	8.8.8.8	192.168.2.7	0xb81b	No error (0)	eu-adsrv.rtbsuperhub.com	tp-rtb-adserver-eu.eu-west-1.elasticbeanstalk.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:17.664822102 CEST	8.8.8.8	192.168.2.7	0xb81b	No error (0)	tp-rtb-adserver-eu.eu-west-1.elasticbeanstalk.com		54.72.255.40	A (IP address)	IN (0x0001)
May 11, 2021 11:50:17.664822102 CEST	8.8.8.8	192.168.2.7	0xb81b	No error (0)	tp-rtb-adserver-eu.eu-west-1.elasticbeanstalk.com		54.247.61.18	A (IP address)	IN (0x0001)
May 11, 2021 11:50:17.673472881 CEST	8.8.8.8	192.168.2.7	0x510a	No error (0)	ads.trafficjunky.net		66.254.114.38	A (IP address)	IN (0x0001)
May 11, 2021 11:50:17.703572989 CEST	8.8.8.8	192.168.2.7	0xde5f	No error (0)	a.adtng.com		216.18.168.166	A (IP address)	IN (0x0001)
May 11, 2021 11:50:18.153424978 CEST	8.8.8.8	192.168.2.7	0xe7bc	No error (0)	ht-cdn2.adtng.com	ht-cdn2.adtng.com.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:18.153424978 CEST	8.8.8.8	192.168.2.7	0xe7bc	No error (0)	ht-cdn2.adtng.com.sds.rncdn7.com		64.210.135.72	A (IP address)	IN (0x0001)
May 11, 2021 11:50:18.153424978 CEST	8.8.8.8	192.168.2.7	0xe7bc	No error (0)	ht-cdn2.adtng.com.sds.rncdn7.com		64.210.135.68	A (IP address)	IN (0x0001)
May 11, 2021 11:50:18.153424978 CEST	8.8.8.8	192.168.2.7	0xe7bc	No error (0)	ht-cdn2.adtng.com.sds.rncdn7.com		64.210.135.70	A (IP address)	IN (0x0001)
May 11, 2021 11:50:18.995031118 CEST	8.8.8.8	192.168.2.7	0x744d	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
May 11, 2021 11:50:18.995031118 CEST	8.8.8.8	192.168.2.7	0x744d	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
May 11, 2021 11:50:18.995031118 CEST	8.8.8.8	192.168.2.7	0x744d	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
May 11, 2021 11:50:18.995031118 CEST	8.8.8.8	192.168.2.7	0x744d	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
May 11, 2021 11:50:18.995031118 CEST	8.8.8.8	192.168.2.7	0x744d	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
May 11, 2021 11:50:18.995031118 CEST	8.8.8.8	192.168.2.7	0x744d	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
May 11, 2021 11:50:18.995031118 CEST	8.8.8.8	192.168.2.7	0x744d	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
May 11, 2021 11:50:18.995031118 CEST	8.8.8.8	192.168.2.7	0x744d	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
May 11, 2021 11:50:19.665263891 CEST	8.8.8.8	192.168.2.7	0x7462	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2021 11:50:19.665263891 CEST	8.8.8.8	192.168.2.7	0x7462	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:19.665263891 CEST	8.8.8.8	192.168.2.7	0x7462	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:19.665263891 CEST	8.8.8.8	192.168.2.7	0x7462	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:19.665263891 CEST	8.8.8.8	192.168.2.7	0x7462	No error (0)	FRA-efz.ms-acdc.office.com		40.101.80.194	A (IP address)	IN (0x0001)
May 11, 2021 11:50:19.665263891 CEST	8.8.8.8	192.168.2.7	0x7462	No error (0)	FRA-efz.ms-acdc.office.com		52.97.179.194	A (IP address)	IN (0x0001)
May 11, 2021 11:50:19.665263891 CEST	8.8.8.8	192.168.2.7	0x7462	No error (0)	FRA-efz.ms-acdc.office.com		40.101.18.34	A (IP address)	IN (0x0001)
May 11, 2021 11:50:19.879065990 CEST	8.8.8.8	192.168.2.7	0x6b6f	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:19.879065990 CEST	8.8.8.8	192.168.2.7	0x6b6f	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:19.879065990 CEST	8.8.8.8	192.168.2.7	0x6b6f	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:19.879065990 CEST	8.8.8.8	192.168.2.7	0x6b6f	No error (0)	FRA-efz.ms-acdc.office.com		40.101.12.98	A (IP address)	IN (0x0001)
May 11, 2021 11:50:19.879065990 CEST	8.8.8.8	192.168.2.7	0x6b6f	No error (0)	FRA-efz.ms-acdc.office.com		52.97.189.66	A (IP address)	IN (0x0001)
May 11, 2021 11:50:19.879065990 CEST	8.8.8.8	192.168.2.7	0x6b6f	No error (0)	FRA-efz.ms-acdc.office.com		40.101.12.82	A (IP address)	IN (0x0001)
May 11, 2021 11:50:21.931201935 CEST	8.8.8.8	192.168.2.7	0xb30f	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
May 11, 2021 11:50:21.931201935 CEST	8.8.8.8	192.168.2.7	0xb30f	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
May 11, 2021 11:50:21.931201935 CEST	8.8.8.8	192.168.2.7	0xb30f	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
May 11, 2021 11:50:21.931201935 CEST	8.8.8.8	192.168.2.7	0xb30f	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
May 11, 2021 11:50:21.931201935 CEST	8.8.8.8	192.168.2.7	0xb30f	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
