



ID: 333815
Sample Name:
DSC_Canon_23.12.2020.zip
Cookbook: default.jbs
Time: 02:36:02
Date: 24/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report DSC_Canon_23.12.2020.zip 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: Ursnif 4
Yara Overview 4
Memory Dumps 5
Sigma Overview 5
Signature Overview 5
AV Detection: 5
Networking: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
E-Banking Fraud: 5
System Summary: 6
Hooking and other Techniques for Hiding and Protection: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 13
Public 13
General Information 13
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 17
ASN 18
JA3 Fingerprints 20
Dropped Files 22
Created / dropped Files 22
Static File Info 47
General 47
File Icon 48
Static PE Info 48
General 48
Entrypoint Preview 48
Rich Headers 49
Data Directories 50
Sections 50

Resources 50
Imports 50
Version Infos 50
Possible Origin 50
Network Behavior 51
Snort IDS Alerts 51
Network Port Distribution 51
TCP Packets 51
UDP Packets 53
ICMP Packets 55
DNS Queries 55
DNS Answers 56
HTTP Request Dependency Graph 58
HTTP Packets 58
HTTPS Packets 58
Code Manipulations 63
Statistics 63
Behavior 63
System Behavior 63
Analysis Process: DSC_Canon_23.12.2020.exe PID: 4120 Parent PID: 5768 63
General 63
File Activities 64
Analysis Process: iexplore.exe PID: 5532 Parent PID: 792 64
General 64
File Activities 64
Registry Activities 65
Analysis Process: iexplore.exe PID: 1376 Parent PID: 5532 65
General 65
File Activities 65
Analysis Process: iexplore.exe PID: 6308 Parent PID: 792 65
General 65
File Activities 66
Registry Activities 66
Analysis Process: iexplore.exe PID: 6720 Parent PID: 6308 66
General 66
File Activities 66
Registry Activities 66
Analysis Process: iexplore.exe PID: 5436 Parent PID: 792 66
General 66
File Activities 67
Registry Activities 67
Analysis Process: iexplore.exe PID: 2156 Parent PID: 5436 67
General 67
File Activities 67
Analysis Process: iexplore.exe PID: 5008 Parent PID: 792 67
General 67
File Activities 68
Registry Activities 68
Analysis Process: iexplore.exe PID: 5920 Parent PID: 5008 68
General 68
File Activities 68
Disassembly 68
Code Analysis 69

Copyright null 2020

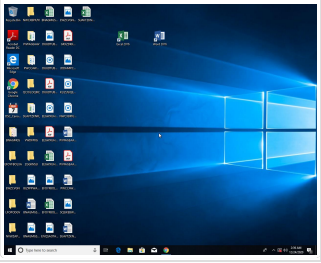
Analysis Report DSC_Canon_23.12.2020.zip

Overview

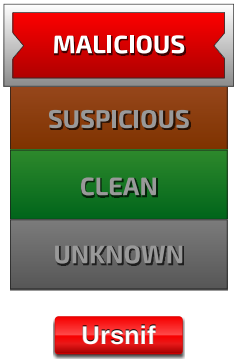
General Information

Sample Name:	DSC_Canon_23.12.2020.zip (renamed file extension from zip to exe)
Analysis ID:	333815
MD5:	1900f3bd2b1848b.
SHA1:	38de4f6bbd82ee5.
SHA256:	dddf5829a3bdcb2.
Tags:	PseudoGate SpelevoEK

Most interesting Screenshot:



Detection

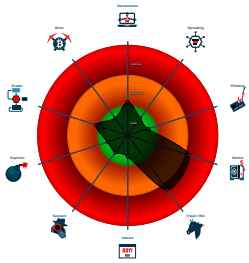


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Yara detected Ursnif
- Creates a COM Internet Explorer ob…
- Machine Learning detection for samp…
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- Antivirus or Machine Learning detec…
- Contains functionality to call native f…
- Contains functionality to dynamically…
- Contains functionality to read the PEB
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…

Classification



Startup

- **System is w10x64**
- DSC_Canon_23.12.2020.exe (PID: 4120 cmdline: 'C:\Users\user\Desktop\DSC_Canon_23.12.2020.exe' MD5: 1900F3BD2B1848B0F4B1A0495F11D84E)
- iexplore.exe (PID: 5532 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1376 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5532 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 6308 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6720 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6308 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 5436 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 2156 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5436 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 5008 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 5920 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5008 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "server": "12",
  "version": "250161",
  "uptime": "195hhNZ",
  "crc": "1",
  "id": "8005",
  "user": "253fc4ee08f8d2d8cdc8873ad5baae71",
  "soft": "3"
}
```


Yara Overview

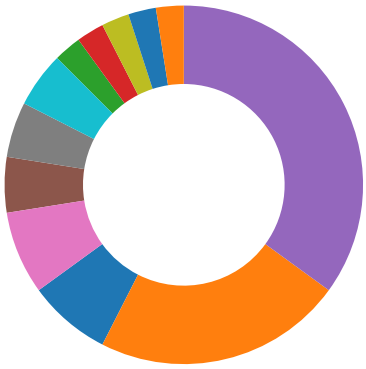
Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.229172287.0000000006578000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.229113119.0000000006578000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.229242754.0000000006578000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.229145685.0000000006578000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.376997150.00000000063FB000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:



Found malware configuration

Machine Learning detection for sample

Networking:



Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Creates a COM Internet Explorer object

Key, Mouse, Clipboard, Microphone and Screen Capturing:



Yara detected Ursnif

E-Banking Fraud:



Yara detected Ursnif

Copyright null 2020

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:

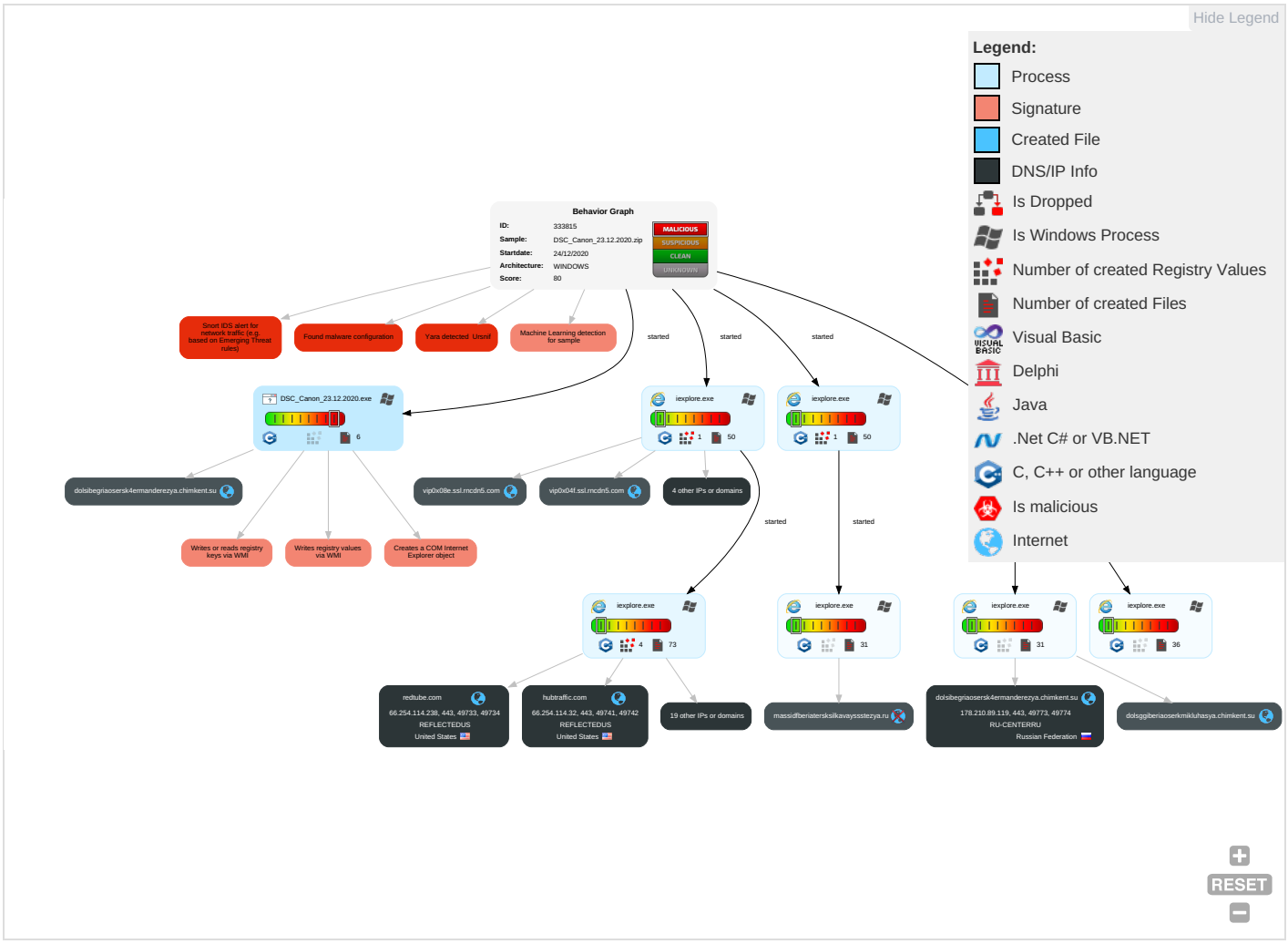


Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Windows Management Instrumentation 2	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Dev Without Authorizat
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizat
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

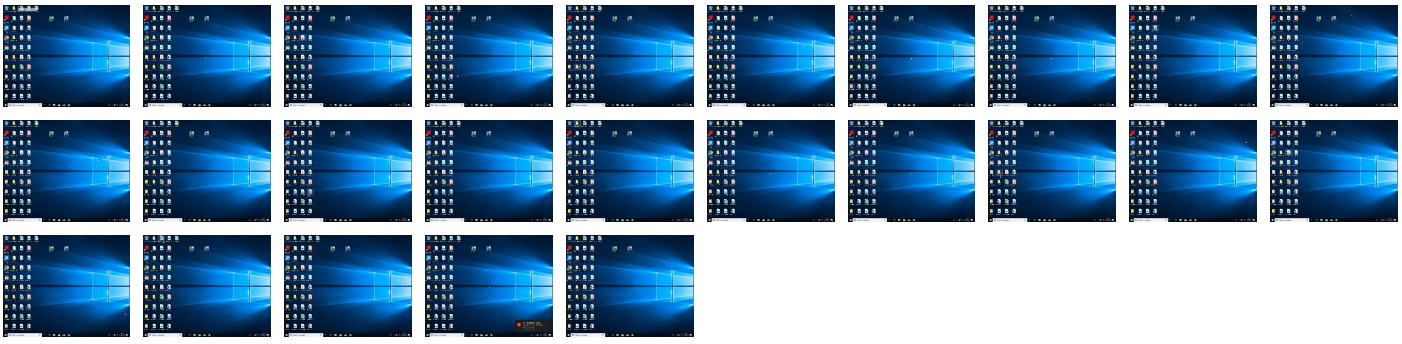
Behavior Graph



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
DSC_Canon_23.12.2020.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.DSC_Canon_23.12.2020.exe.5330000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
0.2.DSC_Canon_23.12.2020.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
0.3.DSC_Canon_23.12.2020.exe.5250000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
cs742.wpc.rncdn4.com	0%	Virustotal		Browse
vip0x04f.ssl.rncdn5.com	0%	Virustotal		Browse
sibedriamasterkkmoderatordstezya.ru	0%	Virustotal		Browse
ei.rdtcdn.com.sds.rncdn7.com	0%	Virustotal		Browse
a.adtng.com	0%	Virustotal		Browse

Copyright null 2020

URLs

Source	Detection	Scanner	Label	Link
http://https://www.etahub.com/trackn?app_id=	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cs742.wpc.rncdn4.com	192.229.221.215	true	false	• 0%, Virustotal, Browse	unknown
stats.l.doubleclick.net	108.177.15.154	true	false		high
redtube.com	66.254.114.238	true	false		high
vip0x04f.ssl.rncdn5.com	205.185.208.79	true	false	• 0%, Virustotal, Browse	unknown
hubtraffic.com	66.254.114.32	true	false		high
sibedriamasterkkmoderatordstezya.ru	45.130.151.85	true	false	• 0%, Virustotal, Browse	unknown
ei.rdtcdn.com.sds.rncdn7.com	67.22.48.100	true	false	• 0%, Virustotal, Browse	unknown
a.adtng.com	216.18.168.166	true	false	• 0%, Virustotal, Browse	unknown
www.google.co.uk	172.217.18.99	true	false		unknown
dolsggiberiaoserkmikluhasya.chimkent.su	178.210.89.119	true	false		unknown
dolsibegriaosersk4ermanderezya.chimkent.su	178.210.89.119	true	false		unknown
ads.trafficjunky.net	66.254.114.38	true	false		high
vip0x08e.ssl.rncdn5.com	205.185.208.142	true	false		unknown
static.trafficjunky.com	unknown	unknown	false		high
cdn.speedcurve.com	unknown	unknown	false		high
www.redtube.com	unknown	unknown	false		high
di.rdtcdn.com	unknown	unknown	false		high
cdn1d-static-shared.phncdn.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
vz-cdn.trafficjunky.net	unknown	unknown	false		high
massidfberiatersksilkavaysstezya.ru	unknown	unknown	false		unknown
ht.redtube.com	unknown	unknown	false		high
ei.rdtcdn.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ei.rdtcdn.com/m=IbTvgzPf2lWL2yZ9sDZvMCZ9cmWqZl1itnVetmY8sy2fgDHjxoZKdn2Kdn28cBVD2BFf2y1yMyWC	V8EBMGK4.htm.21.dr	false		high
http://https://cdn.speedcurve.com/js/lux.js?id=609859533	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=bIa44NVg5p/media/videos/202012/07/38718651/original/8.webp	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=bIa44NVg5p/media/videos/202012/07/38725381/original/9.webp	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=ejrk8f/media/videos/201408/19/860611/original/15.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://cw.rdtcdn.com/media/videos/202012/07/38729421/360P_360K_38729421_fb.mp4	V8EBMGK4.htm.21.dr	false		high
http://https://ci-ph.rdtcdn.com/videos/202011/13/369786102/original/(m=eah-8f)(mh=U81MWqXD4An5YSJW)3.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://ci-ph.rdtcdn.com/videos/202011/13/369786102/original/(m=eGJF8f)(mh=-wbq1RH9rFeTI7M0)	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=ejrk8f/media/videos/201607/21/165172/original/5.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=bIaMwLVg5p/media/videos/202012/07/38718651/original/8.webp	V8EBMGK4.htm.21.dr	false		high

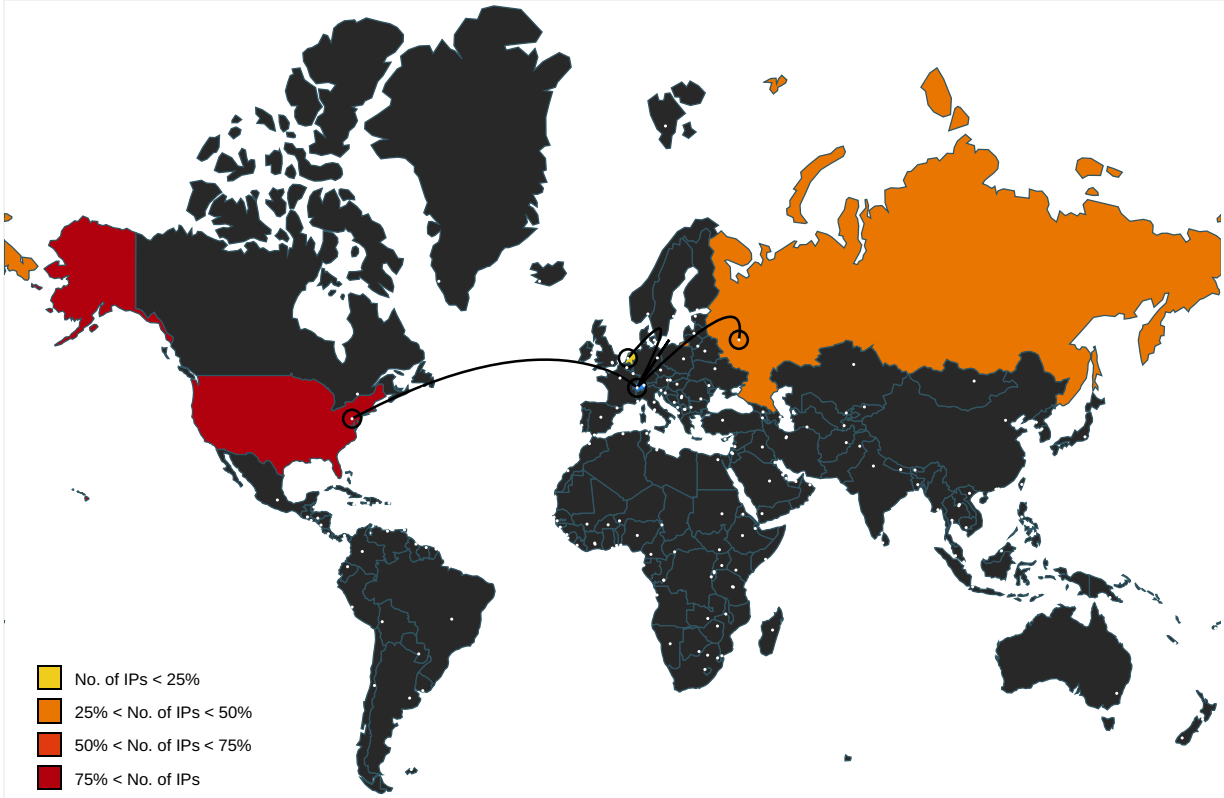
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ei.rdtcdn.com/m=eW0Q8f/media/videos/202012/07/38728641/original/10.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://www.tube8.com/?utm_source=redtube&utm_medium=network-bar&utm_campaign=redtube-networkbar	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=bIaMwLVg5p/media/videos/202012/07/38725381/original/9.webp	V8EBMGK4.htm.21.dr	false		high
http://https://github.com/jquery/jquery-color	jquery-ui-1.10.3[1].js.21.dr	false		high
http://https://dw.rdtcdn.com/media/videos/201612/20/1880893/360P_360K_1880893.mp4	V8EBMGK4.htm.21.dr	false		high
http://https://dw.rdtcdn.com/media/videos/201511/04/1348007/360P_360K_1348007.mp4	V8EBMGK4.htm.21.dr	false		high
http://https://www.redtube.com/?page=2	V8EBMGK4.htm.21.dr	false		high
http://https://di.rdtcdn.com/m=eah-8f/media/videos/202010/15/37001911/original/14.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=bIaC8JVg5p/media/videos/201703/01/2037488/original/6.webp	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/images/pc/category/amateur_001.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://di.rdtcdn.com/m=bIaMwLVg5p/media/videos/202007/30/34644641/original/16.webp	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=bIa44NVg5p/media/videos/201810/15/11133961/original/12.webp	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=eW0Q8f/media/videos/201606/01/1598150/original/15.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=bIaMwLVg5p/media/videos/201806/12/7678031/original/12.webp	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/images/pc/network-bar-sprite.png?v=4a9dc4c355497e	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=eah-8f/media/videos/202012/08/38753051/original/9.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/icons/favicon.png?v=4a9dc4c355497ed4f02c60b9b605e	V8EBMGK4.htm.21.dr, imagestore.dat.21.dr, imagestore.dat.34.dr	false		high
http://https://ei.rdtcdn.com/m=bIaMwLVg5p/media/videos/202012/05/38664591/original/9.webp	V8EBMGK4.htm.21.dr	false		high
http://https://di.rdtcdn.com/m=eW0Q8f/media/videos/202011/30/38518451/original/15.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=bIa44NVg5p/media/videos/202012/05/38664591/original/9.webp	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/images/pc/ajax-loader.gif	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/images/pc/category/mature_001.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=bIa44NVg5p/media/videos/201806/12/7678031/original/12.webp	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=eGJF8f/media/videos/201606/01/1598150/original/15.jpg	V8EBMGK4.htm.21.dr	false		high
http://www.reddit.com/	msapplication.xml4.3.dr	false		high
http://https://ci-ph.rdtcdn.com/videos/202004/03/299834992/original/(m=bIa44NVg5p)(mh=9OitNrdinJF2nc_r)8.we	V8EBMGK4.htm.21.dr	false		high
http://https://ci-ph.rdtcdn.com/m=e_rU8f/pics/pornstars/000/002/511/thumb_95052.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=eGJF8f/media/videos/202012/05/38664591/original/9.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=bIijsHVg5p/media/videos/201412/30/998020/original/15.webp	V8EBMGK4.htm.21.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dw.rdtcdn.com/media/videos/201605/02/1564667/360P_360K_1564667.mp4	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=bIaMwLVg5p/media/videos/202012/08/38754371/original/11.webp	V8EBMGK4.htm.21.dr	false		high
http://https://cw.rdtcdn.com/media/videos/202012/07/38726741/360P_360K_38726741_fb.mp4	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=eGJF8f/media/videos/201902/28/14233291/original/5.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://di.rdtcdn.com/m=bIa44NVg5p/media/videos/202006/03/32270141/original/1.webp	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=eGJF8f/media/videos/202012/08/38753051/original/	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=eW0Q8f/media/videos/201902/28/14233291/original/5.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://static.trafficjunky.com/invocation/embeddedads/	V8EBMGK4.htm.21.dr	false		high
http://https://ci-ph.rdtcdn.com/m=e_rU8f/pics/pornstars/000/260/871/thumb_1024761.jpg	V8EBMGK4.htm.21.dr	false		high
http://designer.videojs.com	video-js[1].css.21.dr	false		high
http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/fonts/rt_font.woff2?v=4a9dc4c355497ed4f02c60b9b60	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/images/pc/category/lesbian_001.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://ci-ph.rdtcdn.com/videos/202002/10/283600732/original/(m=eah-8f)(mh=CPA-BIsCEohICDUU)0.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://dw.rdtcdn.com/media/videos/201606/01/1598150/360P_360K_1598150.mp4	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=bIa44NVg5p/media/videos/201612/20/1880893/original/9.webp	V8EBMGK4.htm.21.dr	false		high
http://https://di.rdtcdn.com/m=eGJF8f/media/videos/202008/14/35096611/original/	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=bIa44NVg5p/media/videos/201802/16/4502521/original/16.webp	V8EBMGK4.htm.21.dr	false		high
http://https://ci.rdtcdn.com/m=eGJF8f/media/videos/202010/15/37001911/original/	V8EBMGK4.htm.21.dr	false		high
http://https://www.etahub.com/trackn?app_id=	timings-1.0.0[1].js.21.dr	false	• Avira URL Cloud: safe	unknown
http://modernizr.com/download/#-video-shiv-cssclasses-load	modernizr[1].js.21.dr	false		high
http://https://ei.rdtcdn.com/m=eah-8f/media/videos/202012/08/38755441/original/11.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=bIaMwLVg5p/media/videos/202012/07/38736091/original/6.webp	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=eW0Q8f/media/videos/202012/08/38753381/original/2.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=bIa44NVg5p/media/videos/202012/07/38736091/original/6.webp	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=eGJF8f/media/videos/201710/27/2578878/original/7.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=ejrk8f/media/videos/201612/20/188093/original/9.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=bIaMwLVg5p/media/videos/201608/29/1701085/original/10.webp	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=eW0Q8f/media/videos/202012/07/38726001/original/10.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=eah-8f/media/videos/202012/07/38725381/original/9.jpg	V8EBMGK4.htm.21.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ei.rdtcdn.com/m=eGJF8f/media/videos/202012/08/38755441/original/11.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://de.redtube.com/	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=bIaMwLVg5p/media/videos/201802/16/4502521/original/16.webp	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=bIaMwLVg5p/media/videos/202012/08/38758551/original/15.webp	V8EBMGK4.htm.21.dr	false		high
http://https://ci-ph.rdtcdn.com/m=bIWpYLVg5p/pics/pornstars/000/020/291/thumb_24861.webp	V8EBMGK4.htm.21.dr	false		high
http://https://cdn1d-static-shared.phncdn.com/timings-1.0.0.js	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=eah-8f/media/videos/201810/15/11133961/original/12.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=eW0Q8f/media/videos/202012/07/38726741/original/14.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://jp.redtube.com/	V8EBMGK4.htm.21.dr	false		high
http://https://dw.rdtcdn.com/media/videos/202008/27/35456791/360P_360K_35456791_fb.mp4	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=eah-8f/media/videos/202012/08/38758001/original/6.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://cw.rdtcdn.com/media/videos/202012/07/38736091/360P_360K_38736091_fb.mp4	V8EBMGK4.htm.21.dr	false		high
http://https://cw.rdtcdn.com/media/videos/202012/07/38725381/360P_360K_38725381_fb.mp4	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=eah-8f/media/videos/202012/07/38726001/original/10.jpg	V8EBMGK4.htm.21.dr	false		high
http://www.twitter.com/	msapplication.xml5.3.dr	false		high
http://https://ei.rdtcdn.com/m=eGJF8f/media/videos/201712/06/2695068/original/	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=eGJF8f/media/videos/202012/07/38739611/original/	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=eW0Q8f/media/videos/201511/04/1348007/original/12.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=bIa44NVg5p/media/videos/201608/29/1701085/original/10.webp	V8EBMGK4.htm.21.dr	false		high
http://https://ci-ph.rdtcdn.com/m=bIWpYLVg5p/pics/pornstars/000/113/421/thumb_1603511.webp	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/js/common/lib/jquery-2.1.3.min.js?v=4a9dc4c355497	V8EBMGK4.htm.21.dr	false		high
http://https://di.rdtcdn.com/m=bIaMwLVg5p/media/videos/202008/27/35456791/original/14.webp	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/js/generated/pc/default-redtube.js?v=4a9dc4c35549	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=bIa44NVg5p/media/videos/201701/18/1942360/original/10.webp	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=eGJF8f/media/videos/201810/15/11133961/original/12.jpg	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/fonts/rt_font.eot?v=4a9dc4c355497ed4f02c60b9b605e	V8EBMGK4.htm.21.dr	false		high
http://https://di.rdtcdn.com/m=eGJF8f/media/videos/202006/23/33015621/original/	V8EBMGK4.htm.21.dr	false		high
http://https://ei.rdtcdn.com/m=bIijsHVg5p/media/videos/201607/13/1645342/original/5.webp	V8EBMGK4.htm.21.dr	false		high
http://https://di.rdtcdn.com/m=bIaMwLVg5p/media/videos/202011/24/38329471/original/14.webp	V8EBMGK4.htm.21.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://di.rdtcdn.com/m=bIaMwLVg5p/media/videos/202006/03/32270141/original/1.webp	V8EBMGK4.htm.21.dr	false		high
http:// https://di.rdtcdn.com/m=eGJF8f/media/videos/201905/24/16763151/original/12.jpg	V8EBMGK4.htm.21.dr	false		high