May 11, 2021 11:50:21.931201935 CEST	8.8.8.8	192.168.2.7	0xb30f	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
May 11, 2021 11:50:21.931201935 CEST	8.8.8.8	192.168.2.7	0xb30f	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
May 11, 2021 11:50:21.931201935 CEST	8.8.8.8	192.168.2.7	0xb30f	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
May 11, 2021 11:50:22.572264910 CEST	8.8.8.8	192.168.2.7	0x2e80	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:22.572264910 CEST	8.8.8.8	192.168.2.7	0x2e80	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:22.572264910 CEST	8.8.8.8	192.168.2.7	0x2e80	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:22.572264910 CEST	8.8.8.8	192.168.2.7	0x2e80	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:22.572264910 CEST	8.8.8.8	192.168.2.7	0x2e80	No error (0)	FRA-efz.ms-acdc.office.com		40.101.80.194	A (IP address)	IN (0x0001)
May 11, 2021 11:50:22.572264910 CEST	8.8.8.8	192.168.2.7	0x2e80	No error (0)	FRA-efz.ms-acdc.office.com		52.97.179.194	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2021 11:50:22.572264910 CEST	8.8.8.8	192.168.2.7	0x2e80	No error (0)	FRA-efz.ms-acdc.office.com		40.101.18.34	A (IP address)	IN (0x0001)
May 11, 2021 11:50:22.798465967 CEST	8.8.8.8	192.168.2.7	0x3d8c	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:22.798465967 CEST	8.8.8.8	192.168.2.7	0x3d8c	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:22.798465967 CEST	8.8.8.8	192.168.2.7	0x3d8c	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:22.798465967 CEST	8.8.8.8	192.168.2.7	0x3d8c	No error (0)	FRA-efz.ms-acdc.office.com		40.101.12.98	A (IP address)	IN (0x0001)
May 11, 2021 11:50:22.798465967 CEST	8.8.8.8	192.168.2.7	0x3d8c	No error (0)	FRA-efz.ms-acdc.office.com		52.97.189.66	A (IP address)	IN (0x0001)
May 11, 2021 11:50:22.798465967 CEST	8.8.8.8	192.168.2.7	0x3d8c	No error (0)	FRA-efz.ms-acdc.office.com		40.101.12.82	A (IP address)	IN (0x0001)
May 11, 2021 11:50:26.324234962 CEST	8.8.8.8	192.168.2.7	0x610c	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
May 11, 2021 11:50:26.324234962 CEST	8.8.8.8	192.168.2.7	0x610c	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
May 11, 2021 11:50:26.324234962 CEST	8.8.8.8	192.168.2.7	0x610c	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
May 11, 2021 11:50:26.324234962 CEST	8.8.8.8	192.168.2.7	0x610c	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
May 11, 2021 11:50:26.324234962 CEST	8.8.8.8	192.168.2.7	0x610c	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
May 11, 2021 11:50:26.324234962 CEST	8.8.8.8	192.168.2.7	0x610c	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
May 11, 2021 11:50:26.324234962 CEST	8.8.8.8	192.168.2.7	0x610c	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
May 11, 2021 11:50:26.324234962 CEST	8.8.8.8	192.168.2.7	0x610c	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
May 11, 2021 11:50:26.987087011 CEST	8.8.8.8	192.168.2.7	0x80e0	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:26.987087011 CEST	8.8.8.8	192.168.2.7	0x80e0	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:26.987087011 CEST	8.8.8.8	192.168.2.7	0x80e0	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:26.987087011 CEST	8.8.8.8	192.168.2.7	0x80e0	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:26.987087011 CEST	8.8.8.8	192.168.2.7	0x80e0	No error (0)	FRA-efz.ms-acdc.office.com		40.101.80.194	A (IP address)	IN (0x0001)
May 11, 2021 11:50:26.987087011 CEST	8.8.8.8	192.168.2.7	0x80e0	No error (0)	FRA-efz.ms-acdc.office.com		52.97.179.194	A (IP address)	IN (0x0001)
May 11, 2021 11:50:26.987087011 CEST	8.8.8.8	192.168.2.7	0x80e0	No error (0)	FRA-efz.ms-acdc.office.com		40.101.18.34	A (IP address)	IN (0x0001)
May 11, 2021 11:50:27.200872898 CEST	8.8.8.8	192.168.2.7	0x6b73	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:27.200872898 CEST	8.8.8.8	192.168.2.7	0x6b73	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:27.200872898 CEST	8.8.8.8	192.168.2.7	0x6b73	No error (0)	outlook.ms-acdc.office.com	FRA-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 11:50:27.200872898 CEST	8.8.8.8	192.168.2.7	0x6b73	No error (0)	FRA-efz.ms-acdc.office.com		40.101.121.2	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2021 11:50:27.200872898 CEST	8.8.8.8	192.168.2.7	0x6b73	No error (0)	FRA-efz.ms-acdc.office.com		40.101.82.66	A (IP address)	IN (0x0001)
May 11, 2021 11:50:27.200872898 CEST	8.8.8.8	192.168.2.7	0x6b73	No error (0)	FRA-efz.ms-acdc.office.com		40.101.83.194	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- outlook.com
- worunekulo.club

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49750	40.97.156.114	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 11, 2021 11:48:41.535617113 CEST	3458	OUT	GET /login/greed/x8W8BNR9UNCZa/Twkc4UWe/ksrEjoqLIMBWgNaXvBBgZQc/7caPZuKhoQ/RRVEx1vfxGm0Ey0rb/Uh6f5JDIXEpV/q_2Bb3SOxEk/K4Ba_2Fm2_2Bk6/1iyy5sVNaXkrgbBDKGzsA/BeIz00apTsUFxLa_/2BumG9e60bYFjKm/ZscTD_2FY9vxRMElqg/FcOC6LblG/vifbEO2R5/iTmOFe.gfk 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: outlook.com Connection: Keep-Alive
May 11, 2021 11:48:41.700164080 CEST	3459	IN	HTTP/1.1 301 Moved Permanently Cache-Control: no-cache Pragma: no-cache Location: https://outlook.com/login/greed/x8W8BNR9UNCZa/Twkc4UWe/ksrEjoqLIMBWgNaXvBBgZQc/7caPZuKhoQ/RRVEx1vfxGm0Ey0rb/Uh6f5JDIXEpV/q_2Bb3SOxEk/K4Ba_2Fm2_2Bk6/1iyy5sVNaXkrgbBDKGzsA/BeIz00apTsUFxLa_/2BumG9e60bYFjKm/ZscTD_2FY9vxRMElqg/FcOC6LblG/vifbEO2R5/iTmOFe.gfk Server: Microsoft-IIS/10.0 request-id: 1e7c4ead-af2b-4301-ba7e-88357dd177fb X-FEServer: CY4PR19CA0026 X-RequestId: ab62c142-8249-45d6-b0fd-42e78b32f24e X-Powered-By: ASP.NET X-FEServer: CY4PR19CA0026 Date: Tue, 11 May 2021 09:48:40 GMT Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49789	193.239.84.195	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 11, 2021 11:49:31.342396021 CEST	4127	OUT	GET /greed/Q7ECAhkT09Dh5Dxzx5NND/wHPvdjMQo9yvTSlz/72Cz1yfrj9oas3F/mlrImmXnF4mFMyXsRS/lAfcYLSQz/emv5Y2LTHh0gnSKiYnKd/yiqaLkEsaxUTLIXXXkb/fKBJ2kKvoXtzyu88vwhB6r/sfNLlep0RDB8s/ZFdFWunl/pI1RYpuDgoeDLfkKFeCA_2F/BTJiso9B2W/oRKpS4iwlP_2BxR5_/2FtiB90t/R.gfk 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: worunekulo.club Connection: Keep-Alive
May 11, 2021 11:49:31.419226885 CEST	4128	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 09:49:31 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=335canep13hvkebpmqaacpani7; path=/; domain=.worunekulo.club 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, 10-Jun-2021 09:49:31 GMT; path=/; domain=.worunekulo.club 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
2	192.168.2.7	49823	193.239.84.195	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 11, 2021 11:49:35.872701883 CEST	4979	OUT	GET /greed/_2FRF_2BPV_2B/kygTBNPD/3KvqYljpUn5GpP9FZL6h4EP/n2hICjjuVt/fRTxCBY_2FTxiYqGE/_2B qBmeHQlfJ/5yN_2BFPPko/aPrCq0LATuM0Yj/xSRcH9YbNoYOYFPU5j0Yb/J6dDSV1S32l5lzwp/s_2BeiZK7kJcTz t/2g0iO1FeUD9_2FG8Cy/0_2FjmfFQ/bCqeiOGFxJJiMTIYqg1G/x6NI_2BxB_2BJKrBrYW/5Jjkit05/lt.gfk 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: worunekulo.club Connection: Keep-Alive Cookie: lang=en; PHPSESSID=335canep13hvkebpmqaacpani7
May 11, 2021 11:49:35.951263905 CEST	4988	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 09:49:35 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache 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
3	192.168.2.7	49843	193.239.84.195	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 11, 2021 11:49:40.827115059 CEST	5354	OUT	GET /greed/F352AkfI75R/nnGZl7kgYZmZtF/n_2BZNmpOaaPMOBPEMfHy/L8scTzRnbkdx1Pzo/s63ydPt_2FI2Z uh/HHNH5EUrwQuwFJC1YQ/kpldDVoYT/fy1ebx7pG01iZFqz4wvc/pjfEO3ohCd1NL4CwgXD/tdqZuz_2B7jufFfWZ KLxYE/aZBP7pGzL7Mr_/2FRlhbYj/y1Ii_2B9s0NXoB_/2Fx.gfk 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: worunekulo.club Connection: Keep-Alive Cookie: lang=en; PHPSESSID=335canep13hvkebpmqaacpani7
May 11, 2021 11:49:40.904372931 CEST	5355	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 09:49:40 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache 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
4	192.168.2.7	49862	193.239.84.195	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 11, 2021 11:49:53.494760990 CEST	9903	OUT	GET /greed/pGZcMLTjvozycR9968/57cPpvkwZ/9qRr4Mue98jwKhB_2Fs5/049L1hlTokuOisRB694/Esl4TOdng jqpGDqBHS_2Fm/kWGIM1nSB_2BE/reszSL96/dYK1VEkrqG8kF7gC7fiisTb/w0fTbIZX6n/nVm_2BA0w9LkgWRTL/ XlRI8guLQdNv/IZNYvrINchH/lGcaeCA61ubYe_2FGE/An.gfk 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: worunekulo.club Connection: Keep-Alive Cookie: lang=en; PHPSESSID=335canep13hvkebpmqaacpani7