http:// https://di.rdtcdn.com/m=eGJF8f/media/videos/201908/11/20264951/original/	V8EBMGK4.htm.21.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.177.15.154	unknown	United States		15169	GOOGLEUS	false
66.254.114.238	unknown	United States		29789	REFLECTEDUS	false
67.22.48.104	unknown	Netherlands		29789	REFLECTEDUS	false
45.130.151.85	unknown	Russian Federation		62415	MARKTELRU	false
192.229.221.215	unknown	United States		15133	EDGECASTUS	false
66.254.114.38	unknown	United States		29789	REFLECTEDUS	false
205.185.208.142	unknown	United States		20446	HIGHWINDS3US	false
205.185.208.79	unknown	United States		20446	HIGHWINDS3US	false
178.210.89.119	unknown	Russian Federation		48287	RU-CENTERRU	false
66.254.114.32	unknown	United States		29789	REFLECTEDUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	333815
Start date:	24.12.2020
Start time:	02:36:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 11s

Copyright null 2020

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DSC_Canon_23.12.2020.zip (renamed file extension from zip to exe)
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:	mal80.bank.troj.winEXE@13/87@24/10
EGA Information:	Failed
HDC Information:	• Successful, ratio: 34.7% (good quality ratio 34.7%) • Quality average: 89.2% • Quality standard deviation: 15.5%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI

Copyright null 2020

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.88.21.125, 104.42.151.234, 88.221.62.148, 104.79.90.110, 51.11.168.160, 92.122.213.247, 92.122.213.194, 152.199.19.161, 20.54.26.129, 67.26.81.254, 8.248.141.254, 8.248.149.254, 67.27.233.254, 67.26.75.254, 151.101.2.217, 151.101.66.217, 151.101.130.217, 151.101.194.217, 172.217.22.110, 205.185.216.42, 205.185.216.10, 216.58.207.68, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, www.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.google-analytics.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, www-google-analytics.l.google.com, ie9comview.vo.msecnd.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, cds.e9q5t8x5.hwcdn.net, ris.api.iris.microsoft.com, ssddl2.microsoft.com, a3.shared.global.fastly.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
108.177.15.154	http://https://bit.do/fL5xF	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://www.canva.com/design/DAEQ9wWiiI4/xe_9LxFtkmjBa9UV_tvT3Q/view?utm_content=DAEQ9wWiiI4&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	Get hash	malicious	Browse	
	http://https://www.canva.com/design/DAEQ9_qXSjI/W-4vWOSA8PP5TXC7Nx9niA/view?utm_content=DAEQ9_qXSjI&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink&d=DwMFAg	Get hash	malicious	Browse	
	http://https://regalawards1-my.sharepoint.com/:b:/g/personal/jordyn_regalawards_com/EUZHp771z3ZIjDTrwc35jZ0Bjs3NzMsYxyWwqOJv02Z5XQ?e=4%3a8EU1Ek&at=9	Get hash	malicious	Browse	
	http://https://assist-linker.com/in/?page=io8273dkskskldue8923&utm_source=2&utm_campaign=w6nlf2rvvdg2lq442snon8hu&subid=master&customer=14	Get hash	malicious	Browse	
	http://https://bit.do/fLVUm	Get hash	malicious	Browse	
	http://perpetual.veteran.az/673616c6c792e64756e6e654070657270657475616c2e636f6d2e6175	Get hash	malicious	Browse	
	http://https://www.canva.com/design/DAEQZJ2RxL4/pSFyhiLxB4Tyh_9wmjeJdw/view?utm_content=DAEQZJ2RxL4&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	
	http://https://spregueenergy.quip.com/p9lsAzXNTc1Y/eFax-Doc	Get hash	malicious	Browse	
	http://https://joom.ag/3wFC	Get hash	malicious	Browse	
	http://https://www.canva.com/design/DAEPTRf7pMA/9LBTlGXJzLzn92u-Q6LJsg/edit	Get hash	malicious	Browse	
	http://https://www.canva.com/design/DAEPSLMcWi8/yJo86tIRDKnniC5F-zI-8A/view?utm_content=DAEPSLMcWi8&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	Get hash	malicious	Browse	
	http://www.authorea.com/496817/s_HUCBQs4gOQpqvMdvqmFQ	Get hash	malicious	Browse	
	http://https://0000000000.doodlekit.com/	Get hash	malicious	Browse	
	http://fx19827c.zizera.com/fx19827c/publisher/login?r=/fx19827c/lite/	Get hash	malicious	Browse	
	http://23.129.64.206	Get hash	malicious	Browse	
	http://https://www.paperturn-view.com/?pid=MTI128610	Get hash	malicious	Browse	
	http://https://simplebooklet.com/paymentdoc1	Get hash	malicious	Browse	
	http://https://simplebooklet.com/paymentfile1	Get hash	malicious	Browse	
	http://https://bit.ly/2IND0ob	Get hash	malicious	Browse	
66.254.114.38	LGwzOM1BAN.exe	Get hash	malicious	Browse	
	invoice_order_57832.zip.exe	Get hash	malicious	Browse	
	5f291381b8e10png.dll	Get hash	malicious	Browse	
	5f291fa0130fcrar.dll	Get hash	malicious	Browse	
66.254.114.238	invoice_order_57832.zip.exe	Get hash	malicious	Browse	
	5f291381b8e10png.dll	Get hash	malicious	Browse	
	5f291fa0130fcrar.dll	Get hash	malicious	Browse	
205.185.208.142	LGwzOM1BAN.exe	Get hash	malicious	Browse	
	invoice_order_57832.zip.exe	Get hash	malicious	Browse	
	5f291381b8e10png.dll	Get hash	malicious	Browse	
	5f291fa0130fcrar.dll	Get hash	malicious	Browse	
205.185.208.79	LGwzOM1BAN.exe	Get hash	malicious	Browse	
	invoice_order_57832.zip.exe	Get hash	malicious	Browse	
	5f291381b8e10png.dll	Get hash	malicious	Browse	
	5f291fa0130fcrar.dll	Get hash	malicious	Browse	
178.210.89.119	2020-10-08_22-04-52.exe	Get hash	malicious	Browse	• stolkgolmishutich.termez.su/
	wallet_keys.exe	Get hash	malicious	Browse	• db-files.com.ru/gate16.php?g=1011744768&k=ACO43XZU8cog8hkcDNk06Ksjb

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DB_Bank_client.exe	Get hash	malicious	Browse	• db-files.com.ru/gate16.php?g=1011744768&k=nQuuJcET2j1i2duL09eyEVqC5
192.229.221.215	LGwzOM1BAN.exe	Get hash	malicious	Browse	
	5f291fa0130fcrar.dll	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
a.adtng.com	SecuriteInfo.com.CIL.StupidStealth.Heur.exe	Get hash	malicious	Browse	• 216.18.168.166
	5f291381b8e10png.dll	Get hash	malicious	Browse	• 216.18.168.166
	5f291fa0130fcrar.dll	Get hash	malicious	Browse	• 216.18.168.166
www.google.co.uk	http://mysp.ac/4kPIV	Get hash	malicious	Browse	• 172.217.18.99
	http://https://gaandt.quip.com/QLStAIvBA1Tg/File-Review	Get hash	malicious	Browse	• 172.217.18.99
	http://ferreirainvestig.com.br/Activacion/cuenta-cdqd/	Get hash	malicious	Browse	• 172.217.18.99
	EHpIMi2I5F.doc	Get hash	malicious	Browse	• 172.217.18.99
	http://y.novobanco.opengateautospray.com/674616e69612e726f7361406e6f766f62616e636f2e7074	Get hash	malicious	Browse	• 172.217.18.99
	http://www.greaudstudio.com/docs/fgn/m8jklv4.dll	Get hash	malicious	Browse	• 172.217.18.99
	http://https://www.canva.com/design/DAEQ9wWiiI4/xe_9LxFtkmjBa9UV_tvT3Q/view?utm_content=DAEQ9wWiiI4&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	Get hash	malicious	Browse	• 172.217.18.99
	http://https://bit.ly/2LFrQTD	Get hash	malicious	Browse	• 172.217.18.99
	http://https://numisconsult.com/blog/e47c4b8720db7445599988579a03c7c5	Get hash	malicious	Browse	• 172.217.18.99
	http://https://www.canva.com/design/DAEQ9_qXSjI/W-4vWOSA8PP5TXC7Nx9niA/view?utm_content=DAEQ9_qXSjI&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink&d=DwMFAg	Get hash	malicious	Browse	• 172.217.18.99
	http://https://secureddoc.unicornplatform.com	Get hash	malicious	Browse	• 172.217.18.99
	http://h4jv5.e3i1g.me?Zs7?L4j=M&9g	Get hash	malicious	Browse	• 172.217.18.99
	http://https://regalawards1-my.sharepoint.com/:b:/g/personal/jordyn_regalawards_com/EUZHp771z3ZIjDTrwc35jZ0Bjs3NzMsYxyWwqOJv02Z5XQ?e=4%3a8EU1Ek&at=9	Get hash	malicious	Browse	• 172.217.18.99
	http://jb092.com/rxlbakzd/goqmmbmi.html?kjmikw5x.3hllr	Get hash	malicious	Browse	• 172.217.18.99
	http://gaandt.quip.com/4HSEAAx2iIx8/File-Review	Get hash	malicious	Browse	• 172.217.18.99
	http://https://www.canva.com/design/DAEQSvwkEYE/TsoYiGCThAljY8VxgRbBCg/view?utm_content=DAEQSvwkEYE&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	Get hash	malicious	Browse	• 172.217.18.99
	http://aanqylta.com	Get hash	malicious	Browse	• 172.217.18.99
	http://https://sharia-point.us-south.cf.appdomain.cloud/redirect/?email=Kristine_Bridges@baylor.edu&data=04|01|Kristine_Bridges@baylor.edu|a64194d2378542e06dfc08d8a2802868|22d2fb35256a459bbcf4dc23d42dc0a4|0|0|637438018615913999|Unknown|TWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0=|0&sdata=smYCgJbR96G/HzImvOXjT6991bTFo5/ZZGjJwucJySM=&reserved=0	Get hash	malicious	Browse	• 172.217.18.99
	http://https://www.premierpawn.com/rrt/xxtb/sharepoints/Root	Get hash	malicious	Browse	• 172.217.18.99
	http://https://greens.us-south.cf.appdomain.cloud/smain/?op=c2FsZXNAZm9yZHdheS5jb20=&/yanief4OLVfRFm.php?83_aJjkvU053dh2qESwbhSn93984jjd8pksh_048jdkkd9n488	Get hash	malicious	Browse	• 172.217.18.99
hubtraffic.com	invoice_order_57832.zip.exe	Get hash	malicious	Browse	• 66.254.114.32
	5f291381b8e10png.dll	Get hash	malicious	Browse	• 66.254.114.32
	5f291fa0130fcrar.dll	Get hash	malicious	Browse	• 66.254.114.32
vip0x04f.ssl.rncdn5.com	invoice_order_57832.zip.exe	Get hash	malicious	Browse	• 205.185.208.79
	5f291381b8e10png.dll	Get hash	malicious	Browse	• 205.185.208.79
	5f291fa0130fcrar.dll	Get hash	malicious	Browse	• 205.185.208.79
stats.l.doubleclick.net	http://d4a687ce4c.lazeruka.ru	Get hash	malicious	Browse	• 108.177.15.156
	http://https://gaandt.quip.com/QLStAIvBA1Tg/File-Review	Get hash	malicious	Browse	• 108.177.15.156
	http://ferreirainvestig.com.br/Activacion/cuenta-cdqd/	Get hash	malicious	Browse	• 108.177.15.157

Copyright null 2020

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://y.novobanco.opengateautospray.com/674616e69612e726f7361406e6f766f62616e636f2e7074	Get hash	malicious	Browse	• 108.177.15.157
	http://https://bit.do/fL5xF	Get hash	malicious	Browse	• 108.177.15.156
	http://https://bit.do/fL5xF	Get hash	malicious	Browse	• 108.177.15.154
	http://www.greaudstudio.com/docs/fgn/m8jklv4.dll	Get hash	malicious	Browse	• 108.177.15.155
	http://https://www.canva.com/design/DAEQ9wWiiI4/xe_9LxFtkmjBa9UV_tvT3Q/view?utm_content=DAEQ9wWiiI4&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	Get hash	malicious	Browse	• 108.177.15.154
	http://https://bit.ly/2LFrQTD	Get hash	malicious	Browse	• 108.177.15.156
	http://https://numisconsult.com/blog/e47c4b8720db7445599988579a03c7c5	Get hash	malicious	Browse	• 108.177.15.155
	http://https://www.canva.com/design/DAEQ9_qXSjI/W-4vWOSA8PP5TXC7Nx9niA/view?utm_content=DAEQ9_qXSjI&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink&d=DwMFAg	Get hash	malicious	Browse	• 108.177.15.154
	http://h4jv5.e3i1g.me?Zs7?L4j=M&9g	Get hash	malicious	Browse	• 74.125.140.155
	http://https://viewer.desygner.com/hOfRd9HPmLB/	Get hash	malicious	Browse	• 64.233.184.156
	http://https://www.compartirwifi.com	Get hash	malicious	Browse	• 64.233.184.155
	http://search.hshipmenttracker.co	Get hash	malicious	Browse	• 64.233.184.155
	http://https://sosefinawinnifredsullivan8-5ce0e.gr8.com/	Get hash	malicious	Browse	• 64.233.184.157
	http://https://app.box.com/s/yihmp2wywbz9lgdbg26g3tc1piwkalab	Get hash	malicious	Browse	• 64.233.184.155
	http://dhi2.webnode.com/contact/	Get hash	malicious	Browse	• 64.233.184.156
	http://bit.ly/2K9I7Q5	Get hash	malicious	Browse	• 64.233.184.155
	http://https://regalawards1-my.sharepoint.com/:b:/g/personal/jordyn_regalawards_com/EUZHp771z3ZIjDTrwc35jZ0Bjs3NzMsYxyWwqOJv02Z5XQ?e=4%3a8EU1Ek&at=9	Get hash	malicious	Browse	• 108.177.15.154
cs742.wpc.rncdn4.com	5f291fa0130fcrar.dll	Get hash	malicious	Browse	• 192.229.221.215
ei.rdtcdn.com.sds.rncdn7.com	invoice_order_57832.zip.exe	Get hash	malicious	Browse	• 64.210.135.72
	5f291381b8e10png.dll	Get hash	malicious	Browse	• 64.210.135.70
	5f291fa0130fcrar.dll	Get hash	malicious	Browse	• 64.210.135.68

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EDGECASTUS	http://https://leapamazon.com/CD/Login2021/Login.htm	Get hash	malicious	Browse	• 152.199.21.118
	http://https://leapamazon.com/CD/Login2021/Login.htm	Get hash	malicious	Browse	• 152.199.21.118
	http://https://www.chronopost.fr/fclV2/authentification.html?numLt=XP091625009FR&profil=DEST&cc=47591&type=MASMail&lang=fr_FR	Get hash	malicious	Browse	• 93.184.221.133
	http://080810matthew.allen08.earlroseconsulting.com/r/?id=hbd659767,2C28c67268,2C28c67269&rd=orka.mk/08x360808x3608?e=#matthew.allen@perpetual.com.au	Get hash	malicious	Browse	• 192.229.221.185
	http://y.novobanco.opengateautospray.com/674616e69612e726f7361406e6f766f62616e636f2e7074	Get hash	malicious	Browse	• 152.199.21.175
	http://g1security.co.tz	Get hash	malicious	Browse	• 152.199.21.141
	http://505010charles.yee50.earlroseconsulting.com/r/?id=hbd659767,2C28c67268,2C28c67269&rd=orka.mk/50x485050x4850?e=#charles.yee@livibank.com	Get hash	malicious	Browse	• 192.229.221.185
	http://505010charles.yee50.earlroseconsulting.com/r/?id=hbd659767,2C28c67268,2C28c67269&rd=orka.mk/50x485050x4850?e=#charles.yee@livibank.com	Get hash	malicious	Browse	• 152.199.23.37
	http://https://omoolowo001.github.io/myfirstrepo/YWNjb3VudHNfbG9nindex.html?scriptID=35662936635352205&cookies=MC4xOTUyNjY0OTg0MzM0NTQ0NQ&token=81117470799998&email=jeaton@nlcmutual.com	Get hash	malicious	Browse	• 152.199.21.175
	http://www.greaudstudio.com/docs/fgn/m8jklv4.dll	Get hash	malicious	Browse	• 68.232.35.12
	http://https://balenpersen.com/TO/financialcrimes@lvmpd.com	Get hash	malicious	Browse	• 152.199.23.72
	http://https://www.canva.com/design/DAEQ9wWiiI4/xe_9LxFtkmjBa9UV_tvT3Q/view?utm_content=DAEQ9wWiiI4&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	Get hash	malicious	Browse	• 152.199.21.175
	http://https://kingkorefitness.com/Inc-Corp/RD-FITT	Get hash	malicious	Browse	• 192.229.221.185

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://kingkorefitness.com/Inc-Corp/RD-FITT	Get hash	malicious	Browse	• 192.229.221.185
	http://https://target-care.webflow.io/	Get hash	malicious	Browse	• 152.199.23.37
	http://https://fultonmv.github.io/amanadpsoptodresi/aru.html?bbre=do9348wesid	Get hash	malicious	Browse	• 152.199.21.175
	http://https://rzh09.github.io/kirapzoxda/adiuew.html?bbre=as83wsdcx	Get hash	malicious	Browse	• 152.199.21.175
	http://https://flcfm.com/sign-on.ce9876/365txt	Get hash	malicious	Browse	• 152.199.21.175
	http://search.hshipmenttracker.co	Get hash	malicious	Browse	• 68.232.35.182
	http://www.almbrandbk.com	Get hash	malicious	Browse	• 152.199.21.175
GOOGLEUS	http://https://fdkl5.csb.app/	Get hash	malicious	Browse	• 172.217.16.130
	http://https://shocking-foregoing-driver.glitch.me	Get hash	malicious	Browse	• 172.217.18.2
	http://https://drive.google.com/file/d/14xCk47e8f1xIRiYz-zhRjpTdCbeIG7Dy/view?usp=sharing_eip&ts=5fe37a3f	Get hash	malicious	Browse	• 172.217.16.129
	http://https://linkprotect.cudasvc.com/url?a=http%3a%2f%2fwww.9499katheige.buttbrothersgroup.com%2f%3fVGH%3da2F0aGVpZ2VAd2NjdWNyZWRpdHVuaW9uLmNvb3A%3d&c=E,1,ltSrt2AaJ8-S_58_41jn_nVZjtrZcUJ9VdfgsP12W46O_R6IKdR3KtEWFbEOjrT1SWc5iDMSCu_En-xJAD5q0JnWFr_L3osRw1Vy4JjVvAGbSTphkVGAXf_rtOA,&typo=1	Get hash	malicious	Browse	• 172.217.16.129
	http://https://www.dropbox.com/s/1jk3ia2o2kx0p1n/Invitation_2036.doc?dl=1	Get hash	malicious	Browse	• 172.217.16.129
	http://https://updates.duetdisplay.com/latestWindows	Get hash	malicious	Browse	• 8.8.8.8
	http://vosb.blondfinish.link/index	Get hash	malicious	Browse	• 172.217.22.46
	http://https://aftersync.com/blog/rightqlik-quick-access-to-common-operations-on-qlikview-files	Get hash	malicious	Browse	• 172.217.16.129
	http://d4a687ce4c.lazeruka.ru	Get hash	malicious	Browse	• 34.102.232.42
	http://https://www.chronopost.fr/fclV2/authentification.html?numLt=XP091625009FR&profil=DEST&cc=47591&type=MASMail&lang=fr_FR	Get hash	malicious	Browse	• 172.217.16.130
	KYC ORDER 22DEC.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	Bel_61.docx	Get hash	malicious	Browse	• 216.239.38.21
	Bel_61.docx	Get hash	malicious	Browse	• 216.239.32.21
	List items.exe	Get hash	malicious	Browse	• 34.102.136.180
	Autodesk_Desktop_App_Bootstrap.exe	Get hash	malicious	Browse	• 8.8.8.8
	http://mysp.ac/4kPIV	Get hash	malicious	Browse	• 173.194.164.121
	FkCodec	Get hash	malicious	Browse	• 35.205.61.67
	14 2212 2020 062_546248.doc	Get hash	malicious	Browse	• 35.200.206.198
	http://xr4vx.mjt.lu/lnk/AUoAABsLUG8AAAAAGfgAAACj9UAAAAAAKt8AABmeABbN0QBf4eQgZ6X6UmPITHmCxUtOpOQ3LgAWb3k/1/7xzJOeWvDV8gVh3D7WayEg/aHR0cHM6Ly9uZXd2b2ljZW1haWxkaXJlY3RvcnltZXNzYWdlLndlZWJseS5jb20v	Get hash	malicious	Browse	• 35.241.186.140
	GDT299-20201222-4219523.doc	Get hash	malicious	Browse	• 35.200.206.198
REFLECTEDUS	SecuriteInfo.com.CIL.StupidStealth.Heur.exe	Get hash	malicious	Browse	• 216.18.168.166
	http://https://signup.kwikvpn.com/	Get hash	malicious	Browse	• 66.254.118.170
	http://cloudz.pw/go?green=carrier%2048gs-036060301%20operation%20manual	Get hash	malicious	Browse	• 208.99.69.133
	http://cloudz.pw/go?green=carrier 48gs-036060301 operation manual	Get hash	malicious	Browse	• 66.254.111.99
	LGwzOM1BAN.exe	Get hash	malicious	Browse	• 66.254.114.41
	http://https://www.google.com/url?q=https%3A%2F%2Fbit.ly%2F34lVoM1&sa=D&sntz=1&usg=AFQjCNGItNrIAWHjWOHF3rvz8pNqtmAYtg	Get hash	malicious	Browse	• 208.99.69.233
	2svozs0lnii.exe	Get hash	malicious	Browse	• 216.18.168.122
	invoice_order_57832.zip.exe	Get hash	malicious	Browse	• 66.254.114.32
	5f291381b8e10png.dll	Get hash	malicious	Browse	• 216.18.168.166
	5f291fa0130fcrar.dll	Get hash	malicious	Browse	• 66.254.114.32
REFLECTEDUS	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	http://https://fdkl5.csb.app/	Get hash	malicious	Browse	• 108.177.15.154 • 66.254.114.38 • 66.254.114.238 • 67.22.48.104 • 205.185.20 8.142 • 205.185.208.79 • 192.229.22 1.215 • 66.254.114.32
	http://https://clarifyescape.com/office/ofc/?signin=	Get hash	malicious	Browse	• 108.177.15.154 • 66.254.114.38 • 66.254.114.238 • 67.22.48.104 • 205.185.20 8.142 • 205.185.208.79 • 192.229.22 1.215 • 66.254.114.32
	http://https://rebrand.ly/Comunicado-23943983	Get hash	malicious	Browse	• 108.177.15.154 • 66.254.114.38 • 66.254.114.238 • 67.22.48.104 • 205.185.20 8.142 • 205.185.208.79 • 192.229.22 1.215 • 66.254.114.32
	http://https://leapamazon.com/CD/Login2021/Login.htm	Get hash	malicious	Browse	• 108.177.15.154 • 66.254.114.38 • 66.254.114.238 • 67.22.48.104 • 205.185.20 8.142 • 205.185.208.79 • 192.229.22 1.215 • 66.254.114.32
	http://https://leapamazon.com/CD/Login2021/Login.htm	Get hash	malicious	Browse	• 108.177.15.154 • 66.254.114.38 • 66.254.114.238 • 67.22.48.104 • 205.185.20 8.142 • 205.185.208.79 • 192.229.22 1.215 • 66.254.114.32
	http://https://shocking-foregoing-driver.glitch.me	Get hash	malicious	Browse	• 108.177.15.154 • 66.254.114.38 • 66.254.114.238 • 67.22.48.104 • 205.185.20 8.142 • 205.185.208.79 • 192.229.22 1.215 • 66.254.114.32