Timestamp	kBytes transferred	Direction	Data
May 11, 2021 11:49:53.580962896 CEST	9904	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 11 May 2021 09:49:53 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache 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
May 11, 2021 11:48:19.992811918 CEST	104.20.184.68	443	192.168.2.7	49718	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		
May 11, 2021 11:48:19.994335890 CEST	104.20.184.68	443	192.168.2.7	49719	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		
May 11, 2021 11:48:25.043406963 CEST	151.101.1.44	443	192.168.2.7	49735	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
May 11, 2021 11:48:25.045233965 CEST	151.101.1.44	443	192.168.2.7	49736	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 11, 2021 11:48:25.045738935 CEST	151.101.1.44	443	192.168.2.7	49734	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		
May 11, 2021 11:48:25.048978090 CEST	151.101.1.44	443	192.168.2.7	49738	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
May 11, 2021 11:48:25.049635887 CEST	151.101.1.44	443	192.168.2.7	49739	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
May 11, 2021 11:48:25.052501917 CEST	151.101.1.44	443	192.168.2.7	49737	CN=*.taboola.com, O="Taboola, Inc", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Nov 25 01:00:00 CET 2020	Mon Dec 27 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
May 11, 2021 11:49:07.675179958 CEST	172.217.19.101	443	192.168.2.7	49776	CN=gmail.com, 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 Apr 13 12:15:46 CEST 2021	Tue Jul 06 12:15:45 CEST 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
May 11, 2021 11:49:07.675256968 CEST	172.217.19.101	443	192.168.2.7	49775	CN=gmail.com, 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 Apr 13 12:15:46 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:15:45 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		
May 11, 2021 11:49:12.897660971 CEST	172.217.19.101	443	192.168.2.7	49785	CN=gmail.com, 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 Apr 13 12:15:46 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:15:45 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		
May 11, 2021 11:49:12.897746086 CEST	172.217.19.101	443	192.168.2.7	49784	CN=gmail.com, 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 Apr 13 12:15:46 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:15:45 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		
May 11, 2021 11:49:17.814146996 CEST	172.217.19.101	443	192.168.2.7	49786	CN=gmail.com, 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 Apr 13 12:15:46 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:15:45 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		
May 11, 2021 11:49:17.814167976 CEST	172.217.19.101	443	192.168.2.7	49787	CN=gmail.com, 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 Apr 13 12:15:46 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:15:45 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
May 11, 2021 11:49:31.468349934 CEST	172.217.19.101	443	192.168.2.7	49791	CN=gmail.com, 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 Apr 13 12:15:46 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:15:45 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		
May 11, 2021 11:49:31.469208002 CEST	172.217.19.101	443	192.168.2.7	49790	CN=gmail.com, 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 Apr 13 12:15:46 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:15:45 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		
May 11, 2021 11:49:31.586395979 CEST	66.254.114.238	443	192.168.2.7	49792	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		
May 11, 2021 11:49:31.592850924 CEST	66.254.114.238	443	192.168.2.7	49793	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		
May 11, 2021 11:49:32.176245928 CEST	66.254.114.32	443	192.168.2.7	49794	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 11, 2021 11:49:32.176672935 CEST	66.254.114.32	443	192.168.2.7	49795	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		
May 11, 2021 11:49:32.274455070 CEST	205.185.208.79	443	192.168.2.7	49797	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		
May 11, 2021 11:49:32.275477886 CEST	205.185.208.79	443	192.168.2.7	49796	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		
May 11, 2021 11:49:32.413266897 CEST	64.210.135.72	443	192.168.2.7	49798	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
May 11, 2021 11:49:32.417588949 CEST	64.210.135.72	443	192.168.2.7	49802	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		
May 11, 2021 11:49:32.417656898 CEST	64.210.135.72	443	192.168.2.7	49801	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		
May 11, 2021 11:49:32.417977095 CEST	64.210.135.72	443	192.168.2.7	49803	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
May 11, 2021 11:49:32.418107986 CEST	64.210.135.72	443	192.168.2.7	49800	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		
May 11, 2021 11:49:32.418452978 CEST	64.210.135.72	443	192.168.2.7	49799	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		
May 11, 2021 11:49:32.924798012 CEST	205.185.208.142	443	192.168.2.7	49806	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		
May 11, 2021 11:49:32.934506893 CEST	205.185.208.142	443	192.168.2.7	49807	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 11, 2021 11:49:33.567441940 CEST	173.194.76.156	443	192.168.2.7	49809	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 Apr 13 12:11:12 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:11:11 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		
May 11, 2021 11:49:33.567478895 CEST	173.194.76.156	443	192.168.2.7	49808	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 Apr 13 12:11:12 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:11:11 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		
May 11, 2021 11:49:33.916044950 CEST	66.254.114.38	443	192.168.2.7	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		
May 11, 2021 11:49:33.916587114 CEST	66.254.114.38	443	192.168.2.7	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		
May 11, 2021 11:49:33.975029945 CEST	172.217.16.99	443	192.168.2.7	49814	CN=www.google.de, 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 Apr 13 12:16:15 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:16:14 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
May 11, 2021 11:49:33.975589037 CEST	172.217.16.99	443	192.168.2.7	49815	CN=www.google.de, 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 Apr 13 12:16:15 CEST 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Jul 06 12:16:14 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		
May 11, 2021 11:49:34.160644054 CEST	64.210.135.70	443	192.168.2.7	49816	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		
May 11, 2021 11:49:34.161583900 CEST	64.210.135.70	443	192.168.2.7	49818	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		
May 11, 2021 11:49:34.163002014 CEST	64.210.135.70	443	192.168.2.7	49817	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		
May 11, 2021 11:49:36.123533964 CEST	66.254.114.238	443	192.168.2.7	49824	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 11, 2021 11:49:36.123568058 CEST	66.254.114.238	443	192.168.2.7	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		
May 11, 2021 11:49:37.514276028 CEST	192.229.221.206	443	192.168.2.7	49831	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		
May 11, 2021 11:49:37.514349937 CEST	192.229.221.206	443	192.168.2.7	49826	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		
May 11, 2021 11:49:37.515934944 CEST	192.229.221.206	443	192.168.2.7	49827	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

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		
					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		
May 11, 2021 11:49:37.525319099 CEST	192.229.221.206	443	192.168.2.7	49830	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		
May 11, 2021 11:49:37.525964975 CEST	192.229.221.206	443	192.168.2.7	49828	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		
May 11, 2021 11:49:37.526519060 CEST	192.229.221.206	443	192.168.2.7	49829	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		
May 11, 2021 11:49:38.635339975 CEST	216.18.168.166	443	192.168.2.7	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		
May 11, 2021 11:49:38.646166086 CEST	216.18.168.166	443	192.168.2.7	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		
May 11, 2021 11:49:38.646704912 CEST	66.254.114.38	443	192.168.2.7	49836	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		
May 11, 2021 11:49:38.646820068 CEST	66.254.114.38	443	192.168.2.7	49837	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		
May 11, 2021 11:49:39.164829016 CEST	64.210.135.70	443	192.168.2.7	49841	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
May 11, 2021 11:49:39.198648930 CEST	64.210.135.70	443	192.168.2.7	49840	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		
May 11, 2021 11:49:41.085050106 CEST	66.254.114.238	443	192.168.2.7	49845	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		
May 11, 2021 11:49:41.085092068 CEST	66.254.114.238	443	192.168.2.7	49844	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		
May 11, 2021 11:49:42.597035885 CEST	54.247.61.18	443	192.168.2.7	49849	CN=eu-adsrv.rtbsuperhub.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Oct 12 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Nov 11 13:00:00 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 11, 2021 11:49:42.608819008 CEST	66.254.114.38	443	192.168.2.7	49850	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		
May 11, 2021 11:49:42.608906031 CEST	66.254.114.38	443	192.168.2.7	49851	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		
May 11, 2021 11:49:42.618354082 CEST	54.247.61.18	443	192.168.2.7	49848	CN=eu-adsrv.rtbsuperhub.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Oct 12 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Nov 11 13:00:00 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 11, 2021 11:49:42.645701885 CEST	192.229.221.215	443	192.168.2.7	49853	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
May 11, 2021 11:49:42.645762920 CEST	192.229.221.215	443	192.168.2.7	49852	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		
May 11, 2021 11:49:53.734014988 CEST	66.254.114.238	443	192.168.2.7	49864	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		
May 11, 2021 11:49:53.734077930 CEST	66.254.114.238	443	192.168.2.7	49863	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		
May 11, 2021 11:49:55.036817074 CEST	192.229.221.206	443	192.168.2.7	49873	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
May 11, 2021 11:49:55.041095972 CEST	192.229.221.206	443	192.168.2.7	49870	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		
May 11, 2021 11:49:55.041819096 CEST	192.229.221.206	443	192.168.2.7	49871	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		
May 11, 2021 11:49:55.042759895 CEST	192.229.221.206	443	192.168.2.7	49874	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
May 11, 2021 11:49:55.043874025 CEST	192.229.221.206	443	192.168.2.7	49872	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		
May 11, 2021 11:49:55.047302961 CEST	192.229.221.206	443	192.168.2.7	49869	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		
May 11, 2021 11:49:55.071100950 CEST	54.247.61.18	443	192.168.2.7	49868	CN=eu-adsrv.rtbsuperhub.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Oct 12 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Nov 11 13:00:00 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 11, 2021 11:49:55.090912104 CEST	54.247.61.18	443	192.168.2.7	49867	CN=eu-adsrv.rtbsuperhub.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Mon Oct 12 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu Nov 11 13:00:00 CET 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	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=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 11, 2021 11:49:55.115293980 CEST	66.254.114.38	443	192.168.2.7	49875	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		
May 11, 2021 11:49:55.115313053 CEST	66.254.114.38	443	192.168.2.7	49876	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		
May 11, 2021 11:49:55.155919075 CEST	216.18.168.166	443	192.168.2.7	49877	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