	http://https://drive.google.com/file/d/14xCk47e8f1xIRiYz-zhRjpTdCbeIG7Dy/view?usp=sharing_eip&ts=5fe37a3f	Get hash	malicious	Browse	• 108.177.15.154 • 66.254.114.38 • 66.254.114.238 • 67.22.48.104 • 205.185.20 8.142 • 205.185.208.79 • 192.229.22 1.215 • 66.254.114.32

Copyright null 2020

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://caganapinc.com/12-22-2020.html	Get hash	malicious	Browse	• 108.177.15.154 • 66.254.114.38 • 66.254.114.238 • 67.22.48.104 • 205.185.208.142 • 205.185.208.79 • 192.229.221.215 • 66.254.114.32
	http://vosb.blondfinish.link/index	Get hash	malicious	Browse	• 108.177.15.154 • 66.254.114.38 • 66.254.114.238 • 67.22.48.104 • 205.185.208.142 • 205.185.208.79 • 192.229.221.215 • 66.254.114.32
	http://https://transformco.gluestar.ga/Y2Fzc2FuZHJhLm11ZWxsZXJAdHJhbnNmb3JtY28uY29t	Get hash	malicious	Browse	• 108.177.15.154 • 66.254.114.38 • 66.254.114.238 • 67.22.48.104 • 205.185.208.142 • 205.185.208.79 • 192.229.221.215 • 66.254.114.32
	http://d4a687ce4c.lazeruka.ru	Get hash	malicious	Browse	• 108.177.15.154 • 66.254.114.38 • 66.254.114.238 • 67.22.48.104 • 205.185.208.142 • 205.185.208.79 • 192.229.221.215 • 66.254.114.32
	http://https://inshemailcheck-b97e716-7a0d37cea8b6i-04f79n27.ams3.digitaloceanspaces.com/domainmailcheckappcoms %2827%29.HTML#jerrym@dwotc.com	Get hash	malicious	Browse	• 108.177.15.154 • 66.254.114.38 • 66.254.114.238 • 67.22.48.104 • 205.185.208.142 • 205.185.208.79 • 192.229.221.215 • 66.254.114.32
	properties.dll	Get hash	malicious	Browse	• 108.177.15.154 • 66.254.114.38 • 66.254.114.238 • 67.22.48.104 • 205.185.208.142 • 205.185.208.79 • 192.229.221.215 • 66.254.114.32
	http://https://bit.ly/3h4DyD8	Get hash	malicious	Browse	• 108.177.15.154 • 66.254.114.38 • 66.254.114.238 • 67.22.48.104 • 205.185.208.142 • 205.185.208.79 • 192.229.221.215 • 66.254.114.32
	http://www.rekmall.net/.well-known/acme-challenge/act_contactar2/admin_cat/mgc_chatbox/information-12/pspbrwse.php?sit=ervw1yb1atp20npd0&remember=quiet&feel=sleep	Get hash	malicious	Browse	• 108.177.15.154 • 66.254.114.38 • 66.254.114.238 • 67.22.48.104 • 205.185.208.142 • 205.185.208.79 • 192.229.221.215 • 66.254.114.32

Copyright null 2020

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://expertgroupnyc.com/reschedule/	Get hash	malicious	Browse	• 108.177.15.154 • 66.254.114.38 • 66.254.114.238 • 67.22.48.104 • 205.185.208.142 • 205.185.208.79 • 192.229.221.215 • 66.254.114.32
	http://080810matthew.allen08.earlroseconsulting.com/r/?id=hbd659767,2C28c67268,2C28c67269&rd=orka.mk/08x360808x3608?e=#matthew.allen@perpetual.com.au	Get hash	malicious	Browse	• 108.177.15.154 • 66.254.114.38 • 66.254.114.238 • 67.22.48.104 • 205.185.208.142 • 205.185.208.79 • 192.229.221.215 • 66.254.114.32
	http://mysp.ac/4kPIV	Get hash	malicious	Browse	• 108.177.15.154 • 66.254.114.38 • 66.254.114.238 • 67.22.48.104 • 205.185.208.142 • 205.185.208.79 • 192.229.221.215 • 66.254.114.32
	http://https://ghpaccounting.com/usa.html	Get hash	malicious	Browse	• 108.177.15.154 • 66.254.114.38 • 66.254.114.238 • 67.22.48.104 • 205.185.208.142 • 205.185.208.79 • 192.229.221.215 • 66.254.114.32
	http://https://dj.4zido.de/i/612BRNn/	Get hash	malicious	Browse	• 108.177.15.154 • 66.254.114.38 • 66.254.114.238 • 67.22.48.104 • 205.185.208.142 • 205.185.208.79 • 192.229.221.215 • 66.254.114.32

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\DOMStore\0UW3VU4U\www.redtube[1].xml	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	39
Entropy (8bit):	2.469670487371862
Encrypted:	false
SSDEEP:	3:D90aK1r0aK1r0aKb:JFK1rFK1rFKb
MD5:	B9C5EB570521110110BB7DFF12AF780D
SHA1:	27F5BEBC2200FD8D0B51A93D1357EA954BE44079
SHA-256:	90171F10A6467C9DC31143859BAB69D045B67B39E2E49D92BB7168B383C4D1AB
SHA-512:	BC81539E62D643808CBDA3D86050058F379B2F0347CE65CBBA9797D386401C886B22AC4C0B2BE68197AE10C83A1E22A14232CD531C8D139DD3C031DB423EA3
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	<root></root><root></root><root></root>

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{0D017A2F-45D4-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.767517638150194
Encrypted:	false
SSDEEP:	48:IwCGcprvGwpLtG/ap8YrGIpc5iGvnZpv50Gooqp95YGo4Rpm53GW2GYrGWET6pmd:r2ZZZp2Y9W5Pt5of5LRM54/oflJMB
MD5:	5CC20F71D94338A5586C1CA9A8CF7FA9
SHA1:	289E46DD5DF3FC7DF0075465E16A6F92972B6124
SHA-256:	EB47CFD434F00C3438E2493FF9933CED6840D3365758262D4565A13064C0BDDF
SHA-512:	9E077B431E53A500D2443E24E400CFB2BAAB65D0E12C4CD85A197CB419FEA04D7EB771F044A9DA1A6F3BC8127B54185CD6640AA871057A78265EF2FCFA83E78 1
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{1C5239CF-45D4-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7692406695775074
Encrypted:	false
SSDEEP:	96:rTZgZv239WkEtkIsfkIPzlMknwPAdVrnwPWB:rTZgZv239WltMfLlMEd5B
MD5:	0596721A9BF92CF006712C88551F6754
SHA1:	051B7C1E3E8B95FE47430C28CE4AEF3B0E1AC3FA
SHA-256:	72F087E71ABA72D172A65BCAFBB3BFBEE2F19E400ECBED3A49B5C0CC41F8A088
SHA-512:	7D40A1EC5C31A7E789EC00C21228E5A860D4CB490057D0CB5807CDAD4BD93D3D9EEDB2F53F75A51939A4C45EC47EE46A70550D6FBA67A8FD9F99EEFF091C7 35
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{29E3FA3F-45D4-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.772122685681542
Encrypted:	false
SSDEEP:	48:IwBGcprlGwpLMG/ap8PrGIpc3+kGvnZpv3+HBGo6qp93+aAGo4Npm3AWGWwAyGW2:r3ZQZO2P9W3+Nt3+HRf3+aDNM3CemEB
MD5:	47432F605803AF1CE3AE1A858A37383E
SHA1:	AC6DEBE39DAA9E0B3434471341BADE73374A8160
SHA-256:	4766B15658BA73CED956057BE68939FF89F03B16AA029512C11149885E0F7A1F
SHA-512:	DAA80DF1918BAE631FFBB7B4CFC2414049A3FC676E0AE0712F4B9C1E41F03BF66F7BE9E7FDA8037B0AB4A9ACA2751CDA922D009A5F3FD9581A27BE41BF484F 70
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{F3308785-45D3-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	29272
Entropy (8bit):	1.7710376505518042
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{F3308785-45D3-11EB-90E4-ECF4BB862DED}.dat	
SSDEEP:	48:IwzGcprmGwpL9G/ap8XrGIpcYxGvnZpvYaGo6qp9Y2kGGo4dpmYfGWwAYGWaT6pe:rJZ+Z52X9WYetYMfY20dMYoc5NB
MD5:	EE6827E64BE51088D842EC94EA269D2C
SHA1:	809AE1B253FC45B0E27ED3729628CE7A19AA3FA0
SHA-256:	6027B569B7A4FB8BCBB2BC55C8584E68AD080CAE4EE3DB22AD64605B08985916
SHA-512:	DFFE2A213B4B48EE40066DEACB73DFD136C4115BB8B3242515C8A3C90EF529A269DDB4508677CC7C58E1A466755B834BEDBB0331E0B0BC6B50AA934F81B9A2 1D
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0D017A31-45D4-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	31344
Entropy (8bit):	1.6737835597566897
Encrypted:	false
SSDEEP:	48:Iw/GcprSGwpamG4pQKGrapbSSRrGQpBSGHHpcPsTGUp8SGzYpmUXYGopGqfaMGyi:rVZaQW68BS0Fjp2PkWuM4YsQ/k2AFzkA
MD5:	776468E2BE7E5617DBDAD28247E52112
SHA1:	B783832CEABBEA7A1660A359B0252635B7302EBC
SHA-256:	9F868A5F159F0CE57294870B5DFFD8A08A75289AF8C923518CA08AD01AAB592C
SHA-512:	89F3F506BA75440035E3DA4928F2BBE147CD0735ECA03FAAB655F6190BA1CB7F2339090DBE6F07D4A8F864ABEE37634641C9A10635D9B251ABCC406C70866FE
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{1C5239D1-45D4-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27304
Entropy (8bit):	1.823035726089773
Encrypted:	false
SSDEEP:	192:rZZaQa6Ak6FjN26kWmMdYi0iK5CYx0iK5CkEciA:rPXFN6hEuPdH0iK5CA0iK5CkEU
MD5:	22CB2D14AC626EA569D2DE464EB28824
SHA1:	F4ED95DA266EE2835EE3920DAA23BB7609256D4C
SHA-256:	41CDE04CDC62BECD771F144DCCE62175F440CCD5983A655C2941EBA3D9192A77
SHA-512:	084E48F65AC96B190F20DE18034E26630E9E96DF1E22AABB373F32FB19171ABB1423118C9BE97C9A025A9689C05EBFA9AC8E36D8B638AE01AF446080E1AAF89 9
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{29E3FA41-45D4-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27316
Entropy (8bit):	1.8257918323292996
Encrypted:	false
SSDEEP:	192:rCqZwnQRG6TSk5Fjt2ckWTMKYWR/OxR/jcuA:r9xj/5hkIQK7R/yR/jQ
MD5:	2A1710900F69A1D4852A5893343144B9
SHA1:	B5741E1C83EFA40E777BC158DD743B052D16565E
SHA-256:	21D60001741A9BFC5E95DE49F1DD55F69AE43C21291D551AB5146FE4A11373B5
SHA-512:	1E0C7A8FFC653C723D597E25996D10A582E43F77BAB05D4D4C376E8B1A4B7DC6C9D8379C0DF2DBE8772B96C673145140E9395709716B373C32FE7528DE69AC0
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{29E3FA41-45D4-11EB-90E4-ECF4BB862DED}.dat	
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{F3308787-45D3-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27276
Entropy (8bit):	1.8162183198824362
Encrypted:	false
SSDEEP:	192:rAZPQ+n687kOFjJ2YkW5M0YeFN7xFNlzfA:rwl+68AOhYcC0zFNNFNlzI
MD5:	BFBCE9556DCE0080533FCDE1BA6B55AD
SHA1:	66BCF5B94184EF9E1C7BF75F2E19E5ADCB776776
SHA-256:	E8250A3D0EB411DC629A83D741576788357549F4E0AD1E84DACE171C6C240D4C
SHA-512:	61A74376AF5D9D3B1A62BA13318CF604BE31EE1DD4442D6A31E08D7D9E7D1765814BEDFD9FAFB176FA0FF8D6E75C93CB260862C0241EF1D5C536B2F49C2D14 2
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.072882793719874
Encrypted:	false
SSDEEP:	12:TMHdNMNxOEUB2nWimI002EtM3MHdNMNxOEUB2nWimI00ObVbkEtMb:2d6NxOOSZHKd6NxOOSZ76b
MD5:	C6E341D17365A4A472937E5688F5D507
SHA1:	B2E61228531A3F3EA60039C953C2CDF7775D4A3A
SHA-256:	80B33930CE7AF80C6958778C317DC145165F75893F1A12F2CC34EEA1717B13F3
SHA-512:	3870125F1DBA733B0D6E75392EF55607B1B39BE9F4713A8A4792C6521682D885950D1ACEFFC7CC7BB5BEA9BECE0A2738B8B8A1AFF8D51DBB872E86E1D2E414 F9
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xc87ef12a,0x01d6d9e0</date>< accdate>0xc87ef12a,0x01d6d9e0</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>0xc87ef12a,0x01d6d9e0</date><accdate>0 xc87ef12a,0x01d6d9e0</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):	653
Entropy (8bit):	5.091520296136899
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kUwnw2nWimI002EtM3MHdNMNxe2kUwnw2nWimI00Obkak6EtMb:2d6NxrMSZHKd6NxrMSZ7Aa7b
MD5:	2F9233A7480EEF9D3D69C275743F8650
SHA1:	17FBA5CBD57DC05FF3290EF4AAF8554CE128C327
SHA-256:	06664E2FFE8766E807525E2741994BA8BD66FFEBDC4AC41DDF32A41EED661E57
SHA-512:	0AC0992A0E107B869CD236F162F8152047DAC03AC7585935ACC3F37B273BD1186431BA4232C035F52A021CA0FC125049D30936C32B2C81A7DD77D9FAF7A258F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xc877ca2a,0x01d6d9e0</date><a ccdate>0xc877ca2a,0x01d6d9e0</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>0xc877ca2a,0x01d6d9e0</date><a ccdate>0xc877ca2a,0x01d6d9e0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Am azon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.090940446287418
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLUB2nWimI002EtM3MHdNMNxvLUB2nWimI00ObmZEtMb:2d6NxvXSZHKd6NxvXSZ7mb
MD5:	043E222BED49C2D879648A18DE448C36
SHA1:	267B9164C79E80E42EA87F3BF77D7A0A2B147396
SHA-256:	7F077C58662F4F84685A2115678F2085C0415CD69FBA98B33F0D6A87677332FE
SHA-512:	DD6DB1B2A64B0CED8828F323FE7A52471A8407A097C8406A52367D401C252D2DD9B8014B5A16441EB43381ECDCBF533E6838682AB7933BBD7ED7A78F81E19C 7
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xc87ef12a,0x01d6d9e0</date> <accdate>0xc87ef12a,0x01d6d9e0</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>0xc87ef12a,0x01d6d9e0</date><accda te>0xc87ef12a,0x01d6d9e0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipe dia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.073323023038145
Encrypted:	false
SSDEEP:	12:TMHdNMNxi+R7R2nWimI002EtM3MHdNMNxi+R7R2nWimI00Obd5EtMb:2d6NxUSZHKd6NxUSZ7Jjb
MD5:	DF5035266A28183CEC0B29BED3B90FB2
SHA1:	49F76ED1D793EF1EBD0A72080A5682DFC79EF9DF
SHA-256:	8164ECCE48DFA14A59CFF7FD8BB4ACA543A867C1F74820E32559E02610C94DD3
SHA-512:	D2BD7609E80DF191E68CF539ED8A98738A9ECD75488AB576608F1321112CB4003AA9EDEA2F1B5CE2D89F5790F7DC504AD9E9E0E47849543701597E64A3B2A86
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xc87c8ed3,0x01d6d9e0</date><acc date>0xc87c8ed3,0x01d6d9e0</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>0xc87c8ed3,0x01d6d9e0</date><accdate>0xc87c8 ed3,0x01d6d9e0</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):	656
Entropy (8bit):	5.107645280083696
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwUB2nWimI002EtM3MHdNMNxhGwUB2nWimI00Ob8K075EtMb:2d6NxQCSZHKd6NxQCSZ7YKajb
MD5:	96A3662600E9536CCFADB800D3C026AA
SHA1:	8148CF91B260F9917EDFDC375CCF2D4ACEC0C39D
SHA-256:	785E1BBCB07F975D18E86FEE9CECBBD7D22202C347CB19D4ADFD1266FC3029C0
SHA-512:	5613A29DF3C27B15C55E2D9BD6AF7875A9B746B02897A411B216352BD039393F2AACD15585A669BD735F961177C9375F20F8FC99D54FEB0C50792A58A08F8FCD
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xc87ef12a,0x01d6d9e0</date>< accdate>0xc87ef12a,0x01d6d9e0</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>0xc87ef12a,0x01d6d9e0</date><accdate>0 xc87ef12a,0x01d6d9e0</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):	653
Entropy (8bit):	5.0654917755450235
Encrypted:	false
SSDEEP:	12:TMHdNMNx0n+R7R2nWimI002EtM3MHdNMNx0n+RB2nWimI00ObxEtMb:2d6Nx0TSZHKd6Nx03SZ7nb
MD5:	0E7A607D9C61DE7FA1689A8F5440D8F2
SHA1:	20463EDCCE7C3760EF809FB716B91345B7EF077F

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
SHA-256:	C9EF85D57145FFC167DEB406B5314CA49375E5608CE88DDCE92B2099C0FC2045
SHA-512:	A0B43C75A8378C89FB0C3742BBEB9375E6C58BB7BF23D1AB92AF9F5DB3EEBB204EF5658EE1B7A9A6BC4CC95201A009E7FB996551297CE47D4BAEA08FD2FDB50E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xc87c8ed3,0x01d6d9e0</date><accdate>0xc87c8ed3,0x01d6d9e0</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>0xc87c8ed3,0x01d6d9e0</date><accdate>0xc87ef12a,0x01d6d9e0</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.098492233685179
Encrypted:	false
SSDEEP:	12:TMHdNMNxx+R7R2nWimI002EtM3MHdNMNxx+R7R2nWimI00Ob6Kq5EtMb:2d6NxtSZHKd6NxtSZ7ob
MD5:	F0630200DD82A7D0072E3DDA3283BCD2
SHA1:	827FF71122C7FF3DE318ED622113569932173504
SHA-256:	CBF63C29A8284B4224F7968736A2D10A15FDEF0F40B84EB08C713CC87FF3FE78
SHA-512:	02E27D2FD3959593572500A23BEFB211C7D516C3E52363105A064FD20CC45770BD3710654B1C024D3DA73ABC3FC3B61E68B96B234991FE9C2A064651A2BB2B7A
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xc87c8ed3,0x01d6d9e0</date><accdate>0xc87c8ed3,0x01d6d9e0</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>0xc87c8ed3,0x01d6d9e0</date><accdate>0xc87c8ed3,0x01d6d9e0</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):	659
Entropy (8bit):	5.0973038555279
Encrypted:	false
SSDEEP:	12:TMHdNMNxcPG2nWimI002EtM3MHdNMNxcPG2nWimI00ObVEtMb:2d6NxsSZHKd6NxsSZ7Db
MD5:	453783AB3AED7625371120F0CD0B33B6
SHA1:	97F632F515E23EA5CD31A92FA482EAE80A33802D
SHA-256:	445C88DC8441C99C9DA82EF03D4F79A680E752FF507F316D605AA1A2D8E49B22
SHA-512:	F5FEC04F93DE1C254C2DEBF6FA789A2494C22E84BFA03774DC3F7D15FBBE66A2CF453568935D6E33063F819D7B0E772A4A60E7F20037BAE44CCD025D775904E
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xc87a2c77,0x01d6d9e0</date><accdate>0xc87a2c77,0x01d6d9e0</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>0xc87a2c77,0x01d6d9e0</date><accdate>0xc87a2c77,0x01d6d9e0</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):	653
Entropy (8bit):	5.0593339152616625
Encrypted:	false
SSDEEP:	12:TMHdNMNxfn+R7R2nWimI002EtM3MHdNMNxfn+R7R2nWimI00Obe5EtMb:2d6NxbSZHKd6NxbSZ7ijb
MD5:	F80F4DA890B6F9701C8854454557BC7A
SHA1:	50F1335836151126E3EFC3E64891A1CB3E2DB697
SHA-256:	F2ED82382F39BF95070AD557B5474197A79B1EFEE17FF1DD0611B8E69E89DA81
SHA-512:	B74EB8A1BB7002BDAB1509A841BBA89BA88452B8CA1E1F2AD91F03AC0D1B0D4760F304DC784FDE52A5FC8EA64559C6F61F76FEB6501182B953C35F40D9FDD7BE
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xc87c8ed3,0x01d6d9e0</date><accdate>0xc87c8ed3,0x01d6d9e0</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>0xc87c8ed3,0x01d6d9e0</date><accdate>0xc87c8ed3,0x01d6d9e0</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\ynfz0jx\imagestore.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	8122
Entropy (8bit):	7.820834533494162
Encrypted:	false
SSDEEP:	192:GSy3NwU5TIm/ZppBpo2UesiW7xLoo6wBt:G/tTIuZpFqeQ6o/t
MD5:	6C3CFEEC77AC3B9C60B89ADB389C055C
SHA1:	0AF747369E3F7A41099A9FD515ECDAAC5298923F
SHA-256:	74934C0B5EC03EE7DF3461D9DE04473AA0C8525BA263D3DCA0C3A4ACFDC59C45
SHA-512:	A1A94C5E121C1F8C51E821D150033C49A1B292F354A9470A88EB5926CCA09883D8202AD20CEE4FF2CCABDAAD638150D8FFE07A14F49873A18C904DA18C5E56C
Malicious:	false
Preview:	o.h.t.t.p.s.:././.e.i...r.d.t.c.d.n...c.o.m./.w.w.w.-.s.t.a.t.i.c./.c.d.n._.f.i.l.e.s./.r.e.d.t.u.b.e./.i.c.o.n.s./.f.a.v.i.c.o.n...p.n.g.?.v.=.4.a.9.d.c.4.c.3.5.5.4.9.7.e.d.4.f.0.2.c.6.0.b.9.b.6.0.5.e.0.4.1.c.5.e.b.7.0.e.0.....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...l:..%.....K.....K..1.}b....|.%.....M.....8.cb.^'.9 *

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt;..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\generated-service_worker_starter-1.0.0[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	3420
Entropy (8bit):	5.145089778442548
Encrypted:	false
SSDEEP:	48:7HaIyDwYawCZ6d6g+FYktiFfxf4KIzOPI5DfCjv+eE09ajIGUTVBlBVNvqw2QRyS:7HaDesd6JF94Lf4nx+x9FTLDVNeQM8
MD5:	252268FDAE62AB6C07F60CD8EE76DD25
SHA1:	A2A8B8D71F1EC4A0708DE8AB925E790A16971935
SHA-256:	CECDB8C1DA82E6EED06DB53AD89A6E3C801FA62AFDF08025413A995D68485DBF
SHA-512:	160FA83DA6A17D1220636236DAD668BAC7DBACC0DDB4D7E7E2B6FB8B975A3E4F3F27EFDC8AA686BCAD98A8A97D87CB9BC9AF5BEE15E6A1D68627580B62A20160
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/js/common/common/generated-service_worker_starter-1.0.0.js
Preview:	var SW_Starter=function(){"use strict";var n=this,o=null;n.init=function(e){n.params=e,n.add_listeners()},n.add_listeners=function(){void 0!==page_params.holida y_promo&&page_params.holiday_promo&&"serviceWorker"in navigator?(window.addEventListener("load",function(){navigator.serviceWorker.register(page_param s.sw_starter_setup.serviceWorkerPath).then(function(e){o=e,n.manageServiceWorkerVersion(),"PushManager"in window&&page_params.user.isLoggedIn&&n.param s.userEnabledNotification?(console.log("Notification Push is supported"),n.askPermission()):console.log("Push messaging is not supported")},function(e){console.log("Servi ceWorker registration failed: ",e)})}),window.addEventListener("appinstalled",function(e){console.log("RedTube App Installed"),n.params.isMobile&&ga("send",{hit Type:"event",eventCategory:"PWA",eventAction:"Add_to_homescreen",eventLabel:"Mobile"})})):(void 0===page_params.holiday_promo||!page_params.holiday_pr omo)&&"serviceWorker"in navigator&&navigator.serviceWorker.g

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ht[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):	2403
Entropy (8bit):	5.247436343926361
Encrypted:	false
SSDEEP:	48:ciktUyCVtyV28jkBNhyPsTzpnJpw35GESC2Nmmqu3YSUFj0ovj/ejS:ciktUyCLIfyPGepGzNyoGjYS
MD5:	2C72DC4409D8E8D156C5F30311186512
SHA1:	39875659C79DE6F22F7E80C8AB104DA0A2821A51
SHA-256:	33580B6BF27BE451A47A5A55F0C9895558EC62188C6EA944F35D7257F25D8E5E
SHA-512:	4E44A8D2AE29B3CD890C9D038123BDC7AABEA52CE1E4EA98EB55F4441F4AE81F7C5D80F9B813FBD39A0CCE52838F6968F0AF3AB4E7632404F8EBCC4DA3D92CF3