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		
May 11, 2021 11:49:55.155986071 CEST	216.18.168.166	443	192.168.2.7	49878	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		
May 11, 2021 11:49:55.410718918 CEST	66.254.114.238	443	192.168.2.7	49885	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		
May 11, 2021 11:49:55.410878897 CEST	66.254.114.238	443	192.168.2.7	49886	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		
May 11, 2021 11:49:56.397809982 CEST	66.254.114.38	443	192.168.2.7	49897	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		
May 11, 2021 11:49:56.397850990 CEST	66.254.114.38	443	192.168.2.7	49898	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
May 11, 2021 11:49:56.421114922 CEST	216.18.168.166	443	192.168.2.7	49899	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		
May 11, 2021 11:49:56.421251059 CEST	216.18.168.166	443	192.168.2.7	49900	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		
May 11, 2021 11:49:56.884752035 CEST	64.210.135.70	443	192.168.2.7	49903	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		
May 11, 2021 11:49:56.886184931 CEST	64.210.135.70	443	192.168.2.7	49904	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		
May 11, 2021 11:49:57.316638947 CEST	64.210.135.72	443	192.168.2.7	49911	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		
May 11, 2021 11:49:57.317187071 CEST	64.210.135.72	443	192.168.2.7	49908	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		
May 11, 2021 11:49:57.317287922 CEST	64.210.135.72	443	192.168.2.7	49909	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		
May 11, 2021 11:49:57.317437887 CEST	64.210.135.72	443	192.168.2.7	49910	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
May 11, 2021 11:49:57.322228909 CEST	205.185.208.142	443	192.168.2.7	49905	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		
May 11, 2021 11:49:57.322300911 CEST	64.210.135.72	443	192.168.2.7	49907	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		
May 11, 2021 11:49:57.323788881 CEST	205.185.208.142	443	192.168.2.7	49906	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		
May 11, 2021 11:49:59.672148943 CEST	66.254.114.238	443	192.168.2.7	49915	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		
May 11, 2021 11:49:59.672343969 CEST	66.254.114.238	443	192.168.2.7	49914	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

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		
May 11, 2021 11:50:00.670340061 CEST	66.254.114.38	443	192.168.2.7	49920	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		
May 11, 2021 11:50:00.670489073 CEST	66.254.114.38	443	192.168.2.7	49921	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		
May 11, 2021 11:50:00.961087942 CEST	64.210.135.70	443	192.168.2.7	49922	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		
May 11, 2021 11:50:00.961966038 CEST	64.210.135.70	443	192.168.2.7	49923	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		
May 11, 2021 11:50:01.513295889 CEST	192.229.221.206	443	192.168.2.7	49924	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

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		
					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		
May 11, 2021 11:50:01.513633966 CEST	192.229.221.206	443	192.168.2.7	49925	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		
May 11, 2021 11:50:01.513731956 CEST	192.229.221.206	443	192.168.2.7	49926	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		
May 11, 2021 11:50:01.513817072 CEST	192.229.221.206	443	192.168.2.7	49928	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		
May 11, 2021 11:50:01.515012026 CEST	192.229.221.206	443	192.168.2.7	49927	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		
May 11, 2021 11:50:03.970041990 CEST	66.254.114.238	443	192.168.2.7	49932	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		
May 11, 2021 11:50:03.970108986 CEST	66.254.114.238	443	192.168.2.7	49931	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		
May 11, 2021 11:50:04.854944944 CEST	216.18.168.166	443	192.168.2.7	49935	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
May 11, 2021 11:50:04.855114937 CEST	216.18.168.166	443	192.168.2.7	49936	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		
May 11, 2021 11:50:04.864460945 CEST	66.254.114.38	443	192.168.2.7	49937	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		
May 11, 2021 11:50:04.864595890 CEST	66.254.114.38	443	192.168.2.7	49938	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		
May 11, 2021 11:50:16.788839102 CEST	66.254.114.238	443	192.168.2.7	49953	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		
May 11, 2021 11:50:16.789460897 CEST	66.254.114.238	443	192.168.2.7	49954	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 11, 2021 11:50:17.762064934 CEST	66.254.114.38	443	192.168.2.7	49962	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		
May 11, 2021 11:50:17.762105942 CEST	66.254.114.38	443	192.168.2.7	49961	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		
May 11, 2021 11:50:17.792038918 CEST	216.18.168.166	443	192.168.2.7	49963	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		
May 11, 2021 11:50:17.792094946 CEST	216.18.168.166	443	192.168.2.7	49964	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		
May 11, 2021 11:50:18.256979942 CEST	64.210.135.72	443	192.168.2.7	49966	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
May 11, 2021 11:50:18.257072926 CEST	64.210.135.72	443	192.168.2.7	49965	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