Malicious:	false
IE Cache URL:	http://https://ht.redtube.com/js/ht.js?site_id=2
Preview:	var htUrl="www.hubtraffic.com",htTrack=htTrack||function(){var t,e,n,r,c=!1,i=!1,o=function(t){return t.replace("http://","").replace("https://","").split(/[\/?#]/)[0]},a=function(t) {var e=RegExp(t+"=.[^;]*");return matched=document.cookie.match(e),!!matched&&matched[0].split("=")[1]},u=function(){if(document.getElementById("htScript").ge tAttribute("src").search("//hubxt.")>-1||document.getElementById("htScript").getAttribute("src").search("//ht.")>-1){var n=a("ARSC2_"+e),r=a("APEC2"+e);(0!=n&&""!=n||""!= r)&&h()}else s(),window.onmessage=function(e){e&&e.origin&&!(e.origin.indexOf(t)>=0)||c||(c=!0,h())}},d=function(){var n=document.createElement("iframe"),r=("ht tps:"==document.location.protocol?"https://":"http://")+t+"/htcheck.html?site_id="+e;n.setAttribute("id","htcheck"),n.setAttribute("src",r),n.setAttribute("frameborder","" 0"),n.width=0,n.height=0,document.body.appendChild(n)},s=function(){document.body?d():window.addEventListener("load",d)},h=function(){!function(){c=!0;var n=doc

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\httpErrorPagesScripts[1]

File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C038
Malicious:	false
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\intersection-observer[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	6944
Entropy (8bit):	5.094817989209454
Encrypted:	false
SSDEEP:	192:dNqiGQ2dWEKr1dTkeEvqAzD9JAx0GpJYhM0twC6Yx:L4dmjeiCYQt0Yx
MD5:	059853B159FD85F8CDE467314FFE566C
SHA1:	F279F588C2D30BC5EDC468EA5B1B0F7BFCF1C2AE
SHA-256:	B9E26E4A296DF7DF8A7C9DB4C2C51C23382E3CFA3E6CA8FCAAD577AA82539404
SHA-512:	077E5A387D8239F063C797650A19BD1340C4B28C3B23D39371146DE9F72EBA9543F6B533B7F245788BFA20856D3425778C3DB75C2DD5C519ABE98E7EA2FC403
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/js/generated/common/intersection-observer.js?v=4a9dc4c355497ed4f02c60b9b605e041c5eb70e0
Preview:	!function(){"use strict";if("object"==typeof window)if("IntersectionObserver"in window&&"IntersectionObserverEntry"in window&&"intersectionRatio"in window.IntersectionObserverEntry.prototype)"isIntersecting"in window.IntersectionObserverEntry.prototype||Object.defineProperty(window.IntersectionObserverEntry.prototype,"isIntersecting",{get:function(){return 0<this.intersectionRatio}});else{var g=window.document,e=[];t.prototype.THROTTLE_TIMEOUT=100,t.prototype.POLL_INTERVAL=null,t.prototype.USE_MUTATION_OBSERVER=!0,t.prototype.observe=function(e){if(!this._observationTargets.some(function(t){return t.element==e})){if(!e||1!=e.nodeTypeythrow new Error("target must be an Element");this._registerInstance(),this._observationTargets.push({element:e,entry:null}),this._monitorIntersections(),this._checkForIntersections()}},t.prototype.unobserve=function(e){this._observationTargets=this._observationTargets.filter(function(t){return t.element!=e}),this._observationTargets.length||(this._unmonito

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\jquery.cookie-1.4.0[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	1438
Entropy (8bit):	5.346655388968134
Encrypted:	false
SSDEEP:	24:NONLbSWZAjBtJRBDzfl01IlxW7TwfiTgeH5byXH8MN2kVHi7ofUb4r:NIZAfZbIc7TYeH5ScMhti74
MD5:	6E7C1D9EE38B147F21D02C20096F7B75
SHA1:	148B2EB4D2AB8EA6812F3D1AF606464368FFF38A
SHA-256:	5D29FEE0A59A316AE7DFD8B0E437407AF05CB6BC9F4646F95EC85B74CBEA4EFE
SHA-512:	D7E8ED2B4E7C60B9BC46CDE421585A2D94E1DBE3A076C6D19F054A7C160E6192BE0CF03349DB076854CAF16F2179C9FFFDA3E827E336337ED7D9F6B49B4C9D51
Malicious:	false
IE Cache URL:	http://https://cdn1d-static-shared.phncdn.com/jquery/jquery.cookie-1.4.0.js
Preview:	/*!. * jQuery Cookie Plugin v1.4.0. * https://github.com/carhartl/jquery-cookie. *. * Copyright 2013 Klaus Hartl. * Released under the MIT license. */.(function(a){if(typeof define==="function"&&define.amd){define(["jquery"],a)}else{a(jQuery)}}(function(f){var a=/\+/g;function d(i){return b.raw?i:encodeURIComponent(i)}function g(i){return b.raw?i:decodeURIComponent(i)}function h(i){return d(b.json?JSON.stringify(i):String(i))}function c(i){if(i.indexOf('"')===0){i=i.slice(1,-1).replace(/\\"/g,'"').replace(/\\\\/g,"\\")}try{i=decodeURIComponent(i.replace(a," "));return b.json?JSON.parse(i):i}catch(j){}}function e(j,i){var k=b.raw?j:c(j);return f.isFunction(i)?i(k):k}var b=f.cookie=function(q,p,v){if(p!==undefined&&!f.isFunction(p)){v=f.extend({},b.defaults,v);if(typeof v.expires==="number"){var r=v.expires,u=v.expires=new Date();u.setTime(+u+r*86400000)}return(document.cookie=[d(q),"=",h(p),v.expires?"; expires="+v.expires.toUTCString():"",v.path?"; path="+v.path:"",v.domain?"; domain="

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\lazyload.min[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\lazyload.min[1].js	
Size (bytes):	6307
Entropy (8bit):	5.100857148211249
Encrypted:	false
SSDEEP:	192:+UBo5/5x5Po9M0BBa9AhGwy5bI4gKvXm7RABZeF0:+mK/5YvB3Gwy5xP0W
MD5:	8283E4E3E49C23283AADEF2DA054A964
SHA1:	D819FA0461D1660BDE6A3712CFF589FCAFEB0EF5
SHA-256:	70F740FC38200AED87924F4C9C661F205F71D97699B4AC56727CECFB927B12E7
SHA-512:	34258834CEC0216A2C5214C9B1B38DC65012ED76EF5AF56FB96295DBE22F2A9ED77D2A34DAB99AC47CB9978C0C151BD96A39C8583A797E7D4EC3F5C65FB860A
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/js/generated/common/lazyload.min.js?v=4a9dc4c355497ed4f02c60b9b605e041c5eb70e0
Preview:	!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?module.exports=e():"function"==typeof define&&define.amd?define(e):(t=t||self).LazyLoad=e()}(this,function(){"use strict";function e(){return(e=Object.assign||function(t){for(var e=1;e<arguments.length;e++){var n=arguments[e];for(var a in n)Object.prototype.hasOwnProperty.call(n,a)&&(t[a]=n[a])}return t}).apply(this,arguments)}var a="undefined"!=typeof window,s=a&&!("onscroll"in window)||"undefined"!=typeof navigator&&/(gle|ing|ro)bot|crawl|spider/i.test(navigator.userAgent),c=a&&"IntersectionObserver"in window,n=a&&"classList"in document.createElement("p"),w=a&&1<window.devicePixelRatio,o={elements_selector:"img",container:s||a?document:null,threshold:300,thresholds:null,data_src:"src",data_srcset:"srcset",data_sizes:"sizes",data_bg:"bg",data_bg_hidpi:"bg-hidpi",data_bg_multi:"bg-multi",data_bg_multi_hidpi:"bg-multi-hidpi",data_poster:"poster",class_applied:"applied",class_loading:"loading",class_loaded:"loaded",class

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\mg_lazyload-v1.0.0[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):	503
Entropy (8bit):	4.92616137335534
Encrypted:	false
SSDEEP:	12:cOg7pXX6epZ0NTPCO46Zj/AWYDffBNl9um+zSyZaQ0aL4:cOg7pHvATqOtKWYDffl9um+nZaQs
MD5:	C75EAAB4A392AEF236888EEC51A43E03
SHA1:	BEB74247B45FDD10376302517282DFA3579A9469
SHA-256:	4D498D4E17132E287AF95C43F6247A797706331E529FB8205A9C1246566A6F1E
SHA-512:	B547082C99F49B0D749F6D3F60E648DF48346EEA633754EC83D2C30A23B1CB1687DE005F6126AF284DBCD0BC3AEEDE6BAD10BAF994126B85ED175E6C8F1013D
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/js/generated/common/mg_lazyload-v1.0.0.js?v=4a9dc4c355497ed4f02c60b9b605e041c5eb70e0
Preview:	!function(){if("function"==typeof window.CustomEvent)return;function t(t,n){n=n||{bubbles:!1,cancelable:!1,detail:void 0};var e=document.createEvent("CustomEvent");return e.initCustomEvent(t,n.bubbles,n.cancelable,n.detail),e}t.prototype=window.Event.prototype,window.CustomEvent=t}();try{window.lazyLoadOptions={elements_selector:".lazy",threshold:50},window.addEventListener("LazyLoad::Initialized",function(t){window.lazyLoadInstance=t.detail.instance},!1)}catch(t){console.log("Error on Lazy Load")}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\redtube_logo[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1809
Entropy (8bit):	5.245831689985034
Encrypted:	false
SSDEEP:	24:2dzATLf37CvX4qm68gAfzp4FnJ9FFlPahXtZVhJwY2clJbZph7zfC:czAvf3WgqPAfz8JdlPahLVhWYPE7pfC
MD5:	08BB075900DD1D14D9CA147CD6DB3A12
SHA1:	91030F1DC0696E5901D60A47F2392187FB474910
SHA-256:	0B93CE59317A2DD4F212565BA372E6C1221C359A3262A953E832E01FE6421E61
SHA-512:	57E6CF164D8720E7CAC20DAF0CB44AA0CECE3101DBA0EF200BDA3C374B0B866D612D17C5387A7C9778887DEA8EF2218402B33FA29188191B153055464ADDA3A
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/images/common/logo/redtube_logo.svg?v=4a9dc4c355497ed4f02c60b9b605e041c5eb70e0
Preview:	<?xml version="1.0" encoding="utf-8"?>. Generator: Adobe Illustrator 22.0.1, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->.<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px".. viewBox="0 0 206 55" style="enable-background:new 0 0 206 55;" xml:space="preserve">.<style type="text/css">...st0{fill:#AE1A20;}...st1{fill:#FEFEFE;}.</style>.<g>..<path class="st0" d="M18.5,29.5c1.4-0.5,5.8-2,5.8-8c0-4.8-3.6-8.2-9.9-8.2H4.1l7,4.5h1.9c3.8,0,5.6,1.6,5.6,4.1S16.4,26,13.7,26...h-2.7l-6.9,4.4v10.2h5.6V30.5H13l5.7,10.1h6.4L18.5,29.5z M0.7,15.3l9.9,6.9L0.7,29V15.3z"/>..<g id="surface32_1_">...<path class="st0" d="M27.1,13.1h18.7v4.8H32.5v6.3h6.4v4.5h-6.4v7.1h14.4v4.8H27.1V13.1z"/>..</g>..<g id="surface40_1_">...<path class="st0" d="M54.9,36.4h2.7c5.3,0,8.2-1.9,8.2-8.9c0-5.4-2.5-8.9-8.3-8.9h-2.6C54.9,18.5,54.9,36.4,54.9,36.4z M49.4,13.1....h7.9c9.9,0,14.1,5.9,14.1,13.7c0,8.9-4.5,13.7-13.1,13.7h-8.9L49.4,13.1L49.4,13.1

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\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):	28909

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\video-index[1].css	
Entropy (8bit):	5.053548137556725
Encrypted:	false
SSDEEP:	384:lH7q9HpmR7R76KMsuyMBqzIOcumTB5YGuJu+c4Xb+zO:xRQu6B5YGuxcHO
MD5:	2D08059D2AC9224A436170A2F8699AD0
SHA1:	36387B1C2C56F96FEA802A28AD39DE7CFAAEF4DD
SHA-256:	CD934289D94026D85AE3CA9BEF60DFF9103C1A40B0C296F836C05FC58DD914F4
SHA-512:	EC6EE27755FA69437CF2398C184D758D07762AE4B6DC2369DCB560AB3B7C473718F4AA8C48DDAE0F69AA2679909EC2BA52905FB31F0AAA7CFDBA29A5B1A403 23
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/css/generated/pc/video-index.css?v=4a9dc4c355497ed4f02c60b9b605e041c5eb70e0
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\0W10PBUV\video[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	downloaded
Size (bytes):	117670
Entropy (8bit):	5.494265555376669
Encrypted:	false
SSDEEP:	1536:ppdgEWZg2eKH+Lsa1iOk5tREV8AzyEqc6OPv79ErimJ0wt0smLkkSOlnE:Zth0vg56OPjOUE
MD5:	8644ED2C939ED4BE418044B36C0972B4
SHA1:	77DBDDFEFA211B02DE9A022CD2DF0A9CF12359DC
SHA-256:	BFED8460EDDE4D997A5933A895E2151B56FD3ACBFA2A5D70FB414BDC60984A6B
SHA-512:	E9F8249EBD2A9570F36EFDBC7912524E7662A269065A7B3C02F657217317E8ECD05AD9EEE79C9102AA88EF594A0BA34A0017A02E5BC634AB44B557DB422D283
Malicious:	false
IE Cache URL:	http://https://vz-cdn.trafficjunky.net/html5video/video.js
Preview:	/*! Video.js v4.12.0 Copyright 2014 Brightcove, Inc. https://github.com/videojs/video.js/blob/master/LICENSE */ .try{.(function() {var b=void 0,f=!0,j=null,l=!1;function m() {return function(){}}function n(a){return function(){return this[a]}}function q(a){return function(){return a}}var s;document.createElement("video");document.createEle ment("audio");document.createElement("track");.function t(a,c,d){if("string"===typeof a){0===a.indexOf("#")&&(a=a.slice(1));if(t.Aa[a])return c&&t.log.warn('Player "'+a+'" is already initialised. Options will not be applied.'),d&&t.Aa[a].I(d),t.Aa[a];a=t.m(a)}if(!a||!a.nodeName)throw new TypeError("The element or ID supplied is not valid. (videojs) ");return a.player||new t.Player(a,c,d)}var videojs=window.videojs=t;t.jc="4.12";t.wd="https:"==document.location.protocol?"https://":"http://";t.VERSION="4.12.0";.t.options= {techOrder:["html5","flash"],html5:{},flash:{},width:300,height:150,defaultVolume:0,playbackRates:[],inactivityTimeout:2E3,children:{med

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\10[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):	13426
Entropy (8bit):	7.953190625823207
Encrypted:	false
SSDEEP:	192:Y1JZnp61FPK2oTnsNxQb80oc1NNCiRBzYDiJZtMRIrCEOpuzn9:sJZxzTssumiWJZtMRIrkM
MD5:	31F266C28A1C5AA9DDB8579623B01E27
SHA1:	3E17CE6C9253C31BE801CFD2FB1DF30F57664907
SHA-256:	E1A9FE5BBCC27EF0A187152DC5CCA69327F9ED1C341A39FEA5AF0F3E1673AACF
SHA-512:	C266CAC29283E2F391BB1B02208F16FD9FBC079457B2477DFC5061A671570E7437C21174E23480A7C18ABE09EA7D1A85B00E72444F5CF0699D65B4D155A8A841
Malicious:	false
IE Cache URL:	http://https://di.rdtcdn.com/m=eW0Q8f/media/videos/202007/16/34055961/original/10.jpg
Preview:	......JFIF.....C.....!....."$".$.....C.....0.."....t~....wi.. .O....k.B..ch.QdZ...s..7E..`...=..Nl.x.VU2.a..z*z/kXey..s....'...~.&..W..eR.....b.8=.%.b;jb[.a..Et..-.t.f\;.h.2..]...r #ZVN.`v.o.uh...}....3.D~..k.....yc....J..E.vQ|.....;a..~.^.z.|., ...9b.sA5..U.)....vn..C.x/y..>...u....F..&.....H.-..c.F.....#H.].U..k.....9.....d..d..]K...#.n.....].....z.:.U_*.^._9:r..3.+...mP.m..au...T.x.....x-...F...."..l}.j(.....k.mZ.|... .i4.w!a..e....u.....] ....4.d0...+.4^..)..{?.0E...!.....#qfS>...:.2.....Y&.B..0Os..w.p....+N#.6....E..W.F...3.".U..ky`.f5J<.....?...=V..2...tk~CX,..c*.._X..a.xnol].t.J4..Tf.(.nV...-..^..H.c..G9..N..3m,..>N.pZ ..m|....0..]y.F.%].(.R..7`.Ko`d.....uU.....WdU.X..>G..h|..<.....t.z..4..Td.K...;.x.n..k.G.....e.....^.....D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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):	9421
Entropy (8bit):	7.928664665322119
Encrypted:	false
SSDEEP:	192:DUgQ6r32XzS5XQe2ZYb/TsYquCe5CyzmQO1nZs:Xd5XMOQYq/ChEpZs

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\14[1].jpg	
MD5:	5BBD60E7FC9B6BCAE03AA0546C8D02D3
SHA1:	311474CF02C56CD78F6E79613276D8E58EDFDE39
SHA-256:	65A967D5FFEA61C50DE2158ED90ABB888A3451E45020176BF1F370F90FFD879E
SHA-512:	A42C0D2B2852D0FE3969D6B1EA81017EF252797DC29743418B80D68EF0F04FD7040E7D1D16672346019991F08FD59D8911450A2CDA258AF905650EDE80D86BD6
Malicious:	false
IE Cache URL:	http://https://di.rdtcdn.com/m=eW0Q8f/media/videos/202010/15/37001911/original/14.jpg
Preview:	.....JFIF.....C.....!......"$".$.....C.....0.."..... .....To?....f...D.....S>.F.j..f..U.zv..)b@....26(.&dnT.....o.@.<....I...6..j.y.3"=..y.qrZ.>]y.]]]..Mx....2.... ....'R.6....P1.L..h....<y.y...6.[...T+...#..#.....2z...s~....D..Y.M<l....x.:. CA..+Q..t.....z_.:.:..].M.l.c.t.$tkr..f...%e...L.k..s...P.....5...*z....{b.,Az.>o....9...l...$8..&.....h.`@~wM\|.e.[.....".....<.....z.4...\.\.D..f@.D.$..dd/_.4...#....e.|.%. .....3+d..d5\..s.V=.. 7rm...y2..g..5...Kj...u.@..... /`.4...G...G+.+r.c.<J.,..NOS..]P..... .X25.....b..L7...S.r...*...22L.L...a.`.....;S\m.]..*T.A..k...m=.3.k.....MD..2*..~.~G.m.....u.E...!M..o...L...#. .@# . [jm.YX.iJ&*8O..0.~-.We..0lC.th.B..cScPi.y..B.s...%zx....a....0;..G.....0..!.d.#&...1o2.d...7...]^...;..i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #00 0000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\V8EBMGK4.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):	505624
Entropy (8bit):	4.919795270172321
Encrypted:	false
SSDEEP:	6144:wtfnaSlkHjDhJnyXIJtogs1IzVyO+Q766U47IUmJV62n81smi1ULqQd3QoA9bQ1e:wt5xb0zitDx/c
MD5:	125E534120B4F219694D67503AD43679
SHA1:	7DCCAA98A8B419A735FF2D9AFE0CB00D27557A96
SHA-256:	6011542FC8C8F02A25802987CC94AE26353D943C5D2BA5D9A73AB151CBEEEDE3
SHA-512:	D0DC2D12512FF2DA63DB88EB0108E5C9FE609498409089F8CBBE889F9D055405D663791205DBBAC649AF1B0C673A25BF7B1D06101E898A51D317CB71551998A
Malicious:	false
Preview:	<!DOCTYPE html>. [if lt IE 7]><html class="ie ie6 language-en" lang="en"><![endif]-->. [if IE 7]><html class="ie ie7 language-en" lang="en"><![endif]-->. [if IE 8]><html class="ie ie8 language-en" lang="en"><![endif]-->. [if IE 9]><html class="ie ie9 language-en" lang="en"><![endif]-->. [if !(IE)]> > <html class="language-en" lang="en"> <![endif]-->. <head>. <title>Free Porn Sex Videos - Redtube - XXX Movies - Home of Videos Porno</title>. .<meta http-equiv="Content-type" content="text/html; charset=UTF-8" />.<meta http-equiv="X-UA-Compatible" content="IE=edge" />.<meta name="msapplication-config" content=" none" />.<meta name="keywords" content="porn, sex,xxx" />. <meta name="description" content="Redtube brings you NEW porn videos every day for free. Enjoy our XXX movies in high quality HD resolution on any device. Get fully immersed with the latest virtual reality sex videos from top adult st

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ads_test[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):	941
Entropy (8bit):	5.196634423570928
Encrypted:	false
SSDEEP:	24:7EjIfNqRRWVJlJDOHaA/92PYP6c5h1f12WsostoXGv6Z17LGmwRUk:7EfwFlO6A/92PYP6c1f12Wbse2v6vvGf
MD5:	5ED83705F6BEBA4D3195FE5155FCBEBF
SHA1:	AA3259819C69554A191D04D17348280AB77DFDB7
SHA-256:	5D639453B9308CDB130DF7E4EF3F19DF3DE97F1051165BB49E1E96C21DB728F4
SHA-512:	DB3BD253A129BFF7B0A5B4322F621319EA0AF3808F3FBA99AC1602F511D893859B736DF1FD2CB67994550722495867 2B2641193D843316EB176460DC7E7C4C26
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ads_test[1].js	
IE Cache URL:	http://https://static.trafficjunky.com/ab/ads_test.js
Preview:	var _0x2d2f=['innerHTML','appendChild','div','adsbox','page_params',' ','createElement','holiday_promo','className','offsetHeight','getElementsByClassName'];(function(_0x3fdd88,_0x2d2f8e){var _0x1d6e20=function(_0x320d01){while(--_0x320d01){_0x3fdd88['push'](_0x3fdd88['shift']());}};_0x1d6e20(++_0x2d2f8e);}(_0x2d2f,0x170));var _0x1d6e=function(_0x3fdd88,_0x2d2f8e){_0x3fdd88=_0x3fdd88-0x0;var _0x1d6e20=_0x2d2f[_0x3fdd88];return _0x1d6e20;};window[_0x1d6e('0xa')]=window['page_params']||{};window[_0x1d6e('0xa')][_0x1d6e('0x2')]=function(){var _0x38d652=document[_0x1d6e('0x1')](_0x1d6e('0x8'));_0x38d652[_0x1d6e('0x6')]=_0x1d6e('0x0');_0x38d652[_0x1d6e('0x3')]=_0x1d6e('0x9');var _0x3afab7=![];try{document['body'][_0x1d6e('0x7')](_0x38d652);_0x3afab7=document[_0x1d6e('0x5')]('adsbox')[0x0][_0x1d6e('0x4')]===0x0;document['body']['removeChild'](_0x38d652);}catch(_0x4d8a06){_0x3afab7=![];}return _0x3afab7===!![]?undefined:!![];}();

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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):	79163
Entropy (8bit):	5.118079330277673
Encrypted:	false
SSDEEP:	1536:LVXor3Hk610Ax2/jr/CU/13/OI6AS/rMD76obNMh5RIleVoQrPLik:Sr3J
MD5:	80689C65E96723C473925C28C0ABB64A
SHA1:	357C52A4E1CBCB22C3A74E429C1A8233B8CA1B4F
SHA-256:	30EEC374FFC1E8B22297D3C5D98A609493741DE40A12033CCF0623BFECA2A74E
SHA-512:	7D0E187B923433150FFD02BC427CB3268AA7040714935C8E195FA6D34A549531F6EBCEA1A961E167A0BCA00ECF3BBD9373C87E4964B9A82ECF9129614DF882C
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/css/generated/pc/default-redtube.css?v=4a9dc4c355497ed4f02c60b9b605e041c5eb70e0
Preview:	.rt_icon{font-family:rt_font!important;speak:none;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_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:before{content:"\e95c"}.rt_no_internet:before{content:"\e95a"}.rt_unlink:before{content:"\e957"}.rt_link:before{content:"\e08d"}.rt_Live_Cams:before{content:"\e958"}.rt_Pip_Circle:before{content:"\e956"}.rt_Pip_Square:before{content:"\e959

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\default-redtube[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):	164215
Entropy (8bit):	5.277968938738448
Encrypted:	false
SSDEEP:	3072:RYx8MrZ8Dw9GXNJFrK57vgv0T6tXy0fL18Uvb3r:8vZ5GFK57vYh
MD5:	2C781C309D262ECF4F710D4227333576
SHA1:	6BD21BB281119B0494B05C196BA2A8F7DA3A3D58
SHA-256:	90A87AB16820F65492E33EDA699BD19479B8DE8A9706FFDA28DA12C5C59BFB02
SHA-512:	16801DA2A15E8FE9023F75BC32CB3DE1C53B99E961343EB55B29020458DC8B4FB4D866D6987985B044C225EA8594966831A4B667881A5692BE1AA15BA0B4A3CF
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/js/generated/pc/default-redtube.js?v=4a9dc4c355497ed4f02c60b9b605e041c5eb70e0
Preview:	!function(e,t){"object"==typeof exports&&"undefined"!=typeof module?module.exports=t():"function"==typeof define&&define.amd?define(t):(e=e||self).Vue=t()}(this,function(){"use strict";var g=Object.freeze({});function D(e){return null==e}function P(e){return null!=e}function T(e){return!0===e}function E(e){return"string"==typeof e||"number"==typeof e||"symbol"==typeof e||"boolean"==typeof e}function F(e){return null!==e&&"object"==typeof e}var a=Object.prototype.toString;function l(e){return"[object Object]"===a.call(e)}function r(e){var t=parseFloat(String(e));return 0<=t&&Math.floor(t)===t&&isFinite(e)}function _(e){return P(e)&&"function"==typeof e.then&&"function"==typeof e.catch}function t(e){return null==e?"":Array.isArray(e)||l(e)&&e.toString===a?JSON.stringify(e,null,2):String(e)}function B(e){var t=parseFloat(e);return isNaN(t)?e:t}function s(e,t){for(var n=Object.create(null),a=e.split(","),r=0;r<a.length;r++)n[a[r]]=!0;return t?function(e){return n[e.toLowerCase()]}:function

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=9002

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\dnserror[1]	
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMo reInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";....//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.su bstring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var pound Index = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\lux[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):	22107
Entropy (8bit):	5.3009921392277475
Encrypted:	false
SSDEEP:	384:NuW8uj1mSAq2pmWOXXpit1GAZAwL9mc2lTyTqZ+wcMOlPcH148TIDcfyyXhoDhg:NuW9MmxXpiSexpmwGjclPJ8TIgqyX2DG
MD5:	BF55DE6060BF94416DE996E2A306230A
SHA1:	12C36CE358AA384C17B22B02A541F63433A824D2
SHA-256:	2F268D279A69B0E891B11CA271274581C29904060421BDE47E2BE30886A3F20C
SHA-512:	A826FAE79873617C6E720FD0CC6543D20C8A41C0171EB47AAB3029CD3E2D3471E4D4A6E7348DC39839F161BDC2C8F696814BF19CD02694B10ED309F1CB781CE
Malicious:	false
IE Cache URL:	http://https://cdn.speedcurve.com/js/lux.js?id=609859533

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\lux[1].js	
Preview:	var LUX=LUX||{};LUX.samplerate=1;var LUX_t_start=Date.now(),LUX=window.LUX||{};LUX=function(){var gaLog=[];dlog("lux.js evaluation start.");var version="210",_errorUrl="https://lux.speedcurve.com/error/",nErrors=0,maxErrors=5;function errorHandler(e){nErrors++,e&&void 0!==e.filename&&void 0!==e.message&&(-1!==e.filename.indexOf("/lux.js?")||-1!==e.message.indexOf("LUX")||nErrors<=maxErrors&&"function"==typeof _sample&&_sample())&&((new Image).src=_errorUrl+"?v="+version+"&id="+getCustomerId()+"&fn="+encodeURIComponent(e.filename)+"&ln="+e.lineno+"&cn="+e.colno+"&msg="+encodeURIComponent(e.message)+"&l="+encodeURIComponent(_getPageLabel())+(connectionType()?"&ct="+connectionType():""))}window.addEventListener("error",errorHandler);var gaPerfEntries="object"==typeof window.LUX_al?window.LUX_al.slice():[];if("function"==typeof PerformanceObserver){var perfObserver=new PerformanceObserver((function(e){e.getEntries().forEach((function(e){gaPerfEntries.push(e)}))}));try{"function"==typeof Pe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\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:	E1C86B7E4DC06653B63C32A125EB69FA7FFF2EEF72544D692FE91EC16BB3D85BEDC37E3666756D82F95DF73E8C469FF0F3B64DA1259D4B9DF0E9A6AD17BA34C9
Malicious:	false
IE Cache URL:	http://https://vz-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.cssText=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\MEEXW4H4\site_sprite[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 42 x 471, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	3787
Entropy (8bit):	7.899716864079092
Encrypted:	false
SSDEEP:	96:zvrPecXH3iDChbDrbod2RMUcPiBhPdDG0iT6ovyzS:zZ4dizcPifPdDpi+xu
MD5:	BFC6AC50D0EA19FFC3A6AEC75325E1FC
SHA1:	CEC78D41498937E7FB7EEEF35DCCD0E9D4F79371
SHA-256:	C8DC62ED5D22FF5ECB018B0F7804CF23438E960967B364CC48E1892862538020
SHA-512:	76ACBC24FDE26BA4E5A8FC06F18F2510F1CABDDF17BD97089B8E288875A1E516981B87E023006F5EEC45CE40854229F625787F3127B864227AC36010F0A1B8C3
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/images/pc/site_sprite.png?v=4a9dc4c355497ed4f02c60b9b605e041c5eb70e0
Preview:	.PNG.....IHDR...*.....f8....XPLTE.....<.{....."&.. .".. .iu..!.. ..... .".!..".{... .{...!..!.....#....l$.{...!."&.. .{..~+....{..{..{...$..$..2.{..{...!.{..{... ....{..{.....`O..... ..7..!....{.....{..{.. .....{.....{...4.....#'....!%.....{..{....xb :.."....{..u(M>..... .{.....#....q..d....%.....y..u.....vy.....m....}.....OR.....mp.;>.....47.....EI.<..2..... .UX.....n...j..hk.ad.JM.',.....{~.\_.....i..]..V.....9.... ...t..`..F..>..2.....L...\..T..BD.67.+,.....M.....C.....\tRNS.....~\L.m!.....9..D..[..m,).....# ....F...~V.....v^O9).....m...A.s;....IDATx...Mk.0..q...m....J.....14_F..NB0w...c..v.....PV..7.1';..kK..a..?.....O.e/..!. .t.).@U..e.j.WJlb.[.1...F..dvw&...T...:.....:.lxC.8@b<?.d..J.'.@. ....)cB.,%.#.Gt.....}...F...]...4/`.L.....c%U.....c.+.8=R.j.1.....x...ci.Rb..U^.Y.f....%.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\video-js[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text
Category:	downloaded
Size (bytes):	27990
Entropy (8bit):	5.011201483519688
Encrypted:	false
SSDEEP:	384:xFMXat67oQnZoBHW+oc+M15oigxwOztw/nHfF82rFXd0:PMjrWhW+x+k+bxwOztK/F82rFi
MD5:	4B6360D4985D7621A945B389F7B6C2D4
SHA1:	A0D4A315A506853E02F28396204A20263E579E77
SHA-256:	FEFE18CFC7E1ACAF6CDE669234B5AF62723695C6EFE43C8E2EBCC19AC2A35FB1
SHA-512:	D97680447F103A8F562ACF44F4AF7713E19F7A36485BD994F531C886D97C5F466D44CC0222BCB0DE1722E07D08A60D58D0D77D59FC9097FE7D8F333211646205
Malicious:	false
IE Cache URL:	http://https://vz-cdn.trafficjunky.net/html5video/video-js.css

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\video-js[1].css	
Preview:	/*!.Video.js Default Styles (http://videojs.com).Version 4.12.0.Create your own skin at http://designer.videojs.com.*/./* SKIN.================================ ==.The main class name for all skin-specific styles. To make your own skin,.replace all occurrences of 'vjs-default-skin' with a new name. Then add your new.skin name to your video tag instead of the default skin..e.g. <video class="video-js my-skin-name">.*/../.vjs-default-skin {. color: #cccccc;.}./* Custom Icon Font.----------.The control icons are from a custom font. Each icon corresponds to a char cter.(e.g. "\e001"). Font icons allow for easy scaling and coloring of icons..*/.@font-face {. font-family: 'VideoJS';. src: url('font/vjs.eot');. src: url('font/vjs.eot?#iefix') format('embedded-opentype'), url('font/vjs.woff') format('woff'), url('font/vjs.ttf') format('truetype'), url('font/vjs.svg#icomoon') form

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #00 0000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\ads_batch[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	12356
Entropy (8bit):	5.346890660247692
Encrypted:	false
SSDEEP:	192:74N+lsN+yhUpgy4KpmqpG29gy4KpmqpG2jGN+yhUpgy4KpmqpG2Y:7wEEzhVPmuzhVD
MD5:	C4AC00EEC71FE50A0AC77C7859E5F08B
SHA1:	83543FB116A178D9F38861776DD680876E51B93B
SHA-256:	877CF7F7234B687EB978140A9F7F6A8FBD6925B15C0298CE45E3F59843C24B00
SHA-512:	AAEC98B404681BB4414F0278A5A9DA959FD437D969056429399D63061E79969EC1FF798CF32CFCB00638F6FBA4E77E6678A399DD3309260EA21937B6E9FB9062
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=31C245E9-8274-44E0-99FC-D9CEDF246D2C&data=%5B%7B%22spots%22%3A%5B%7B%22zone%22%3A11531%7D%5D%7D%5D
Preview:	[{"ad_id":1490001181,"member_id":52,"campaign_id":1002577791,"country_code":"CH","zone_id":"11531","link":"https://ads.trafficjunky.net/click?url=https%3A%2F%2Fwww.securegfm.com%2F38c6b20f-b4f9-485e-be75-49b76368ae57%3FSID%3Dtj-desktop-rt-ts-int%26SID2%3Dall-Redtube%2520PC-%2520Top%2520Right%2520Square%26SID3%3D315x300_sep112%26SID4%3DRedtube%2520PC-%2520Top%2520Right%2520Square\u0026amp;click_data=QAAAADQAAADr8ONfAAAAAAAAAALLQAACy0AAAAAAB_H8I7HZ3PWG21HT4AAAAAAAAAAAEAAAAAAAAAAAAAAAA==\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=70_160877386 7132933126_49704_3559\u0026amp;s_kw=0\u0026amp;kw=%7B%7D\u0026amp;ano=5\u0026amp;imptype=0\u0026amp;adtype=html5\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=4b4aeb67aebb72a01cc16ccc99e420e2ee84cc

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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):	10656
Entropy (8bit):	5.441319936534521
Encrypted:	false
SSDEEP:	192:EOx1N+L5a/uamJN+Qgy4KVm0qpG2FN+++gy4KVm0qpG2XX5a/uamJN+Qgy4KVm0D:HxDgSLXvBSLu
MD5:	20E175FC3C0E2819EC8FCCBDC9D35C1A
SHA1:	C20F73BBE6D8453ABC888C55815223884019E46E
SHA-256:	6CFD50AC724270ED64AF873935930032AE0C94A4CA0B65A3FD72E1E48B69ED18
SHA-512:	9347FCDA75E7C519E849B36FC7E03869869F85108B65725175FF0912DA365CA5DB08DD83E4B6EE9DFFE144D5CD5BBA39A956DD885BA7639EBDE0567A0C965EB
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\ads_batch[2].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=31C245E9-8274-44E0-99FC-D9CEDF246D2C&data=%5B%7B%22spots%22%3A%5B%7B%22zone%22%3A11571%7D%5D%7D%5D
Preview:	[{"ad_id":1423916801,"member_id":7290,"campaign_id":1003617561,"country_code":"CH","zone_id":"11571","link":"https://ads.trafficjunky.net/click?url=\u0026amp;click_data=QAAAAHocAADr8ONfAAAAAAAAAAAR0R4AMy0AAAAAAAAZ_dE7AT_fVP_gyT0AAAAAAAAAAAABAAAAAAAAAAAAAA==\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=70_160877386715469085 7_49704_1130\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=aa61827d70971524d5b6d51dc4715f0557643f6f","img_url":"https://a.adtng.com/get/10008675?time=1572467498430","isdefault":1,"html":"\u003cHTML\u003e\u003cHEAD\u003e\u003cTITLE\u003eAd delivery system\u003c/TITLE\u003e\u003cmeta name=\"keywords\" content=\"1003617561\" def=\

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\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:	3469D45A06E7CB96315457D8AF8575FD1F8FF86D5DD5EA2D6FBA53E6DC6A21CAF559C504735DD74D85D4AF922B6198B8DAE200BAAF0CFAB793A18A179F95BE44
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/css/generated/pc/default-redtube_logged_out.css?v=4a9dc4c355497ed4f02c60b9b605e041c5eb70e0
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\PSUEOSZZ\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\embeddedads.es5.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	74264
Entropy (8bit):	5.318067979167158
Encrypted:	false
SSDEEP:	1536:Yg2Kjk5Q91kYiII7J/S/D+4u6tmshmMGR:3j5HTJGD+4u6tmSm1
MD5:	8D68710C4E9598889B26DA9DBD37F13F
SHA1:	296156EB4CC77C97329ACA99FAE3FBFB03E9BDF7
SHA-256:	480D42742F9505F30CFED8E89F4264A2CA09E5CB13B2190803B4E5EBF31FCC88
SHA-512:	C95EB2EA5D205D7C2A705889A176E552BC02617442F89992736F4DDB1D50BB6774C0A637AD192089C15FA9BB14A21CBC88D007B2463A939A5157900657AF7D54
Malicious:	false
IE Cache URL:	http://https://static.trafficjunky.com/invocation/embeddedads/production/embeddedads.es5.min.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\embeddedads.es5.min[1].js	
Preview:	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?define("JS Ads for Publishers",[],t):"object"==typeof exports?exports["JS Ads for Publishers"]=t():e["JS Ads for Publishers"]=t()}(window,(function(){return function(e){var t={};function n(r){if(t[r])return t[r].exports;var o=t[r]={i:r,l:!1,exports:{}};return e[r].call(o.exports,o,o.exports,n),o.l=!0,o.exports}return n.m=e,n.c=t,n.d=function(e,t,r){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var r=Object.create(null);if(n.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var o in e)n.d(r,o,function(t){return e[t]}.bind(null,o));return r},

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\jquery-2.1.3.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	84320
Entropy (8bit):	5.370493917084567
Encrypted:	false
SSDEEP:	1536:AP1vk7i6GUHdXXeyQazBu+4HhiO2wd0uJO1z6/A4fGAub0i4ULgGiyz4npa98Hrb:z4UdWJiz6UAIJ8pa98Hrb
MD5:	32015DD42E9582A80A84736F5D9A44D7
SHA1:	41B4BFBAA96BE6D1440DB6E78004ADE1C134E276
SHA-256:	8AF93BD675E1CFD9ECC850E862819FDAC6E3AD1F5D761F970E409C7D9C63BDC3
SHA-512:	EDA31B5C7D371D4B3ACCED51FA92F27A417515317CF437AAE09A47C3ACC8A36BDBB5A5E70F0FBFD82D3725EDF45850DDE8CA52C20F9A2D6E038B8EAACEE3CF1
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/js/common/lib/jquery-2.1.3.min.js?v=4a9dc4c355497ed4f02c60b9b605e041c5eb70e0
Preview:	/*! jQuery v2.1.3 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */.!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k={},l=a.document,m="2.1.3",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return d.call(this)},get:function(a){return null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a,b){return n.each(this,a,b)},map:function(a){return this.pushStack(n.map(this,functi

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\jquery-ui-1.10.3[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	235535
Entropy (8bit):	5.222046709642086
Encrypted:	false
SSDEEP:	3072:57dcE5lTfovYhuURaCWJEvQyyfyqrfHJ05wDS3+l7wWZjn+w:5766TfomuU02vaC5ws+SWZ7+w
MD5:	376C27BAD9C60530EB35FF15E063CD93
SHA1:	9A2812684D117FB58B751334F57C3EA0C03F4A20
SHA-256:	B5D9FC44A3D2066E1A56FDFF96ABFFB90021022B07AE3C77361ED7B80438DF03
SHA-512:	273A91314D1CD6F4678C9E81881988B2A6C4D7287092A2F11E5DF753505D054222DFAFB57EB94B5DA901D2B9CCDE8B449CE21844C8C186152C390431C409696
Malicious:	false
IE Cache URL:	http://https://cdn1d-static-shared.phncdn.com/jquery-ui-1.10.3.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\jquery-ui-1.10.3[1].js	
Preview:	/*! jQuery UI - v1.10.3 - 2013-05-03.* http://jqueryui.com.* Includes: jquery.ui.core.js, jquery.ui.widget.js, jquery.ui.mouse.js, jquery.ui.draggable.js, jquery.ui.droppable.js, jquery.ui.resizable.js, jquery.ui.selectable.js, jquery.ui.sortable.js, jquery.ui.effect.js, jquery.ui.accordion.js, jquery.ui.autocomplete.js, jquery.ui.button.js, jquery.ui.datepicker.js, jquery.ui.dialog.js, jquery.ui.effect-blind.js, jquery.ui.effect-bounce.js, jquery.ui.effect-clip.js, jquery.ui.effect-drop.js, jquery.ui.effect-explode.js, jquery.ui.effect-fade.js, jquery.ui.effect-fold.js, jquery.ui.effect-highlight.js, jquery.ui.effect-pulsate.js, jquery.ui.effect-scale.js, jquery.ui.effect-shake.js, jquery.ui.effect-slide.js, jquery.ui.effect-transfer.js, jquery.ui.menu.js, jquery.ui.position.js, jquery.ui.progressbar.js, jquery.ui.slider.js, jquery.ui.spinner.js, jquery.ui.tabs.js, jquery.ui.tooltip.js.* Copyright 2013 jQuery Foundation and other contributors; Licensed MIT */.(function(b,f){var a=0,e=

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\popunder.min[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	24776
Entropy (8bit):	5.227843500926117
Encrypted:	false
SSDEEP:	384:3Tv6EGcupbRreD8IgXdQQO/Jl9Ka51Wrx+mO7IggHiNcwf3L6tC1/JnaXi3gTVFN:b+IkdQQO/JlWrxzO7IfiNcK1/5aXiiT
MD5:	2D7B75977A340B02735916EB89035160
SHA1:	D64B0BF7D21087A8AAC6B893DEF60BF30F85F851
SHA-256:	E8512D7EDA09AB851A97A02F3214B5EDBDED3CBD11BE861BEB0C623F8EB6B8AE
SHA-512:	7BE69BFFEC0E71D720380AA365513FE0190FFFC05FA925205A5CDB878E0380D4733DD204EF8B490C2CD9B0571CF2855CF7221D21D6DA74CF71BD630AB091C1C
Malicious:	false
IE Cache URL:	http://https://static.trafficjunky.com/invocation/popunder/production/popunder.min.js
Preview:	!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?define("_1yz6ewa2mfs",[],t):"object"==typeof exports?exports._1yz6ewa2mfs=t():e._1yz6ewa2mfs=t()}(window,(function(){return function(e){var t={};function n(r){if(t[r])return t[r].exports;var o=t[r]={i:r,l:!1,exports:{}};return e[r].call(o.exports,o,o.exports,n),o.l=!0,o.exports}return n.m=e,n.c=t,n.d=function(e,t,r){n.o(e,t)||Object.defineProperty(e,t,{enumerable:!0,get:r})},n.r=function(e){"undefined"!=typeof Symbol&&Symbol.toStringTag&&Object.defineProperty(e,Symbol.toStringTag,{value:"Module"}),Object.defineProperty(e,"__esModule",{value:!0})},n.t=function(e,t){if(1&t&&(e=n(e)),8&t)return e;if(4&t&&"object"==typeof e&&e&&e.__esModule)return e;var r=Object.create(null);if(n.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:e}),2&t&&"string"!=typeof e)for(var o in e)n.d(r,o,function(t){return e[t]}.bind(null,o));return r},n.n=function(e){var t=e&&e.__esMo

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\timings-1.0.0[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	3187
Entropy (8bit):	5.190303506246706
Encrypted:	false
SSDEEP:	48:tuStgz6UFeR9Rh+zj5Hzh9b4cuKIoc71TKPQrMIbxD8CD7:tu2gz6UFeXP+zj5H5VCBT7dD8CH
MD5:	71F3A664DEFDA2F5724EAA072FC45C3C
SHA1:	FA1F57C353C958870FC31BA122849A6018341598
SHA-256:	5D0FEC532F2E7D4DC5A759EA0967583C0886585C3765DD79D58E38F0BFB7E877
SHA-512:	579708C88646A626E0FAED55E587E92E706B207EE6FA1D10C81A27D82F9B77FBB90ED6DE5EF5B12FBF4386FA65B45B36EAF1DFF6C48F0B9E90CDD23AD2C3A90D
Malicious:	false
IE Cache URL:	http://https://cdn1d-static-shared.phncdn.com/timings-1.0.0.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\timings-1.0.0[1].js	
Preview:	function MGPerformance(a){var b=this;var c=performance.timing;b.interval=600;if(a!=null){b.interval=a}b.callbacks=[];b.listen=function(d){if(c.loadEventEnd>0){b.callback(d)}else{b.callbacks.push(d)}};b.setInterval=function(d){b.interval(d)};b.callback=function(g){var h=c.domainLookupEnd-c.domainLookupStart;var d=c.connectEnd-c.connectStart;var e=c.responseStart-c.navigationStart;var f=c.redirectEnd-c.redirectStart;var i=c.domComplete-c.navigationStart;var l=c.domInteractive-c.navigationStart;var k=c.domContentLoadedEventEnd-c.navigationStart;var j=c.loadEventEnd-c.navigationStart;g(h,d,e,f,l,i,k,j)};b.test=function(){if(c.loadEventEnd>0){for(var d in b.callbacks){if(b.callbacks.hasOwnProperty(d)){b.callback(b.callbacks[d])}}}else{b.interval-=200;if(b.interval<100){b.interval=100}setTimeout(function(){b.test()},b.interval)}};setTimeout(function(){b.test()},b.interval)}function MGPerformanceTiming(a,c){var b=this;b.settings=c;b.ajax=function(f){try{var d=new XMLHttpRequest();d.open("GET"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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):	8555
Entropy (8bit):	7.917264844485398
Encrypted:	false
SSDEEP:	192:lIUFk4FejvXBm9/FRO60yY+p+w6OIUfu89d4ifY/wMh:FkMejJmngJyYVOI8z9A4c
MD5:	5E1327B127850C364235CE47908828A9
SHA1:	9326ED46ADAF088B16CF6C63FAC70E6FB9E5488A
SHA-256:	E58C9B11E4D5883C454CEA97F86A5348435A6FD9CB7617596792C71FCE7FD6F0
SHA-512:	D09AFA7E713465F487753738CE77CF7A978D09B64E4A41FFF4DE13054B00941A280CBC90624E09B873F9A16673DF2BCD15597CAEC7427BFABF9ACA51988BCBC7
Malicious:	false
IE Cache URL:	http://https://di.rdtcdn.com/m=eW0Q8f/media/videos/201908/11/20264951/original/12.jpg
Preview:	......JFIF.....C.....!......"$".$.....C.....0.."..... ` .3c.D.&...\..w+.F.rp....S.,.5....f.v.....Yj.....'g....4tk.._L..:.LH..7V.Z...c"V.t(..dh...:^r.4.63.m.Z.a...[.N..X.AC..]....{../....b.H*.M...R....;.,.9T.1T<w...;.-\.3^.w&_.....G.Q..l...O..../..$l*.Le.&.d.b.3;k..Yt..NF.....<....9..n...[....4;~;..y....<v".IP.Hq.HQ..H..e..@....b.O.....6.V.q...zG.....T....N=.59.}1.....vz)...#.1$...&*,.....Q$d.).n.....!7.K...;..f..4..?G.....FX....x..S. (O....A.A.....E.u.u.u.c..[C....3..L.;....T..n.....t....2:....>K6..#.....0"c.....D.....kF.P..KW*C..1.<y.(...U...KV.2._.y..4u..)`.....9...3~.gm.av....h...%U.(...o.X.jlY.QY...?O'b....~}....n ..;...[..Y..:.N.;6.l...G...Bgjgu..kVU..$.$.t..1.r._u.t4....t\..t.X.^.....>...ZS.....hweN. ..$.*I!..I

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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):	12721
Entropy (8bit):	7.953901551011159
Encrypted:	false
SSDEEP:	192:Z1H+6Z1FCq6mUSeOWdGIYNDeujS/3HBa7f7rJvSkTuTVbO9MyYtjfiipjoD/sPyx:Z1F/VBUFNYV/G/3HBaTECkxwM51orMyx
MD5:	A72DF8DEC91488A3D7F3D0ECE010DAC5
SHA1:	0A35534888B5251E85C74DD143C317459E553530
SHA-256:	292709633755DB5919EBEB109E66A6D94C101C87948E8B9057347F4B2B719D73
SHA-512:	B0B43EAE912B90D1E79D0AF533A545E287304BFF000C723ED5DC98CC9CA928AD77EC1CCCC621B700D6454D00987E9B0AC37D9AED1F125B659DF84ABE9100DA2
Malicious:	false
IE Cache URL:	http://https://di.rdtcdn.com/m=eW0Q8f/media/videos/202008/27/35456791/original/14.jpg
Preview:	......JFIF.....C.....!......"$".$.....C.....0.."..... f..fn.l...;f .2.`..I.G0,.w.....8..d/3b..OE..e.'.....!8...!.K.....z&kc.n..C..c.....K...v.....P.F.9,.....8.._7Tv.fEW.....f8.....j.y?.....(.;!.X.Q..3.o..!.....W...?.[..&=CI.....`...Z._YU.=..J.....K..[.Q..s.? E ...R.z.....J.z._G1G.....rts`....8z&l..)A.:../H...)2.1k6..5F...V....#.S>+`.....2...;..U.....K.....iP}.2...uc...0.....W.}.=....F.f9....{ry.%....$..K.K.....4...b..j. ..)..+.C^^..|E.X.....y..& ;si.....y{...v..8IF..%y.C|O..2.....l!R}NU...P |..z..4*L0.X<.C.r.a...a.;...9...Ns..d../.Y..%..=.6.s.....38...~\b^.....k..Q2C6..v<x.d...n`..|..VC....`N...&..~7..U.i!T@9V./...I!D1F.\T./'j.V]I. ....q.z..XY.q..#.../]..<RA..zqwF...v.i....t..*.*%q.W..U_..O..-.g]..:....i.S6Z..a.G...o[c.34*..N..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\16[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):	8538
Entropy (8bit):	7.9085043771264685
Encrypted:	false
SSDEEP:	192:et93ze7zMowZFLX9BvHG8Aiz+WXiMaxzOvV7y7PtkvhPw6NmJ+1O:mS7zMRXtxHqizJaxzelZP/N6+1O
MD5:	62D635F526D654B2D17DA322B0B8F512
SHA1:	176339C49D4BD94B301A96D714A79C16CB54EF1F
SHA-256:	A8D4044CA336A0868AE2C13BEAD7137EBED549B791A9B98087E43A5475C22EA9
SHA-512:	68EF9E9C1BCAE8F7D33410B52EB25A06D8270FE14621F0460D822047B1DBE3DAF058DB0058AC44FBCBBE8A34695F495126A16F7EA0CEB84E3F353675EFB48EF6
Malicious:	false
IE Cache URL:	http://https://di.rdtcdn.com/m=eW0Q8f/media/videos/202007/30/34644641/original/16.jpg

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\16[1].jpg	
Preview:	......JFIF.....C.....!......"$".$.....C.....0.."..... .....A. hJr.DN.M:.[t....(..(...t...l.mVW..li.h....J.n~.N...c.h...Q04n9.M|o:.7t.t.#. .....D.t..P.lr.....r.....g.=s.....<.....E...k.d...8;&.J.....6%..\..t.n.VP..g.6....C.s.PN.....L.`.J....5..Y.v..Uj. .V.g8,..n..3.gH.....*...1t6.5.....L.1uC#Lw..c..9I.h0.A(JY.o8..#.}..l.....).....Cy.!..i.fgE....5.3.@.# .&.\<B{r...hhq]...O.....O7.....3E..XtR.K^5:.:.Fjm..9YF.i..Vo/pA...s..4.....J....r. ..lU8.UEa..C...._WE...]7<...=v.)^Dm.N....v[UrT]ox>.5.^.^!|..#...h..V^.5F....`..z.Q.U..B...R".^.....u.;t}.o|&.5t.pDB...];.S..n>...z.:...&..I.-.....6..(&c9.5&.x.K,..j.0q..bj.....J..8..P....LI ..I..a.7.O5c.....vYX..{].3....;T-.g.5:.....0G'iz[r.at....f..;I.j.y.br..TP.....y.tVz33....).9.ai.~.:+.:..../...Y.N.....e....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\4[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):	12752
Entropy (8bit):	7.947951185730925
Encrypted:	false
SSDEEP:	384:3QAnpZNAcJmyf5ESF3u9NlEbABboAU4S2w11xdOLxS:37AByKDlEbqboNFPDuS
MD5:	3201F10D82B845D14A238C620CE13231
SHA1:	1B2FB822BFC17FD674E58AF4A333EA163EE4629B
SHA-256:	EFAFC17F44FB87A6CC7386F0ED9C66B8C29F78F26720A30C10861E78C424AF75
SHA-512:	59EC75EF45434D785FDA8890A9E085EFDACA2867ED9996F5025F8D30F6A7DF1D69AE3E4B6933204FEC6219C96542135C14CAE1A7704F40E50F9D2092D3FD477
Malicious:	false
IE Cache URL:	http://https://di.rdtcdn.com/m=eW0Q8f/media/videos/202008/14/35096611/original/4.jpg
Preview:	......JFIF.....C.....!....."$".$.....C.....0.."..... .....8.....y.]} ,...c..m..G@....t..X=....b.....4.a{...(.....I=IX..%":zr....a.fm.e..3G.h.....&K...c...=....UK.U.t..A.U..&.;..h..Vd...+....74.|..b=t....CM..j.|(.4.....g.q.x.u....2....=_J..)..UV.V.....F.I.N..j...[ey5{ ...../tY...A..-.Ej.LN~.3....j..&q.M}.{.....;C.ul.Q....1...k.WJ.X..w.^e.E... ..M1.1y.j.UX...C.Ui}+.t..ohb.Z..t"$.Z.....c.9.<G...C>.C.>.v..t.E&...w^]]?.M.=..D..D...%*.a.J...H.V..o...7..nd. L...E.&.b....,.\..J..:.w...M-.d..U~...v..L....K...M5.z.^c.P.Ky....N..\.,.~.+.^.].Y.<.YX.4...uE.....X.....}4.>.2.w..QygY.9t],uv.....R.....w..o.....I_..a.....s.m8.h.E[.T....g}.....i.X.....Sk..I....[..`..T*..`.e.....W5N..!.....].5...S.J8.&...UD.:U.6J..v.Y..1y.#e.....Yc.H..:....l..C...+p..T6Q.....E;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\analytics[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	47051
Entropy (8bit):	5.516264124030958
Encrypted:	false
SSDEEP:	768:ryOveCSBZfsnt5XqY/yPndFTkoWY3SoavqVy2rlebYUDTJC6g0stZm:ryJNDfs5hYdFTwY3SorSg0su
MD5:	53EE95B384D866E8692BB1AEF923B763
SHA1:	A82812B87B667D32A8E51514C578A5175EDD94B4
SHA-256:	E441C3E2771625BA05630AB464275136A82C99650EE2145CA5AA9853BEDEB01B
SHA-512:	C1F98A09A102BB1E87BFDF825A725B0E2CC1DBEDB613D1BD9E8FD9D8FD8B145104D5F4CACA44D96DB14AC20F2F51B4C653278BFC87556E7F00E48A5FA6231 AD
Malicious:	false
IE Cache URL:	http://https://www.google-analytics.com/analytics.js
Preview:	(function(){/*.. Copyright The Closure Library Authors.. SPDX-License-Identifier: Apache-2.0.*/.var l=this||self,m=function(a,b){a=a.split(".");var c=l;a[0]in c||"undefin ed"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c=c[d]&&c[d]!==Object.prototype[d]?c[d]:c[d]={}:c[d]=b};var q= function(a,b){for(var c in b)b.hasOwnProperty(c)&&(a[c]=b[c])},r=function(a){for(var b in a)if(a.hasOwnProperty(b))return!0;return!1};var t=/^(?:(?:https?|mailto|ftp):|[^:/?#]*(?: [/?#]|$))/i;var u=window,v=document,w=function(a,b){v.addEventListener?v.addEventListener(a,b,!1):v.attachEvent&&v.attachEvent("on"+a,b)};var x={},y=function(){x .TAGGING=x.TAGGING\|\|[];x.TAGGING[1]=!0};var z=/:[0-9]+$/,A=function(a,b,c){a=a.split("&");for(var d=0;d<a.length;d++){var e=a[d].split("=");if(decodeURIComponen t(e[0]).replace(/\+/g," ")===b)return b=e.slice(1).join("="),c?b:decodeURIComponent(b).replace(/\+/g," ")}},D=function(a,b){b&&(b=String(b).toLowerCase());if("p

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\default-redtube_logged_out[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	6043
Entropy (8bit):	5.105879346031891
Encrypted:	false
SSDEEP:	96:KM8zXfG6V2o+zScJzVTb20ogw+8zNzuIKD679d8b7fTpERQqA3W3DC:DZ6VNg7TKEo0679cbT2RQqA3W3DC
MD5:	6E0958AE85C65140246914D2EE46D5A9
SHA1:	2B7A8027F00F1F0F3F6F153EBC50838CB8E0C696
SHA-256:	6E4E6D59FEAEB182DBC41AC2A59E8EECBCCD2D0A53EA40D87127963C27BDF363
SHA-512:	D813FD5E049CD8A0181B8D472CB8F00ACAFB8F4FB435EB83697AE20B4D6319F0F8CE327162DB3C7D141611CBCC5430A23D0348DA488CE21D654672080EE5AB 1
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/js/generated/pc/default-redtube_logged_out.js?v=4a9dc4c355497ed4f02c60b9b605e041c5eb70e0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\default-redtube_logged_out[1].js	
Preview:	var LoginForm=function(){"use strict";var _=this;_.defaultSettings={mainLoginDiv_id:"login_form",disableLoginDiv_class:"disable_login_container",usernameInput_id:"login_username",passwordInput_id:"login_password",activeSubMenu_class:"sub_menu_active",login_submit:"js-loginSubmitModal",login_modal:"login_modal"},_.init=function(e){_.params=$.extend(!0,_.defaultSettings,e),_.add_listeners(),_.recaptchaEnable=_.isRecaptchaEnable()},_.add_listeners=function(){$(".login_form_X").click(function(){_.params.disableLogin?$("."+_.params.disableLoginDiv_class).slideUp():$("#"+_.params.mainLoginDiv_id).slideUp(),_.resetErrorMessages(),$('input[name="username"]').val(""),$('input[name="password"]').val("")}),$("#js_loginform").on("submit",function(e){e.preventDefault(),e.stopImmediatePropagation(),_.submitLogin()}),$(".login_rt_premium_btn").click(function(){_.openOauthDialog("/rtplogin")}),$(".js_pornhub_login").click(function(){_.openOauthDialog("/phlogin")}),$("#signup_link_in_modal").on("click"

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=0
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~.....b.....$..s...7tRNS.a.o(,.s....e.....q*.....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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:	24D8415BA26BACC508A38F9969F723E91E3B0B5DDB02CEC30EC0D86B9E47D597DF22CCDD674CC7A6F8D5436E2FDF2BD24F1821B4410865F5BC54478BEC175AA
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/icons/favicon.png?v=4a9dc4c355497ed4f02c60b9b605e041c5eb70e0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\favicon[1].png	
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|.. ..!i.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\WJ8I2OL4\mg_utils-2.0.0[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):	14153
Entropy (8bit):	5.277686454888841
Encrypted:	false
SSDEEP:	384:WobYwSvYTwhJrO8+UyQWjrTgkwZpL/COip6as6n:/sJEQWPTe9hip6m
MD5:	1D7150ABF71EE8C49527D683B5D88438
SHA1:	1F995AFA08E57AB95092372098819BD05D6F9EB4
SHA-256:	DF6A5AEA449B57843ABEC0F2D1CECBCEC6F5C98966C57BE76F636E4A747087D3
SHA-512:	576D0C060693866FDF77BD8BED7D5260FAF41A4B087770DFB28B9E5C853D8D6670C74B7B320E382059840917EEDE7BF7D0951F0EA587BF7F4AD1E5A681330C3
Malicious:	false
IE Cache URL:	http://https://cdn1d-static-shared.phncdn.com/mg_utils-2.0.0.js
Preview:	var MG_Utils={browser:{hasTouchSupport:("createTouch" in document),version:(navigator.userAgent.toLowerCase().match(/.+(?:rv|it|ra|ie)[\/:]([\d.]+)/)||[])[1],androidversion:function(){var a=navigator.userAgent.match(/\s*Android\s*([0-9]+)\.?([0-9]+)?\.?([0-9]+)?\s*/);return(a&&a[1]&&a[2])?parseFloat(a[1]+"."+a[2]):(a&&a[1])?parseFloat(a[1]):false)},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(){return(navigator.userAgent.toLowerCase().match(/Windows CE|IEMobile|Windows Phone OS/i)||"XDomainRequest" in window)?true:false},highPixelDensityDisplay:(window.devicePixelRatio>=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\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):	48060
Entropy (8bit):	6.2648630160418834
Encrypted:	false
SSDEEP:	768:ZRwhMsV40y4lnnpBc5Kf+i3VR1eUK+BmCVPOiDD8slFbGT5DCRz0MykLEfVY34tR:ZKhMTynpoy+Y31ecBtVPOMDXlFwyyE4N
MD5:	93220023AE9520229A04CA5964FDCCC3
SHA1:	F22969F25CF88A3B9BB0D11ED995884D080C8A27
SHA-256:	190E2653D9DC2D656C300C53CF8D74259433E822137BC00D4E82B4C6BA75BBBB
SHA-512:	DB10F02973C99B06C66F9C7BB3E067347D9F9AFAC24D4EF58327C23F98EADCB74F71FFB0E5C3EF59355A585CB86F7B0155219379B658BD9CD1D6F06111BBFDB5
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/fonts/rt_font.eot?v=4a9dc4c355497ed4f02c60b9b605e041c5eb70e0
Preview:	.....LP.....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..NV.....6hhea.C.....0...$hmtx...$...T....loca.9Gl...P....maxp.....P... name.`.....p....post..... .....,..latn.....liga..... .....:.....~.....}.....}.....}...~.....3.....@...;....@...@..... ....-.2.a.p.r.u.w...P.l.|.....d.;.... .... .-.2.a.o.r.u.w...P.l.|.....:..... .....C.....79.....79.....79.....79.....79..... .....79.....79.....79.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\video-index[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):	151079
Entropy (8bit):	5.220594916970685
Encrypted:	false
SSDEEP:	1536:IsUFXF+e1Yu3iYya9f92y82tccdIl9TTzjhKcxaP2On3fAWpMFGLQCMj+Z/:KXFlYzU9f9VdgRPjhKcxV4fA0oE
MD5:	67B759D14D2DD2FF01FE3A42B8E9B641
SHA1:	0055043865318F2CACA1A6C80B6F7BF8CF540FC2
SHA-256:	160D15C7488310249677AAC7B58B7E147434D51500134391E27B0FDFB3295C01
SHA-512:	0DA92CFD33A4B744C28F43DCBDFE2AC3B06C20E293DBFD6C5D43D21F54A5584BEF152A430124894B96E62C66F1E745C21F4F52EA1857B4A2658322480BB88BDC
Malicious:	false
IE Cache URL:	http://https://ei.rdtcdn.com/www-static/cdn_files/redtube/js/generated/pc/video-index.js?v=4a9dc4c355497ed4f02c60b9b605e041c5eb70e0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\video-index[1].js	
Preview:	!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?module.exports=e():"function"==typeof define&&define.amd?define(e):(t=t||self).Vue=e()}(this ,function(){"use strict";var g=Object.freeze({});function j(t){return null==t}function L(t){return null!=t}function S(t){return!0===t}function O(t){return"string"==typeof t||"numbe r"==typeof t||"symbol"==typeof t||"boolean"==typeof t}function R(t){return null!==t&&"object"==typeof t}var i=Object.prototype.toString;function l(t){return"[object Objec t]"===i.call(t)}function r(t){var e=parseFloat(String(t));return 0<=e&&Math.floor(e)===e&&isFinite(t)}function y(t){return L(t)&&"function"==typeof t.then&&"function"==typeof t.catch}function e(t){return null==t?"":Array.isArray(t)||l(t)&&t.toString===i?JSON.stringify(t,null,2):String(t)}function N(t){var e=parseFloat(t);return isNaN(e)?t:e}function a(t,e){for(var n=Object.create(null),i=t.split(","),r=0;r<i.length;r++)n[i[r]]=!0;return e?function(t){return n[t.toLowerCase()]}:function

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.21211232961955
Encrypted:	false
SSDEEP:	3:oVXVPgWdojdAW8JOGXnFPgWdojXn:o9WWdojd9qGWdojX
MD5:	D23E513E7BE4216D61140EF21DE93D7C
SHA1:	49D8A13AB5A712DC303ABED37E46CCD1CACD5847
SHA-256:	5EDD9BCC35154424E5055AC6B13949388CAB1DB08C3291FAA0D13718922B0ED8
SHA-512:	8B3A80316F54829D7E2639700D3B503F659E84DC094C6C6249A9002B85B6F2184F06F8F55E821A15D7B5DCAC11F86F9A6868926E723C2F64D06253145A941DE0
Malicious:	false
Preview:	[2020/12/24 02:38:32.202] Latest deploy version: ..[2020/12/24 02:38:32.202] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF07CE18EF49690518.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39505
Entropy (8bit):	0.5454312960847011
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+c6gBq00iK5Cp0iK5Cl0iK5CK:H5R5x5B
MD5:	B0ECFB7F3DD8105EE5615832DA0E929B
SHA1:	2366DD967A62569772BC8AF885EF662B041E7D8C
SHA-256:	27FBEE2CBB7DD0C217D83466AC827077A3A16BE13AECD4011E3864F14E9D4E77
SHA-512:	C2EA1FAAB22BA93D2FD1145F73250107ECF7A3198501D4AB24461D27C25851ADCF2DB48066C691C0B1A20A58A7FBD4748BF898EA08CE1F68FCEF5190F5C9DD 4
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF1780119403EA8AE0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	38853
Entropy (8bit):	0.36585122155011307
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+lLpYUIU4qfawqfaaqfa3:kBqoxKAuvScS+lLpY77W8p
MD5:	1BE6672E8C82AE35E6B4809970C1BB4D
SHA1:	2F7364CCA387CD62685D55886AFB670B29915E67
SHA-256:	4DCC484000CCA9D66FDEB69134873B26112AF73FE7ABB7CB6568802049C43468
SHA-512:	959A88BCA9810DFB5E14EED9B02BDE018D69AA8553DF012E2B144E52A177AEB69C6AEAD8F625F535A034AA32B774E85821B189356CB4EA284E9EB9603E71CD 6C
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF2792CC1130C1EFC3.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12933

C:\Users\user\AppData\Local\Temp\~DF2792CC1130C1EFC3.TMP	
Entropy (8bit):	0.4094286301010582
Encrypted:	false
SSDEEP:	12:c9lCg5/9lCgeK9l26an9l26an9l8fRsrF9l8fRsR9lTqsBj+/4j+3Ye:c9lLh9lLh9lIn9lIn9loAF9loo9lWZnN
MD5:	9ADFC0503FEA48F905049FA7EB69BF7D
SHA1:	8C4E792C7B16F34D82A10605B10B4747093B7416
SHA-256:	D3F2650D6AE0EE73B2119F50CB86E04FDA12DBDD135644604CBA144D15CE4CD3
SHA-512:	E0C95A3B9CAE535AFF212DCE8CB27002591876AD01928BD9B89797B5F5132ACA16C8278410BFA0D74EC51D9AA9CCB42BFED187A6B5130D1DFA52D171F6AEA0D
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFC430449BEEBB0167.TMP	
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

General

SSDEEP:	6144:9F0HdV67elw1KYkOrrzKtg3YmNyKfJ8631L:T0HdPt67bImQCO6F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....>..._..._..._....!..._....7..._....0..._....._..._..._....>..._.... ..._....%..._..Rich._.....PE..L...A..^.....

File Icon



Icon Hash:	b2a678e8ccc8ccd4

Static PE Info

General

Entrypoint:	0x5163ab0
Entrypoint Section:	UPX1
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, BYTES_REVERSED_HI, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x5E7FD341 [Sat Mar 28 22:44:17 2020 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:	6ed4f5f04d62b18d96b26d6db7c18840

Entrypoint Preview

Instruction
pushad
mov esi, 05127000h
lea edi, dword ptr [esi-04D26000h]
push edi
jmp 00007F7F4CD3FFADh
nop
mov al, byte ptr [esi]
inc esi
mov byte ptr [edi], al
inc edi
add ebx, ebx
jne 00007F7F4CD3FFA9h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jc 00007F7F4CD3FF8Fh
mov eax, 00000001h
add ebx, ebx
jne 00007F7F4CD3FFA9h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc eax, eax
add ebx, ebx
jnc 00007F7F4CD3FFADh
jne 00007F7F4CD3FFCAh
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh

Copyright null 2020

Instruction
adc ebx, ebx
jc 00007F7F4CD3FFC1h
dec eax
add ebx, ebx
jne 00007F7F4CD3FFA9h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc eax, eax
jmp 00007F7F4CD3FF76h
add ebx, ebx
jne 00007F7F4CD3FFA9h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc ecx, ecx
jmp 00007F7F4CD3FFF4h
xor ecx, ecx
sub eax, 03h
jc 00007F7F4CD3FFB3h
shl eax, 08h
mov al, byte ptr [esi]
inc esi
xor eax, FFFFFFFFh
je 00007F7F4CD40017h
sar eax, 1
mov ebp, eax
jmp 00007F7F4CD3FFADh
add ebx, ebx
jne 00007F7F4CD3FFA9h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jc 00007F7F4CD3FF6Eh
inc ecx
add ebx, ebx
jne 00007F7F4CD3FFA9h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jc 00007F7F4CD3FF60h
add ebx, ebx
jne 00007F7F4CD3FFA9h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc ecx, ecx
add ebx, ebx
jnc 00007F7F4CD3FF91h
jne 00007F7F4CD3FFABh
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jnc 00007F7F4CD3FF86h
add ecx, 02h
cmp ebp, FFFFFB00h
adc ecx, 02h
lea edx, dword ptr [edi+ebp]
cmp ebp, FFFFFFFCh
jbe 00007F7F4CD3FFB0h
mov al, byte ptr [edx]

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4d669e4	0x88	.rsrc
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4d64000	0x29e4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x0	0x0	
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
UPX0	0x1000	0x4d26000	0x0	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
UPX1	0x4d27000	0x3d000	0x3ce00	False	0.813193820585	data	7.44423697365	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x4d64000	0x3000	0x2c00	False	0.678444602273	data	5.86308201623	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
AFX_DIALOG_LAYOUT	0x4d57718	0x2	ISO-8859 text, with no line terminators		
RT_BITMAP	0x4c88820	0xcee48	empty	Slovenian	Slovenia
RT_ICON	0x4d64260	0x25a8	data	Slovenian	Slovenia
RT_STRING	0x4d578e0	0x432	data		
RT_STRING	0x4d57d18	0x2d4	data		
RT_ACCELERATOR	0x4d57668	0xb0	data		
RT_GROUP_ICON	0x4d6680c	0x14	data	Slovenian	Slovenia
RT_VERSION	0x4d66824	0x1c0	data		

Imports

DLL	Import
KERNEL32.DLL	LoadLibraryA, ExitProcess, GetProcAddress, VirtualProtect

Version Infos

Description	Data
InternalSurname	reboud.exe
Product	1.7.6
FileVersions	1.0.5.4
LegalCo	Copyri (C) 2019, patrition
Translation	0x0439 0x00fa

Possible Origin

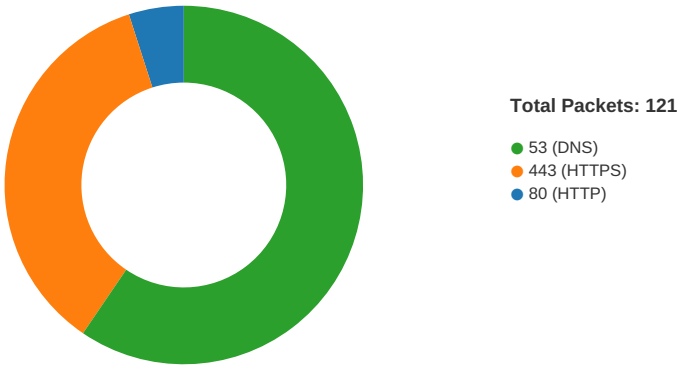
Language of compilation system	Country where language is spoken	Map
Slovenian	Slovenia	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/24/20-02:37:46.026303	UDP	2014376	ET TROJAN Possible Zeus .ru CnC Domain Generation Algorithm (DGA) Lookup Detected	61292	53	192.168.2.3	8.8.8.8
12/24/20-02:37:49.360245	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
12/24/20-02:38:10.571269	UDP	2014376	ET TROJAN Possible Zeus .ru CnC Domain Generation Algorithm (DGA) Lookup Detected	56881	53	192.168.2.3	8.8.8.8
12/24/20-02:38:10.571269	UDP	2014363	ET TROJAN Lookup of Algorithm Generated Zeus CnC Domain (DGA)	56881	53	192.168.2.3	8.8.8.8
12/24/20-02:38:10.659249	UDP	2014376	ET TROJAN Possible Zeus .ru CnC Domain Generation Algorithm (DGA) Lookup Detected	53642	53	192.168.2.3	8.8.8.8
12/24/20-02:38:10.659249	UDP	2014363	ET TROJAN Lookup of Algorithm Generated Zeus CnC Domain (DGA)	53642	53	192.168.2.3	8.8.8.8
12/24/20-02:38:10.729170	UDP	2014376	ET TROJAN Possible Zeus .ru CnC Domain Generation Algorithm (DGA) Lookup Detected	55667	53	192.168.2.3	8.8.8.8
12/24/20-02:38:10.729170	UDP	2014363	ET TROJAN Lookup of Algorithm Generated Zeus CnC Domain (DGA)	55667	53	192.168.2.3	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 24, 2020 02:37:46.118794918 CET	49731	80	192.168.2.3	45.130.151.85
Dec 24, 2020 02:37:46.119348049 CET	49732	80	192.168.2.3	45.130.151.85
Dec 24, 2020 02:37:46.200088024 CET	80	49731	45.130.151.85	192.168.2.3
Dec 24, 2020 02:37:46.200275898 CET	49731	80	192.168.2.3	45.130.151.85
Dec 24, 2020 02:37:46.202168941 CET	80	49732	45.130.151.85	192.168.2.3
Dec 24, 2020 02:37:46.202270031 CET	49731	80	192.168.2.3	45.130.151.85
Dec 24, 2020 02:37:46.202358961 CET	49732	80	192.168.2.3	45.130.151.85
Dec 24, 2020 02:37:46.283205986 CET	80	49731	45.130.151.85	192.168.2.3
Dec 24, 2020 02:37:46.322294950 CET	80	49731	45.130.151.85	192.168.2.3
Dec 24, 2020 02:37:46.322377920 CET	49731	80	192.168.2.3	45.130.151.85
Dec 24, 2020 02:37:46.397644043 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.397891998 CET	49734	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.440257072 CET	443	49733	66.254.114.238	192.168.2.3

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 24, 2020 02:37:46.440362930 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.440555096 CET	443	49734	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.440653086 CET	49734	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.447663069 CET	49734	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.447721004 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.490855932 CET	443	49734	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.490915060 CET	443	49734	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.490932941 CET	49734	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.490961075 CET	443	49734	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.490995884 CET	49734	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.491012096 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.491028070 CET	49734	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.491061926 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.491082907 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.491091967 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.491115093 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.491139889 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.537842035 CET	49734	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.537914991 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.544667959 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.581501961 CET	443	49734	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.581533909 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.581558943 CET	49734	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.581597090 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.624587059 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.771382093 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.771430016 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.771471977 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.771502018 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.771615028 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.771657944 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.771662951 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.771703959 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.771770954 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.771809101 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.771846056 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.771883011 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.771898031 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.771909952 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.771970987 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.772042990 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.777590036 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.777632952 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.777676105 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.777714968 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.814603090 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.814707994 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.814743996 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.814757109 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.814763069 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.814795017 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.814805984 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.814838886 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.814847946 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.814888954 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.814908981 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.814933062 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.814944029 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.814984083 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.814985991 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.815047979 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.815087080 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.815130949 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.815135002 CET	49733	443	192.168.2.3	66.254.114.238

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 24, 2020 02:37:46.815170050 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.815188885 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.815207005 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.815243959 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.815260887 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.815265894 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.815327883 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.815352917 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.815393925 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.815402031 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.815431118 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.815444946 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.815491915 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.815505981 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.815535069 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.815563917 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.815593004 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.815642118 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.815650940 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.815684080 CET	443	49733	66.254.114.238	192.168.2.3
Dec 24, 2020 02:37:46.815696001 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.815721035 CET	49733	443	192.168.2.3	66.254.114.238
Dec 24, 2020 02:37:46.815753937 CET	49733	443	192.168.2.3	66.254.114.238

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 24, 2020 02:36:49.203433990 CET	64185	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:36:49.251615047 CET	53	64185	8.8.8.8	192.168.2.3
Dec 24, 2020 02:36:50.333081961 CET	65110	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:36:50.381189108 CET	53	65110	8.8.8.8	192.168.2.3
Dec 24, 2020 02:36:51.497034073 CET	58361	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:36:51.545039892 CET	53	58361	8.8.8.8	192.168.2.3
Dec 24, 2020 02:36:52.701231956 CET	63492	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:36:52.752042055 CET	53	63492	8.8.8.8	192.168.2.3
Dec 24, 2020 02:36:53.841545105 CET	60831	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:36:53.900887012 CET	53	60831	8.8.8.8	192.168.2.3
Dec 24, 2020 02:36:54.997400045 CET	60100	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:36:55.048275948 CET	53	60100	8.8.8.8	192.168.2.3
Dec 24, 2020 02:36:56.212095976 CET	53195	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:36:56.260240078 CET	53	53195	8.8.8.8	192.168.2.3
Dec 24, 2020 02:36:57.376426935 CET	50141	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:36:57.427171946 CET	53	50141	8.8.8.8	192.168.2.3
Dec 24, 2020 02:36:58.575144053 CET	53023	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:36:58.631314993 CET	53	53023	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:00.038775921 CET	49563	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:00.095182896 CET	53	49563	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:00.458803892 CET	51352	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:00.517673969 CET	53	51352	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:01.274328947 CET	59349	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:01.322405100 CET	53	59349	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:01.561866999 CET	57084	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:01.631120920 CET	53	57084	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:01.642741919 CET	58823	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:01.699209929 CET	53	58823	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:01.707029104 CET	57568	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:01.763371944 CET	53	57568	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:02.473685026 CET	50540	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:02.524420977 CET	53	50540	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:03.587966919 CET	54366	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:03.644565105 CET	53	54366	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:04.713720083 CET	53034	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:04.761665106 CET	53	53034	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:18.859056950 CET	57762	53	192.168.2.3	8.8.8.8

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 24, 2020 02:37:18.919811964 CET	53	57762	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:19.310959101 CET	55435	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:19.358918905 CET	53	55435	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:23.474611044 CET	50713	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:23.533730030 CET	53	50713	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:30.474350929 CET	56132	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:30.533601046 CET	53	56132	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:31.475256920 CET	56132	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:31.540822983 CET	53	56132	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:32.489505053 CET	56132	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:32.550947905 CET	53	56132	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:34.506273985 CET	56132	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:34.566695929 CET	53	56132	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:35.726986885 CET	58987	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:35.793651104 CET	53	58987	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:38.136723995 CET	56579	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:38.195261955 CET	53	56579	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:38.505677938 CET	56132	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:38.564927101 CET	53	56132	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:44.948062897 CET	60633	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:45.007919073 CET	53	60633	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:46.026303053 CET	61292	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:46.095722914 CET	53	61292	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:46.346815109 CET	63619	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:46.394562960 CET	53	63619	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:46.915760994 CET	64938	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:46.917771101 CET	61946	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:46.921535969 CET	64910	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:46.935003996 CET	52123	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:46.963644981 CET	53	64938	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:46.967212915 CET	56130	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:46.969189882 CET	53	64910	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:46.985398054 CET	53	61946	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:47.002279043 CET	53	52123	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:47.017934084 CET	53	56130	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:47.029638052 CET	56338	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:47.057180882 CET	59420	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:47.060168982 CET	58784	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:47.077347040 CET	53	56338	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:47.113642931 CET	53	59420	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:47.119947910 CET	53	58784	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:47.350717068 CET	63978	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:47.398698092 CET	53	63978	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:48.014115095 CET	62938	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:48.081427097 CET	53	62938	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:48.222477913 CET	55708	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:48.270303011 CET	53	55708	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:48.301721096 CET	56803	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:48.305263996 CET	55359	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:48.305280924 CET	58306	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:48.305783987 CET	57145	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:48.328541994 CET	64124	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:48.354007959 CET	53	57145	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:48.397896051 CET	53	64124	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:49.312308073 CET	56803	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:49.312347889 CET	55359	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:49.312473059 CET	58306	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:49.360126019 CET	53	56803	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:49.363025904 CET	53	55359	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:49.368534088 CET	53	58306	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:53.739440918 CET	49361	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:53.787264109 CET	53	49361	8.8.8.8	192.168.2.3
Dec 24, 2020 02:37:56.431735992 CET	63150	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:37:56.489908934 CET	53	63150	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 24, 2020 02:38:09.501672983 CET	53279	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:38:09.562516928 CET	53	53279	8.8.8.8	192.168.2.3
Dec 24, 2020 02:38:10.571269035 CET	56881	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:38:10.644783974 CET	53	56881	8.8.8.8	192.168.2.3
Dec 24, 2020 02:38:10.659249067 CET	53642	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:38:10.715802908 CET	53	53642	8.8.8.8	192.168.2.3
Dec 24, 2020 02:38:10.729170084 CET	55667	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:38:10.790369987 CET	53	55667	8.8.8.8	192.168.2.3
Dec 24, 2020 02:38:28.651516914 CET	54833	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:38:28.699342012 CET	53	54833	8.8.8.8	192.168.2.3
Dec 24, 2020 02:38:30.785828114 CET	62476	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:38:30.842276096 CET	53	62476	8.8.8.8	192.168.2.3
Dec 24, 2020 02:38:32.262295961 CET	49705	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:38:32.320193052 CET	53	49705	8.8.8.8	192.168.2.3
Dec 24, 2020 02:38:33.206744909 CET	61477	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:38:33.382185936 CET	53	61477	8.8.8.8	192.168.2.3
Dec 24, 2020 02:38:35.941158056 CET	61633	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:38:35.997598886 CET	53	61633	8.8.8.8	192.168.2.3
Dec 24, 2020 02:38:57.119313955 CET	55949	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:38:57.267679930 CET	53	55949	8.8.8.8	192.168.2.3
Dec 24, 2020 02:39:33.617337942 CET	57601	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:39:33.676454067 CET	53	57601	8.8.8.8	192.168.2.3
Dec 24, 2020 02:39:34.206001043 CET	49342	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:39:34.256776094 CET	53	49342	8.8.8.8	192.168.2.3
Dec 24, 2020 02:39:34.809109926 CET	56253	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:39:34.868257046 CET	53	56253	8.8.8.8	192.168.2.3
Dec 24, 2020 02:39:35.310066938 CET	49667	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:39:35.366261959 CET	53	49667	8.8.8.8	192.168.2.3
Dec 24, 2020 02:39:35.756771088 CET	55439	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:39:35.813083887 CET	53	55439	8.8.8.8	192.168.2.3
Dec 24, 2020 02:39:36.266427994 CET	57069	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:39:36.325771093 CET	53	57069	8.8.8.8	192.168.2.3
Dec 24, 2020 02:39:36.777247906 CET	57659	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:39:36.825185061 CET	53	57659	8.8.8.8	192.168.2.3
Dec 24, 2020 02:39:37.399914980 CET	54717	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:39:37.456448078 CET	53	54717	8.8.8.8	192.168.2.3
Dec 24, 2020 02:39:38.118830919 CET	63975	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:39:38.175044060 CET	53	63975	8.8.8.8	192.168.2.3
Dec 24, 2020 02:39:38.555934906 CET	56639	53	192.168.2.3	8.8.8.8
Dec 24, 2020 02:39:38.615134954 CET	53	56639	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Dec 24, 2020 02:37:49.360244989 CET	192.168.2.3	8.8.8.8	cffe	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 24, 2020 02:37:46.026303053 CET	192.168.2.3	8.8.8.8	0xff85	Standard query (0)	sibedriama sterkkmode ratordstezya.ru	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:46.346815109 CET	192.168.2.3	8.8.8.8	0xb9b	Standard query (0)	www.redtube.com	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:46.915760994 CET	192.168.2.3	8.8.8.8	0x977d	Standard query (0)	cdn1d-static-shared.phncdn.com	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:46.917771101 CET	192.168.2.3	8.8.8.8	0x75b8	Standard query (0)	ei.rdtcdn.com	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:46.921535969 CET	192.168.2.3	8.8.8.8	0xc430	Standard query (0)	static.trafficjunky.com	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:46.935003996 CET	192.168.2.3	8.8.8.8	0xc973	Standard query (0)	ei.rdtcdn.com	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:46.967212915 CET	192.168.2.3	8.8.8.8	0xc042	Standard query (0)	ht.redtube.com	A (IP address)	IN (0x0001)

Copyright null 2020

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 24, 2020 02:37:47.029638052 CET	192.168.2.3	8.8.8.8	0xa5ec	Standard query (0)	cdn1d-static-shared.phncdn.com	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:47.057180882 CET	192.168.2.3	8.8.8.8	0xe1cc	Standard query (0)	static.trafficjunky.com	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:47.060168982 CET	192.168.2.3	8.8.8.8	0x5a3	Standard query (0)	cdn.speedcurve.com	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:48.014115095 CET	192.168.2.3	8.8.8.8	0x4413	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:48.222477913 CET	192.168.2.3	8.8.8.8	0x347e	Standard query (0)	di.rdtcdn.com	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:48.301721096 CET	192.168.2.3	8.8.8.8	0x4136	Standard query (0)	a.adtng.com	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:48.305280924 CET	192.168.2.3	8.8.8.8	0xdb0	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:48.305783987 CET	192.168.2.3	8.8.8.8	0x16b1	Standard query (0)	ads.trafficjunky.net	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:48.328541994 CET	192.168.2.3	8.8.8.8	0x9165	Standard query (0)	vz-cdn.trafficjunky.net	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:49.312308073 CET	192.168.2.3	8.8.8.8	0x4136	Standard query (0)	a.adtng.com	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:49.312473059 CET	192.168.2.3	8.8.8.8	0xdb0	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)
Dec 24, 2020 02:38:10.571269035 CET	192.168.2.3	8.8.8.8	0x18b9	Standard query (0)	massidfberiatersksilkavayssstezya.ru	A (IP address)	IN (0x0001)
Dec 24, 2020 02:38:10.659249067 CET	192.168.2.3	8.8.8.8	0xb013	Standard query (0)	massidfberiatersksilkavayssstezya.ru	A (IP address)	IN (0x0001)
Dec 24, 2020 02:38:10.729170084 CET	192.168.2.3	8.8.8.8	0x89b	Standard query (0)	massidfberiatersksilkavayssstezya.ru	A (IP address)	IN (0x0001)
Dec 24, 2020 02:38:33.206744909 CET	192.168.2.3	8.8.8.8	0xbc85	Standard query (0)	dolsggiberiaoserkmikluhasya.chimkent.su	A (IP address)	IN (0x0001)
Dec 24, 2020 02:38:35.941158056 CET	192.168.2.3	8.8.8.8	0xe260	Standard query (0)	dolsggiberiaoserkmikluhasya.chimkent.su	A (IP address)	IN (0x0001)
Dec 24, 2020 02:38:57.119313955 CET	192.168.2.3	8.8.8.8	0x116a	Standard query (0)	dolsibegriaosersk4ermanderezya.chimkent.su	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 24, 2020 02:37:46.095722914 CET	8.8.8.8	192.168.2.3	0xff85	No error (0)	sibedriamasterkkmoderatordstezya.ru		45.130.151.85	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:46.394562960 CET	8.8.8.8	192.168.2.3	0xb9b	No error (0)	www.redtube.com	redtube.com		CNAME (Canonical name)	IN (0x0001)
Dec 24, 2020 02:37:46.394562960 CET	8.8.8.8	192.168.2.3	0xb9b	No error (0)	redtube.com		66.254.114.238	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:46.963644981 CET	8.8.8.8	192.168.2.3	0x977d	No error (0)	cdn1d-static-shared.phncdn.com	vip0x08e.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Dec 24, 2020 02:37:46.963644981 CET	8.8.8.8	192.168.2.3	0x977d	No error (0)	vip0x08e.ssl.rncdn5.com		205.185.208.142	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:46.969189882 CET	8.8.8.8	192.168.2.3	0xc430	No error (0)	static.trafficjunky.com	vip0x04f.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Dec 24, 2020 02:37:46.969189882 CET	8.8.8.8	192.168.2.3	0xc430	No error (0)	vip0x04f.ssl.rncdn5.com		205.185.208.79	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:46.985398054 CET	8.8.8.8	192.168.2.3	0x75b8	No error (0)	ei.rdtcdn.com	ei.rdtcdn.com.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)
Dec 24, 2020 02:37:46.985398054 CET	8.8.8.8	192.168.2.3	0x75b8	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		67.22.48.100	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 24, 2020 02:37:46.985398054 CET	8.8.8.8	192.168.2.3	0x75b8	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		67.22.48.102	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:46.985398054 CET	8.8.8.8	192.168.2.3	0x75b8	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		67.22.48.104	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:47.002279043 CET	8.8.8.8	192.168.2.3	0xc973	No error (0)	ei.rdtcdn.com	ei.rdtcdn.com.sds.rncdn7.com		CNAME (Canonical name)	IN (0x0001)
Dec 24, 2020 02:37:47.002279043 CET	8.8.8.8	192.168.2.3	0xc973	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		67.22.48.104	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:47.002279043 CET	8.8.8.8	192.168.2.3	0xc973	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		67.22.48.100	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:47.002279043 CET	8.8.8.8	192.168.2.3	0xc973	No error (0)	ei.rdtcdn.com.sds.rncdn7.com		67.22.48.102	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:47.017934084 CET	8.8.8.8	192.168.2.3	0xc042	No error (0)	ht.redtube.com	hubtraffic.com		CNAME (Canonical name)	IN (0x0001)
Dec 24, 2020 02:37:47.017934084 CET	8.8.8.8	192.168.2.3	0xc042	No error (0)	hubtraffic.com		66.254.114.32	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:47.077347040 CET	8.8.8.8	192.168.2.3	0xa5ec	No error (0)	cdn1d-static-shared.phncdn.com	vip0x08e.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Dec 24, 2020 02:37:47.077347040 CET	8.8.8.8	192.168.2.3	0xa5ec	No error (0)	vip0x08e.ssl.rncdn5.com		205.185.208.142	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:47.113642931 CET	8.8.8.8	192.168.2.3	0xe1cc	No error (0)	static.trafficjunky.com	vip0x04f.ssl.rncdn5.com		CNAME (Canonical name)	IN (0x0001)
Dec 24, 2020 02:37:47.113642931 CET	8.8.8.8	192.168.2.3	0xe1cc	No error (0)	vip0x04f.ssl.rncdn5.com		205.185.208.79	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:47.119947910 CET	8.8.8.8	192.168.2.3	0x5a3	No error (0)	cdn.speedcurve.com	a3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Dec 24, 2020 02:37:48.081427097 CET	8.8.8.8	192.168.2.3	0x4413	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Dec 24, 2020 02:37:48.081427097 CET	8.8.8.8	192.168.2.3	0x4413	No error (0)	stats.l.doubleclick.net		108.177.15.154	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:48.081427097 CET	8.8.8.8	192.168.2.3	0x4413	No error (0)	stats.l.doubleclick.net		108.177.15.156	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:48.081427097 CET	8.8.8.8	192.168.2.3	0x4413	No error (0)	stats.l.doubleclick.net		108.177.15.157	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:48.081427097 CET	8.8.8.8	192.168.2.3	0x4413	No error (0)	stats.l.doubleclick.net		108.177.15.155	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:48.270303011 CET	8.8.8.8	192.168.2.3	0x347e	No error (0)	di.rdtcdn.com	cds.e9q5t8x5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Dec 24, 2020 02:37:48.354007959 CET	8.8.8.8	192.168.2.3	0x16b1	No error (0)	ads.trafficjunky.net		66.254.114.38	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:48.397896051 CET	8.8.8.8	192.168.2.3	0x9165	No error (0)	vz-cdn.trafficjunky.net	cs742.wpc.rncdn4.com		CNAME (Canonical name)	IN (0x0001)
Dec 24, 2020 02:37:48.397896051 CET	8.8.8.8	192.168.2.3	0x9165	No error (0)	cs742.wpc.rncdn4.com		192.229.221.215	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:49.360126019 CET	8.8.8.8	192.168.2.3	0x4136	No error (0)	a.adtng.com		216.18.168.166	A (IP address)	IN (0x0001)
Dec 24, 2020 02:37:49.368534088 CET	8.8.8.8	192.168.2.3	0xdb0	No error (0)	www.google.co.uk		172.217.18.99	A (IP address)	IN (0x0001)
Dec 24, 2020 02:38:10.644783974 CET	8.8.8.8	192.168.2.3	0x18b9	Name error (3)	massidfberiatersksilkavayssstezya.ru	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 24, 2020 02:38:10.715802908 CET	8.8.8.8	192.168.2.3	0xb013	Name error (3)	massidfber iatersksil kavayssste zya.ru	none	none	A (IP address)	IN (0x0001)
Dec 24, 2020 02:38:10.790369987 CET	8.8.8.8	192.168.2.3	0x89b	Server failure (2)	massidfber iatersksil kavayssste zya.ru	none	none	A (IP address)	IN (0x0001)
Dec 24, 2020 02:38:33.382185936 CET	8.8.8.8	192.168.2.3	0xbc85	No error (0)	dolsggiber iaoserkmik luhasya.ch imkent.su		178.210.89.119	A (IP address)	IN (0x0001)
Dec 24, 2020 02:38:35.997598886 CET	8.8.8.8	192.168.2.3	0xe260	No error (0)	dolsggiber iaoserkmik luhasya.ch imkent.su		178.210.89.119	A (IP address)	IN (0x0001)
Dec 24, 2020 02:38:57.267679930 CET	8.8.8.8	192.168.2.3	0x116a	No error (0)	dolsibegri aosersk4er manderezya .chimkent.su		178.210.89.119	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- sibedriamasterkkmoderatordstezya.ru

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49731	45.130.151.85	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Dec 24, 2020 02:37:46.202270031 CET	648	OUT	GET /images/sje5aInP_2FBPBp_2BAl3/cvYbYvSzTnTKrfpE/nbYHZH5fysfLPKE/K09HrIJ7BiKsBPG6Y5/TqSYD5_2F/q_2B0B1iuaVLokvNJd6_/2FZDNlcbb_2F8i1QipQ/i6czioBzvfu_2FP7RTx1L_/2BwKEk5SwMT_2/BPKppBDl/RPtff5N.avi HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: sibedriamasterkkmoderatordstezya.ru Connection: Keep-Alive
Dec 24, 2020 02:37:46.322294950 CET	649	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 24 Dec 2020 01:37:52 GMT Server: Apache/2.4.6 (CentOS) PHP/5.4.16 X-Powered-By: PHP/5.4.16 Set-Cookie: PHPSESSID=1bbskqd36mekt96ku07dqjp7g6; path=/; domain=.sibedriamasterkkmoderatordstezya.ru 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=Sat, 23-Jan-2021 01:37:52 GMT; path=/; domain=.sibedriamasterkkmoderatordstezya.ru 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
Dec 24, 2020 02:37:46.490961075 CET	66.254.114.238	443	192.168.2.3	49734	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
Dec 24, 2020 02:37:46.491082907 CET	66.254.114.238	443	192.168.2.3	49733	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		
Dec 24, 2020 02:37:47.118592978 CET	67.22.48.104	443	192.168.2.3	49735	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		
Dec 24, 2020 02:37:47.120383024 CET	67.22.48.104	443	192.168.2.3	49736	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		
Dec 24, 2020 02:37:47.120577097 CET	67.22.48.104	443	192.168.2.3	49737	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		
Dec 24, 2020 02:37:47.120986938 CET	67.22.48.104	443	192.168.2.3	49738	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		
Dec 24, 2020 02:37:47.129934072 CET	66.254.114.32	443	192.168.2.3	49742	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		
Dec 24, 2020 02:37:47.137748957 CET	66.254.114.32	443	192.168.2.3	49741	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		
Dec 24, 2020 02:37:47.138626099 CET	67.22.48.104	443	192.168.2.3	49740	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		
Dec 24, 2020 02:37:47.147269964 CET	67.22.48.104	443	192.168.2.3	49739	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		
Dec 24, 2020 02:37:47.205574989 CET	205.185.208.142	443	192.168.2.3	49743	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		
Dec 24, 2020 02:37:47.207876921 CET	205.185.208.142	443	192.168.2.3	49744	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		
Dec 24, 2020 02:37:47.209623098 CET	205.185.208.79	443	192.168.2.3	49745	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Dec 24, 2020 02:37:47.211497068 CET	205.185.208.79	443	192.168.2.3	49746	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		
Dec 24, 2020 02:37:48.192884922 CET	108.177.15.154	443	192.168.2.3	49752	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 Nov 10 15:34:37 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Feb 02 15:34:36 CET 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		
Dec 24, 2020 02:37:48.193988085 CET	108.177.15.154	443	192.168.2.3	49751	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 Nov 10 15:34:37 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Feb 02 15:34:36 CET 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		
Dec 24, 2020 02:37:48.456746101 CET	66.254.114.38	443	192.168.2.3	49760	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		
Dec 24, 2020 02:37:48.456861973 CET	66.254.114.38	443	192.168.2.3	49759	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
Dec 24, 2020 02:37:48.499335051 CET	192.229.221.215	443	192.168.2.3	49761	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		
Dec 24, 2020 02:37:48.529695034 CET	192.229.221.215	443	192.168.2.3	49762	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		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: DSC_Canon_23.12.2020.exe PID: 4120 Parent PID: 5768

General

Start time:	02:36:53
Start date:	24/12/2020
Path:	C:\Users\user\Desktop\DSC_Canon_23.12.2020.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DSC_Canon_23.12.2020.exe'
Imagebase:	0x400000
File size:	261632 bytes
MD5 hash:	1900F3BD2B1848B0F4B1A0495F11D84E
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: 00000000.00000003.229172287.0000000006578000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.229113119.0000000006578000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.229242754.0000000006578000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.229145685.0000000006578000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.376997150.00000000063FB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.229065121.0000000006578000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.229223769.0000000006578000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.600985801.00000000061FF000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.430970592.00000000062FD000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.229257710.0000000006578000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.229204464.0000000006578000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5532 Parent PID: 792

General

Start time:	02:36:59
Start date:	24/12/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7956e0000
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: iexplore.exe PID: 1376 Parent PID: 5532

General

Start time:	02:36:59
Start date:	24/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5532 CREDAT:17410 /prefetch:2
Imagebase:	0x11f0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6308 Parent PID: 792

General

Start time:	02:37:42
Start date:	24/12/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7956e0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright null 2020

Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6720 Parent PID: 6308

General

Start time:	02:37:44
Start date:	24/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6308 CREDAT:17410 /prefetch:2
Imagebase:	0x11f0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5436 Parent PID: 792

General

Start time:	02:38:08
Start date:	24/12/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7956e0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 2156 Parent PID: 5436

General

Start time:	02:38:08
Start date:	24/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5436 CREDAT:17410 /prefetch:2
Imagebase:	0x11f0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5008 Parent PID: 792

General

Start time:	02:38:31
Start date:	24/12/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7956e0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5920 Parent PID: 5008

General

Start time:	02:38:31
Start date:	24/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5008 CREDAT:17410 /prefetch:2
Imagebase:	0x11f0000
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

Disassembly

Copyright null 2020

Code Analysis