System Behavior

Analysis Process: loaddll32.exe PID: 5784 Parent PID: 5692

General

Start time:	11:48:13
Start date:	11/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\FuiZSHt8Hx.dll'
Imagebase:	0x1290000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
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: 00000000.00000003.299753602.0000000001C58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299604342.0000000001C58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.505193431.000000000195E000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299890118.0000000001C58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.456134462.0000000001ADB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299841625.0000000001C58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299876033.0000000001C58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299860809.0000000001C58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299789667.0000000001C58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.299718018.0000000001C58000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 4912 Parent PID: 5784

General

Start time:	11:48:13
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\FuiZSHt8Hx.dll',#1
Imagebase:	0x870000
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: regsvr32.exe PID: 5728 Parent PID: 5784

General

Start time:	11:48:13
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe

Wow64 process (32bit):	true
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\FuiZSHt8Hx.dll
Imagebase:	0x1040000
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: 00000002.00000003.352305744.0000000005B58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.352331416.0000000005B58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.352017911.0000000005B58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.352085595.0000000005B58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.352161012.0000000005B58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.352376422.0000000005B58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.352264793.0000000005B58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.352363162.0000000005B58000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.502162475.00000000059DB000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 5408 Parent PID: 4912

General

Start time:	11:48:14
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\FuiZSHt8Hx.dll',#1
Imagebase:	0xf10000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 00000003.00000003.312963650.0000000004E18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.463276502.0000000004C9B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.313024101.0000000004E18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.313081481.0000000004E18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.313097201.0000000004E18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.312908121.0000000004E18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.313049365.0000000004E18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.312877235.0000000004E18000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000003.313002300.0000000004E18000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 4680 Parent PID: 5784

General

Start time:	11:48:14
Start date:	11/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Internet Explorer\iexplore.exe
Imagebase:	0x7ff688f10000
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	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: rundll32.exe PID: 5508 Parent PID: 5784

General

Start time:	11:48:14
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\FuiZSHt8Hx.dll,DllRegisterServer
Imagebase:	0xf10000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 00000005.00000003.471813854.0000000004E3B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.323949143.0000000004FB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.323823967.0000000004FB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.323904731.0000000004FB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.323930913.0000000004FB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.323972319.0000000004FB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.323708729.0000000004FB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.323857578.0000000004FB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.323786241.0000000004FB8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 4456 Parent PID: 4680

General

Start time:	11:48:15
Start date:	11/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:17410 /prefetch:2
Imagebase:	0xd40000
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: 2148 Parent PID: 4680

General

Start time:	11:48:39
Start date:	11/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:17428 /prefetch:2
Imagebase:	0xd40000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: iexplore.exe PID: 6552 Parent PID: 4680

General

Start time:	11:48:47
Start date:	11/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:17432 /prefetch:2
Imagebase:	0xd40000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: iexplore.exe PID: 1148 Parent PID: 4680

General

Start time:	11:48:52
Start date:	11/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:82970 /prefetch:2

Imagebase:	0xd40000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: iexplore.exe PID: 3152 Parent PID: 4680

General

Start time:	11:49:05
Start date:	11/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:17448 /prefetch:2
Imagebase:	0xd40000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: iexplore.exe PID: 6504 Parent PID: 4680

General

Start time:	11:49:06
Start date:	11/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:82976 /prefetch:2
Imagebase:	0xd40000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: iexplore.exe PID: 4164 Parent PID: 4680

General

Start time:	11:49:11
Start date:	11/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:82990 /prefetch:2
Imagebase:	0xd40000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: iexplore.exe PID: 6564 Parent PID: 4680

General

Start time:	11:49:16
Start date:	11/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:17476 /prefetch:2
Imagebase:	0xd40000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 3264 Parent PID: 4680

General

Start time:	11:49:29
Start date:	11/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:83006 /prefetch:2
Imagebase:	0xd40000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 6576 Parent PID: 4680

General

Start time:	11:49:29
Start date:	11/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:17480 /prefetch:2
Imagebase:	0xd40000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 5828 Parent PID: 4680

General

Start time:	11:49:34
Start date:	11/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:17492 /prefetch:2
Imagebase:	0xd40000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: iexplore.exe PID: 6684 Parent PID: 4680

General

Start time:	11:49:39
Start date:	11/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4680 CREDAT:83014 /prefetch:2
Imagebase:	0xd40000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis