ID: 553343
Sample Name: 1nJGU59JPU
Cookbook: default.jbs
Time: 17:58:15
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

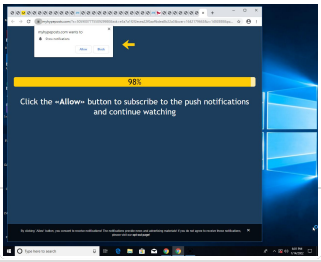
Windows Analysis Report 1nJGU59JPU

Overview

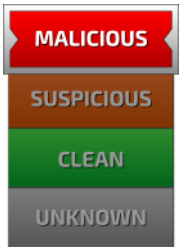
General Information

Sample Name:	1nJGU59JPU (renamed file extension from none to exe)
Analysis ID:	553343
MD5:	aea21ab88cca72..
SHA1:	5241d6fd4013ec8.
SHA256:	498421bc4c78ba..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection

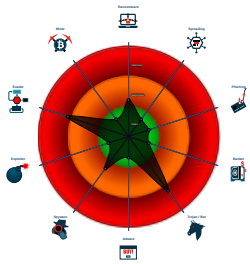


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Snort IDS alert for network traffic (e....
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for subm...
- Antivirus / Scanner detection for sub...
- Multi AV Scanner detection for dropp...
- Performs DNS queries to domains w...
- Connects to many IPs within the sam...
- Drops executable to a common third...
- .NET source code contains method ...
- Obfuscated command line found
- Machine Learning detection for dropp...
- Antivirus or Machine Learning detec

Classification



Process Tree

- **System is w10x64**
- 1nJGU59JPU.exe (PID: 6704 cmdline: "C:\Users\user\Desktop\1nJGU59JPU.exe" MD5: AEA21AB88CCA720A34EC1C9C4794F82A)
  - 1nJGU59JPU.tmp (PID: 6680 cmdline: "C:\Users\user\AppData\Local\Temp\is-5FEVP.tmp\1nJGU59JPU.tmp" /SL5="$22016E,506086,422400,C:\Users\user\Desktop\1nJGU59JPU.exe" MD5: 91D64D52451891441D23398DD3A6E05E)
    - 7((_8888YTR(.exe (PID: 1364 cmdline: "C:\Users\user\AppData\Local\Temp\is-H3FQR.tmp\7((_8888YTR(.exe" /S /UID=rec7 MD5: F97D18BAE067594234DC3EA8E06D10A1)
      - Vahutuqeke.exe (PID: 7024 cmdline: "C:\Users\user\AppData\Local\Temp\32-0401d-119-d44a2-34100e2dbea8e\Vahutuqeke.exe" MD5: 7F9B48E1096C162D3D0615E43D935A04)
        - chrome.exe (PID: 4864 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.profitabletrustednetwork.com/e2q8zu9hu?key=a971bbe4a40a7216a1a87d8f455f71e6 MD5: C139654B5C1438A95B321BB01AD63EF6)
          - chrome.exe (PID: 4168 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1556,9627623661114225042,16842326924946872670,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1908 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
        - chrome.exe (PID: 6784 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.profitabletrustednetwork.com/b1fsmdd9m?key=7e872dab99d78bffc4aa0c1e6b062dad MD5: C139654B5C1438A95B321BB01AD63EF6)
          - chrome.exe (PID: 7648 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1564,16917623383291386263,6472938917553362493,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1856 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
        - chrome.exe (PID: 6868 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1851483 MD5: C139654B5C1438A95B321BB01AD63EF6)
          - chrome.exe (PID: 5544 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1536,6457543823163007411,15253291914772866949,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1728 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
        - chrome.exe (PID: 3572 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1851513 MD5: C139654B5C1438A95B321BB01AD63EF6)
          - chrome.exe (PID: 8560 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1532,10546296038144766013,8885457530477492480,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1852 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
        - chrome.exe (PID: 4068 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://www.directdexchange.com/jump/next.php?r=2087215 MD5: C139654B5C1438A95B321BB01AD63EF6)
          - chrome.exe (PID: 9188 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1536,5678826982049071516,14035945569805029 64,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1860 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
        - chrome.exe (PID: 7020 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.directdexchange.com/jump/next.php?r=4263119 MD5: C139654B5C1438A95B321BB01AD63EF6)
        - chrome.exe (PID: 7200 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?id=1294231 MD5: C139654B5C1438A95B321BB01AD63EF6)
        - chrome.exe (PID: 7376 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1492888&var=3 MD5: C139654B5C1438A95B321BB01AD63EF6)
        - chrome.exe (PID: 7768 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1343177&var=3 MD5: C139654B5C1438A95B321BB01AD63EF6)
        - chrome.exe (PID: 8224 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?id=1339680 MD5: C139654B5C1438A95B321BB01AD63EF6)
        - chrome.exe (PID: 9180 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1620783&var=3 MD5:

C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 4456 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?id=1343178 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 2948 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.cloud-security.xyz/u/script/redirect.php?zoneid=465 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 6944 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.cloud-security.xyz/u/script/redirect.php?zoneid=466 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 8612 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.profitabletrustednetwork.com/e2q8zu9hu?key=a971bbe4a40a7216a1a87d8f455f71e6 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 9420 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.profitabletrustednetwork.com/b1fsmdd9m?key=7e872dab99d78bffc4aa0c1e6b062dad MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 9968 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1851483 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 3244 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1851513 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 4908 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://www.directdexchange.com/jump/next.php?r=2087215 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 5224 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.directdexchange.com/jump/next.php?r=4263119 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 7620 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?id=1294231 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 8032 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1492888&var=3 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 10004 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1343177&var=3 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 7800 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?id=1339680 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 10324 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1620783&var=3 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 10548 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?id=1343178 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 10948 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.cloud-security.xyz/u/script/redirect.php?zoneid=465 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 11136 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.cloud-security.xyz/u/script/redirect.php?zoneid=466 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 6280 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.profitabletrustednetwork.com/e2q8zu9hu?key=a971bbe4a40a7216a1a87d8f455f71e6 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 2524 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.profitabletrustednetwork.com/b1fsmdd9m?key=7e872dab99d78bffc4aa0c1e6b062dad MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 11508 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1851483 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 11948 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1851513 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 10356 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://www.directdexchange.com/jump/next.php?r=2087215 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 6972 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.directdexchange.com/jump/next.php?r=4263119 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 11876 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?id=1294231 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 12528 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1492888&var=3 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 12900 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1343177&var=3 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 13260 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?id=1339680 MD5: C139654B5C1438A95B321BB01AD63EF6)
- chrome.exe (PID: 11436 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1620783&var=3 MD5: C139654B5C1438A95B321BB01AD63EF6)

- Kixysyshysy.exe (PID: 5256 cmdline: "C:\Users\user\AppData\Local\Temp\8e-e5544-da4-a2b8a-aabe03824c51e\Kixysyshysy.exe" MD5: D63BDAFB7AAA3B7C513EB42F1A867157)
  - cmd.exe (PID: 10708 cmdline: "C:\Windows\System32\cmd.exe" /k C:\Users\user\AppData\Local\Temp\uau4vlym.1bx\installer.exe /qn CAMPAIGN="654" & exit MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 8556 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - installer.exe (PID: 11516 cmdline: C:\Users\user\AppData\Local\Temp\uau4vlym.1bx\installer.exe /qn CAMPAIGN="654" MD5: C313DDB7DF24003D25BF62C5A218B215)
- irecord.exe (PID: 4932 cmdline: "C:\Program Files\internet explorer\ROOKKLCFJB\irecord.exe" /VERYSILENT MD5: F3E69396BFCB70EE59A828705593171A)
  - irecord.tmp (PID: 6708 cmdline: "C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp" /SL5="$50038,5808768,66560,C:\Program Files\internet explorer\ROOKKLCFJB\irecord.exe" /VERYSILENT MD5: B5FFB69C517BD2EE5411F7A24845C829)
    - I-Record.exe (PID: 6244 cmdline: "C:\Program Files (x86)\i-record\I-Record.exe" -silent -desktopShortcut -programMenu MD5: 13C3BA689A19B325A19AB62CBE4C313C)

- ZHunuhebaqu.exe (PID: 6892 cmdline: "C:\Program Files (x86)\windows multimedia platform\ZHunuhebaqu.exe" MD5: 9D8A50291AF41031974A371A0F8C5601)
- ZHunuhebaqu.exe (PID: 6916 cmdline: "C:\Program Files (x86)\windows multimedia platform\ZHunuhebaqu.exe" MD5: 9D8A50291AF41031974A371A0F8C5601)
  - Windows Update.exe (PID: 5188 cmdline: "C:\Program Files (x86)\windows multimedia platform\Windows Update.exe" MD5: D7CC834FB3ED6B3F67C017CD8FAA920C)
    - Vahutuqeke.exe (PID: 10800 cmdline: "C:\Users\user\AppData\Local\Temp\32-0401d-119-d44a2-34100e2dbea8e\Vahutuqeke.exe" MD5: 7F9B48E1096C162D3D0615E43D935A04)
    - TOHWVYYPNL.exe (PID: 10088 cmdline: "C:\Users\user\AppData\Local\Temp\c1-1f5b7-b4f-e62a7-a11f96f3c009f\TOHWVYYPNL.exe" MD5: D63BDAFB7AAA3B7C513EB42F1A867157)

- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Networking:

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

Performs DNS queries to domains with low reputation

Connects to many IPs within the same subnet mask (likely port scanning)

Data Obfuscation:

.NET source code contains method to dynamically call methods (often used by packers)

Obfuscated command line found

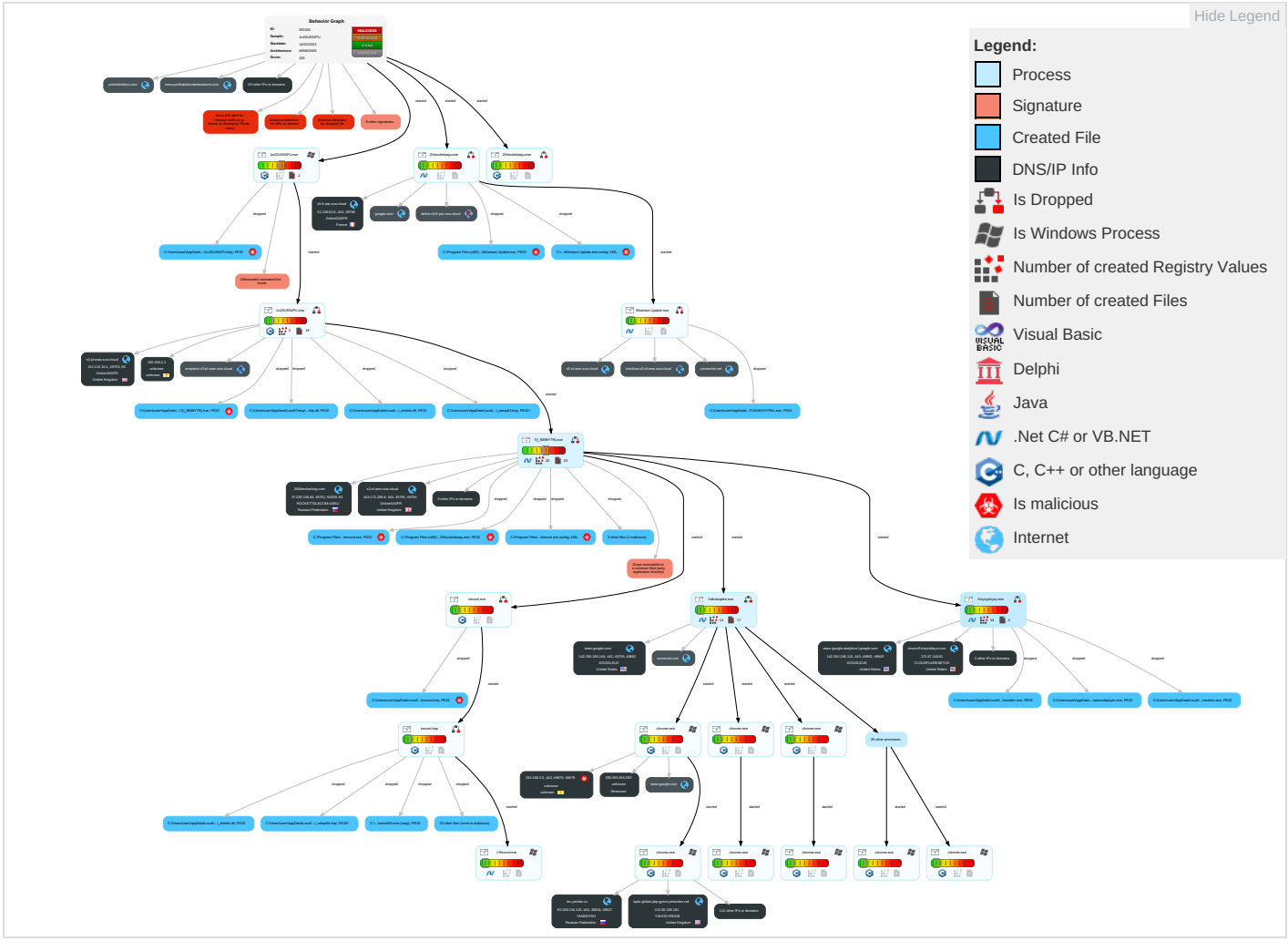
Persistence and Installation Behavior:

Drops executable to a common third party application directory

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Native API 2	Registry Run Keys / Startup Folder 1 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1 1 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encrypt Channe
Domain Accounts	Command and Scripting Interpreter 1 2	Logon Script (Windows)	Access Token Manipulation 1	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-St Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 1 2	Software Packing 1 1	NTDS	System Information Discovery 3 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Applica Layer Protocc
Cloud Accounts	Cron	Network Logon Script	Registry Run Keys / Startup Folder 1 1	Timestomp 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Applica Layer Protocc
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Security Software Discovery 1 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Process Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commc Used P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 1 1 3	Proc Filesystem	Virtualization/Sandbox Evasion 3 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer P
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 3 1	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pr
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Access Token Manipulation 1	Network Sniffing	System Owner/User Discovery 3	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protocc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Process Injection 1 2	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pr

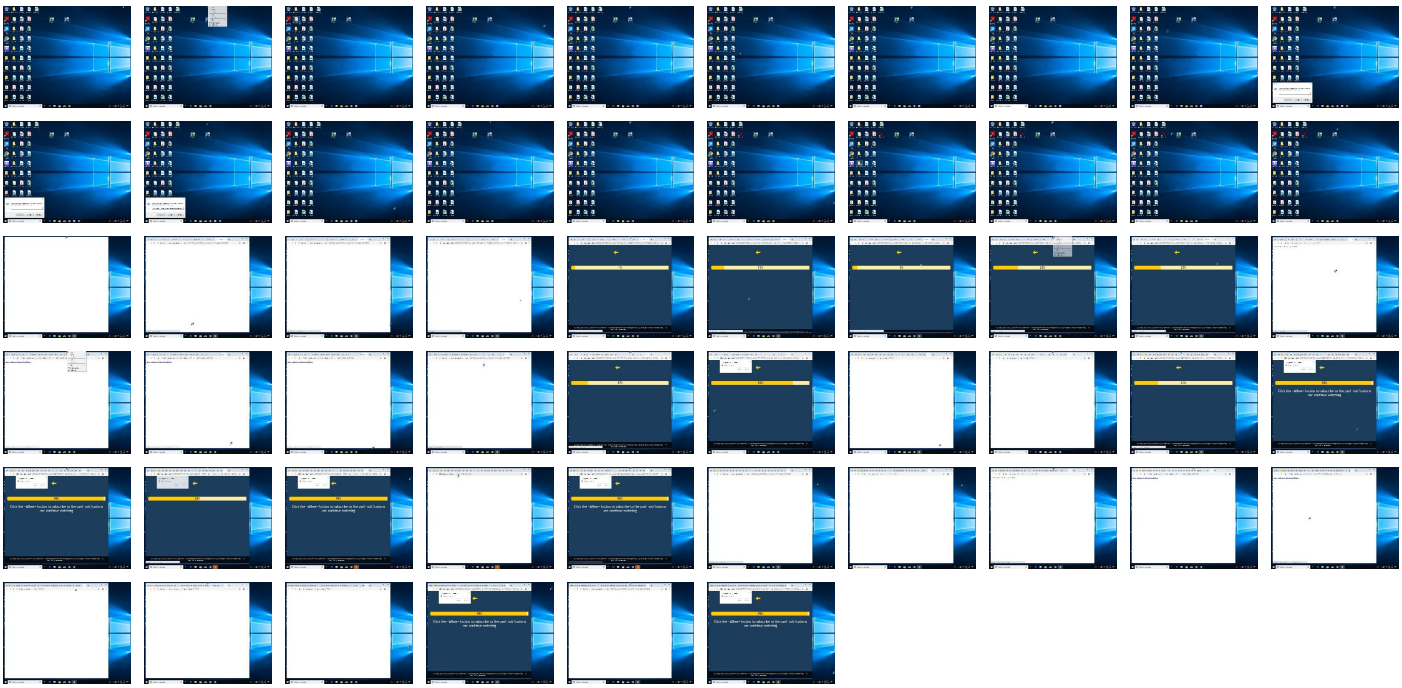
Behavior Graph

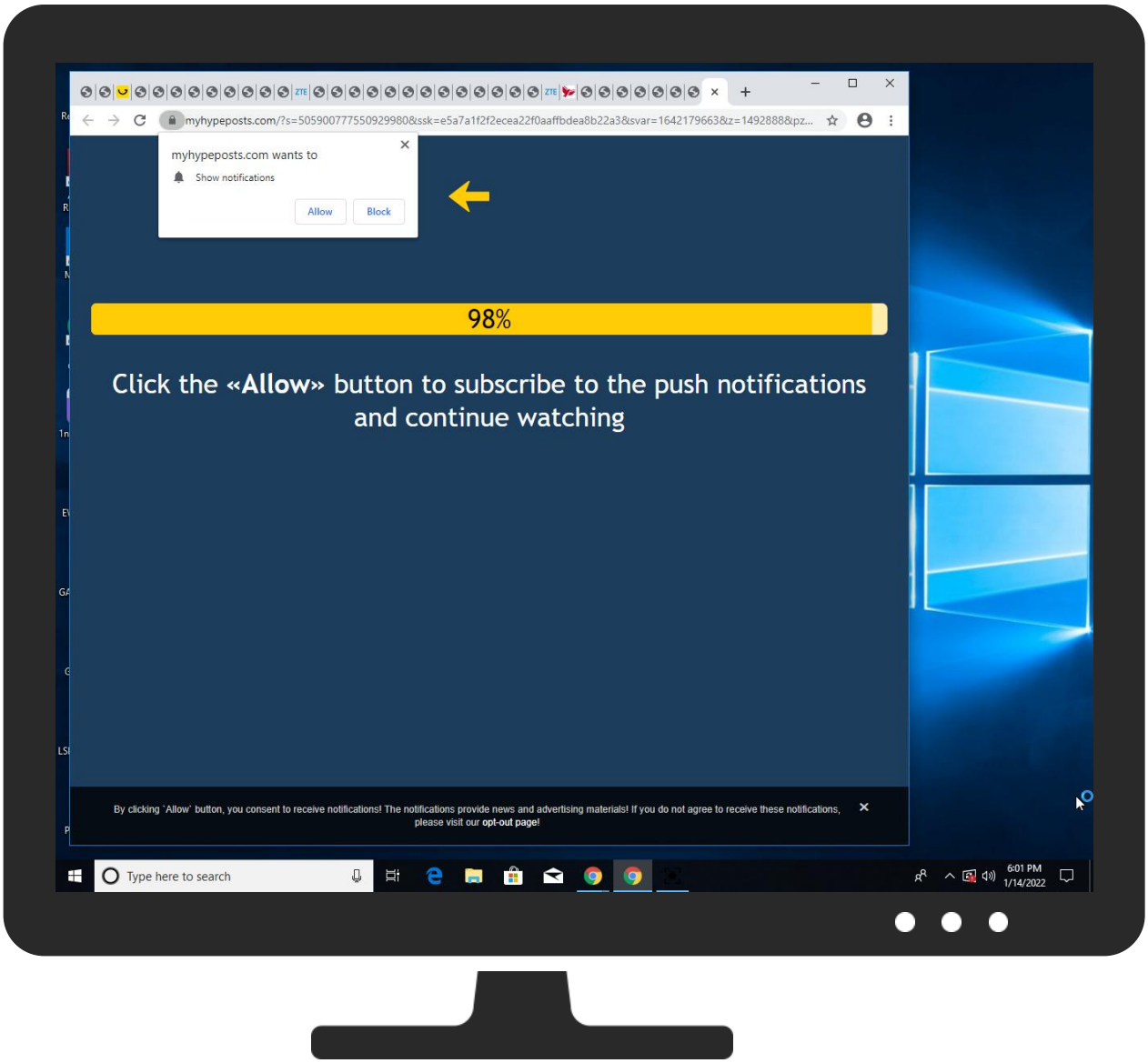


Screenshots

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
1nJGU59JPU.exe	25%	Virustotal		Browse
1nJGU59JPU.exe	31%	Metadefender		Browse
1nJGU59JPU.exe	57%	ReversingLabs	Win32.Downloader.Chebka	
1nJGU59JPU.exe	100%	Avira	HEUR/AGEN.1142105	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\Windows Multimedia Platform\ZHunuhebaqu.exe	100%	Avira	TR/Dldr.Agent.pwjwe	
C:\Program Files (x86)\Windows Multimedia Platform\Windows Update.exe	100%	Avira	HEUR/AGEN.1139393	
C:\Program Files (x86)\Windows Multimedia Platform\ZHunuhebaqu.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Windows Multimedia Platform\Windows Update.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Windows Multimedia Platform\Windows Update.exe	20%	Metadefender		Browse
C:\Program Files (x86)\Windows Multimedia Platform\Windows Update.exe	79%	ReversingLabs	Win32.Adware.CSDIMonetize	
C:\Program Files (x86)\Windows Multimedia Platform\ZHunuhebaqu.exe	34%	Metadefender		Browse
C:\Program Files (x86)\Windows Multimedia Platform\ZHunuhebaqu.exe	78%	ReversingLabs	ByteCode-MSIL.Trojan.Zilla	
C:\Program Files (x86)\i-record\AForge.Video.FFMPEG.dll (copy)	0%	Metadefender		Browse
C:\Program Files (x86)\i-record\AForge.Video.FFMPEG.dll (copy)	0%	ReversingLabs		
C:\Program Files (x86)\i-record\AForge.Video.dll (copy)	3%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\i-record\AForge.Video.dll (copy)	0%	ReversingLabs		
C:\Program Files (x86)\i-record\I-Record.exe (copy)	3%	Metadefender		Browse
C:\Program Files (x86)\i-record\I-Record.exe (copy)	4%	ReversingLabs		
C:\Program Files (x86)\i-record\avcodec-53.dll (copy)	0%	Metadefender		Browse
C:\Program Files (x86)\i-record\avcodec-53.dll (copy)	0%	ReversingLabs		
C:\Program Files (x86)\i-record\avdevice-53.dll (copy)	0%	Metadefender		Browse
C:\Program Files (x86)\i-record\avdevice-53.dll (copy)	2%	ReversingLabs		
C:\Program Files (x86)\i-record\avfilter-2.dll (copy)	0%	Metadefender		Browse
C:\Program Files (x86)\i-record\avfilter-2.dll (copy)	2%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.0.Kixysyshysy.exe.ef0000.4.unpack	100%	Avira	HEUR/AGEN.1126168		Download File
0.1.1nJGU59JPU.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
26.0.Windows Update.exe.f60000.0.unpack	100%	Avira	HEUR/AGEN.1139393		Download File
10.0.Kixysyshysy.exe.ef0000.0.unpack	100%	Avira	HEUR/AGEN.1126168		Download File
26.0.Windows Update.exe.f60000.4.unpack	100%	Avira	HEUR/AGEN.1139393		Download File
1.2.1nJGU59JPU.tmp.400000.0.unpack	100%	Avira	HEUR/AGEN.1108750		Download File
3.0.7((_8888YTR(.exe.600000.0.unpack	100%	Avira	HEUR/AGEN.1126168		Download File
10.0.Kixysyshysy.exe.ef0000.2.unpack	100%	Avira	HEUR/AGEN.1126168		Download File
26.2.Windows Update.exe.f60000.0.unpack	100%	Avira	HEUR/AGEN.1139393		Download File
0.2.1nJGU59JPU.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
3.2.7((_8888YTR(.exe.600000.0.unpack	100%	Avira	HEUR/AGEN.1126168		Download File
0.0.1nJGU59JPU.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
26.0.Windows Update.exe.f60000.2.unpack	100%	Avira	HEUR/AGEN.1139393		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.amazon.com.mx	0%	URL Reputation	safe	
http://vexacion.com/afu.php?zoneid=1851513	1%	Virustotal		Browse
http://vexacion.com/afu.php?zoneid=1851513	100%	Avira URL Cloud	malware	
http://https://www.profitabletrustednetwork.com/b1fsmdd9m?key=7e872dab9	0%	Avira URL Cloud	safe	
http://productsdetails.online/Series/za3ma_za3ma.php	3%	Virustotal		Browse
http://productsdetails.online/Series/za3ma_za3ma.php	0%	Avira URL Cloud	safe	
http://vexacion.com/?z=1492888&syncedCookie=true	100%	Avira URL Cloud	malware	
http://https://www.profitabletrustednetwork.com/b1fsmdd9m?key=7e872dab99d78bffc4aa0c1e6b062dadC:	0%	Avira URL Cloud	safe	
http://onepiece.s3.pl-waw.scw.cloud/pub-carousel/I-Record.exe	0%	Avira URL Cloud	safe	
http://korolova.s3.nl-ams.scw.cloud/adv-control/I-Record.exeL	0%	Avira URL Cloud	safe	
http://onepiece.s3.pl-waw.scw.cloud/pub-carousel/I-Record.exL	0%	Avira URL Cloud	safe	
http://https://www.profitabletrustednetwork.com/b1fsmdd9m?key=7e872dab99d78bffc4aa0c1e6b062dadRr	0%	Avira URL Cloud	safe	
http://www.innosetup.com/	0%	URL Reputation	safe	
http://https://connectini.net/Series/SuperNitouDisc.php	0%	Avira URL Cloud	safe	
http://https://autopush.meet.sandbox.google.comM	0%	Avira URL Cloud	safe	
http://https://www.amazon.co.br	0%	URL Reputation	safe	
http://vexacion.com/afu.php?zoneid=1851483leSystem	100%	Avira URL Cloud	malware	
http://https://autopush.meet.sandbox.google.comb	0%	Avira URL Cloud	safe	
http://vexacion.com/?z=1851513&syncedCookie=false	100%	Avira URL Cloud	malware	
http://vexacion.com/afu.php?zoneid=1851483z	100%	Avira URL Cloud	malware	
http://vexacion.com/afu.php?zoneid=1343177&var=3	100%	Avira URL Cloud	malware	
http://https://www.amazon.co.uk	0%	URL Reputation	safe	
http://korolova.s3.nl-ams.scw.cloud/adv-control/I-Record.	0%	Avira URL Cloud	safe	
http://https://autopush.meet.sandbox.google.comlow-2G	0%	Avira URL Cloud	safe	
http://https://connectini.net	0%	URL Reputation	safe	
http://https://korolova.s3.nl-ams.scw.cloud/electroman/uptoda_5a5uaqs98d3qj2w5.exe	0%	Avira URL Cloud	safe	
http://vexacion.com/?z=1851483&syncedCookie=false	100%	Avira URL Cloud	malware	
http://fpdownload.ma)	0%	Avira URL Cloud	safe	
http://vexacion.com/?z=1294231&syncedCookie=false	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://https://delice.s3.fr-par.scw.cloud	0%	Avira URL Cloud	safe	
http://https://i-record.org	0%	Avira URL Cloud	safe	
http://https://korolova.s3.nl-ams.scw.cloud	0%	Avira URL Cloud	safe	
http://www.remobjects.com/psU	0%	URL Reputation	safe	
http://https://delice.s3.fr-par.scw.cloud/run-data/rec_76nqyh7qvdmyuas4	0%	Avira URL Cloud	safe	
http://vexacion.com/afu.php?zoneid=1851483C:	100%	Avira URL Cloud	malware	
http://vexacion.com/?z=1339680&syncedCookie=false	100%	Avira URL Cloud	malware	
http://korolova.s3.nl-ams.scw.cloud/adv-control/I-Record.exe	0%	Avira URL Cloud	safe	
http://https://korolova.s3.nl-ams.shZ	0%	Avira URL Cloud	safe	
http://mitrichsoftware.wordpress.comB	0%	URL Reputation	safe	
http://https://connectini.net/S2S/Disc/Disc.php?ezok=lylach7&tesla=7	0%	Avira URL Cloud	safe	
http://onepiece.s3.pl-waw.scw.cloud/pub-carousel/I-Record.exeeRR	0%	Avira URL Cloud	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome=	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	142.250.184.227	true	false		high
s3.nl-ams.scw.cloud	163.172.208.8	true	false		high
d1s33wn15r3bpe.cloudfront.net	13.224.96.124	true	false		high
monorail-production-web-apps-a-us-east1-10.shopifycloud.com	34.138.230.116	true	false		high
d6gl2ual1jt2h.cloudfront.net	13.224.96.80	true	false		high
d2h3z7munabi1z.cloudfront.net	13.224.96.122	true	false		high
d28ndrjbfdkv0d.cloudfront.net	13.224.96.45	true	false		high
directdexchange.com	35.201.70.46	true	false		high
di7rtopbiewfz.cloudfront.net	13.224.96.103	true	false		high
ekr.zdassets.com	104.18.70.113	true	false		high
www.google.com	142.250.185.164	true	false		high
littlecdn.com	104.22.25.116	true	false		high
nginx.1cros.net	18.184.39.239	true	false		high
toa.mygametoa.com	34.64.183.91	true	false		high
google.com	142.250.186.110	true	false		high
seo.apps.avada.io	151.101.1.195	true	false		high
cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com	35.169.187.184	true	false		high
cdn.shopify.com	151.101.1.12	true	false		high
assets.prod.abebookscdn.com	13.224.96.28	true	false		high
d1qcny5kzqmo9s.cloudfront.net	13.224.96.6	true	false		high
d2ovawmze1vtgu.cloudfront.net	13.224.96.120	true	false		high
oneimpress.io	136.244.117.138	true	false		high
googleads.g.doubleclick.net	142.250.185.226	true	false		high
chimpstatic.com	23.50.98.104	true	false		high
www.google.co.uk	142.250.186.99	true	false		high
vexacion.com	139.45.197.236	true	false		high
cdn.langshop.app	104.21.51.248	true	false		high
clients.l.google.com	172.217.16.142	true	false		high
stun.l.google.com	142.250.154.127	true	false		high
googlehosted.l.googleusercontent.com	142.250.181.225	true	false		high
s.w.org	192.0.77.48	true	false		high
data.abebooks.com	3.86.136.12	true	false		high
mc.yandex.ru	93.158.134.119	true	false		high
goodnotification.net	172.67.138.139	true	false		high
htagzdownload.pw	35.205.61.67	true	false		high
www.cloud-security.xyz	172.67.215.223	true	false		high
static.shareasale.com	104.16.227.72	true	false		high
www.adsaro.net	104.26.4.235	true	false		high
propeller-tracking.com	139.45.197.240	true	false		high
affiliates-abebooks-com.customtraffic.impactradius.com	35.244.197.23	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
cdntechone.com	172.67.131.171	true	false		high
cdn.admitad-connect.com	104.26.5.175	true	false		high
diromalxx.com	62.122.170.197	true	false		high
myhypeposts.com	139.45.197.139	true	false		high
accounts.google.com	142.250.184.205	true	false		high
atzekromchan.com	139.45.197.238	true	false		high
app.avada.io	151.101.1.195	true	false		high
iplogger.org	148.251.234.83	true	false		high
api.privy.com	104.22.20.108	true	false		high
widgets.automizely.com	104.19.168.102	true	false		high
d21fnsp1pg8r6b.cloudfront.net	13.224.96.58	true	false		high
edge.gycpi.b.yahoodns.net	87.248.118.23	true	false		high
c.xyzgamec.com	172.67.143.225	true	false		high
dxozrhxfn9bwf.cloudfront.net	13.224.96.4	true	false		high
yonhelioliskor.com	139.45.197.251	true	false		high
curtainshare.su	172.67.133.243	true	false		high
messengerview.1talking.net	52.38.191.23	true	false		high
www.profitabletrustednetwork.com	192.243.59.12	true	false		high
d3lp7swsejht2u.cloudfront.net	13.224.96.124	true	false		high
sdks.am-static.com	104.18.28.218	true	false		high
static.zdassets.com	104.18.72.113	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
d2393mmhak2ysp.cloudfront.net	13.224.96.116	true	false		high
datatechone.com	37.48.68.71	true	false		high
b.dxyzgame.com	172.67.164.165	true	false		high
star-mini.c10r.facebook.com	157.240.17.35	true	false		high
www.ojrq.net	34.95.127.121	true	false		high
stats.l.doubleclick.net	108.177.15.154	true	false		high
dyjtibcz3b48v.cloudfront.net	13.224.96.86	true	false		high
static.addtoany.com	172.67.39.148	true	false		high
connectini.net	162.0.210.44	true	false		high
tpx.tesseradigital.com	35.157.179.180	true	false		high
source3.boys4dayz.com	172.67.148.61	true	false		high
dr35amawwlvaz.cloudfront.net	13.224.96.15	true	false		high
shops.myshopify.com	23.227.38.74	true	false		high
d8bc12a0-pushowlbackend-pu-0f8c-1616299444.us-east-1.elb.amazonaws.com	34.196.60.195	true	false		high
d1lytq8w52fohg.cloudfront.net	13.224.96.29	true	false		high
spdc-global.pbp.gysm.yahoodns.net	212.82.100.181	true	false		high
ztedevices.zendesk.com	104.16.51.111	true	false		high
p-chzh00.kxcdn.com	94.126.16.223	true	false		high
s3.pl-waw.scw.cloud	151.115.10.1	true	false		high
shopify.privy.com	104.22.21.108	true	false		high
product-labels-pro.bsscommerce.com	104.26.1.133	true	false		high
d2pbcviywxotf2.cloudfront.net	13.224.96.72	true	false		high
www-google-analytics.l.google.com	142.250.186.110	true	false		high
www-googletagmanager.l.google.com	142.250.186.136	true	false		high
fonts.shopifycdn.com	151.101.1.12	true	false		high
ad.admitad.com	185.26.99.58	true	false		high
gp.gamebuy768.com	172.67.143.210	true	false		high
360devtracking.com	37.230.138.66	true	false		high
my.rtmark.net	139.45.195.8	true	false		high
d155tv9w8vktl.cloudfront.net	13.224.96.88	true	false		high
s3.fr-par.scw.cloud	51.159.62.6	true	false		high
d1h4d6cj0c830c.cloudfront.net	13.224.96.30	true	false		high
dashboard.wheelio-app.com	52.173.139.125	true	false		high
widget-mediator.zopim.com	3.120.252.147	true	false		high
xhr.invl.co	18.136.177.10	true	false		high
monorail-edge.shopifysvc.com	unknown	unknown	false		high
glsdk.logsss.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://vexacion.com/afu.php?zoneid=1851513	true	• 1%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://vexacion.com/?z=1492888&syncedCookie=true	true	• Avira URL Cloud: malware	unknown
http://onepiece.s3.pl-waw.scw.cloud/pub-carousel/I-Record.exe	false	• Avira URL Cloud: safe	unknown
http://vexacion.com/?z=1851513&syncedCookie=false	true	• Avira URL Cloud: malware	unknown
http://vexacion.com/afu.php?zoneid=1343177&var=3	true	• Avira URL Cloud: malware	unknown
http://vexacion.com/?z=1851483&syncedCookie=false	true	• Avira URL Cloud: malware	unknown
http://vexacion.com/?z=1294231&syncedCookie=false	true	• Avira URL Cloud: malware	unknown
http://vexacion.com/?z=1339680&syncedCookie=false	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.177.15.154	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
35.201.70.46	directdexchange.com	United States		15169	GOOGLEUS	false
18.136.177.10	xhr.invl.co	United States		16509	AMAZON-02US	false
142.250.185.226	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
172.67.131.171	cdntechone.com	United States		13335	CLOUDFLARENETUS	false
157.240.17.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false
151.101.1.12	cdn.shopify.com	United States		54113	FASTLYUS	false
51.159.62.6	s3.fr-par.scw.cloud	France		12876	OnlineSASFR	false
13.224.96.30	d1h4d6cj0c830c.cloudfront.net	United States		16509	AMAZON-02US	false
172.67.39.148	static.addtoany.com	United States		13335	CLOUDFLARENETUS	false
93.158.134.119	mc.yandex.ru	Russian Federation		13238	YANDEXRU	false
37.230.138.66	360devtracking.com	Russian Federation		203674	ROCKETTELECOM-ASRU	false
142.250.154.127	stun.l.google.com	United States		15169	GOOGLEUS	false
142.250.186.110	google.com	United States		15169	GOOGLEUS	false
142.250.184.227	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
104.18.72.113	static.zdassets.com	United States		13335	CLOUDFLARENETUS	false
104.26.4.235	www.adsaro.net	United States		13335	CLOUDFLARENETUS	false
13.224.96.72	d2pbcviywxotf2.cloudfront.net	United States		16509	AMAZON-02US	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
13.224.96.103	di7rtopbiewfz.cloudfront.net	United States		16509	AMAZON-02US	false
172.217.16.142	clients.l.google.com	United States		15169	GOOGLEUS	false
172.67.148.61	source3.boys4dayz.com	United States		13335	CLOUDFLARENETUS	false
104.21.51.248	cdn.langshop.app	United States		13335	CLOUDFLARENETUS	false
104.22.21.108	shopify.privy.com	United States		13335	CLOUDFLARENETUS	false
37.48.68.71	datatechone.com	Netherlands		60781	LEASEWEB-NL-AMS-01NetherlandsNL	false
104.26.1.133	product-labels-pro.bsscommerce.com	United States		13335	CLOUDFLARENETUS	false
13.224.96.4	dxozrhxfn9bwf.cloudfront.net	United States		16509	AMAZON-02US	false
139.45.197.139	myhypeposts.com	Netherlands		9002	RETN-ASEU	false
172.67.215.223	www.cloud-security.xyz	United States		13335	CLOUDFLARENETUS	false
13.224.96.86	dyjtibcz3b48v.cloudfront.net	United States		16509	AMAZON-02US	false
104.22.25.116	littlecdn.com	United States		13335	CLOUDFLARENETUS	false
18.184.39.239	nginx.1cros.net	United States		16509	AMAZON-02US	false
104.22.20.108	api.privy.com	United States		13335	CLOUDFLARENETUS	false
163.172.208.8	s3.nl-ams.scw.cloud	United Kingdom		12876	OnlineSASFR	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
104.18.70.113	ekr.zdassets.com	United States		13335	CLOUDFLARENETUS	false
192.243.59.12	www.profitabletrustednetwork.com	Dominica		39572	ADVANCEDHOSTERS-ASNL	false
13.224.96.45	d28ndrjbfdkv0d.cloudfront.net	United States		16509	AMAZON-02US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.196.60.195	d8bc12a0-pushowlbackend-pu-0f8c-1616299444.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
172.67.138.139	goodnotification.net	United States		13335	CLOUDFLARENETUS	false
212.82.100.181	spdc-global.pbp.gysm.yahoodns.net	United Kingdom		34010	YAHOO-IRDGB	false
35.169.187.184	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
162.0.210.44	connectini.net	Canada		35893	ACPCA	false
139.45.195.8	my.rtmark.net	Netherlands		9002	RETN-ASEU	false
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	false
23.50.98.104	chimpstatic.com	United States		16625	AKAMAI-ASUS	false
139.45.197.251	yonhelioliskor.com	Netherlands		9002	RETN-ASEU	false
151.101.1.195	seo.apps.avada.io	United States		54113	FASTLYUS	false
104.16.227.72	static.shareasale.com	United States		13335	CLOUDFLARENETUS	false
52.173.139.125	dashboard.wheelio-app.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
136.244.117.138	oneimpress.io	United States		20473	AS-CHOOPAUS	false
13.224.96.122	d2h3z7munabi1z.cloudfront.net	United States		16509	AMAZON-02US	false
13.224.96.58	d21fnsp1pg8r6b.cloudfront.net	United States		16509	AMAZON-02US	false
142.250.185.164	www.google.com	United States		15169	GOOGLEUS	false
34.138.230.116	monorail-production-web-apps-a-us-east1-10.shopifycloud.com	United States		2686	ATGS-MMD-ASUS	false
148.251.234.83	iplogger.org	Germany		24940	HETZNER-ASDE	false
185.26.99.58	ad.admitad.com	Germany		44066	DE-FIRSTCOLOwwwfirst-colonetDE	false
142.250.184.205	accounts.google.com	United States		15169	GOOGLEUS	false
13.224.96.124	d1s33wn15r3bpe.cloudfront.net	United States		16509	AMAZON-02US	false
142.250.186.136	www-googletagmanager.l.google.com	United States		15169	GOOGLEUS	false
142.250.186.99	www.google.co.uk	United States		15169	GOOGLEUS	false
104.19.168.102	widgets.automizely.com	United States		13335	CLOUDFLARENETUS	false
104.18.28.218	sdks.am-static.com	United States		13335	CLOUDFLARENETUS	false
52.38.191.23	messengerview.1talking.net	United States		16509	AMAZON-02US	false
35.157.179.180	tpx.tesseradigital.com	United States		16509	AMAZON-02US	false
94.126.16.223	p-chzh00.kxcdn.com	Switzerland		21069	ASN-METANETRoutingpeeringissuesnocmetanetchCH	false
104.26.5.175	cdn.admitad-connect.com	United States		13335	CLOUDFLARENETUS	false
13.224.96.29	d1lytq8w52fohg.cloudfront.net	United States		16509	AMAZON-02US	false
139.45.197.240	propeller-tracking.com	Netherlands		9002	RETN-ASEU	false
87.248.118.23	edge.gycpi.b.yahoodns.net	United Kingdom		203220	YAHOO-DEBDE	false
139.45.197.238	atzekromchan.com	Netherlands		9002	RETN-ASEU	false
139.45.197.236	vexacion.com	Netherlands		9002	RETN-ASEU	false
151.115.10.1	s3.pl-waw.scw.cloud	United Kingdom		12876	OnlineSASFR	false
142.250.181.225	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
54.174.190.185	unknown	United States		14618	AMAZON-AESUS	false

Private

IP
192.168.2.1
192.168.2.3

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553343
Start date:	14.01.2022
Start time:	17:58:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1nJGU59JPU (renamed file extension from none 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:	76
Number of new started drivers analysed:	1
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@226/292@152/78
EGA Information:	• Successful, ratio: 22.2%
HDC Information:	• Successful, ratio: 14% (good quality ratio 13.2%) • Quality average: 83.5% • Quality standard deviation: 27.2%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:59:23	Autostart	Run: HKLM64\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce system recover "C:\Program Files (x86)\windows multimedia platform\ZHunuhebaqu.exe"
17:59:27	API Interceptor	1x Sleep call for process: 7((_8888YTR(.exe modified
17:59:38	API Interceptor	40x Sleep call for process: Vahutuqeke.exe modified
17:59:44	API Interceptor	1x Sleep call for process: ZHunuhebaqu.exe modified
18:00:58	API Interceptor	2x Sleep call for process: Windows Update.exe modified
18:01:43	Task Scheduler	Run new task: AdvancedUpdater path: C:\Program Files (x86)\AW Manager\Windows Manager\Windows Updater.exe s>/silentall -nofreqcheck -nogui
18:01:43	Task Scheduler	Run new task: AdvancedWindowsManager #1 path: C:\Program Files (x86)\AW Manager\Windows Manager\AdvancedWindowsManager.exe s>-v 110 -t 8080
18:01:45	Task Scheduler	Run new task: AdvancedWindowsManager #2 path: C:\Program Files (x86)\AW Manager\Windows Manager\AdvancedWindowsManager.exe s>-v 111 -t 8080
18:01:46	Task Scheduler	Run new task: AdvancedWindowsManager #3 path: C:\Program Files (x86)\AW Manager\Windows Manager\AdvancedWindowsManager.exe s>-v 112 -t 8080
18:01:47	Task Scheduler	Run new task: AdvancedWindowsManager #4 path: C:\Program Files (x86)\AW Manager\Windows Manager\AdvancedWindowsManager.exe s>-v 113 -t 8080
18:01:48	Task Scheduler	Run new task: AdvancedWindowsManager #5 path: C:\Program Files (x86)\AW Manager\Windows Manager\AdvancedWindowsManager.exe s>-v 114 -t 8080
18:01:48	Task Scheduler	Run new task: AdvancedWindowsManager #6 path: C:\Program Files (x86)\AW Manager\Windows Manager\AdvancedWindowsManager.exe s>-v 115 -t 8080

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\Windows Multimedia Platform\Windows Update.exe	
Process:	C:\Program Files (x86)\Windows Multimedia Platform\ZHunuhebaqu.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	592384
Entropy (8bit):	6.472227586131542
Encrypted:	false
SSDEEP:	6144:1up1DUXu/7+QxDiM5snMvB0EmKLZPDvOBpqgOMuJOXDGoKNWN:1ud7hf3bvOBpXKOXDgWN
MD5:	D7CC834FB3ED6B3F67C017CD8FAA920C
SHA1:	EDEFE5391017B4860575CAB883CFE837659D80F3
SHA-256:	7AEF85A8D5EDB22FC2DACA9E74B6AC1410F874D5B03CE98BA06207886123DE65
SHA-512:	88349800C06693BD7A9BA22F83A0CE7351B26165CA03BD26F1CF0C86C6243B2CF40951419273269734C172112569DD2454D13D1C671A34BC54E2D321483BDC25
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 20%, Browse • Antivirus: ReversingLabs, Detection: 79%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a..... .....>... ...@....@.. .....`..... ..@.....@>..K...`..t.....@.....=..... ....H.....text..... ... .`.sdata.....@.....$.....@....rsr c...t...`.....(.....@..@.reloc.....@.....@..B.....

C:\Program Files (x86)\Windows Multimedia Platform\Windows Update.exe.config	
Process:	C:\Program Files (x86)\Windows Multimedia Platform\ZHunuhebaqu.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1810
Entropy (8bit):	5.029991107025393
Encrypted:	false
SSDEEP:	24:2dZmhW3aXfygeOygjOgC5XgtXdXkBHnUdQzFDWby2GpyI:cccAfyge7gjOgCNgBRkBHUdQzqQ
MD5:	A2EBF843442988EE2D667E9C7FC28CE1
SHA1:	7F24C475BB217C448090DCE593ABEE8957B7B1D4
SHA-256:	8A0D5D6C5AB131BAB9C8A29A7BCC81D6470EC515F2E4BCA977A4FE62FD156ACC
SHA-512:	1B56DB588131023F427E0476582E3381A818D9659C75B34D094630909482D1A540480F95CF663C1700B2D54431C5539D969EBD332A3F017BE29A8212872D2B84
Malicious:	**true**
Reputation:	unknown

C:\Program Files (x86)\Windows Multimedia Platform\Windows Update.exe.config	
Preview:	<?xml version="1.0" encoding="utf-8" ?>..<configuration>.. <startup useLegacyV2RuntimeActivationPolicy="true">.. <supportedRuntime version="v2.0.50727"/>.. .. <supportedRuntime version="v3.5"/> "The .NET Framework version 3.0 and 3.5 use version 2.0.50727 of the CLR.".. -->.. <supportedRuntime version="v4.0" sku ".NETFramework,Version=v4.0,Profile=Client" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0.1,Profile=Client" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0.1" />.. <supportedRuntime v ersion="v4.0" sku =".NETFramework,Version=v4.0.2,Profile=Client" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0.2" />.. <supported Runtime version="v4.0" sku =".NETFramework,Version=v4.0.3,Profile=Client" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0.3" />.. < supportedRuntime version="v4

C:\Program Files (x86)\Windows Multimedia Platform\ZHunuhebaqu.exe	
Process:	C:\Users\user\AppData\Local\Temp\is-H3FQR.tmp\7((_8888YTR(.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	34304
Entropy (8bit):	5.910423200451303
Encrypted:	false
SSDEEP:	768:RV+hcHOK/z+KPmaM8XZVoChjE0fVZwTV8d2VzaG5po0YE4ZjNDBYcLdjF:LSEOK/iLN8X7oChjE0dZwh8dEzaGcDd/
MD5:	9D8A50291AF41031974A371A0F8C5601
SHA1:	F10A94B3D3EAC38FB5278816B20EF1EEDCBF7430
SHA-256:	BCEBBD53B06FED08A014F9FD5501F1FA4594BC2A88D472E396D5F45CC936D531
SHA-512:	C2D9CEC73082F8BBE71274EF7D721FA2BFCBA0AEB958AD3B052F798407E02DFB14C9A8CC7A106727A8DB04633F13530D0BB481C4E68D8490907B7565967434C E
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 34%, Browse • Antivirus: ReversingLabs, Detection: 78%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a....."...0..^...&.....\|... .....@.. ....@.....\|..O.....".....X{..... ....H.....text....\... ...^..... ..`.rsrc...."....$...`.....@..@.reloc..... .....@..B.....|.....H.....p...H8.....f.....6.(....(....*.*z.,..{.....{....o.....(....*..0.....(....s.....s....}.....s....}.....s....}.....(.....{.....o..... {..... ....s....o.....{....r...po.....{.... ....s....o.....{.....o ....{.....r...po!...o"....{.....s#...o$....{.....o.....{.... .....8s....o.....{....r'..po.....{.... ....s....o.....{.....o ....{.....r5..po!...o"....{.....o .....{....(%...o&....{....('...o(....{..

C:\Program Files (x86)\Windows Multimedia Platform\ZHunuhebaqu.exe.config	
Process:	C:\Users\user\AppData\Local\Temp\is-H3FQR.tmp\7((_8888YTR(.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1234
Entropy (8bit):	5.09824893497494
Encrypted:	false
SSDEEP:	24:2dZmht+SDfy4GOy4TO4q5X4tndGubyB8GRyF:ccdfy4G74TO4qN4hRN
MD5:	98D2687AEC923F98C37F7CDA8DE0EB19
SHA1:	F6DCFCDCFE570340ECDBBD9E2A61F3CB4F281BA7
SHA-256:	8A94163256A722EF8CC140BCD115A5B8F8725C04FE158B129D47BE81CB693465
SHA-512:	95C7290D59749DF8DF495E04789C1793265E0F34E0D091DF5C0D4AEFE1AF4C8AC1F5460F1F198FC28C4C8C900827B8F22E2851957BBAEA5914EA962B3A1D059
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8" ?>..<configuration>.. <startup useLegacyV2RuntimeActivationPolicy="true">.. <system.xml.serialization>.. <xmlSerializer useLegacySerializerGeneration="true"/>.. </system.xml.serialization>.. <supportedRuntime version="v2.0.50727"/>.. <supportedRuntime version="v4.0" sku = ".NETFramework,Version=v4.0,Profile=Client" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0.1,Profile=Client" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0.1" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0.2,Profile=Client" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0.2" />.. <supportedRuntime version=" v4.0" sku =".NETFramework,Version=v4.0.3,Profile=Client" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0.3" />.. <supportedRuntime vers ion="v4.0" sku =".NETFramework,Version=v

C:\Program Files (x86)\i-record\AForge.Video.FFMPEG.dll (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	61952
Entropy (8bit):	6.035911862086533
Encrypted:	false
SSDEEP:	768:SxyXJysfxmBrHgXMI32glxbr3ZpS3kPZY/UuVTodlyQTzIKNXKkHq:SxyXJpfxurHOlltT7pZcVToHXnK
MD5:	5F60669A79E4C4285325284AB662A0C0
SHA1:	5B83F8F2799394DF3751799605E9292B21B78504
SHA-256:	3F6AA370D70259DC55241950D669D2BF3DC7B57A0C45C6A2F8DEC0D8C8CC35B0
SHA-512:	6EC9FE576DAA4FDE11A39A929DD23AB44297521C4D23352AF1A78716CC3EC7927AA6949D5F7AF638148E58E5B6D1D16043AD1A7B0DABB8103ACC07D0D4C8A 2F

C:\Program Files (x86)\i-record\AForge.Video.FFMPEG.dll (copy)	
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....>.-wz.C$z.C$z.C$].8$~.C$s..$x.C$s..$t.C$s..$|.C$s..$w.C$z.B$*.C$s..$|.C$s..${.C$Richz.C$.....PE..L....r.Q.....!....6.....C.....P.....0.....d'....@.....\..... ..\...Q.....HR..@.....P..`.....Q..H.....text...M4.....6..... ..`.rdata.....P.....:.....@..@.data.....@....rsrc.....@..@.reloc.....

C:\Program Files (x86)\i-record\AForge.Video.dll (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	20992
Entropy (8bit):	5.329873635101462
Encrypted:	false
SSDEEP:	384:Wu9f/hWFwLX+WJ7gfZLTswhHDlOdKaCxkyf0l:HfpZL9uxE9Cxd8l
MD5:	0BD34AA29C7EA4181900797395A6DA78
SHA1:	DDFFDCEF29DADDC36CA7D8AE2C8E01C1C8BB23A8
SHA-256:	BAFA6ED04CA2782270074127A0498DDE022C2A9F4096C6BB2B8E3C08BB3D404D
SHA-512:	A3734660C0ABA1C2B27AB55F9E578371B56C82754A3B7CFD01E68C88967C8DADA8D202260220831F1D1039A5A35BD1A67624398E689702481AC056D1C1DDCDE
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....q.Q.....!.....J.....h... .....@.. .....I... ..@.....g..K.....P.....dg..... ....H.....text...4H... ...J..... ..`.rsrc...P.....L.....@..@.rel oc.....P.....@..B.....h.....H.....H:...-.....P .....{hV[h..j...+I....k.rQ2..P+.C..O..k.p....`.v..W.+...&....o..".U..0."n.mZ.p.T..h..Z+...Q ...Rz}.j.....v..=./....MI4....0..).....{.....(....t.....|.....(...+...3.*....0..).....{.....(....t.....|.....(...+...3.*6.{.....o....*6.{.....o....*6.{.....o....*6.{.....o....*6.{.....o....*..{....*..{....*"..}....*2.{....o....*2.{... .o....*2.{....o....*....0.....{.....}.....*.0.....{....o.

C:\Program Files (x86)\i-record\I-Record.exe (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	893952
Entropy (8bit):	6.030046224100464
Encrypted:	false
SSDEEP:	12288:FCx6G3fxQ3hyRHyUlv0CZI3jhLRHyUNVS3fxQ:FCx6G3ysRSRMCS3ZRSIS3y
MD5:	13C3BA689A19B325A19AB62CBE4C313C
SHA1:	8B0BA8FC4EAB09E5AA958699411479A1CE201A18
SHA-256:	696822FCDD3382BA02DFCCE45EC4784D65EF44ADF7D1FAC2520B81F8CE007CF9
SHA-512:	387095EC1CCFD7F4E2DAC8522FD72B3199447AD750133BF3719810952262321845F6590457AB4C950F5CF9C5FDA93377710E7B8D940B04D6C80252F1CCF8033E
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 4%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...g..`.....0..z...(..... .....@.. ..... ..@.....8...O.....%..... ..... ..H.....text....y... ...z..... ..`.rsrc....%.....&...|.....@..@.rel oc.....@..B.....I.....H.....=...*.....g..X0.....0.....(.....(....{ ....o.....}.....}.....(.....(....}.....(.....(....}.....s....}.....~....}.....{.....(....o.....{ ...(....o.....s....}.....s....}.....{....r...pr...po.....+-.{....r...p..X.;...(...(!.....o"...o.....X..(!....i2..{.....o#....{.....{.....s$...o%....{....r)..po&....{....r1..po'....{.....@...((...()...o%....{.....o#. ...{.....((...()...o%....{.....o#....{.....o*...*....0..

C:\Program Files (x86)\i-record\avcodec-53.dll (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	13698048
Entropy (8bit):	6.1332248766906226
Encrypted:	false
SSDEEP:	196608:1VhJ9+5snt6w5xrYk/c8XC0iFVfZQNviW1GVwcZcru/umSggLCT7wZ72qh/TDtMA:1TJYwsF+vVrruB6W+p51
MD5:	65F639A2EDA8DB2A1EA40B5DDB5A2ED4
SHA1:	3F32853740928C5E88B15FDC86C95A2EBD8AEB37
SHA-256:	E4E41C0C1C85E2AEAFF1BEA914880D2CB01B153A1A9CEDDCCAF05F8B5362210D
SHA-512:	980B6A5511716073D5EEB8B5437C6F23BDA300402C64D05D2A54DA614E3EF1412743EC5BB4100E54699D7A74F8C437560CB9FAA67824CBBABDF1F9399945E21

C:\Program Files (x86)\i-record\avcodec-53.dll (copy)	
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}5#O.....#.....i. .....e.....:..... ..... 8.t....@8.....8.....p8..... D8.....text.....`..`.data...h.....@.`..rdata...3..... 3..b.....@.`@.rodata..(...0...*.....@.`@.bss....@.i..`.....`..edata..t.... 8.....<.....@.0@.idata.....@8.....Z.....@.0..CRT....0....`8.....t..... .....@.0..tls.... ....p8.....v.....@.0..reloc.....8.....x.....@.0B..... .....

C:\Program Files (x86)\i-record\avdevice-53.dll (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	350208
Entropy (8bit):	6.788773677473835
Encrypted:	false
SSDEEP:	6144:atApu+grbTd0MXaHb7fwgHi2vxiZoupJa8blmh3f6KmzUwE9X4:a6ulrbTdoHb7Xi2vxiZoupfluTwE9I
MD5:	F55981382A554EECFC3A513F1EE48E87
SHA1:	D1FD3F977ABD66BA70516E501FC65189D39AE3FA
SHA-256:	186CAD160DF5ACC1B9530E6F08FCE3FC6752FFEB851EAF57E6BC9D33D42F27DC
SHA-512:	ADBA4A4C530043BAE64CDE455AC0306B1FC08A5A7DB46133F5D0C8823D22ACF812A2E2F253932C3BD240765F1D28E80427FE9653317F1D35FB16D34E712F69A
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 2%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}5#O.....#.....T..... .....xm..... .....:Z.. ....D.....'.....H...0.....text.....`.P`.data.....@.`..rdata..<....0 .....@.`@.bss.....~... .....`..edata.....@.0@.idata..D..... .....@.0..CRT....,.....,.....@.0..tls.... .....@.0..rel oc...'.....(...0.....@.0B..... .....

C:\Program Files (x86)\i-record\avfilter-2.dll (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	924672
Entropy (8bit):	6.433619127597792
Encrypted:	false
SSDEEP:	12288:uBUgJ5aa7butTNq/+nUCwnvxsSqG5wMe/aSaCTC1PZBQcFFyj2LgAN4dwR:uiCXONq/Y5oZrwB/aSaCTAxCfqcjdi
MD5:	5E1E575F8125B787CD521A5107CD8272
SHA1:	8603FF88BADD2CD24BD41F6B82B570A325C47920
SHA-256:	4E424DFB83931963B3BDCBA931DDD1EBB5E302792F992170227BF7181E705C47
SHA-512:	143C541A0C9AB70B2C3A82842A81CCE153D1143E4DFB172CC99F5EFC8DC8B17CD5546D0F499A10BB1FA6974D7230E56A931E94C1EE47D669A8EBCF05187CF8 E2
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 2%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}5#O.....#.....f.. .....ld.....I.. ....@.....`..\.....?.....@d.....text...$.....`.P`.data....S.....T.....@.`..rdata.. [...p...\...J.....@.`@.bss.....e.....`..edata.....@.....@.0@.idata..\...`.....@.0..CRT....,.....@.0..tls.... ....@.0..reloc...?.....@.....@.0B..... .....

C:\Program Files (x86)\i-record\avformat-53.dll (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	2523136
Entropy (8bit):	6.303082429751349
Encrypted:	false
SSDEEP:	49152:qXk+2XJrm/rMbrxMCSmhfShEGFpdDVne4BP8XC6M3eNTVox/FW4Dp:qXk+2oTMRMmhfShEGFppVe4BP8y6AeE
MD5:	11340A55F155A904596BF3A13788A93A
SHA1:	92A2F79717F71696EBDE3C400AA52804EDA5984E
SHA-256:	B26B2DF18537B3DF6706AA9E743D1A1E511A6FD21F7F7815F15EF96BB09A85E9

C:\Program Files (x86)\i-record\avformat-53.dll (copy)	
SHA-512:	2DC2BB8B0B4A38DDEE62D85FDF7C551B0B77F5B9C7791CF82A00EEA847F86006DF5139874381DD6DB739BB77EC008BE9F32185EC71CA8BE603F7FE515662C7B
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}5#O.....#.....\|&..2.. .....j.....'.....T.&. ....%.....%.,,..... &.....&.....%.....text...X.....`.p`.data...P.....@.`..rdata...${.....|.....@.`@.bss.....1...p%.....`..edata.....%.....P%.....@.0@.idata..,,....%.....f%.....@.0..CRT....0.....&.....%.....@.0..tls.... ..... &.....%.....@.0..reloc..... &.....%.....@.0B.....

C:\Program Files (x86)\i-record\avutil-51.dll (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	139776
Entropy (8bit):	6.418573138423396
Encrypted:	false
SSDEEP:	3072:G+PT/YkOkRgHzlc5XROode1FZ6rkp7dPVPU:tPT/YNAgHzS1szf7dPVs
MD5:	78128217A6151041FC8F7F29960BDD2A
SHA1:	A6FE2FA059334871181F60B626352E8325CBDDA8
SHA-256:	678CA4D9F4D4AD1703006026AFE3DF5490664C05BB958B991C028CE9314757F7
SHA-512:	5F534A8B186797046526CFB29F95E89E90C555CF54CC8E99A801DFE9327433C9C0FD2CB63A335ADE606075C9FAB5173C1AD805242CEB04BC1FD78F37DA166D8
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}5#O.....#.....J.. .....h..... ....`.....,.....x.....text...d.....`.P`.data...x.....@.P..rdata...M..... .N.....@.`@.bss....@I.....`..edata.....`.....@.0@.idata.....@.0..CRT....,.....@.0..tls.... ..... @.0..reloc..,.....@.0B.....

C:\Program Files (x86)\i-record\i-record.exe.config (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	196
Entropy (8bit):	4.875810934197674
Encrypted:	false
SSDEEP:	6:TMV0klGkfVymRMT4/0xC/ya7VNQlchAW4QIm:TMG1GEVymhsSj23xm
MD5:	871947926C323AD2F2148248D9A46837
SHA1:	0A70FE7442E14ECFADD2932C2FB46B8DDC04BA7A
SHA-256:	F3D7125A0E0F61C215F80B1D25E66C83CD20ED3166790348A53E0B7FAF52550E
SHA-512:	58D9687495C839914D3AA6AE16677F43A0FA9A415DBD8336B0FCACD0C741724867B27D62A640C09828B902C69AC8F5D71C64CDADF87199E7637681A5B87DA3E
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0"?>..<configuration>.. <startup useLegacyV2RuntimeActivationPolicy="true">.. .. <supportedRuntime version="v2.0.50727" sku="Client"/></startup>..</configuration>..

C:\Program Files (x86)\i-record\is-2J58U.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	13698048
Entropy (8bit):	6.1332248766906226
Encrypted:	false
SSDEEP:	196608:1VhJ9+5snt6w5xrYk/c8XC0iFVfZQNviW1GVwcZcru/umSggLCT7wZ72qh/TDtMA:1TJYwsF+vVrruB6W+p51
MD5:	65F639A2EDA8DB2A1EA40B5DDB5A2ED4
SHA1:	3F32853740928C5E88B15FDC86C95A2EBD8AEB37
SHA-256:	E4E41C0C1C85E2AEAFF1BEA914880D2CB01B153A1A9CEDDCCAF05F8B5362210D
SHA-512:	980B6A5511716073D5EEB8B5437C6F23BDA300402C64D05D2A54DA614E3EF1412743EC5BB4100E54699D7A74F8C437560CB9FAA67824CBBABDF1F9399945E21
Malicious:	false
Reputation:	unknown

C:\Program Files (x86)\i-record\is-2J58U.tmp	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}5#O.....#.....i. .....e.....;..... 8.t....@8.....8.....p8..... D8.....text.....`..`.data...h.....@.`..rdata...3..... 3..b.....@.`@.rodata..(...0...*.....@.`@.bss....@.i..`.....`..edata..t.... 8.....<.....@.0@.idata.....@8.....Z.....@.0..CRT....0....`8.....t..... .....@.0..tls.... ....p8.....v.....@.0..reloc.....8.....x.....@.0B.....

C:\Program Files (x86)\i-record\is-3FQP6.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	302592
Entropy (8bit):	6.633285367699617
Encrypted:	false
SSDEEP:	6144:ciLkDvPGXiVtitatdtgt68zHkZe+IT3d4dKX8K36P0ViLLgovP7x6+wglZ:ciL2vOU8bkZe+Ud4de4gQwg7
MD5:	564DCA64680D608517721CDBE324B1D6
SHA1:	F2683FA13772FC85C3EA4CFFA3D896373A603AD3
SHA-256:	F9550ACE57CE5B19ADD143E507179DC601A832B054963D1C3B5C003F1A8149CC
SHA-512:	1D80E9DE29320201C988E8B11036C423D83620E99BCADEC5142EB14B6513E49D9B41904E92154139E327CD5CC6F058B4BB467EE4FBB342794296E0DFE774DC7
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}5#O.....#..... .....0....j.....v... ....i.....D.....text.....`.P`.data...<....0.....@.P..rdata..$=...@ ...>.....@.`@.rodata.....X.....@.P@.bss....X.....`..edata..i.....Z.....@.0@.idata.....v.....@.0..CRT....,.....~..... ..@.0..tls.... .....@.0..reloc.....@.0B..... .....

C:\Program Files (x86)\i-record\is-685QJ.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	924672
Entropy (8bit):	6.433619127597792
Encrypted:	false
SSDEEP:	12288:uBUgJ5aa7butTNq/+nUCwnvxsSqG5wMe/aSaCTC1PZBQcFFyj2LgAN4dwR:uiCXONq/Y5oZrwB/aSaCTAxCfqcjdi
MD5:	5E1E575F8125B787CD521A5107CD8272
SHA1:	8603FF88BADD2CD24BD41F6B82B570A325C47920
SHA-256:	4E424DFB83931963B3BDCBA931DDD1EBB5E302792F992170227BF7181E705C47
SHA-512:	143C541A0C9AB70B2C3A82842A81CCE153D1143E4DFB172CC99F5EFC8DC8B17CD5546D0F499A10BB1FA6974D7230E56A931E94C1EE47D669A8EBCF05187CF8 E2
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}5#O.....#.....f.. .....ld.....l.. ....@.....`..\.....?.....@d.....text...$.....`.P`.data....S.....T.....@.`..rdata.. [...p...\...J.....@.`@.bss.....e.....`..edata.....@.....@.0@.idata..\....`.....@.0..CRT....,.....@.0..tls.... ....@.0..reloc...?.....@.....@.0B..... .....

C:\Program Files (x86)\i-record\is-9KFTG.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	161280
Entropy (8bit):	6.279414522219196
Encrypted:	false
SSDEEP:	3072:PxxxxRxRw6B3L9Qaa6aa66z1lQh6608Hv5ZgWdM+VYOt/wY0vns:PxxxxRxRw6BWaa6aa66z1ll+8Hv56W2J
MD5:	D2636C9E6E302341B59E244B8C71F3C1
SHA1:	42490A1EFAD20A1D4A908CCEA118F41C5B636016
SHA-256:	FE62D3E0876142D72379C2C36623BFF4F71E31B1FD86C5B865E36A5A2C278C0F
SHA-512:	34A8AAB392EC2815E8DCC6A63A6A5D02EACC2269AE45C11F9CE82083B4391132D7A32EE872983E9B0A9B85455AACA711C38638AEF9A9CE6A57DF237A3CDC1 6F
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}5#O.....#.....J...r..... .....`....j..... ..... ..... .....text....H.....J.....`.P`.data.....`.....N.....@.0..rdata.....p .....P.....@.`@.bss.....`..edata.....d.....@.0@.idata.....f.....@.0..CRT....,.....l.....@.0..tls.... .....n.....@.0..rel oc.....p.....@.0B..... .....

C:\Program Files (x86)\i-record\is-9KFTG.tmp

C:\Program Files (x86)\i-record\is-CUGLT.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	2523136
Entropy (8bit):	6.303082429751349
Encrypted:	false
SSDEEP:	49152:qXk+2XJrm/rMbrxMCSmhfShEGFpdDVne4BP8XC6M3eNTVox/FW4Dp:qXk+2oTMRMmhfShEGFppVe4BP8y6AeE
MD5:	11340A55F155A904596BF3A13788A93A
SHA1:	92A2F79717F71696EBDE3C400AA52804EDA5984E
SHA-256:	B26B2DF18537B3DF6706AA9E743D1A1E511A6FD21F7F7815F15EF96BB09A85E9
SHA-512:	2DC2BB8B0B4A38DDEE62D85FDF7C551B0B77F5B9C7791CF82A00EEA847F86006DF5139874381DD6DB739BB77EC008BE9F32185EC71CA8BE603F7FE515662C7B
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}5#O.....#.....\|&..2.. .....j.....'.....T.&. ....%.....%.,,..... &.....&.....%.....text...X.....`.p`.data...P.....@.`..rdata..${.....|.....@.`@.bss.....1...p%.....`..edata.....%.....P%.....@.0@.idata..,,...%.....f%.....@.0..CRT....0.....&.....%.....@.0..tls.... ..... &.....%.....@.0..reloc..... &.....%.....@.0B.....

C:\Program Files (x86)\i-record\is-ESLKL.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	893952
Entropy (8bit):	6.030046224100464
Encrypted:	false
SSDEEP:	12288:FCx6G3fxQ3hyRHyUIv0CZI3jhLRHyUNVS3fxQ:FCx6G3ysRSRMCS3ZRSIS3y
MD5:	13C3BA689A19B325A19AB62CBE4C313C
SHA1:	8B0BA8FC4EAB09E5AA958699411479A1CE201A18
SHA-256:	696822FCDD3382BA02DFCCE45EC4784D65EF44ADF7D1FAC2520B81F8CE007CF9
SHA-512:	387095EC1CCFD7F4E2DAC8522FD72B3199447AD750133BF3719810952262321845F6590457AB4C950F5CF9C5FDA93377710E7B8D940B04D6C80252F1CCF8033E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...g..`.....0..z...(..... .....@.. .....@.....8...O.....%..... ..... ..H.....text....y... ...z..... ..`.rsrc....%.....&...\|.....@..@.reloc.....@..B.....\|.....H.....=...*.....g..X0.....0.....(.....(.....{ ....o.....}.....}.....(.....(....}.....(.....(....}.....s....}.....~....}.....{.....(....o.....{ ...(....o.....s....}.....s....}.....{....r...pr...po.....+-.{....r...p..X.;...(...(!.....o"...o.....X..(!....i2..{.....o#....{.....{.....s$...o%....{....r)..po&....{....r1..po'....{.....@...((...()...o%....{.....o#. ...{.....((...()...o%....{.....o#....{.....o*...*....0..

C:\Program Files (x86)\i-record\is-IGHFO.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	61952
Entropy (8bit):	6.035911862086533
Encrypted:	false
SSDEEP:	768:SxyXJysfxmBrHgXMI32glxbr3ZpS3kPZY/UuVTodlyQTzIKNXKkHq:SxyXJpfxurHOlltT7pZcVToHXnK
MD5:	5F60669A79E4C4285325284AB662A0C0
SHA1:	5B83F8F2799394DF3751799605E9292B21B78504
SHA-256:	3F6AA370D70259DC55241950D669D2BF3DC7B57A0C45C6A2F8DEC0D8C8CC35B0
SHA-512:	6EC9FE576DAA4FDE11A39A929DD23AB44297521C4D23352AF1A78716CC3EC7927AA6949D5F7AF638148E58E5B6D1D16043AD1A7B0DABB8103ACC07D0D4C8A2F
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....>.-wz.C$z.C$z.C$].8$~.C$s..$x.C$s..$t.C$s..$\|.C$s..$w.C$z.B$*.C$s..$\|.C$s..${.C$Richz.C$.....PE..L....r.Q.....!....6.....C.....P.....0.....d'....@.....\..... ..\...Q.....HR..@.....P..`.....Q..H.....text...M4.....6..... ..`.rdata.....P.....:.....@..@.data.....@....rsrc.....@..@.reloc.....@..B.....

C:\Program Files (x86)\i-record\is-IGHFO.tmp	

C:\Program Files (x86)\i-record\is-L76RD.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	35840
Entropy (8bit):	6.073375793840483
Encrypted:	false
SSDEEP:	768:qTS4nJhuLN8gVrooUNTrhYFK2SoXl2hoHqcVvYjpS/:qbnruJ8gtMxrhN2Zl2hgqyvY
MD5:	85E7D6000E076B4C071D49EE1B6B6122
SHA1:	79A21E2D4402A8CDC989FD96C2096BB737B67E43
SHA-256:	F10C1553BBDB2205953ED6AE2DBDD1CDA2219EB594CBA776AB0529790BBF6449
SHA-512:	5E2A763939F8ABD47BA3686FD777F0EC0D1CBBC04E00F1B17277DEC7F98CFB6C9F729B9856F49ED6343684F562A4D552A160802DF25296723262B811D96DE92E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}5#O.....#.....`..... .....p....|p..... ..... .....D.....<.....H.....text...D_.....`.....`.P`.data.....p.....d.....@.0..rdata..... .....f.....@.`@.bss.....`..edata..D.....z.....@.0@.idata..<.....|.....@.0..CRT....,.....@.0..tls.... .....@.0..rel oc..... .....@.0B..... .....

C:\Program Files (x86)\i-record\is-O4BO6.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	350208
Entropy (8bit):	6.788773677473835
Encrypted:	false
SSDEEP:	6144:atApu+grbTd0MXaHb7fwgHi2vxiZoupJa8blmh3f6KmzUwE9X4:a6ulrbTdoHb7Xi2vxiZoupfluTwE9I
MD5:	F55981382A554EECFC3A513F1EE48E87
SHA1:	D1FD3F977ABD66BA70516E501FC65189D39AE3FA
SHA-256:	186CAD160DF5ACC1B9530E6F08FCE3FC6752FFEB851EAF57E6BC9D33D42F27DC
SHA-512:	ADBA4A4C530043BAE64CDE455AC0306B1FC08A5A7DB46133F5D0C8823D22ACF812A2E2F253932C3BD240765F1D28E80427FE9653317F1D35FB16D34E712F69A
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}5#O.....#.....T..... .....xm..... .....:Z.. ....D.....'.....H...0.....text.....`.P`.data.....@.`..rdata..<....0 .....@.`@.bss.....~... .....`..edata.....@.0@.idata..D..... .....@.0..CRT....,.....,.....@.0..tls.... .....@.0..rel oc...'.....(...0.....@.0B..... .....

C:\Program Files (x86)\i-record\is-PVRDV.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	20992
Entropy (8bit):	5.329873635101462
Encrypted:	false
SSDEEP:	384:Wu9f/hWFwLX+WJ7gfZLTswhHDlOdKaCxkyf0l:HfpZL9uxE9Cxd8l
MD5:	0BD34AA29C7EA4181900797395A6DA78
SHA1:	DDFFDCEF29DADDC36CA7D8AE2C8E01C1C8BB23A8
SHA-256:	BAFA6ED04CA2782270074127A0498DDE022C2A9F4096C6BB2B8E3C08BB3D404D
SHA-512:	A3734660C0ABA1C2B27AB55F9E578371B56C82754A3B7CFD01E68C88967C8DADA8D202260220831F1D1039A5A35BD1A67624398E689702481AC056D1C1DDCDE
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....q.Q.....!.....J.....h... .....@.. .....I... ..@.....g..K.....P.....dg..... ....H.....text...4H... ...J..... ..`.rsrc...P.....L.....@..@.rel oc.....P.....@..B.....h.....H.....H:...-.....P ..... .....{hV[h..j...+I....k.rQ2..P+.C..O..k.p....`.v..W.+...&....o..".U..0."n.mZ.p.T..h..Z+...Q ...Rz}.j.....v..=./....MI4....0..).....{.....(....t.....|.....(...+...3.*....0..).....{.....(....t.....|.....(...+...3.*6.{.....o....*6.{.....o....*6.{.....o....*6.{.....o....*6.{.....o....*..{....*..{....*"..}....*2.{....o....*2.{... .o....*2.{....o....*....0.....{.....}.....*.0.....{....o.

C:\Program Files (x86)\i-record\is-QLPAO.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	139776
Entropy (8bit):	6.418573138423396
Encrypted:	false
SSDEEP:	3072:G+PT/YkOkRgHzlc5XROode1FZ6rkp7dPVPU:tPT/YNAgHzS1szf7dPVs
MD5:	78128217A6151041FC8F7F29960BDD2A
SHA1:	A6FE2FA059334871181F60B626352E8325CBDDA8
SHA-256:	678CA4D9F4D4AD1703006026AFE3DF5490664C05BB958B991C028CE9314757F7
SHA-512:	5F534A8B186797046526CFB29F95E89E90C555CF54CC8E99A801DFE9327433C9C0FD2CB63A335ADE606075C9FAB5173C1AD805242CEB04BC1FD78F37DA166D8
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}5#O.....#.....J.. .....h..... ....`.....x.....text...d.....`.P`.data...x.....@.P..rdata...M..... .N.....@.`@.bss....@I.....`..edata.....`.....@.0@.idata.....@.0..CRT....,.....@.0..tls.... ..... @.0..reloc.,.....@.0B..... .....

C:\Program Files (x86)\i-record\is-T1381.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	732325
Entropy (8bit):	6.50131566843987
Encrypted:	false
SSDEEP:	12288:4QhCh1/aLmSKrPD37zzH2A6QGgx/bsQYq9KgERkVfzrrNVyblD4cNaftyx9Q8:4QYh1yLmSKrPD37zzH2A6QD/IpqggE2s
MD5:	40248A8DE5A1793ADB591DB2452DAEAB
SHA1:	9DAEFDA6A90C63ED0527344F62413D95ADF46937
SHA-256:	475D52BE2EDCABC926F60351ABCD9FC7C6E1E71D6CACA9D6DB516DBA81E9C0C9
SHA-512:	C470793F5038E2FA4B5A9770DD9D35FBCBDD80CF686D66C28725B034D4472628F9A9C4DC4F9DE91201754C388EDF0F4EEFAA40BA300773C182EA73158356C9D
Malicious:	false
Reputation:	unknown
Preview:	MZP.....@.....InUn.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....n.....@.....@.....@.....&.....l0.....0..... ....CODE....$..... ..`DATA.... .....@...BSS.....idata...&.....(.....@....tls.....rdata..... .. ..@..P.reloc.....0.....@..P.rsrc...l0.....2.....@..P.....f.....@..P..... .....

C:\Program Files (x86)\i-record\is-V48G5.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	196
Entropy (8bit):	4.875810934197674
Encrypted:	false
SSDEEP:	6:TMV0kIGkfVymRMT4/0xC/ya7VNQlchAW4QIm:TMG1GEVymhsSj23xm
MD5:	871947926C323AD2F2148248D9A46837
SHA1:	0A70FE7442E14ECFADD2932C2FB46B8DDC04BA7A
SHA-256:	F3D7125A0E0F61C215F80B1D25E66C83CD20ED3166790348A53E0B7FAF52550E
SHA-512:	58D9687495C839914D3AA6AE16677F43A0FA9A415DBD8336B0FCACD0C741724867B27D62A640C09828B902C69AC8F5D71C64CDADF87199E7637681A5B87DA3E
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0"?>..<configuration>.. <startup useLegacyV2RuntimeActivationPolicy="true">.. .. <supportedRuntime version="v2.0.50727" sku="Client"/></startup>..</configuration>..

C:\Program Files (x86)\i-record\postproc-52.dll (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	161280
Entropy (8bit):	6.279414522219196
Encrypted:	false
SSDEEP:	3072:PxxxxRxRw6B3L9Qaa6aa66z1lQh6608Hv5ZgWdM+VYOt/wY0vns:PxxxxRxRw6BWaa6aa66z1lI+8Hv56W2J
MD5:	D2636C9E6E302341B59E244B8C71F3C1

C:\Program Files (x86)\i-record\postproc-52.dll (copy)	
SHA1:	42490A1EFAD20A1D4A908CCEA118F41C5B636016
SHA-256:	FE62D3E0876142D72379C2C36623BFF4F71E31B1FD86C5B865E36A5A2C278C0F
SHA-512:	34A8AAB392EC2815E8DCC6A63A6A5D02EACC2269AE45C11F9CE82083B4391132D7A32EE872983E9B0A9B85455AACA711C38638AEF9A9CE6A57DF237A3CDC1 6F
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}5#O.....#.....J...r..... .....`.....j..... ..... .....text....H.....J.....`.P`.data.....`.....N.....@.0..rdata.....p .....P.....@.`@.bss.....`..edata.....d.....@.0@.idata.....f.....@.0..CRT....,.....l.....@.0..tls.... .....n.....@.0..rel oc.....p.....@.0B..... .....

C:\Program Files (x86)\i-record\swresample-0.dll (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	35840
Entropy (8bit):	6.073375793840483
Encrypted:	false
SSDEEP:	768:qTS4nJhuLN8gVrooUNTrhYFK2SoXl2hoHqcVvYjpS/:qbnruJ8gtMxrhN2Zl2hgqyvY
MD5:	85E7D6000E076B4C071D49EE1B6B6122
SHA1:	79A21E2D4402A8CDC989FD96C2096BB737B67E43
SHA-256:	F10C1553BBDB2205953ED6AE2DBDD1CDA2219EB594CBA776AB0529790BBF6449
SHA-512:	5E2A763939F8ABD47BA3686FD777F0EC0D1CBBC04E00F1B17277DEC7F98CFB6C9F729B9856F49ED6343684F562A4D552A160802DF25296723262B811D96DE92E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}5#O.....#.....`..... .....p....|p..... ..... .....D.....<.....H.....text...D_.....`.....`.P`.data.....p.....d.....@.0..rdata..... .....f.....@.`@.bss.....`..edata..D.....z.....@.0@.idata..<.....|.....@.0..CRT....,.....@.0..tls.... .....@.0..rel oc.....@.0B..... .....

C:\Program Files (x86)\i-record\swscale-2.dll (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	302592
Entropy (8bit):	6.633285367699617
Encrypted:	false
SSDEEP:	6144:ciLkDvPGXiVtitatdtgt68zHkZe+IT3d4dKX8K36P0ViLLgovP7x6+wglZ:ciL2vOU8bkZe+Ud4de4gQwg7
MD5:	564DCA64680D608517721CDBE324B1D6
SHA1:	F2683FA13772FC85C3EA4CFFA3D896373A603AD3
SHA-256:	F9550ACE57CE5B19ADD143E507179DC601A832B054963D1C3B5C003F1A8149CC
SHA-512:	1D80E9DE29320201C988E8B11036C423D83620E99BCADEC5142EB14B6513E49D9B41904E92154139E327CD5CC6F058B4BB467EE4FBB342794296E0DFE774DC7
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}5#O.....#..... .....0....j.....v... ....i.....D.....text.....`.P`.data...<....0.....@.P..rdata..$=...@ ...>.....@.`@.rodata.....X.....@.P@.bss....X.....`..edata..i.....Z.....@.0@.idata.....v.....@.0..CRT....,.....~..... ..@.0..tls.... .....@.0..reloc.....@.0B..... .....

C:\Program Files (x86)\i-record\unins000.dat	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	data
Category:	dropped
Size (bytes):	1880
Entropy (8bit):	4.613545026553328
Encrypted:	false
SSDEEP:	48:3qEfE0gR94xwROnryvmshIfLste8BtFLMLQvBNl:aE8dbSwbLMLQvB3
MD5:	7E0C79B7F08AF7D6F28801B2A21F54E2
SHA1:	949CD63879B6EC7D66CD37EC06464842DD98174E
SHA-256:	9FAE74783723E4DFB19DDD9C1793518A83BD42242C135867127DA0D476EEE062
SHA-512:	9C99B63C9990B9316318F71A8CB72F633FC74411E05EEFD4C1A34EF859E80E8B020A503C104C1CCAC4D55189F3434B336DE1413B45050D522C8BD4FA5CD8711
Malicious:	false
Reputation:	unknown

C:\Program Files (x86)\i-record\unins000.dat	
Preview:	Inno Setup Uninstall Log (b).....{EF8AF121-AE7E-4BCC-B632-4562E9EF3D46}.....i-record..... .....0.....X...%.....s...o.R.....?....8 35180.user.C:\Program Files (x86)\i-record.....;..... ....C:\Program Files (x86)\i-record>C:\ProgramData\Microsoft\Windows\Start Menu \Programs\(Default).(Default).english.....!....C:\Program Files (x86)\i-record.....2...,C:\Program Files (x86)\i-record\I-Record.exe.....6...0C:\Program Files (x86)\i-re cord\AForge.Video.dll.....=...7C:\Program Files (x86)\i-record\AForge.Video.FFMPEG.dll.....4....C:\Program Files (x86)\i-record\avcodec-53.dll.....5.

C:\Program Files (x86)\i-record\unins000.exe (copy)	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	732325
Entropy (8bit):	6.50131566843987
Encrypted:	false
SSDEEP:	12288:4QhCh1/aLmSKrPD37zzH2A6QGgx/bsQYq9KgERkVfzrrNVyblD4cNaftyx9Q8:4QYh1yLmSKrPD37zzH2A6QD/IpqggE2s
MD5:	40248A8DE5A1793ADB591DB2452DAEAB
SHA1:	9DAEFDA6A90C63ED0527344F62413D95ADF46937
SHA-256:	475D52BE2EDCABC926F60351ABCD9FC7C6E1E71D6CACA9D6DB516DBA81E9C0C9
SHA-512:	C470793F5038E2FA4B5A9770DD9D35FBCBDD80CF686D66C28725B034D4472628F9A9C4DC4F9DE91201754C388EDF0F4EEFAA40BA300773C182EA73158356C9D
Malicious:	false
Reputation:	unknown
Preview:	MZP.....@.....InUn.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....n.....@.....@.....@.....&.....l0.....0..... ....CODE....$..... ..`DATA.... .....@...BSS.....idata...&.....(.....@....tls.....rdata..... .. ..@..P.reloc.....0.....@..P.rsrc...l0.....2.....@..P.....f.....@..P..... .....

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	unknown
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR. AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GM DS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Program Files\internet explorer\ROOKKLCFJB\irecord.exe	
Process:	C:\Users\user\AppData\Local\Temp\is-H3FQR.tmp\7((_8888YTR(.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6055915
Entropy (8bit):	**7.998684734240505**
Encrypted:	**true**
SSDEEP:	98304:0d0hjokHDJzCDN29BiGALZkp/r9S/exLbnFshZyiIZH3XeWZAdX10eKC4KBPfcin:c+EqaN2nidCp/r9S/SqwNXbTeKUr2e/J
MD5:	F3E69396BFCB70EE59A828705593171A
SHA1:	D4DF6A67E0F7AF5385613256DBF485E1F2886C55
SHA-256:	C970B8146AFBD7347F5488FD821AE6ADE4F355DCB29D764B7834CE8A1754105F
SHA-512:	4743B9BF562C1B8616F794493123160DE95BA15451AFFACF286AFF6D2AF023A07D7942A8753C3FDCCF8D294F99B46ADEE8AC58F6A29D42DEA973A9DE6A77D2F
Malicious:	**true**
Reputation:	unknown

C:\Program Files\internet explorer\ROOKKLCFJB\irecord.exe	
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....b.....@.....p.....@.....@.....P.....8P..... .....CODE....0..... ..`DATA....P.....@...BSS.....idata..P.....@....tls.....rdata..... .....@..P.reloc.....@..P.rsrc...8P.....R.....@..P.....@.....@..P..... .....

C:\Program Files\internet explorer\ROOKKLCFJB\irecord.exe.config	
Process:	C:\Users\user\AppData\Local\Temp\is-H3FQR.tmp\7((_8888YTR(.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1234
Entropy (8bit):	5.09824893497494
Encrypted:	false
SSDEEP:	24:2dZmht+SDfy4GOy4TO4q5X4tndGubyB8GRyF:ccdfy4G74TO4qN4hRN
MD5:	98D2687AEC923F98C37F7CDA8DE0EB19
SHA1:	F6DCFCDCFE570340ECDBBD9E2A61F3CB4F281BA7
SHA-256:	8A94163256A722EF8CC140BCD115A5B8F8725C04FE158B129D47BE81CB693465
SHA-512:	95C7290D59749DF8DF495E04789C1793265E0F34E0D091DF5C0D4AEFE1AF4C8AC1F5460F1F198FC28C4C8C900827B8F22E2851957BBAEA5914EA962B3A1D059
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8" ?>..<configuration>.. <startup useLegacyV2RuntimeActivationPolicy="true">.. <system.xml.serialization>.. <xmlSerializer useLegacySerializerGeneration="true"/>.. </system.xml.serialization>.. <supportedRuntime version="v2.0.50727"/>.. <supportedRuntime version="v4.0" sku = ".NETFramework,Version=v4.0,Profile=Client" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0" />.. <supportedRuntime version="v4.0" sku ="".NETFramework,Version=v4.0.1,Profile=Client" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0.1" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0.2,Profile=Client" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0.2" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0.3,Profile=Client" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0.3" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\i-record.lnk	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Archive, ctime=Sat Jan 15 00:59:28 2022, mtime=Sat Jan 15 00:59:28 2022, atime=Thu Jul 1 20:39:18 2021, length=893952, window=hide
Category:	dropped
Size (bytes):	1092
Entropy (8bit):	4.605884238511235
Encrypted:	false
SSDEEP:	24:8m1wAdOEPkBRA78qadQqd+UUMbQX7aB6m:8m1wAdOg+i7vadQqdHTbQmB6
MD5:	17F2E251C2EFA0A7DEA5E5D872DFFA43
SHA1:	30B541C5F75C37F06C312465030AC9A22EFA5386
SHA-256:	F31F22CE5C3BF92BD6D69DDC956D001CB495429D41D312FFA1BBF2A250FE7A80
SHA-512:	CC091836D4E47EA4C1F5FCEB98E62AFE3317D50B8BB6403C3736F0CAEBE51A072311569DD8DABA54CFA43FE259056DD9D680FA348DA46717CE8CDC9E9D96C 9E
Malicious:	false
Reputation:	unknown
Preview:	L.....F.... ....o.....n.....P.O. .:i.....+00.../C:\.....1.....7Suy..PROGRA~2.....L./TZ.....V.....#..P.r.o.g.r.a.m. .F.i.l.e.s. .(.x .8.6.)...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.7.....Z.1...../Tr...i-record..B...../To./Tr.....B.....4n].i.-.r.e.c.o.r.d.....f.2.....R. .I-Record.exe..J...../To./To.....J.....I.- .R.e.c.o.r.d...e.x.e.....[.....-.....Z.....:.....C:\Program Files (x86)\i-record\I-Record.exe..8.....\.....\.....\.....\.....\.....\P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.i.-.r.e.c.o.r.d.\.I.- .R.e.c.o.r.d...e.x.e...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.i.-.r.e.c.o.r.d.....*.....@Z|...K.J.....`.....X.....835180.....!a..%.H.VZAj.....M.....-..!a..%.H.VZAj. .....M.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6

C:\Users\Public\Desktop\i-record.lnk	
Process:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Archive, ctime=Sat Jan 15 00:59:28 2022, mtime=Sat Jan 15 00:59:28 2022, atime=Thu Jul 1 20:39:18 2021, length=893952, window=hide
Category:	dropped
Size (bytes):	1080
Entropy (8bit):	4.599727169577846
Encrypted:	false
SSDEEP:	24:8m199SdOEPkBRA78qgdQqd+UUMbQX7aB6m:8m17SdOg+i7vgdQqdHTbQmB6
MD5:	BF6CFBF70E2FFF7626DA62C78B3EBE01
SHA1:	4D6984701D530BB612A1A8430BE86736117CE1F0
SHA-256:	E7E167C15411E3D5C5A7B3942E391107E26CECDC88470737CA7933597A51FE89
SHA-512:	43E11FB45E21FAFCC6C2DC026AACF768232A3568B9CD65AC8C3214A7D9BCB02D8DFAFB68A28350F26A77A781EB2E2EA6444C101D93CA29B7A2008B52EB3A6 7E
Malicious:	false
Reputation:	unknown

C:\Users\Public\Desktop\i-record.lnk	
Preview:	L.....F.... ....o.....n.....P.O. .:i.....+00.../C:\.....1...../To...PROGRA~2.....L./Tr.....V.....pS..P.r.o.g.r.a.m. .F.i.l.e.s. .(.x .8.6.)...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.7.....Z.1...../Tr...i-record..B...../To./Tr.....B.....4n].i.-.r.e.c.o.r.d.....f.2.....R. .I-Record.exe..J...../To./To.....J.....I.-.R.e.c.o.r.d...e.x.e.....[.....-.....Z.....:.....C:\Program Files (x86)\i-record\I-Record.exe..2.....\.....\.....\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.i.-.r.e.c.o.r.d.\.I.-.R.e.c.o .r.d...e.x.e...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.i.-.r.e.c.o.r.d.....*.....@Z|...K.J.....`.....X.....835180.....!a..%.H.VZAj.....M.....-..!a..%.H.VZAj.....M..... ....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1

C:\Users\user\AppData\Local\Google\Chrome\User Data\060318a3-b94a-41fc-a860-ee030a599821.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	96692
Entropy (8bit):	3.7485830855829416
Encrypted:	false
SSDEEP:	1536:erAa4/1QNVt2a46e7y6XlpC4G32rVA+f60RUl3:9qPdePTKP
MD5:	4D6069737BE889CEA1769A746D69F3EA
SHA1:	6456EFBA4D0BA91C28831F5827470FF9D92C34DB
SHA-256:	E15EC1436AA771FF268BB56A6F8A44C17DBE30360CC9E7B63EBC7D709775DEB4
SHA-512:	F1B3FC020260DD4E8440586C1CC183A2B4C19228D2617C0E4C9A343A19E2C0B36FB90092F50F22A0A35D77B195A90E9843B5B96FF8824DB76614A21B980F82A7
Malicious:	false
Reputation:	unknown
Preview:	.y.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....P8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\07769093-3e13-4e95-bb79-4c74058c9fd7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	87023
Entropy (8bit):	6.1023214340506655
Encrypted:	false
SSDEEP:	1536:SzKGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SzKFcbXafIB0u1GOJmA3iuR+
MD5:	7B6D2C95722E4F94C56BB69D04BF5AD3
SHA1:	47E2AB110602A3092D639E11B51345B10BC97574
SHA-256:	8F0DC8D9ABC8BCA4B4249B7C9B0020079ABF9C64FA13476379B8F50AC1DF2855
SHA-512:	B1BE7C00418665B17DA0965A35C780F5CCEC8DF89D9F8B1F880EE8F5C21A0D2623D6FFD46E515CE41F1E5D40AA401F044142FAA2D73AC8189D2B35A8B416A2F
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"os_crypt":{" encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxh oUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDX n4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displayurl":true ,"group_name_matcher":"*Shockwave Flash*","help_url":"https://support.google.com/chrome/?p=plugin_flash","lang":"en-US","mime_type

C:\Users\user\AppData\Local\Google\Chrome\User Data\0cb48084-29fa-4a6f-9f40-114ac34fd18b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	87023
Entropy (8bit):	6.102344390088214
Encrypted:	false
SSDEEP:	1536:S6sEGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SZEFcbXafIB0u1GOJmA3iuR+
MD5:	34EE4743F494C9A0B52CABB248CE46C4
SHA1:	39C9477FDF140A2CAE11F03F2DF09473A619C594
SHA-256:	03DA766EE2D7EEDD671F84AB6569603B04682575E681259F8B51D30CA3798741
SHA-512:	56EE26BDC35FA20C69AF91717EFF27D56AAEC2749A3F2E5CA086494B5842D0AB32A8DD87EBA7AFEA451205B3BA11BDC6F4DD664BF56160C0D35FF74CA9E841F1
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Google\Chrome\User Data\0cb48084-29fa-4a6f-9f40-114ac34fd18b.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displayurl":true,"group_name_matcher":"*Shockwave Flash*","help_url":"https://support.google.com/chrome/?p=plugin_flash","lang":"en-US","mime_type

C:\Users\user\AppData\Local\Google\Chrome\User Data\0ec449e8-5c88-408b-aa05-14f5959ea301.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87023
Entropy (8bit):	6.1023214340506655
Encrypted:	false
SSDEEP:	1536:SzKGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SzKFcbXafIB0u1GOJmA3iuR+
MD5:	7B6D2C95722E4F94C56BB69D04BF5AD3
SHA1:	47E2AB110602A3092D639E11B51345B10BC97574
SHA-256:	8F0DC8D9ABC8BCA4B4249B7C9B0020079ABF9C64FA13476379B8F50AC1DF2855
SHA-512:	B1BE7C00418665B17DA0965A35C780F5CCEC8DF89D9F8B1F880EE8F5C21A0D2623D6FFD46E515CE41F1E5D40AA401F044142FAA2D73AC8189D2B35A8B416A2F
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displayurl":true,"group_name_matcher":"*Shockwave Flash*","help_url":"https://support.google.com/chrome/?p=plugin_flash","lang":"en-US","mime_type

C:\Users\user\AppData\Local\Google\Chrome\User Data\2a352428-b82d-44cc-acf6-e210f45b0703.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	201886
Entropy (8bit):	6.073786268148317
Encrypted:	false
SSDEEP:	6144:5hhzKWygeGkVGFHhk9Ff5aqfIlUOoSiuRB:5fHygeGQGFH4fKoK
MD5:	1CD2294505A8CCB2FF736F5B6440A476
SHA1:	3B54F1D11AD1E258508374A61B869D5B72B3B43A
SHA-256:	25CC46211B4F231C81A267E3AA1A890F9D4469C99B8AAB5C36EFD5D844B38F54
SHA-512:	C917D01DB9B342F47F58D594299FE423C1381D6B627E916F7D2485106C9DCC9F1CE5EE1A03AF2A23B36850A8C1A193612A53066BBFDF506C7A9E9CCD11B326D
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642211990913784e+12,"network":1.642179592e+12,"ticks":173925942.0,"uncertainty":3215335.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\2fb646dc-2bb2-4b03-934e-fa9cabbee97f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87023
Entropy (8bit):	6.102344390088214
Encrypted:	false
SSDEEP:	1536:S6sEGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SZEFcbXafIB0u1GOJmA3iuR+
MD5:	34EE4743F494C9A0B52CABB248CE46C4
SHA1:	39C9477FDF140A2CAE11F03F2DF09473A619C594
SHA-256:	03DA766EE2D7EEDD671F84AB6569603B04682575E681259F8B51D30CA3798741
SHA-512:	56EE26BDC35FA20C69AF91717EFF27D56AAEC2749A3F2E5CA086494B5842D0AB32A8DD87EBA7AFEA451205B3BA11BDC6F4DD664BF56160C0D35FF74CA9E84F1
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Google\Chrome\User Data\2fb646dc-2bb2-4b03-934e-fa9cabbee97f.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displayurl":true,"group_name_matcher":"*Shockwave Flash*","help_url":"https://support.google.com/chrome/?p=plugin_flash","lang":"en-US","mime_type

C:\Users\user\AppData\Local\Google\Chrome\User Data\384c10ff-4881-4fb3-9b0d-a0ef79881884.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	87023
Entropy (8bit):	6.102336873525247
Encrypted:	false
SSDEEP:	1536:SpVGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SpVFcbXaflB0u1GOJmA3iuR+
MD5:	DA9653119F223132C1526C3E0EC077BF
SHA1:	E4FAB93681249D1EF267A05789FED324597DCA3E
SHA-256:	C57636F3165CF32D07AA3087ACB86D80F2DEB92A585E076CB9F449BB509A232C
SHA-512:	04EF62515DB821851B79623869661FD692E2C10EA8D169A301F73C916B4B0D53DC08945B3AD74914FB692C4DB4C5769AF9EFD5BB090B9007B0996C1A6840592D
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displayurl":true,"group_name_matcher":"*Shockwave Flash*","help_url":"https://support.google.com/chrome/?p=plugin_flash","lang":"en-US","mime_type

C:\Users\user\AppData\Local\Google\Chrome\User Data\3b4ce552-267b-4573-8641-8d67ea85735e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	193410
Entropy (8bit):	6.044893289845874
Encrypted:	false
SSDEEP:	3072:VvYef5nSzKWSlyU1ofmG81QcrXlLGF4chBrHWU4lFfSIFcbXaflB0u1GOJmA3iu7:ShzKWygeGkVGFHhk9Ff5aqfllUOoSiu7
MD5:	7ACED79F58557BC5EC667D134A9B5642
SHA1:	234EC929B404E877B6AD627B02AA84C7F2792781
SHA-256:	F86E0253DCC2475FB0FAE8F9DA02AEDEE7D725AD38594E944677979B28E0867B
SHA-512:	F91C748BBA1AC15185F976D0BAC5C82FB20884105706F2CB01F817B7F6246098C8225DB36BE8C99FEFAC7BCB1CC6DD510DAE9BF02EC04E39085D30B90427FED
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642211990913784e+12,"network":1.642179592e+12,"ticks":173925942.0,"uncertainty":3215335.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799055175"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\48f6465b-2f30-4fa7-b37a-72a5407f11c4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	87023
Entropy (8bit):	6.102338485338001
Encrypted:	false
SSDEEP:	1536:STgGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:STgFcbXaflB0u1GOJmA3iuR+
MD5:	8E2F8F89DB2CAF888AB331BD143E407F
SHA1:	B430B3995D4731C4C3F491BF569B7A20F729B833
SHA-256:	62F4D2BFC01B96B2077FAE23FE5CC8A251E5069B30DDCF9880A5B4742F37C7DE
SHA-512:	F6DC15A21D5AC02F922EC85D4ABBCBAB1BE80ECB905D46649F4C82CB4AB5A6DF8C649B490ACEC7F89D7D89272B98BEF7A892A21976830898C2A4FACCA8B2BA66
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Google\Chrome\User Data\48f6465b-2f30-4fa7-b37a-72a5407f11c4.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displayurl":true,"group_name_matcher":"*Shockwave Flash*","help_url":"https://support.google.com/chrome/?p=plugin_flash","lang":"en-US","mime_type

C:\Users\user\AppData\Local\Google\Chrome\User Data\509563ce-f6c0-4fec-b0ff-e8243dd21084.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	99384
Entropy (8bit):	3.748534380475307
Encrypted:	false
SSDEEP:	1536:x1rAa4/1QNVtPaS6e7y6clpC4G32rVA+f60RUlE:SqP8eKTKs
MD5:	83BA490BF38F9C96526B06468EA94B39
SHA1:	98765A41D76707081317AC9A1A22985FA9114F33
SHA-256:	7310BE4623D2FCBB0C9C336DCFCF9C2A08623776CCA4DC113643ECBE5D6E8838
SHA-512:	2676DCBC0800683EC538305B9AC2AA940E2898C68AB9E310CC07F2B3A40389168D08AA3CD996EDA7E47D3C6CFDD55EBDB7A45BDC2E8F3614C369601F3CA5664
Malicious:	false
Reputation:	unknown
Preview:	4.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....P8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\53441e9b-d872-4af6-8fc5-2604a1bfb5a4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	201886
Entropy (8bit):	6.073788559857476
Encrypted:	false
SSDEEP:	6144:MChzKWygeGkVGFHhk9Ff5aqfIlUOoSiuRB:MUHygeGQGFH4fKoK
MD5:	5E09B3DC8CD45D2DF51597E39B7B7055
SHA1:	C10EB76BC4BD2E1E8FDCFA3127B288C3A08586E8
SHA-256:	BD1A3F6019F5F7E8DD8458E6F6B19A6AD361275E084B0F57721B25DA745D7EE9
SHA-512:	E0D5BABD1EBC880EF113D96D2463F3F1234F0334026E46E8BF44D4897E87D0208ED1AD66C60501B8F11D38DA4CF8FB526D9B449E0BF3429A62D93217A7448AA
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642211990913784e+12,"network":1.642179592e+12,"ticks":173925942.0,"uncertainty":3215335.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799055175"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\5d2bd48d-f819-4744-9b96-ed502f000e0c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	193410
Entropy (8bit):	6.044893921894573
Encrypted:	false
SSDEEP:	3072:gvYef5nSzKWSlyU1ofmG81QcrXlLGF4chBrHWU4lFfSIFcbXafIB0u1GOJmA3iu7:PhzKWygeGkVGFHhk9Ff5aqfIlUOoSiu7
MD5:	0E7E77C16A47851D33CB2D12795A04AE
SHA1:	B9C7CF57128D9B237B93C4B31B0A3351CE1F1748
SHA-256:	BF9F32B0C51F80B7D950E7F8C74FB2D93D2D203612BA22E5ADA1F84972DDD6AB
SHA-512:	2557E21D488517ABB45692B2C2EA986122DD0F8E6148168F35B51C40E789FB81D2C1DD6BF190DA5C36262F22EF0E7B6F082A44649C3FF52E19D000822DA513AD
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Google\Chrome\User Data\5d2bd48d-f819-4744-9b96-ed502f000e0c.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642211990913784e+12,"network":1.642179592e+12,"ticks":173925942.0,"uncertainty":3215335.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799055175"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\78731a7f-df64-434a-8f83-15684fc0d669.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	201886
Entropy (8bit):	6.073785244383911
Encrypted:	false
SSDEEP:	6144:ythzKWygeGkVGFHhk9Ff5aqfIlUOoSiuRB:yDHygeGQGFH4fKoK
MD5:	5E8E234D05A95EBED86C46796271E854
SHA1:	E98E5A9A700CDBCDED9BC1AC1EE86B3224CD2520
SHA-256:	46FFAC06F898487FA2FA4C3578A55B4CB03D3D7904C381C2EBF39C0558AB2F69
SHA-512:	DE8E4216B25D7C2D5D9A3C2CA8F1D01B2A82BAD93B67D69F5EE08796AE44A6557698640C0DD109B2DE9D5E44B8EAADD34649BFC29AAB932B244F73C6DBE0853D
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642211990913784e+12,"network":1.642179592e+12,"ticks":173925942.0,"uncertainty":3215335.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\8cabe9d0-39a8-490c-b8bd-16c3682641bc.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	201884
Entropy (8bit):	6.073785817152966
Encrypted:	false
SSDEEP:	6144:S8hzKWygeGkVGFHhk9Ff5aqfIlUOoSiuRB:SqHygeGQGFH4fKoK
MD5:	78D236A0381521BC8A86E4163A648EF9
SHA1:	A83B3E7968292F99379021C810EE2388FF7925D2
SHA-256:	B00BD16B6D5E869CDBE3C8FD635284EC2DB400CAA9C39F0BFD6A68B0DA349BB7
SHA-512:	010DD206E23E618B93ABE1210945A8D6550BB4EB83A2C35051D783BAA14C359941F4F57AED6DB15E73DE49D8D36B3663590E046C9AE94A3276BCAF2F8BBB3902
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642211990913784e+12,"network":1.642179592e+12,"ticks":173925942.0,"uncertainty":3215335.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\8d340414-6271-4a96-bccf-462b615529df.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	193410
Entropy (8bit):	6.044893784629742
Encrypted:	false
SSDEEP:	3072:kvYef5nSzKWSlyU1ofmG81QcrXlLGF4chBrHWU4lFfSIFcbXafIB0u1GOJmA3iu7:jhzKWygeGkVGFHhk9Ff5aqfIlUOoSiu7
MD5:	A055433B72CF7B7EDCE922863C69B3A2
SHA1:	10565919D9320A5593EB3BC6DD9481D104FDBF1D
SHA-256:	27980493B7EED8C4B95D561E1611866D55B6773302E86B047D745A6990FF0A6F
SHA-512:	DBF1B04425B4CACA0A5F45CB6C6CD427537FD891F93A3DC78AAA691CFD3BED8C0A1EBEFE1327D49CDCF06242C22E090048F8D33BB2B72BF0C0EABE1B505976D
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\8d340414-6271-4a96-bccf-462b615529df.tmp	
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642211990913784e+12,"network":1.642179592e+12,"ticks":173925942.0,"uncertainty":3215335.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799055175"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\964f75b3-7187-4f98-8a54-465863dba7a9.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	201886
Entropy (8bit):	6.073786883979914
Encrypted:	false
SSDEEP:	6144:lJhzKWygeGkVGFHhk9Ff5aqfIlUOoSiuRB:lHHygeGQGFH4fKoK
MD5:	143A9A10B6BEF56D4E24DB7B9A04FD0B
SHA1:	9445768C55814109CC03534F7366D35C594DAD05
SHA-256:	21BC1159693C544CA9FE45C23698E3422EB1A53B2E350A5E7A5B28F430FE86AE
SHA-512:	2F1522089FC89FF78ABBC16F50D981A70E8C3EB19E374E6212BF0A2CA584F30CB90307D6C5A490C5D8AE120B60B8A461BB557A4A61B2374860C82A8A059794D
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642211990913784e+12,"network":1.642179592e+12,"ticks":173925942.0,"uncertainty":3215335.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"132459510166079 96"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\9a56d51c-1ad0-46a0-83a1-a14e6fc34019.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	201886
Entropy (8bit):	6.073787764652342
Encrypted:	false
SSDEEP:	6144:eZhzKWygeGkVGFHhk9Ff5aqfIlUOoSiuRB:eXHygeGQGFH4fKoK
MD5:	A17F0CD58E6982444DC9774253BBFC13
SHA1:	69D65A5523EE31461C16303E07C01C42AD3E4213
SHA-256:	5B246B9DCB2BC0FE367C31ED94081A9C223088DBBD86171D857E76FF1105BDBA
SHA-512:	B6235D99D4422297F9F891AB514A984C238FF201EF0DB40C80D525655A983201DB70B222F5DE974A2C7807AECE0D7E8355A7F157A459A8761E3ACB2A4E08E2E7
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.642211990913784e+12,"network":1.642179592e+12,"ticks":173925942.0,"uncertainty":3215335.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799055175"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	40
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1n:+ftlE1n
MD5:	BD4642AD6C750A12D912B20BCB92E14D
SHA1:	C549F0F48FDD4FBC62E51AC26D7E185160CE2123
SHA-256:	4FD71FE78DFE203137C89C9FB0734358FF432F2BC83338112DC7B830F9B30F2C
SHA-512:	04410D12EF327614C3AF1251C9906BFEB2977211A7F53CBB08A8C01F9465A382CD001E51AB936A0D196D359F1DECDDAEAF5E7D1DBD49CE5F4FF91BF5C332B6CF
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Preview:	sdPC....................s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0fc95c24-a8c0-4351-879e-9c25d20d841a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	203
Entropy (8bit):	5.357931438899175
Encrypted:	false
SSDEEP:	6:YAQNFd7mTNRE9RfSHJR8wXwlmUUAnIMp562SQ:YFmTo9RAJ9+UAnI5ZQ
MD5:	B4523F32354BD52E6EA676966F2F56D3
SHA1:	43F0896E81AF44ABB20BC6F6525AA3EAD1AD3B1A
SHA-256:	D03F780572A87B90143BED77BB9B94894A4BD0904B782884C4B4FC37160C2F8A
SHA-512:	0B2818DCDC66D9369EB001270C1C28AB5B39915A44D6E6171B8882B4FC46C037105BDF59C4CA6BB6A4BE4AF811AE3DE03068FDCA203D34DAE13CC9E512ABE A15
Malicious:	false
Reputation:	unknown
Preview:	{"expect_ct":[],"sts":[{"expiry":1673748044.155013,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts _observed":1642212044.155018}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\15f2de4a-b30c-4e97-b9f0-7abadcab161f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	15601
Entropy (8bit):	5.603016535905718
Encrypted:	false
SSDEEP:	384:xytxLlVczX31kXqKf/pUZNCgVLH2HfDFrU6ny43:ILlWb31kXqKf/pUZNCgVLH2HfxrUiy4
MD5:	93D6BF1469C6C4D2B98856E6A62AA03D
SHA1:	3169BEABF09A25AF7F37D5A1A4603E100B06E8C0
SHA-256:	683B7B0E632F4B1D890B3EFC0184B7EC5F731900293D30FBAF22B6ED72ABB910
SHA-512:	6CAF83508E48D2BBF6308FC3BC4948E90D0402C4E06B919A17B768F8DE963E2D3C012F9D2B2416EBB79BC44276AE1457E1FD1A89A8DC5DA8B57A4BAD4F4DD 6F
Malicious:	false
Reputation:	unknown
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13286685586190235","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1bb1a9ce-0df5-40c3-b01b-22e51eaf0fef.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	6421
Entropy (8bit):	5.057946674008993
Encrypted:	false
SSDEEP:	96:nBYa5o9pcKI1ok0JCvqRzbRLL8tkx27kWMk7kbMkTkQZMkBkLu49bOTQVuwn:nBYF9pci4CJbZ6kx4kWnkbnkaNkLnl
MD5:	B3A15759BE50845E8FF2C7A70AF5C518
SHA1:	B3C1B9B0B8A29643948BBAEFB348AA67A2455021
SHA-256:	099564691B9D122E1952F6A7168837B31DBA86AF7422F0C6F9443B54A7E86C47
SHA-512:	49B27AF18F0F510159F8F17A55B470BB540CE2C64DC2D5EC26EDAEEF1837EED4A9885DB721FAD9E0D6356C1328B7BC01217AA08759B2D46A6F9FF02E615ED0 C
Malicious:	false
Reputation:	unknown
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13286685589837284","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcom e_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top": 10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0 ","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1ee425c6-fed2-4742-a702-101af8a2f64b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	6436
Entropy (8bit):	5.058702222288133
Encrypted:	false
SSDEEP:	96:nBYaGo9pcKIZok0JCXRjRLL8KkB27kWMk7kbMkTkQZMkBkLuKAbOTQVuwn:nBYg9pc24XJZpkB4kWnkbnkaNkLA
MD5:	C7D80AD84036736F59651D9EA2173736
SHA1:	4C85301AED5731A2C8593F838FB9F33024B4826F
SHA-256:	405A01F86001F82C775F8BD83E7875495932AED3B54F5439D69DF1194F00E9C1
SHA-512:	58F8B9FA644A76EF10973B47D36AB44DDBCB744A16B59B543A7E885F2FB5D674185C650A463B0D87FCB774EBCF278F6ACC37B6732498EB3D994ADB8D0AC072 3
Malicious:	false
Reputation:	unknown
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13286685589837284","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1fa9df1c-c008-45b0-ab90-e29fc4135cd2.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	15427
Entropy (8bit):	5.60045079464293
Encrypted:	false
SSDEEP:	384:xyt8LlVczX31kXqKf/pUZNCgVLH2HfDFrUv6y4j:vLlWb31kXqKf/pUZNCgVLH2HfxrUSyY
MD5:	E8EA1A66268E606F7413F14F05E439C5
SHA1:	3F4CF906E87A6E1614CB17DBA58E9E20E06652B9
SHA-256:	0A13A0669348151690E1CAAEC5FF81849B7333C541E72C02F8B94A3E96D4D855
SHA-512:	5AC3B7ECA8043194531F1A01B26F37148DE0E57E75AC3830CC22AC1FC1CB3468B2631F97E0C630786EB425918948B995D19F3FBBC6FA93B2D36362B09037275A
Malicious:	false
Reputation:	unknown
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13286685586190235","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\24983b7e-0ca9-4ff7-9317-f4ca6c7a0134.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	6466
Entropy (8bit):	5.059047858826831
Encrypted:	false
SSDEEP:	96:nBYaeo9pcKIDok0JCAR0RtL8rkj2fk4OckKuUkQZMkBk1KEXbOTQVuwn:nBY29pcY4ASfgkjwk4nkK1katk1B
MD5:	4C235652D1B67B63BE8D6E8AE1C8A0A0
SHA1:	2C3EF68F466E6A479E1BB78B57C0BE28BAA72A95
SHA-256:	B7B2EA17D1A48F8CDD7FFEBFC4BEA5B69C8A973F2FD9770FEE1419B536EF0968
SHA-512:	8AD48A25A5A8C934AF157F87864DBEAEDFB581E114113EA51E284BD37711A2EF6C8984D6DE414B86D1F3FD26BFA8EF8F957F60A7DEA7618C1D3D8D0085D4BF 4D
Malicious:	false
Reputation:	unknown
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13286685589837284","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2a1fa16e-d47a-4078-a976-02ffc7ee4cf4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2a1fa16e-d47a-4078-a976-02ffc7ee4cf4.tmp	
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.31474210096592
Encrypted:	false
SSDEEP:	6:YAQNFdr09RfSHJR8wXwlmUUAnIMp5bHqSQ:Yx09RAJ9+UAnIy1Q
MD5:	3CD4B7FFA23B8358FC970DE67E2F25B6
SHA1:	B06A9713E7B7E256719E6BB0962C694F44CCCF23
SHA-256:	C0E160FA5FE5FBC81C34B4E6113008C90A0FD7D5830948C9C3644E733D5B7056
SHA-512:	C282156CB22B220BE92FBC2448DFC34EA0B9F3AF4D039792DE32E1C8BDD109CDDAB142F90E6DFC28160A07C70A4F5E8D89C8DE23F0FB228A20033C89310589 D
Malicious:	false
Reputation:	unknown
Preview:	{"expect_ct":[],"sts":[{"expiry":1673748011.146834,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1642212011.14684}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2a253b65-69ca-4624-843d-8ca1d46e60f6.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5710
Entropy (8bit):	5.023314353382551
Encrypted:	false
SSDEEP:	96:nBYCRX9pcKIPok0JCxRyL8GkmrrAkF1xkKSMkVbOTQVuwn:nBY49pcY4xEFkmrkkFrktJ
MD5:	678EDCFB8D81C3033FDE2FAB6945862B
SHA1:	15998A638BE010C32B339F243E7BA1222892D680
SHA-256:	5551DD53F33327CB133097A30AC75CD3EE546B06615FA9A313743AD2D83085E1
SHA-512:	93DF5EA9A0F05CF9C1B1CE6784052CBB2DD24A37258E4F8DF5C6E10BF96E784ABD3BCD2B801BA3B93C4C3251DF1300FA69455CD333103EC294B11D48134FF8 5
Malicious:	false
Reputation:	unknown
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13286685589837284","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2aa3f2e3-9ee1-47b1-a86e-883765e669f6.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	203
Entropy (8bit):	5.33511402783637
Encrypted:	false
SSDEEP:	6:YAQNFd/M2J4WE9RfSHJR8wXwlmUUAnIMp5+SQ:YBa9RAJ9+UAnIoQ
MD5:	53F4FAC9B0F0137EFAC140A82F465AE3
SHA1:	92320B13E4D64B0DDFEA6092D2362DBEE37AA92A
SHA-256:	60B735F4820092451FE2DDE0BD066C0B9B71E087ED5ECE4F956D481B526B7F97
SHA-512:	12D5C3708E54CD58C4EF8F5C1BD7ED82ECA212E448015C575FB1A92743DE8A5E8DE600150D070B3A8EF2A79FDE19F9B75BD44AEDFBC152AFF8659D1B1D9F3 E4
Malicious:	false
Reputation:	unknown
Preview:	{"expect_ct":[],"sts":[{"expiry":1673748003.214701,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1642212003.214708}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\59712dd3-f01d-4659-8be1-277572c9443a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3971
Entropy (8bit):	4.915856083788975
Encrypted:	false
SSDEEP:	96:JOXGDHazMxLrxpJ6VT1EzqONahrGH6M4Yabu2KfH:JOXGDHazMxLVpJ6VTKzqONahrm6hYeuJ
MD5:	B67ECE08A69125C00AF32C1926450DDF

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\59712dd3-f01d-4659-8be1-277572c9443a.tmp	
SHA1:	C0D4FDAD73DD7D8CCAB41C69189FDDF7EEFB8568
SHA-256:	33A4E10325AC13AB35C188F2CCD13565F58987C0C726534B7ACE13209C3B6FB7
SHA-512:	7D0ED33640350A807DDFC1C86387AE2D292ABC5DA25413D23B8FCC5AC874C476305989F7B76337FA3F911D9F47BC2E359161C2967E9E8A79DEC0D772AA64FB D
Malicious:	false
Reputation:	unknown
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13289277591908025","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13289277591912361","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13289277592147257","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"e

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5d95fd30-ea03-4a19-9ab3-9eee3d6eae4b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	6422
Entropy (8bit):	5.052593361236239
Encrypted:	false
SSDEEP:	96:nBYVTo9pcKIbok0JCOR/mRWL8mka2mkR1BkbMkskF19kkO7bOTQVuwn:nBYC9pc44O4YVkadkRHkbYkFnkk0
MD5:	7B4C7F35A417823BFF8D31528D72EFA3
SHA1:	49C44FE62A00FC648ADE27460C4C817EFF4519D2
SHA-256:	A50074F6E8353EBA1224DF5019DF9D97D4587643E9BBFC073871DF64DFF42B93
SHA-512:	B3E90B481469790E3F34C2180F3E068831A9F453874A20829CE9A1823E41CC4FE2FC5076D4E5A29B4B740D8A58ACB1692D04B24D633A2B837095DB3F7E39C5E0
Malicious:	false
Reputation:	unknown
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13286685589837284","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":false,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\71d92515-c24b-458c-b276-9b0491b8ca4b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	15774
Entropy (8bit):	5.6057420139077605
Encrypted:	false
SSDEEP:	384:xytxLIVczX31kXqKf/pUZNCgVLH2HfDFrUVpy4q:ILlWb31kXqKf/pUZNCgVLH2HfxrUfy5
MD5:	6CE97826B87CDF05446E665F07CCB74A
SHA1:	C8F838DEDFC2F64234BD8C504D581927CDD073EB
SHA-256:	2D5A0B6971DA28B867E461C8EA65410D8C12F699D37A283A9BA6F5D831A91B75
SHA-512:	39744507D8352B7E7025889791982BDC3217C5156549AC871921A9F2D824AEAFB0AF61A2533A9CE979AFD2BA8A7E00EB565C3DDB8B84FAF10FE285F0A98ECC0
Malicious:	false
Reputation:	unknown
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13286685586190235","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	190
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlXNQxlXNQxlXNQxlXNQxlXNQxlXNQxlXNQxlXNQxlXNQxlXNQxlX:qTCTCTCTCTCTCTCTCTCT
MD5:	BD4367115C311692E06B63F1793B0624
SHA1:	CD807FEF06588E7C56FDB1A3A2CE15EF04955A16
SHA-256:	46ED76C989FA492AF602D813EAF61C17EDD71251674807A443B8F9CCC988292A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
SHA-512:	98E63595B75951B719868396E11CA9153B7B987DD9737E3DEC67E067C9A68AB706FE993BDB8DB86D664D7353D9DC7D742D10430DDD0FE5F0847C687FCB257E5
Malicious:	false
Reputation:	unknown
Preview:	.f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	unknown
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlXNQxlX:qTCT
MD5:	51A2CBB807F5085530DEC18E45CB8569
SHA1:	7AD88CD3DE5844C7FC269C4500228A630016AB5B
SHA-256:	1C43A1BDA1E458863C46DFAE7FB43BFB3E27802169F37320399B1DD799A819AC
SHA-512:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985DF
Malicious:	false
Reputation:	unknown
Preview:	.f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.244677970975067
Encrypted:	false
SSDEEP:	6:MIrZ2oE9+q2PWXp+N23iKKdK25+Xqx8chI+IFUtqVTIrnFhJZmwYVTIr49VkwOWM:MIm9+va5KkTXfchI3FUtuIrvJ/0Ic9V6
MD5:	293400E54E2BC9EDDC14547FA613B4CE
SHA1:	237634D5D9C8083172FE7858AF649996E576D88C
SHA-256:	520C45199E0D25EE23090033AA865C3E7AE73933D98AFB6480833D9C7ACBDA77
SHA-512:	F93DDA68C8D0C4E5A780D2B22F93317FDF6F6BE456B2D41E2CDB59BC6330C700D05D2B5F85F1E70689C15D92510D48E372313D126A5B88B2019729AF4E25FB7
Malicious:	false
Reputation:	unknown
Preview:	2022/01/14-18:00:17.777 18dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/01/14-18:00:17.882 18dc Recovering log #3.2022/01/14-18:00:17.883 18dc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.244677970975067
Encrypted:	false
SSDEEP:	6:MIrZ2oE9+q2PWXp+N23iKKdK25+Xqx8chI+IFUtqVTIrnFhJZmwYVTIr49VkwOWM:MIm9+va5KkTXfchI3FUtuIrvJ/0Ic9V6
MD5:	293400E54E2BC9EDDC14547FA613B4CE
SHA1:	237634D5D9C8083172FE7858AF649996E576D88C
SHA-256:	520C45199E0D25EE23090033AA865C3E7AE73933D98AFB6480833D9C7ACBDA77
SHA-512:	F93DDA68C8D0C4E5A780D2B22F93317FDF6F6BE456B2D41E2CDB59BC6330C700D05D2B5F85F1E70689C15D92510D48E372313D126A5B88B2019729AF4E25FB7
Malicious:	false
Reputation:	unknown
Preview:	2022/01/14-18:00:17.777 18dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/01/14-18:00:17.882 18dc Recovering log #3.2022/01/14-18:00:17.883 18dc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\000\t\.usage	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	1.4575187496394222
Encrypted:	false
SSDEEP:	3:ZlKwQsl:W
MD5:	35A6C3B4FE838413993C88D9DB65C73E
SHA1:	FBC0F9716FCDC03C7FCF908FED2C5ED73A5452F6
SHA-256:	DA74921979C4034FB77F61A6295C7C4D9A2196C831760D546E36AD959F240D23
SHA-512:	6AAD96386A306AFC8DFE170B4A84B7591E2F98F11FBEB5F81456E9CE806D3A7734B962F174E6B1904A23CE395F69C5809EF52B851BC0B5B207CB21BB974158D
Malicious:	false
Reputation:	unknown
Preview:	....FSU5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\000\t\Paths\000001.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	unknown
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\000\t\Paths\CURRENT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\000\t\Paths\CURRENT (copy)	
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\000\t\Paths\MANIFEST-000001	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	41
Entropy (8bit):	4.704993772857998
Encrypted:	false
SSDEEP:	3:scoBAIxQRDKIVjn:scoBY7jn
MD5:	5AF87DFD673BA2115E2FCF5CFDB727AB
SHA1:	D5B5BBF396DC291274584EF71F444F420B6056F1
SHA-256:	F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4
SHA-512:	DE34583A7DBAFE4DD0DC0601E8F6906B9BC6A00C56C9323561204F77ABBC0DC9007C480FFE4092FF2F194D54616CAF50AECBD4A1E9583CAE0C76AD6DD7C23 5B
Malicious:	false
Reputation:	unknown
Preview:	.|.."....leveldb.BytewiseComparator.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\001\t\.usage	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	1.4575187496394222
Encrypted:	false
SSDEEP:	3:ZlKwQsl:W
MD5:	35A6C3B4FE838413993C88D9DB65C73E
SHA1:	FBC0F9716FCDC03C7FCF908FED2C5ED73A5452F6
SHA-256:	DA74921979C4034FB77F61A6295C7C4D9A2196C831760D546E36AD959F240D23
SHA-512:	6AAD96386A306AFC8DFE170B4A84B7591E2F98F11FBEB5F81456E9CE806D3A7734B962F174E6B1904A23CE395F69C5809EF52B851BC0B5B207CB21BB974158D
Malicious:	false
Reputation:	unknown
Preview:	....FSU5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\001\t\Paths\000001.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	unknown
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\001\t\Paths\CURRENT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\001\t\Paths\CURRENT (copy)	
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	unknown
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\001\t\Paths\MANIFEST-000001	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	41
Entropy (8bit):	4.704993772857998
Encrypted:	false
SSDEEP:	3:scoBAIxQRDKIVjn:scoBY7jn
MD5:	5AF87DFD673BA2115E2FCF5CFDB727AB
SHA1:	D5B5BBF396DC291274584EF71F444F420B6056F1
SHA-256:	F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4
SHA-512:	DE34583A7DBAFE4DD0DC0601E8F6906B9BC6A00C56C9323561204F77ABBC0DC9007C480FFE4092FF2F194D54616CAF50AECBD4A1E9583CAE0C76AD6DD7C23 5B
Malicious:	false
Reputation:	unknown
Preview:	.|.."....leveldb.BytewiseComparator.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\000001.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	unknown
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\CURRENT. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	unknown
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\MANIFEST-000001	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	41
Entropy (8bit):	4.704993772857998
Encrypted:	false
SSDEEP:	3:scoBAIxQRDKIVjn:scoBY7jn

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\File System\Origins\MANIFEST-000001	
MD5:	5AF87DFD673BA2115E2FCF5CFDB727AB
SHA1:	D5B5BBF396DC291274584EF71F444F420B6056F1
SHA-256:	F9D31B278E215EB0D0E9CD709EDFA037E828F36214AB7906F612160FEAD4B2B4
SHA-512:	DE34583A7DBAFE4DD0DC0601E8F6906B9BC6A00C56C9323561204F77ABBC0DC9007C480FFE4092FF2F194D54616CAF50AECBD4A1E9583CAE0C76AD6DD7C23 5B
Malicious:	false
Reputation:	unknown
Preview:	.|.."....leveldb.BytewiseComparator.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8850
Entropy (8bit):	6.532622194033951
Encrypted:	false
SSDEEP:	192:81UDo/PmrzTVvFU0S9fRL5G1FPdg5LT71rC:2N/MvFUBJR5AFPdgC
MD5:	3F3E8002F3F113C2036B7F4922F6A4F1
SHA1:	952356D2E240DFA0A74DF5C0196976899BE95235
SHA-256:	E4B8141AA2174036ACE9BFAB0FA84C39E6774AA48455A0C30AA76751DCADDD0C
SHA-512:	D34362FFDD16A19413C69B8325A5A6C4EEE9223F649344F7FCA8313B461A026B85EB128D83C9218D113AD8493BE55C3A2501B862E8D3D30B37504C4F1D48DD5
Malicious:	false
Reputation:	unknown
Preview:	....."...P..1620783..allow..com..false..http..press..syncedcookie..vexacion..z..1642179603. 409903015c2b7ed6e92e0d4c6dd27795..4662709..4662728..505900524 751835698..https..l..myhypeposts..pz..s..ssk..svar..tb..wgyvpknmpvy53zb..3v3cj5letupakyxz6td..afu..kw..php..redirect..rid..var..zoneid..3..1339680..1642179600. 3af9b8dcd0ec704c87dac0b0bdef5110..505900515532763711..id..1851483..true..1642179593..505900484117418050. d610e53a03bbe0e8e47c68d23c28437c..1 851513..505900483718967923..1492888..505900482712334729..1294231..brand..gearbest..now..popular..promotion..sale..stores..1308..45687009..505900482569 728225..bestseller..cid..html..lkid..rdk..rk3..special..www..1343177..1642179592. 2c5bc1308d1f2e08e4319e64656e2c76..505900482569728021. 7e872dab99d78b ffc4aa0c1e6b062dad..b1fsmdd9m..key..profitabletrustednetwork..4263119..directdexchange..jump..next..r. a971bbe4a40a7216a1a87d8f455f71e6..e2q8zu9hu*... P....1294231.....1308.6....1339680. ....1343177.A....1492888.,....1620783.....164217959

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_myhypeposts.com_0.indexeddb.leveldb\000001.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	unknown
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_myhypeposts.com_0.indexeddb.leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6090
Entropy (8bit):	4.251860817316623
Encrypted:	false
SSDEEP:	96:zlN7RjjJ7RvApY1nZBBghCSfyk67FkejjdqA1uTV:5N7RjjJ7RvApGZBGnQFbPdqmc
MD5:	7E9584F772922945100FF742E8B6E92B
SHA1:	185779E744321C8F6815FE199AEF647D497DCF7A
SHA-256:	611EEBF7FF0D0E282DE1977184D10C9BF789B32A3E16B79F03A20E49C2B24712
SHA-512:	41B929F38E89BC0FCFD461DEA60990233A28810693033A459BF181043C5982A4A976D8C1465B8C634BD596C4D8C09400CEA1910C3FACF4331543E640EC5E0BA6
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_myhypeposts.com_0.indexeddb.leveldb\000003.log	
Preview:	. ...2....(.o"...................................$...x.......................M.......h.t.t.p.s._.m.y.h.y.p.e.p.o.s.t.s...c.o.m._.0.@.1..s.w.D.a.t.a.b.a.s.e......................n.......................C..... ..h.t.t.p.s._.m.y.h.y.p.e.p.o.s.t.s...c.o.m._.0.@.1..r.9.0.d.b...................T..n.......................C.......h.t.t.p.s._.m.y.h.y.p.e.p.o.s.t.s...c.o.m._.0.@.1..d.g.y.e.3....................X.p...... ....E.......h.t.t.p.s._.m.y.h.y.p.e.p.o.s.t.s...c.o.m._.0.@.1..m.5.j.l.5.i....................Z..n.......................C.......h.t.t.p.s._.m.y.h.y.p.e.p.o.s.t.s...c.o.m._.0.@.1..n.q.k.7.h...... ....#*..V............................2.................................2...2....c.s.u.s.m......2........v.a.l.u.e......2..........2..........2..........2..........2..........2.......... ...c.s.u.s.m........2.........2...........................2...................2........2......

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_myhypeposts.com_0.indexeddb.leveldb\000004.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	10171
Entropy (8bit):	5.089689282811738
Encrypted:	false
SSDEEP:	96:cddqx8BvF7czO18GYJGFYNEvx9xKDNtBjmjSu91H78P/kxWd:cddqxQvFUzGFWtBjmjSu91H7KkY
MD5:	7582FE29E7FCF420D82924A375E06AFE
SHA1:	369C6A22D98ED7A3C1D0A8BE4C222FBAD8DB6028
SHA-256:	8F8E3B493E43BA23A12D08138AB7141A4B38E1C7823BAA2BE2ACE16F07B59324
SHA-512:	C31A052EC33E467A88A17EDE293463D420E87AA753A5F7B083258BD9FEFC1AB3C4CBE7D46286DF7F5964CAC18F8F1E4A8C23E718082037CEC95B2D56E548D7A
Malicious:	false
Reputation:	unknown
Preview:	..&.V............................2................................2.........................".n.......................C......h.t.t.p.s._.m.y.h.y.p.e.p.o.s.t.s...c.o.m._.0.@.1..6.r.a.v.e....................xu................ ....2....l.1.r.d.t......2........v.a.l.u.e......2..........2..........2..........2..........2..........2............l.1.r.d.t.......2.........2..........................2...................2........2...................2...... ..2...................2........2...................2........2...................2........2...................2........2...................2........2...................2........2......................l.1.r.d.t........................2.....\.'. ....2................2...S......................2................2................2................2................2................2................2................2................2................2................2................2.... ....2..Z.E.K.........

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_myhypeposts.com_0.indexeddb.leveldb\000005.ldb	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3505
Entropy (8bit):	6.208091236622558
Encrypted:	false
SSDEEP:	96:FybwppnVtWgVTZqE4SDzvY4O4RiwV/ROB:Fybw3neEzDDYZ4RlQ
MD5:	A68F85A9C8868D7A20C5FFEBDDEA1DA5
SHA1:	397CDE60F4FD7400546DA1BF0B95C98659FDF8D4
SHA-256:	6E8559422E2E89DB4E75C20FF6EE249F46DCBB337BBF9E53ACEF10EF70122408
SHA-512:	F71A24D25FD71B7877849DA32EB3FDB7D82512C215A619184EDA97C5DCE63AFA9C12C48D5828A7BC08F7C598BA2681A5BCF9C612ED50234D0B63B99E8D94219
Malicious:	false
Reputation:	unknown
Preview:	. ...@........................2...x$........................y.........s............;.$.9.%.........29....9..... .2.......?...........2?....?......_.$.x.I......=..29....9...... .r.$.9.n.....Bb..29.....(...$.-...-g....>..!....w.N.c.s.....Bi..2c...:c.-..c......B...JN.=.:N.-..N...N....JN.=q:N.M..N.........N.......2..=W.... .2............................l...t.r.a.c.k.S.t.o.r.e.......*... ....5 2..........."....."..........."....."..........."....."..........."....."..........."....."..........."....."..F2......&.1.....1......................!.............z...... ....9..0.!...../.......a.,...c.s.u.s.m%..1. ....5..2...".-...")..3...",..."")..4...".+..."Yb.....5.&.1.*...1!....6...".)..."..%..7...".(..."........8...".'...")..9..!..&..%....-..:..!.....%....1...9....!.............a.$...e.d.6.b%..............%.U^.Z.....&.1... ..1)......"....."))......"....."i9....."....."))......"....."))......"....."))......"....."")..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_myhypeposts.com_0.indexeddb.leveldb\000006.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	17312
Entropy (8bit):	5.24992160599379
Encrypted:	false
SSDEEP:	96:d30KLuWHrKxj4C+LR8+oAmCTGE1oYrP4mGlFy6FIe1lg7hOcUMotnhHF5:F0KLuL94C+S9FcN4s6FX1KkhMotnhHF5
MD5:	AB5B509E204913A095E67E21803A50CC
SHA1:	36C970A714BC2975E55A79BFE5A7A0EB99E97EA9
SHA-256:	443A29C59395CC1B38CFFC5E88B2C830AF8ACC753B5BBF9FBFE57F40DAD342EE
SHA-512:	C52987959A16EFDF613B85695808E2FD3B973885DC0AB1F26690BE957CC482E66E3B0FFC6782C37DDC56C3F445BF6D5AA6D1F8EFB6AE26A44C1B5FBFC321FB0
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_myhypeposts.com_0.indexeddb.leveldb\000006.log	
Preview:	.r>.....2.....Ql.....q.u.a.l.i.t.y.F.o.r.m.....2.....2.....#.!.....q.u.a.l.i.t.y.F.o.r.m...ra.k.....2.....q.u.a.l.i.t.y.F.o.r.m.....o".IMI.".SWI..".SHI..".SAHI..".WXI.".WYI.".WWI..".WHI..".WIWI..".WIHI..".CWI..".WFCI.".PL"..https://myhypeposts.com/?s=505900587444097862&ssk=f3317077d3774f5218c1e8cb4ad6ad5c&svar=1642179618&z=1851513&pz=4662709&tb=4662728&l=WGYVPKNMPvY53zb".DRF".".NPI.".PTI.".NBI.".NGI.".NWI.".CFI.".IXF".NAVLNG".en-US".ISTF".WGL".Google SwiftShader".HILI.".AAT{.....2..B.....(...$.....2.....2.....2.....q.u.a.l.i.t.y.F.o.r.m.....o".IMI.".SWI..".SHI..".SAHI..".WXI.".WYI.".WWI.".WHI.".WIWI..".WIHI..".CWI..".WFCI.".PL"..https://myhypeposts.com/?s=505900484117418050&ssk=d610e53a03bbe0e8e47c68d23c28437c&svar=1642179593&z=1851483&pz=4662709&tb=4662728&l=WGYVPKNMPvY53zb".DRF".".NPI.".PTI.".NBI.".NGI.".

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_myhypeposts.com_0.indexeddb.leveldb\000007.ldb	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4902
Entropy (8bit):	6.450336956439142
Encrypted:	false
SSDEEP:	96:3f5qD2uEyAgDVIrt5/RWFD2djoo2XwiMwAOmWG3F7ZA+5cMpq:PgdVCmDkooIwJw2ZCMpq
MD5:	C22E240DE7C402E56E59D2B09D67D011
SHA1:	2E28C942EE791682DE1CA077FB06244FA04295F9
SHA-256:	A0AE03AAB59A749AE3E74F57706BBA99CE44239EFE7F4078B10B0DE9CC55A9ED
SHA-512:	5C2706521DF232453A495082624C6FA8FF55BA5D5C9FBE622BE58DDB14FBA143E4690E270450D0F08FB25DDBCE6FB5BD9E34C9E24737925B5B3B86850A4503D
Malicious:	false
Reputation:	unknown
Preview:	.!$...../..... .....$.....2.....3.....9.....P.....#.....2s....s.....2.....*.?.p.....d..2?....?.....$.9.....B ..29....9 ..(...$...~.....>.....N.c.*.....B%..2c.=N:c....k.c...c...V.N.c.@.....4..2c.....b.$.9.^.....BY..^9.:..Q.....N5.....B...2j..i.....N.....B....c..c.B...JN.].:....B.....B...JN.].:N...BN....N...JN..M.....N.....2B...UH .....A.D...l.1.r.d.t.....+.....+.....+ 2.....".>".....2.~....1.....S.....".>".....".>".....".>".....".>".....".>".....".....!..... ....q1...1.....R. ....|.....q.u.a.l.i.t.y.F.o.r.m.....,.....X.....-.....12.....B.....A6....E6...A6 k.h.4.x.4E6.. .....%....U6.....".....".....".....".5:.....&.1.....1I6.....".....!.....".....!6.....".....!6.....").....E6...M6....A6....E6

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_myhypeposts.com_0.indexeddb.leveldb\000008.ldb	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2236
Entropy (8bit):	6.380801396069204
Encrypted:	false
SSDEEP:	48:3DNAAsR4L8ExsnOKDm86nsyhN8Wr2/1ItKMA2d+Q4c:3xAAi4fmnOWm86syh2KuO4w+Y
MD5:	91AFBE42D07ECAB1D7AEA0438A7BB6F7
SHA1:	091F88ACD37F16461C5EFA17C806C640CB715EBC
SHA-256:	541183348841E92735F1AAC1DA71FE1049E6C1B4A1850B81DB984F044E63CDD5
SHA-512:	D47B65747E27EB1F9CEBFEF95EA28F2FF7C8C8DCFBE41CC4764AB656B2023E7E6AA84873D16BF2346F9866FCA40E37113C7CFE02C644B9F703AAA688F5B2B770
Malicious:	false
Reputation:	unknown
Preview:	..../.....(.....2....$.....B.....-..... ..(...$.....>.....B...JN....N..:N...BN....N....JN....N..:N..-.....d.....5.z.5.o.2.....2 ...6 ..... D.....2.....c...#.c...c 4.x.g.h.f.c..2 ..c. ..... .c...c.....d.....$.O.....q.u.a.l.i.t.y.F.o.r.m.....o".IMI.".SWI..".SHI..".SAHI..".WXI.".WYI..HWI..".WHI..".WIWI.....HI..".C...FCI.".PL"..https://myhypeposts.com/?s=505900515532763711&ssk=3af9b8dcd0ec704c87dac0b0bdef5110&svar=1642179600&z=1339680&pz=4662709&tb=4662728&l=WGYVPKNMPvY53zb".DRF".".NPI...T...NB...NG...W...LCFI.".IXF".NAVLNG".en-US".ISTF".WGL".Google SwiftShader".HILI.".AAT{.....A.%...-.....e7.2..).A.....0.....a..<I....h.t.t.p.s._.m.y.h.y.p.e.p.o.s.t.s...c.o.m._.0.@.1..1.5.0.5.h.0.\D.8....6.r.a.v.e.....8.:..g.6.e.n.g...,8.:..n.q.k.7.h...)<.:..r.9.0.d.b....d.8....s.w.D.a.t.a.b.a.s.e.....n...{.. .....x.....m.....2...|....t...c.k.S.tE..e.....}. .....~.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_myhypeposts.com_0.indexeddb.leveldb\000009.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6267
Entropy (8bit):	5.191486249939528
Encrypted:	false
SSDEEP:	48:Ca2/QC9O5H+7vgDxFp0IhoCiLZo1/e09Qfh63sn7iWaynXZnY3lCTkLDxF4r6Jqk:EEg1sCyyXFhQuWJqvM
MD5:	0C7F6DF290AB9642C857B1EBE763411F
SHA1:	5F5882C5A7FDC47F1F763953835A56B99FEF08CC
SHA-256:	92A20640D6D0AC5699220703B0F99ED660BA687DECCA4015008E7D0F5707E860
SHA-512:	0F6DF0E6EC39AFD1330F4CF803ADB9C8768A0059A78695B37206764A6F0BDD935F99520A3369BF4699E20CC071FF416F082B780E3FEA51CFEFD1FA74B35100D4
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_myhypeposts.com_0.indexeddb.leveldb\000009.log	
Preview:	$..1...s.....2.....t.....2./.....2./.....C.....h.t.t.p.s._.m.y.h.y.p.e.p.o.s.t.s...c.o.m._.0.@.1..q.q.w.v.r.....2./.....J.H.C.....h.t.t .p.s._.m.y.h.y.p.e.p.o.s.t.s...c.o.m._.0.@.1..q.q.w.v.r....s..<..x.....2./.....2./.....sg....{.....!...|.....2.0.....2.0..... .....C.....h.t.t.p.s._.m.y.h.y.p.e.p.o.s.t.s...c.o.m._.0.@.1..4.z.i.m.m.....2.0.....J.H.C.....h.t.t.p.s._.m.y.h.y.p.e.p.o.s.t.s...c.o.m._.0.@.1..4.z.i.m.m....<..... ....2.0.....2.0.....M..n.....b.D.....2.1.....2.1.....C.....h.t.t.p.s._.m.y.h.y.p.e.p.o.s.t.s...c.o.m._.0.@.1..x.m.l.6.p. .....2.1.....J.H.C.....h.t.t.p.s._.m.y.h.y.p.e.p.o.s.t.s...c.o.m._.0.@.1..x.m.l.6.p...6.F.<.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_myhypeposts.com_0.indexeddb.leveldb\000010.ldb	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7688
Entropy (8bit):	6.596335675465701
Encrypted:	false
SSDEEP:	96:o9wbPCvlvGRL+EyajfUJ1IT+UJJjaXin3El46b3Z8nqGAW++AvctmSKvjhbaw1:oC7L2O41IT+KaXin3/5bwqR8jehbaw1
MD5:	252D8F030A7475323013B93B54D7F789
SHA1:	2F92CADEA05748D7D7A48F3DB983A2E0EA24059B
SHA-256:	0C5705124ECE6038306AD35C94EF379F6B8D24DC15805EF44CF84ACC74873B58
SHA-512:	7369AEAEEF5F4371887E5060F02322C97F6C21DAA89B53AF7EB57120320206FF8EB7617ABAE82EE4C78DF6F7B467EE84B3E78EE4BEBA11A68E1A49939886A988
Malicious:	false
Reputation:	unknown
Preview:	. (.....C.....?.....(.....2.....a.....t.....".....X.2.....s...B..4..... ....(...$.....>.....&.j.....c.....c..c...*.c...Y...B....c..c.. ...c...Y...B....c..c...2.c. .Y...B....c..c...6.c.(.Y...B!..2...$...k..k...:.k.0.Y...B,...c..c...>.c.8.Y...B4...c..c...R.c.k.Y...B<...c..c...J.c.T.Y....H..2c...u..... .^.9.w./....h..29....9..u..!.N.?. f.5...Ba..2?..x:....A;..q...a..".b.c...Y...B...2c...:c....`2c....c.#...N.....2X.....$...$...B...2.....%...N.....2X.....&...$...B...^.:....!.2....!..'...N.....2X.....U..(...*...B...24.....).. .N...B....X..X.*...N...B....X..X.+...N...B....X..X.,...N...B....X..X.-...N.....2X...5.....B...i.^$.:h...Ae2h... .....X.....G..2...3.....3.....-.....#...h...!.....q.u.a.l.i.t.y. F.o.r.m....[...:.....E.....p.....p....&.p....p. .:.....f.....b.....o".IMI.".SWI..".SHI..".SAHI..".WXI.".WYI

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_myhypeposts.com_0.indexeddb.leveldb\000011.ldb	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3727
Entropy (8bit):	6.49675167988841
Encrypted:	false
SSDEEP:	96:w/fGsLn12bx4LdKICHmdHoNetqRJq082nCk:wHGs4bx4LdKIC+HieMR
MD5:	4AE99AA0F9E59E3BCD952F67A388BF51
SHA1:	2C476C0B2A826FE80702033B52B6162419B5DAD9
SHA-256:	C3E4DC65954D5964A69E4EF00950DC4F34156514D035A1AADB1084CC30102542
SHA-512:	59E28C1208DFB7450FB92721503059826F2D62F94FC04D312EF653F0BBE2F88FA9C266E9FB52D7850811A97FCC9A987902C73825F1952F95C898671990C30633
Malicious:	false
Reputation:	unknown
Preview:	. ...(.....2...3$.....#.....$.....%.....&.....'.....(.....).....*.....+.....,.....-.....B..... ..(...$.....>.....2.#.....iX.....#$.....%..!.....q.u.a.l.i .t.y.F.o.r.m.....1..b1.....o".IMI.".SWI..".SHI..".SAHI..".WXI.".WYI...W.(,WHI.".WIWI.....HI..".C...FCI.".PL"..https://myhypeposts.com/?s=5059005875070117 39&ssk=f3317077d3774f5218c1e8cb4ad6ad5c&svar=1642179618&z=1851483&pz=4662709&tb=4662728&l=WGYVPKNMPvY53zb".DRF".".NPI...T...NB...NG.....LCFI .".IXF".NAVLNG".en-US".ISTF".WGL".Google SwiftShader".HILI.".AAT{.....!.D.....2.....%1.....).d.....z.0.0.w.p..... ..... 2.....>.....>.....>.....>.....>..... ...>.....>.....&1.....!).<.....j.0.u.7.f...-..2./....2/..../..... %...-.....'.r.....#.....L.....J.E.....h.t.t.p.s._.m.y.h.y.p.e.p.o.s.t.s...c.o.m._.0.@.1..1.5.0.5.h.. ....y....`e..O.....e..(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_myhypeposts.com_0.indexeddb.leveldb\000012.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3951
Entropy (8bit):	4.958141632536597
Encrypted:	false
SSDEEP:	48:Ip8WICTParU3EONJarK956qxzu2/J/bD/Wi+nktHli1K/rwpeTYdEfl+:IfbarjEIExzu2/J/bD/6ktFpi
MD5:	28887AB06F5D577EA134B70FB30D1DAF
SHA1:	5E722200845AA218EBDDF0F2383EB9AD7BCB8B12
SHA-256:	CAB8742BE448B4A6E3A50EC8E45ABD69103AEC956FD8E1B47B9ED05E51F288CD
SHA-512:	AD8217FF6B13C8E07FA029E548460A1A60F90D9E4C15CA17281A38BC1DBBBDF0726994D917E854D848EA9E402C6EB3769BADA0E1DA14EF2E95918013764CA64 5
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_myhypeposts.com_0.indexeddb.leveldb\000012.log	
Preview:	.....2.....q.u.a.l.i.t.y.F.o.r.m.....o".IMI.".SWI..".SHI..".SAHI..".WXI.".WYI.".WWI..".WHI..".WIWI..".WIHI..".CWI..".WFCI.".PL"..https://myhypeposts.com/?s=505900695376130792&ssk=039f6dfa059502ca247bcb272925fa64&svar=1642179644&z=1620783&pz=4662709&tb=4662728&l=WGYVPKNMPvY53zb".DRF".".NPI.".PTI.".NBI.".NGI.".NWI.".CFI.".IXF".NAVLNG".en-US".ISTF".WGL".Google SwiftShader".HILI.".AAT{.....2.9B.....(...$.....2.9.....2.....2.9.....q.u.a.l.i.t.y.F.o.r.m.....o".IMI.".SWI..".SHI..".SAHI..".WXI.".WYI.".WWI..".WHI..".WIWI..".WIHI..".CWI..".WFCI.".PL"..https://myhypeposts.com/?s=505900691089547970&ssk=e5913e8a9df253b093df5b2b029e6db5&svar=1642179643&z=1339680&pz=4662709&tb=4662728&l=WGYVPKNMPvY53zb".DRF".".NPI.".PTI.".NBI.".NGI.".NWI.".CFI.".IXF".NAVLNG".en-US".ISTF".WGL".Google SwiftShader".HILI.".AAT{..9(Vn.....C.....h.t.t.p.s._.m.y.h.y.p.e.p.o.s.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_myhypeposts.com_0.indexeddb.leveldb\000013.ldb	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3302
Entropy (8bit):	6.533827910994587
Encrypted:	false
SSDEEP:	96:b+gR4wt6YOXN9hH8+h1iQOBp9CBv3lEskn7VzcUmWH:b+gRtjOX3++h1iQO8lEbZzTHH
MD5:	87A2430D3D0EF2A63D40724B4D5D57F0
SHA1:	3F8E8E0B612B8D4637D8BDF9ED3D1F4882005FA2
SHA-256:	5546C141A32CBCD552F5AD893867CE4A3A0D49310AC2CDD3E694AF264484D1C8
SHA-512:	3DE018B8AA7E4E355EB86E1449C7E92E313B931F94A7FA46A8E77E3944980040C04FBE7AA4D1B45CB4F8E563F1D0E272E13789CB84D2F1E1E4A36E96A1CD1294
Malicious:	false
Reputation:	unknown
Preview:	. (.....{.....x..$.....2.#.....$.....%.....&.....s.../.y.....t.....0...$....\|..2.....B.2.1...*.....24....4.....2...$...B...2..... ..(...$...h...%c....>.....3...N...B....X..X.4...N...B....X..X.5...N.....2X...5.....6...$...B...^..:6...!326...!6.7...N...B...2X....8...N...B....X..X.....2.#Q.....]....$.....%.-.....&.....'.<.....!...../.!..z.....!l....J..w....H.C...l...h.t.t.p.s._.m.y.h.y.p.e.p.o.s.t.s...c.o.m._.0.@.1..q.q.w.v.r.....u.^8.....0.....%2.....44.z.i.m.m.....}.^.....1.....%2.....,x.m.l.6.p...2.....^..!).....#2.....%t.!.....q.u.a.l.i.t.y.F.o.r.....0....1..b1.....o".IMI.".SWI..".SHI..".SAHI..".WXI.".WYI..HWI..".WHI..".WIWI.....HI..".C...FCI.".PL"..https://myhypeposts.com/?s=505900654292923296&ssk=a26a2db6b8611d

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_myhypeposts.com_0.indexeddb.leveldb\000014.ldb	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4478
Entropy (8bit):	6.5423037741806995
Encrypted:	false
SSDEEP:	96:JfEk96GfR3XGy+3LOBOJ9x7WzRugGB1Sn9sEHHl1DyUmUZv:JcW6WRmy+bO0DCzRuvSn9sM1+4
MD5:	C67C74D6296187D4F2A5359D43CDB1EA
SHA1:	0282CFF2161224D83D99045D9E24A5DC5AB8BB04
SHA-256:	3C843E28857D295B64108B9552791E02291E292E510D42344881432EE9AC682F
SHA-512:	6284B3F13FA0B0B28CA4DE6609BA592EF3785755138FE2E862BE5EAADB8ADBA4D426F9DA256060F874DE29969A3C92D1153309311D94891C580945EEBC0B64A
Malicious:	false
Reputation:	unknown
Preview:	."...........$.....,.....2...3$.....'...<....(.....).....*.....+.....,.....-.....s.v..../.y...0.....1.....2.....2.3.....4.....5.....6.....7.....8.....'.....X.....#(.....%..!.....a.s.k.G.i.d.r.a.t.o.r.....m..../.k./..b/..RK.....o".gidratorOAID" 9e0881623ede4761988854597c23d8e5".skipInstallF".okT{.....%*D.....2.....#).....:.....y.....#*.....#.....:.....y.....#!..2.+.....)...../.....:.....y.....#,.....#..8q.u.a.l.i.t.y.Fa0,.m.....0...u4V1.....IMI.".SWI..".SHI..".SAHI..".WXI.".WY..HWI..".WHI..".WIWI...HI..".C...FCI.".PL"..https://myhypeposts.com/?s=505900629496197269&ssk=d85215d55460398524e3fbcf7c224e17&svar=1642179627&z=1294231&pz=4662709&tb=4662728&l=WGYVPKNMPvY53zb".DRF".".NPI...T...NB...NG...W...LCFI.".IXF".NAVLNG".en-US".ISTF".WGL".Google SwiftShader".HILI.".AAT{.....A.2.....-1.....Qd.....d.z.7.i.f..... ..... 2.....>.....>.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_myhypeposts.com_0.indexeddb.leveldb\000015.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4518
Entropy (8bit):	5.04298641908171
Encrypted:	false
SSDEEP:	48:xFqFBh/Fd+8W+PKzyZnuWAFOtRbNJ3JltBxUUlDNx2/pms/sheoMkyN6sIKB:rkhjiYnjAFgVNJ3JltBxU+a/cVDeB
MD5:	57944BBFAAAD904799A5CDAF464A1167
SHA1:	84A1E157E0F274FB701F4EDD1B809464F3AC1E93
SHA-256:	1F0ED59E80D2BB0D4452DFC3660D564BFD60B9D54F3C43734E7D6D9FB786AD1D
SHA-512:	C3F19721715788E2E55E2491416612AC50D46D407F0EF4B1B023B4F1A22B59DA7A10409F7FFB50E8265141A76F0451A5EE10C0CAF6D50095E33ABC5FC678F76E
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_myhypeposts.com_0.indexeddb.leveldb\000015.log	
Preview:	v.9.V..u.....2.>.....2.>.....+....x.....2....x.a.w.6.2.....2.....v.a.l.u.e.....2.....2.....2.....2.....2.....2.....2.....x.a.w.6.2.....2.>.....2.>.....2.>.....2.....2.>.....2.....2.>.....2.....2.>.....2.....2.>.....2.....2.>.....2.....2.>.....2.....2.>.....2.....2.>.....x.a.w.6.2...l.....a.s.k.G.i.d.r.a.t.o.r.....2.<.....2.<.....#.!.....a.s.k.G.i.d.r.a.t.o.r.....W^.....2.....q.u.a.l.i.t.y.F.o.r.m.....o".IMI.".SWI..".SHI..".SAHI..".WXI.".WYI.".WWI..".WHI..".WIWI..".WIHI..".CWI..".WFCI.".PL"..https://myhypeposts.com/?s=505900702070239868&ssk=47f99a09ee92c199fb48945f8e680bf4&svar=1642179645&z=1343178&pz=4662709&tb=4662728&l=WGYVPKNMPvY53zb".DRF".".N

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_myhypeposts.com_0.indexeddb.leveldb\000016.ldb	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PGP\011Secret Key -
Category:	dropped
Size (bytes):	2382
Entropy (8bit):	6.354670846827625
Encrypted:	false
SSDEEP:	48:VC3c+1J69hSbx8SDPzu+MycJM9S40xDp/DgHp5NxjN1pPa6S:VCMwJ69ou8zlfz98xDp/QpTRjrS
MD5:	25388E3BEDAD9B5FB57B7FDFB15921B9
SHA1:	02A144172C00D26D3C8F45A5F82F80A2A4919377
SHA-256:	AB9152A9DFD4390A449EC2F574A918CA4F543E776872F6B57CD40DA05116E62B
SHA-512:	FC6FD022D8C834DBD537485E323BA2E17BAC682545EC524DD6BCD7B1C486081892B96772766851E26B7C4E1303C246A99188FCD25ABF4A23924D6F9A2F67E94
Malicious:	false
Reputation:	unknown
Preview:	..(.....=.....7.....$.....2.'.<.....(.D...).H...*.L...+.P...,T...-.`.....d...9.....B..... ..(...$.....>.....:.$.N.....).2.:....2`...`....:..$.....2.....B<..J$....=.6.N...B1..2|...:.....%,1.....'1*...;.X....(.....A.....B.....C.....).-.E...-.F.....G.....*.-.I...-.J....K....%...2.+.3.M...3.N.....O.....,.-.Q...-.R.....S.....-.-...U.....V.....W.....X.....Y.....Z.....[.....\....]....^.....,_.....a.....b.....c...../.-...e.....f.....#9.!.....!.....q.u.a.l.i.t.y.F.o.r.m.....A>.....1..b1.....o".IMI.".SWI..".SHI..".SAHI..".WXI.".WYI..HWI..".WHI..".WIWI.....HI..".C...FCI.".PL"..https://myhypeposts.com/?s=50590069108954797 0&ssk=e5913e8a9df253b093df5b2b029e6db5&svar=1642179643&z=1339680&pz=4662709&tb=4662728&l=WGYVPKNMPvY53zb".DRF".".NPI...T...NB...NG...W...LCFI.".IXF".NAVLNG".en-US".ISTF".WGL".Google SwiftShader".HILI.".AAT{.....!.D.....2.....:1.....).....a.D...h.l.s.0.j

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_myhypeposts.com_0.indexeddb.leveldb\000017.ldb	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4499
Entropy (8bit):	6.482217612705725
Encrypted:	false
SSDEEP:	96:seNq8+h18eoh5jjJ1x9Bd816yv9y7sUt6pw6AA:sAT+h18vB9Bd4cq
MD5:	3CB2AB2799A38505796875CAC884175E
SHA1:	2408A419A2FF6A63F5299ACC29C792543A100F4A
SHA-256:	D9A9312CF611C01D62A9AE380421B3F03045DB50EA062D05460A0BE2B5B03207
SHA-512:	7686854B4DC0D15AE97FA26E80AE2AE82D805A299CAC26B40127A196C839C3A81AD5B79BC1703AE40D080BAB115B78D5AF82FE25767FD72F759253CAF354843
Malicious:	false
Reputation:	unknown
Preview:	. .....$.....=.....,.....2...3$...../.y."....0.....1.....2.....3.....4.....5.....6.....7.....8.....9.....:.$.....2.;.....B<....."..... ..(...$.....>.....=.6.N...../.,...u..X.....0.....%.....e....J.....H.C...I...h.t.t.p.s._.m.y.h.y.p.e.p.o.s.t.s...c.o.m._.0.@.1..4.z.i.m.m.....}.^.....1.....%2.....4x.m.l.6.p.....^..!).....#2.....%t.!.....q.u.a.l.i.t.y.F.o.r.....0....1..b1.....o".IMI.".SWI..".SHI..".SAHI..".WXI.".WYI..HWI..".WHI..".WIWI.....HI..".C...FCI.".PL"..https://myhypeposts.com/?s=505900654292923296&ssk=a26a2db6b8611d56986c1a0e1dbb7ce3&svar=1642179634&z=1492888&pz=4662709&tb=4662728&l=WGYVPKNMPvY53zb".DRF".".NPI...T...NB...NG...W...LCFI.".IXF".NAVLNG".en-US".ISTF".WGL".Google SwiftShader".HILI.".AAT{.....A.D.....2.....#39...-.9.@.a.s.k.G.i.d.r.a.t!. .....m..../.k5.V/..K.)..I.gidratorOAID" 9e0881623ede4761988854597c23d8e5".skipInstallF".okT{.....y.....#...2.4

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_myhypeposts.com_0.indexeddb.leveldb\000018.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	938
Entropy (8bit):	3.8598505113259143
Encrypted:	false
SSDEEP:	24:NJgsSOCU+Cy6zcB0zxhrwGcackVJ5AFAn:NJgrb6zjzxGGRlean
MD5:	31A3DC31513AAE501FA0E101BE1C620F
SHA1:	62903A9C70879495F8DEA60C60CE8C3EA3665AB3
SHA-256:	8AC3B8009D567D7E4D6806E0C3E49FE909112EF356BFA2795ADEEE6324138007
SHA-512:	D3122E44B549AF8FC26E7298CE260D60C1D9D2790DD58F9BA92EB560FDA611657707B3AE35B440372212007BC4006BCFE8058A5AD88163E3500A4D50825D3F4D
Malicious:	false
Reputation:	unknown
Preview:	.....2.F.....2.F.....C.....h.t.t.p.s._.m.y.h.y.p.e.p.o.s.t.s...c.o.m._.0.@.1..z.i.g.5.s.....2.F.....J.H.C.....h.t.t.p.s._.m.y.h.y.p.e.p.o.s.t.s...c.o.m._.0.@.1..z.i.g.5.s.....<.....2.F.....2.F.....m{.....2.G.....2.G.....E.....h.t.t.p.s._.m.y.h.y.p.e.p.o.s.t.s...c.o.m._.0.@.1..7.3.k.l.y.g.....2.G.....L.J.E.....h.t.t.p.s._.m.y.h.y.p.e.p.o.s.t.s...c.o.m._.0.@.1..7.3.k.l.y.g...B..{<.....2.G.....2.G.....' f.....y.'.....2.0.....2.0.S.W.....2.1.....2.1.....2.....2.....2.....2.....2.....2.....2.....2.....p.m.f.7.x.....x.h.1.z.w.....x.h.1.z.w

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_myhypeposts.com_0.indexeddb.leveldb\000018.log

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.557126264231974
TrID:	• Win32 Executable (generic) a (10002005/4) 98.86% • Inno Setup installer (109748/4) 1.08% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02%
File name:	1nJGU59JPU.exe
File size:	767327
MD5:	aea21ab88cca720a34ec1c9c4794f82a
SHA1:	5241d6fd4013ec8251df46e231665471a8ca70db
SHA256:	498421bc4c78ba9bf7c9d669bd9958cf2c0c1cc89e94288800fe004400821ef3
SHA512:	9503ec3b595db2edee075254da608284a0ffbe33b4f86e3e703293f49c73ef7e5069454608ee23a9f3b3062ef3325e9bed0b4d9b6e8a7e3239942033eb400f38
SSDEEP:	12288:VQi3rNSH1v6m6URA3PhOop1hf39Wkv8xwJYyHDZ:VQi7NSH1ChhvpdUMYY
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	92ae923131328fd2

Static PE Info

General

Entrypoint:	0x40a5f8
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	1
OS Version Minor:	0
File Version Major:	1
File Version Minor:	0
Subsystem Version Major:	1
Subsystem Version Minor:	0
Import Hash:	884310b1928934402ea6fec1dbd3cf5e

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0x9d30	0x9e00	False	0.605295688291	data	6.63174764106	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0xb000	0x250	0x400	False	0.306640625	data	2.7547169535	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0xc000	0xe90	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0xd000	0x950	0xa00	False	0.414453125	data	4.4307330698	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0xe000	0x8	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0xf000	0x18	0x200	False	0.052734375	data	0.20448815744	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x10000	0x8c4	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x11000	0x5bf28	0x5c000	False	0.0497728430707	data	3.70186542619	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 17:59:06.175853968 CET	192.168.2.3	8.8.8.8	0xba32	Standard query (0)	onepiece.s3.pl-waw.scw.cloud	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:12.285691023 CET	192.168.2.3	8.8.8.8	0x731d	Standard query (0)	connectini.net	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:16.034671068 CET	192.168.2.3	8.8.8.8	0x2bd9	Standard query (0)	korolova.s3.nl-ams.scw.cloud	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:23.862294912 CET	192.168.2.3	8.8.8.8	0xcc56	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:24.636439085 CET	192.168.2.3	8.8.8.8	0xbedf	Standard query (0)	connectini.net	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:26.324240923 CET	192.168.2.3	8.8.8.8	0x7357	Standard query (0)	360devtracking.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:27.484349966 CET	192.168.2.3	8.8.8.8	0x3d7f	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 17:59:28.449507952 CET	192.168.2.3	8.8.8.8	0xa659	Standard query (0)	google.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:30.219702005 CET	192.168.2.3	8.8.8.8	0x28c7	Standard query (0)	connectini.net	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:38.205148935 CET	192.168.2.3	8.8.8.8	0xc754	Standard query (0)	google.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:39.573856115 CET	192.168.2.3	8.8.8.8	0x6378	Standard query (0)	delice.s3.fr-par.scw.cloud	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:51.559262991 CET	192.168.2.3	8.8.8.8	0xe57e	Standard query (0)	www.profitabletrustednetwork.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:51.590251923 CET	192.168.2.3	8.8.8.8	0x4572	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:51.591309071 CET	192.168.2.3	8.8.8.8	0x50cd	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:51.599661112 CET	192.168.2.3	8.8.8.8	0x40a7	Standard query (0)	www.directdexchange.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:51.673480034 CET	192.168.2.3	8.8.8.8	0xf47b	Standard query (0)	vexacion.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:52.250751019 CET	192.168.2.3	8.8.8.8	0x2709	Standard query (0)	propeller-tracking.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:52.251521111 CET	192.168.2.3	8.8.8.8	0x6b2f	Standard query (0)	my.rtmark.net	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:52.848311901 CET	192.168.2.3	8.8.8.8	0xc228	Standard query (0)	myhypeposts.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:52.940594912 CET	192.168.2.3	8.8.8.8	0xdd6	Standard query (0)	www.gearbest.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:53.477303028 CET	192.168.2.3	8.8.8.8	0xe227	Standard query (0)	order.gearbest.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:53.477361917 CET	192.168.2.3	8.8.8.8	0xe715	Standard query (0)	css.gbtcdn.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:53.775610924 CET	192.168.2.3	8.8.8.8	0x13d0	Standard query (0)	littlecdn.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:53.865844011 CET	192.168.2.3	8.8.8.8	0x259f	Standard query (0)	uidesign.gbtcdn.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:54.498920918 CET	192.168.2.3	8.8.8.8	0xb2d	Standard query (0)	cart.gearbest.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:54.499605894 CET	192.168.2.3	8.8.8.8	0x4ae0	Standard query (0)	analytics.logsss.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:55.614378929 CET	192.168.2.3	8.8.8.8	0x27f4	Standard query (0)	mc.yandex.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:55.651604891 CET	192.168.2.3	8.8.8.8	0x89cf	Standard query (0)	gloimg.gbtcdn.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:55.652194977 CET	192.168.2.3	8.8.8.8	0x340c	Standard query (0)	des.gbtcdn.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:55.872147083 CET	192.168.2.3	8.8.8.8	0x78d5	Standard query (0)	atzekromchan.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:55.878343105 CET	192.168.2.3	8.8.8.8	0x5405	Standard query (0)	yonhelioliskor.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.545088053 CET	192.168.2.3	8.8.8.8	0xff	Standard query (0)	login.gearbest.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.575033903 CET	192.168.2.3	8.8.8.8	0xc0a7	Standard query (0)	perf.logsss.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.600128889 CET	192.168.2.3	8.8.8.8	0x8ab1	Standard query (0)	review.gbtcdn.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.741909981 CET	192.168.2.3	8.8.8.8	0x59be	Standard query (0)	s.logsss.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.742604971 CET	192.168.2.3	8.8.8.8	0x1349	Standard query (0)	rum.logsss.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.826940060 CET	192.168.2.3	8.8.8.8	0x1026	Standard query (0)	user.gearbest.com	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:58.263587952 CET	192.168.2.3	8.8.8.8	0x28a5	Standard query (0)	cdntechone.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:01.941284895 CET	192.168.2.3	8.8.8.8	0xaeb2	Standard query (0)	datatechone.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:01.956765890 CET	192.168.2.3	8.8.8.8	0xe190	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:02.141746998 CET	192.168.2.3	8.8.8.8	0xba46	Standard query (0)	stun.l.google.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:02.634026051 CET	192.168.2.3	8.8.8.8	0x24db	Standard query (0)	cur.gearbest.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:06.819338083 CET	192.168.2.3	8.8.8.8	0x79b1	Standard query (0)	www.cloud-security.xyz	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:07.512303114 CET	192.168.2.3	8.8.8.8	0x93ed	Standard query (0)	nginx.1cros.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 18:00:09.087116003 CET	192.168.2.3	8.8.8.8	0x1cb0	Standard query (0)	tpx.tesseradigital.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:09.088449001 CET	192.168.2.3	8.8.8.8	0xf826	Standard query (0)	www.adsaro.net	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:09.252504110 CET	192.168.2.3	8.8.8.8	0x9c4a	Standard query (0)	oneimpress.io	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:09.861385107 CET	192.168.2.3	8.8.8.8	0xf051	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:10.602412939 CET	192.168.2.3	8.8.8.8	0xad30	Standard query (0)	goodnotification.net	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:10.732114077 CET	192.168.2.3	8.8.8.8	0x20b9	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:11.133533001 CET	192.168.2.3	8.8.8.8	0x70c0	Standard query (0)	glsdk.logsss.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:11.136516094 CET	192.168.2.3	8.8.8.8	0xaa75	Standard query (0)	affiliate.gearbest.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:11.363468885 CET	192.168.2.3	8.8.8.8	0xcf3a	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:11.575772047 CET	192.168.2.3	8.8.8.8	0xf53d	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:17.273499966 CET	192.168.2.3	8.8.8.8	0x9666	Standard query (0)	360devtracking.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:17.409063101 CET	192.168.2.3	8.8.8.8	0xf510	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:18.205861092 CET	192.168.2.3	8.8.8.8	0x3508	Standard query (0)	s.w.org	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:19.050473928 CET	192.168.2.3	8.8.8.8	0x6421	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:19.452752113 CET	192.168.2.3	8.8.8.8	0xe25e	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:20.252223969 CET	192.168.2.3	8.8.8.8	0x3466	Standard query (0)	connectini.net	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:20.802227974 CET	192.168.2.3	8.8.8.8	0x6acd	Standard query (0)	ad.admitad.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:21.062474966 CET	192.168.2.3	8.8.8.8	0x3f15	Standard query (0)	ma.logsss.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:21.101854086 CET	192.168.2.3	8.8.8.8	0xaed4	Standard query (0)	global.ztedevices.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:21.910901070 CET	192.168.2.3	8.8.8.8	0xd6ba	Standard query (0)	fonts.shopifycdn.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:22.017016888 CET	192.168.2.3	8.8.8.8	0x948f	Standard query (0)	cdn.shopify.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:23.244107962 CET	192.168.2.3	8.8.8.8	0x7297	Standard query (0)	cdn.judge.me	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:24.644357920 CET	192.168.2.3	8.8.8.8	0xe527	Standard query (0)	s.yimg.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:25.302155972 CET	192.168.2.3	8.8.8.8	0x91a6	Standard query (0)	messengerview.1talking.net	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:26.254939079 CET	192.168.2.3	8.8.8.8	0xe3d	Standard query (0)	sp.analytics.yahoo.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:26.411655903 CET	192.168.2.3	8.8.8.8	0x2b12	Standard query (0)	monorail-edge.shopifysvc.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:26.779730082 CET	192.168.2.3	8.8.8.8	0x9697	Standard query (0)	xhr.invl.co	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:26.881041050 CET	192.168.2.3	8.8.8.8	0x2ef9	Standard query (0)	shopify.privy.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:26.881598949 CET	192.168.2.3	8.8.8.8	0xac85	Standard query (0)	chimpstatic.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.113897085 CET	192.168.2.3	8.8.8.8	0x4225	Standard query (0)	product-labels-pro.bsscommerce.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.125132084 CET	192.168.2.3	8.8.8.8	0xb6d1	Standard query (0)	app.avada.io	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.295773029 CET	192.168.2.3	8.8.8.8	0xfa51	Standard query (0)	api.privy.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.299947023 CET	192.168.2.3	8.8.8.8	0xeefd	Standard query (0)	widgets.automizely.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.603312969 CET	192.168.2.3	8.8.8.8	0x1dfb	Standard query (0)	www.dwin1.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.686059952 CET	192.168.2.3	8.8.8.8	0xa37b	Standard query (0)	static.shareasale.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.694292068 CET	192.168.2.3	8.8.8.8	0xaf8d	Standard query (0)	cdn.langshop.app	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 18:00:27.726985931 CET	192.168.2.3	8.8.8.8	0x59a9	Standard query (0)	seo.apps.avada.io	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:28.126565933 CET	192.168.2.3	8.8.8.8	0x1095	Standard query (0)	cdn.pushowl.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:28.290705919 CET	192.168.2.3	8.8.8.8	0xa96a	Standard query (0)	static.zdassets.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:28.921658039 CET	192.168.2.3	8.8.8.8	0x7a0f	Standard query (0)	sdks.am-static.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:29.125704050 CET	192.168.2.3	8.8.8.8	0x46cc	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:29.331573963 CET	192.168.2.3	8.8.8.8	0x53aa	Standard query (0)	dashboard.wheelio-app.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:29.449156046 CET	192.168.2.3	8.8.8.8	0x9228	Standard query (0)	ekr.zdassets.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:29.840296984 CET	192.168.2.3	8.8.8.8	0x3571	Standard query (0)	api.pushowl.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:29.969346046 CET	192.168.2.3	8.8.8.8	0xd758	Standard query (0)	static.addtoany.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:30.339354992 CET	192.168.2.3	8.8.8.8	0x3cef	Standard query (0)	cdn.admitad-connect.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:36.088850021 CET	192.168.2.3	8.8.8.8	0xc246	Standard query (0)	source3.boys4dayz.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:37.688186884 CET	192.168.2.3	8.8.8.8	0xba85	Standard query (0)	ztedevices.zendesk.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:39.478080034 CET	192.168.2.3	8.8.8.8	0xdda5	Standard query (0)	korolova.s3.nl-ams.scw.cloud	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:43.121243954 CET	192.168.2.3	8.8.8.8	0xa63a	Standard query (0)	diromalxx.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:47.319962978 CET	192.168.2.3	8.8.8.8	0xb5e9	Standard query (0)	widget-mediator.zopim.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:52.966371059 CET	192.168.2.3	8.8.8.8	0xbd5d	Standard query (0)	myhypeposts.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:52.966726065 CET	192.168.2.3	8.8.8.8	0xef35	Standard query (0)	vexacion.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:52.973500013 CET	192.168.2.3	8.8.8.8	0xc06c	Standard query (0)	propeller-tracking.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:53.009041071 CET	192.168.2.3	8.8.8.8	0x99a8	Standard query (0)	my.rtmark.net	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:54.647622108 CET	192.168.2.3	8.8.8.8	0xacc1	Standard query (0)	affiliates.abebooks.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:54.789912939 CET	192.168.2.3	8.8.8.8	0x8d88	Standard query (0)	www.ojrq.net	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:55.020181894 CET	192.168.2.3	8.8.8.8	0x861d	Standard query (0)	www.abebooks.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:55.375932932 CET	192.168.2.3	8.8.8.8	0xb0ba	Standard query (0)	www.directdexchange.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:56.293359041 CET	192.168.2.3	8.8.8.8	0x96dd	Standard query (0)	assets.prod.abebookscdn.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:56.301424980 CET	192.168.2.3	8.8.8.8	0x1764	Standard query (0)	littlecdn.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:56.350408077 CET	192.168.2.3	8.8.8.8	0x498d	Standard query (0)	mc.yandex.ru	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:56.406610012 CET	192.168.2.3	8.8.8.8	0x77fe	Standard query (0)	assets.brightspot.abebooks.a2z.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:57.436661959 CET	192.168.2.3	8.8.8.8	0x5e08	Standard query (0)	yonhelioliskor.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:57.499407053 CET	192.168.2.3	8.8.8.8	0xf16d	Standard query (0)	atzekromchan.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:58.608336926 CET	192.168.2.3	8.8.8.8	0x829f	Standard query (0)	cdntechone.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:59.217936039 CET	192.168.2.3	8.8.8.8	0x964e	Standard query (0)	360devtracking.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:59.232311964 CET	192.168.2.3	8.8.8.8	0x82f2	Standard query (0)	libs.coremetrics.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:59.264671087 CET	192.168.2.3	8.8.8.8	0xe0c4	Standard query (0)	data.abebooks.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:02.217909098 CET	192.168.2.3	8.8.8.8	0x64c8	Standard query (0)	datatechone.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:02.773077011 CET	192.168.2.3	8.8.8.8	0x2235	Standard query (0)	stun.l.google.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:04.362252951 CET	192.168.2.3	8.8.8.8	0xaae6	Standard query (0)	pictures.abebooks.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 18:01:05.965379000 CET	192.168.2.3	8.8.8.8	0xd079	Standard query (0)	www.gearbest.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.704235077 CET	192.168.2.3	8.8.8.8	0x8870	Standard query (0)	cart.gearbest.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.704941988 CET	192.168.2.3	8.8.8.8	0xf764	Standard query (0)	css.gbtcdn.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.705682039 CET	192.168.2.3	8.8.8.8	0xb0cb	Standard query (0)	analytics.logsss.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.720598936 CET	192.168.2.3	8.8.8.8	0x9cca	Standard query (0)	order.gearbest.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.029329062 CET	192.168.2.3	8.8.8.8	0x2ce4	Standard query (0)	des.gbtcdn.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.030222893 CET	192.168.2.3	8.8.8.8	0x9ffe	Standard query (0)	gloimg.gbtcdn.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.051502943 CET	192.168.2.3	8.8.8.8	0x7986	Standard query (0)	login.gearbest.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.101716995 CET	192.168.2.3	8.8.8.8	0xac8b	Standard query (0)	perf.logsss.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.119756937 CET	192.168.2.3	8.8.8.8	0x9219	Standard query (0)	review.gbtcdn.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.125135899 CET	192.168.2.3	8.8.8.8	0x7976	Standard query (0)	rum.logsss.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.130778074 CET	192.168.2.3	8.8.8.8	0x5752	Standard query (0)	s.logsss.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.150393963 CET	192.168.2.3	8.8.8.8	0xb28f	Standard query (0)	uidesign.gbtcdn.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.153031111 CET	192.168.2.3	8.8.8.8	0xe3a4	Standard query (0)	user.gearbest.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:08.264955044 CET	192.168.2.3	8.8.8.8	0x65	Standard query (0)	c.xyzgamec.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:08.762690067 CET	192.168.2.3	8.8.8.8	0xd0dd	Standard query (0)	google.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:08.947207928 CET	192.168.2.3	8.8.8.8	0xcb38	Standard query (0)	htagzdownload.pw	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:09.123049021 CET	192.168.2.3	8.8.8.8	0x9e0d	Standard query (0)	b.dxyzgame.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:09.179246902 CET	192.168.2.3	8.8.8.8	0x664f	Standard query (0)	connectini.net	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:09.182390928 CET	192.168.2.3	8.8.8.8	0xab06	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:09.612056971 CET	192.168.2.3	8.8.8.8	0x4e8	Standard query (0)	connectini.net	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:12.703178883 CET	192.168.2.3	8.8.8.8	0x5121	Standard query (0)	360devtracking.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:13.217866898 CET	192.168.2.3	8.8.8.8	0xba2b	Standard query (0)	source3.boys4dayz.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:13.226937056 CET	192.168.2.3	8.8.8.8	0x2d8a	Standard query (0)	www.profitabletrustednetwork.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:14.119004011 CET	192.168.2.3	8.8.8.8	0xbaa5	Standard query (0)	htagzdownload.pw	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:14.741812944 CET	192.168.2.3	8.8.8.8	0x36ac	Standard query (0)	c.xyzgamec.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:15.341080904 CET	192.168.2.3	8.8.8.8	0x6726	Standard query (0)	b.dxyzgame.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:15.788100958 CET	192.168.2.3	8.8.8.8	0x260a	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:17.179016113 CET	192.168.2.3	8.8.8.8	0xc8d	Standard query (0)	gp.gamebuy768.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:18.098428965 CET	192.168.2.3	8.8.8.8	0x2fde	Standard query (0)	curtainshare.su	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:24.160653114 CET	192.168.2.3	8.8.8.8	0xb349	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:24.562561989 CET	192.168.2.3	8.8.8.8	0xc405	Standard query (0)	gp.gamebuy768.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:27.178447008 CET	192.168.2.3	8.8.8.8	0x4137	Standard query (0)	curtainshare.su	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:30.224138975 CET	192.168.2.3	8.8.8.8	0x6b0e	Standard query (0)	gp.gamebuy768.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:31.557362080 CET	192.168.2.3	8.8.8.8	0x67a8	Standard query (0)	toa.mygametoa.com	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:31.557624102 CET	192.168.2.3	8.8.8.8	0xa506	Standard query (0)	toa.mygametoa.com	28	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 17:59:06.206561089 CET	8.8.8.8	192.168.2.3	0xba32	No error (0)	onepiece.s3.pl-waw.scw.cloud	s3.pl-waw.scw.cloud		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 17:59:06.206561089 CET	8.8.8.8	192.168.2.3	0xba32	No error (0)	s3.pl-waw.scw.cloud		151.115.10.1	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:12.304639101 CET	8.8.8.8	192.168.2.3	0x731d	No error (0)	connectini.net		162.0.210.44	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:16.052409887 CET	8.8.8.8	192.168.2.3	0x2bd9	No error (0)	korolova.s3.nl-ams.scw.cloud	s3.nl-ams.scw.cloud		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 17:59:16.052409887 CET	8.8.8.8	192.168.2.3	0x2bd9	No error (0)	s3.nl-ams.scw.cloud		163.172.208.8	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:23.882371902 CET	8.8.8.8	192.168.2.3	0xcc56	No error (0)	www.google.com		142.250.185.164	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:24.663446903 CET	8.8.8.8	192.168.2.3	0xbedf	No error (0)	connectini.net		162.0.210.44	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:26.345438004 CET	8.8.8.8	192.168.2.3	0x7357	No error (0)	360devtracking.com		37.230.138.66	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:27.504630089 CET	8.8.8.8	192.168.2.3	0x3d7f	No error (0)	iplogger.org		148.251.234.83	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:28.476730108 CET	8.8.8.8	192.168.2.3	0xa659	No error (0)	google.com		142.250.186.110	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:30.241123915 CET	8.8.8.8	192.168.2.3	0x28c7	No error (0)	connectini.net		162.0.210.44	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:38.223534107 CET	8.8.8.8	192.168.2.3	0xc754	No error (0)	google.com		142.250.186.110	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:39.606467009 CET	8.8.8.8	192.168.2.3	0x6378	No error (0)	delice.s3.fr-par.scw.cloud	s3.fr-par.scw.cloud		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 17:59:39.606467009 CET	8.8.8.8	192.168.2.3	0x6378	No error (0)	s3.fr-par.scw.cloud		51.159.62.6	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:51.609693050 CET	8.8.8.8	192.168.2.3	0x4572	No error (0)	accounts.google.com		142.250.184.205	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:51.618907928 CET	8.8.8.8	192.168.2.3	0x50cd	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 17:59:51.618907928 CET	8.8.8.8	192.168.2.3	0x50cd	No error (0)	clients.l.google.com		172.217.16.142	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:51.622243881 CET	8.8.8.8	192.168.2.3	0x40a7	No error (0)	www.directdexchange.com	directdexchange.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 17:59:51.622243881 CET	8.8.8.8	192.168.2.3	0x40a7	No error (0)	directdexchange.com		35.201.70.46	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:51.692517996 CET	8.8.8.8	192.168.2.3	0xf47b	No error (0)	vexacion.com		139.45.197.236	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:51.809232950 CET	8.8.8.8	192.168.2.3	0xe57e	No error (0)	www.profitabletrustednetwork.com		192.243.59.12	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:51.809232950 CET	8.8.8.8	192.168.2.3	0xe57e	No error (0)	www.profitabletrustednetwork.com		192.243.59.13	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:52.269655943 CET	8.8.8.8	192.168.2.3	0x2709	No error (0)	propeller-tracking.com		139.45.197.240	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:52.270467997 CET	8.8.8.8	192.168.2.3	0x6b2f	No error (0)	my.rtmark.net		139.45.195.8	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:52.867340088 CET	8.8.8.8	192.168.2.3	0xc228	No error (0)	myhypeposts.com		139.45.197.139	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 17:59:52.981616974 CET	8.8.8.8	192.168.2.3	0xdd6	No error (0)	www.gearbest.com	d1lytq8w52fohg.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 17:59:52.981616974 CET	8.8.8.8	192.168.2.3	0xdd6	No error (0)	d1lytq8w52fohg.cloudfront.net		13.224.96.29	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:52.981616974 CET	8.8.8.8	192.168.2.3	0xdd6	No error (0)	d1lytq8w52fohg.cloudfront.net		13.224.96.39	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:52.981616974 CET	8.8.8.8	192.168.2.3	0xdd6	No error (0)	d1lytq8w52fohg.cloudfront.net		13.224.96.43	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:52.981616974 CET	8.8.8.8	192.168.2.3	0xdd6	No error (0)	d1lytq8w52fohg.cloudfront.net		13.224.96.84	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:53.501107931 CET	8.8.8.8	192.168.2.3	0xe227	No error (0)	order.gearbest.com	di7rtopbiewfz.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 17:59:53.501107931 CET	8.8.8.8	192.168.2.3	0xe227	No error (0)	di7rtopbiewfz.cloudfront.net		13.224.96.103	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:53.501107931 CET	8.8.8.8	192.168.2.3	0xe227	No error (0)	di7rtopbiewfz.cloudfront.net		13.224.96.79	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:53.501107931 CET	8.8.8.8	192.168.2.3	0xe227	No error (0)	di7rtopbiewfz.cloudfront.net		13.224.96.31	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:53.501107931 CET	8.8.8.8	192.168.2.3	0xe227	No error (0)	di7rtopbiewfz.cloudfront.net		13.224.96.106	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:53.515254021 CET	8.8.8.8	192.168.2.3	0xe715	No error (0)	css.gbtcdn.com	dyjtibcz3b48v.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 17:59:53.515254021 CET	8.8.8.8	192.168.2.3	0xe715	No error (0)	dyjtibcz3b48v.cloudfront.net		13.224.96.86	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:53.515254021 CET	8.8.8.8	192.168.2.3	0xe715	No error (0)	dyjtibcz3b48v.cloudfront.net		13.224.96.29	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:53.515254021 CET	8.8.8.8	192.168.2.3	0xe715	No error (0)	dyjtibcz3b48v.cloudfront.net		13.224.96.33	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:53.515254021 CET	8.8.8.8	192.168.2.3	0xe715	No error (0)	dyjtibcz3b48v.cloudfront.net		13.224.96.95	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:53.795486927 CET	8.8.8.8	192.168.2.3	0x13d0	No error (0)	littlecdn.com		104.22.25.116	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:53.795486927 CET	8.8.8.8	192.168.2.3	0x13d0	No error (0)	littlecdn.com		104.22.24.116	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:53.795486927 CET	8.8.8.8	192.168.2.3	0x13d0	No error (0)	littlecdn.com		172.67.10.98	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:53.889276028 CET	8.8.8.8	192.168.2.3	0x259f	No error (0)	uidesign.gbtcdn.com	d21fnsp1pg8r6b.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 17:59:53.889276028 CET	8.8.8.8	192.168.2.3	0x259f	No error (0)	d21fnsp1pg8r6b.cloudfront.net		13.224.96.58	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:53.889276028 CET	8.8.8.8	192.168.2.3	0x259f	No error (0)	d21fnsp1pg8r6b.cloudfront.net		13.224.96.11	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:53.889276028 CET	8.8.8.8	192.168.2.3	0x259f	No error (0)	d21fnsp1pg8r6b.cloudfront.net		13.224.96.18	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:53.889276028 CET	8.8.8.8	192.168.2.3	0x259f	No error (0)	d21fnsp1pg8r6b.cloudfront.net		13.224.96.69	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:54.520239115 CET	8.8.8.8	192.168.2.3	0x4ae0	No error (0)	analytics.logsss.com	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 17:59:54.520239115 CET	8.8.8.8	192.168.2.3	0x4ae0	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		35.169.187.184	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 17:59:54.520239115 CET	8.8.8.8	192.168.2.3	0x4ae0	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		54.174.190.185	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:54.520239115 CET	8.8.8.8	192.168.2.3	0x4ae0	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		34.230.152.110	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:54.520239115 CET	8.8.8.8	192.168.2.3	0x4ae0	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		52.87.105.69	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:54.524480104 CET	8.8.8.8	192.168.2.3	0xb2d	No error (0)	cart.gearbest.com	d2ovawmze1vtgu.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 17:59:54.524480104 CET	8.8.8.8	192.168.2.3	0xb2d	No error (0)	d2ovawmze1vtgu.cloudfront.net		13.224.96.120	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:54.524480104 CET	8.8.8.8	192.168.2.3	0xb2d	No error (0)	d2ovawmze1vtgu.cloudfront.net		13.224.96.2	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:54.524480104 CET	8.8.8.8	192.168.2.3	0xb2d	No error (0)	d2ovawmze1vtgu.cloudfront.net		13.224.96.27	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:54.524480104 CET	8.8.8.8	192.168.2.3	0xb2d	No error (0)	d2ovawmze1vtgu.cloudfront.net		13.224.96.116	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:55.634155989 CET	8.8.8.8	192.168.2.3	0x27f4	No error (0)	mc.yandex.ru		93.158.134.119	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:55.634155989 CET	8.8.8.8	192.168.2.3	0x27f4	No error (0)	mc.yandex.ru		77.88.21.119	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:55.634155989 CET	8.8.8.8	192.168.2.3	0x27f4	No error (0)	mc.yandex.ru		87.250.250.119	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:55.634155989 CET	8.8.8.8	192.168.2.3	0x27f4	No error (0)	mc.yandex.ru		87.250.251.119	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:55.675110102 CET	8.8.8.8	192.168.2.3	0x89cf	No error (0)	gloimg.gbtcdn.com	d1h4d6cj0c830c.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 17:59:55.675110102 CET	8.8.8.8	192.168.2.3	0x89cf	No error (0)	d1h4d6cj0c830c.cloudfront.net		13.224.96.30	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:55.675110102 CET	8.8.8.8	192.168.2.3	0x89cf	No error (0)	d1h4d6cj0c830c.cloudfront.net		13.224.96.122	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:55.675110102 CET	8.8.8.8	192.168.2.3	0x89cf	No error (0)	d1h4d6cj0c830c.cloudfront.net		13.224.96.51	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:55.675110102 CET	8.8.8.8	192.168.2.3	0x89cf	No error (0)	d1h4d6cj0c830c.cloudfront.net		13.224.96.41	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:55.676491022 CET	8.8.8.8	192.168.2.3	0x340c	No error (0)	des.gbtcdn.com	d155tv9w8vktl.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 17:59:55.676491022 CET	8.8.8.8	192.168.2.3	0x340c	No error (0)	d155tv9w8vktl.cloudfront.net		13.224.96.88	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:55.676491022 CET	8.8.8.8	192.168.2.3	0x340c	No error (0)	d155tv9w8vktl.cloudfront.net		13.224.96.124	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:55.676491022 CET	8.8.8.8	192.168.2.3	0x340c	No error (0)	d155tv9w8vktl.cloudfront.net		13.224.96.71	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:55.676491022 CET	8.8.8.8	192.168.2.3	0x340c	No error (0)	d155tv9w8vktl.cloudfront.net		13.224.96.7	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:55.889350891 CET	8.8.8.8	192.168.2.3	0x78d5	No error (0)	atzekromchan.com		139.45.197.238	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:55.896055937 CET	8.8.8.8	192.168.2.3	0xcafb	No error (0)	www-google tagmanager.l.google.com		142.250.186.136	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 17:59:55.896919966 CET	8.8.8.8	192.168.2.3	0x5405	No error (0)	yonhelioli skor.com		139.45.197.251	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.568950891 CET	8.8.8.8	192.168.2.3	0xff	No error (0)	login.gear best.com	dxozrhxfn9bwf.cloudfront. net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 17:59:56.568950891 CET	8.8.8.8	192.168.2.3	0xff	No error (0)	dxozrhxfn9 bwf.cloudf ront.net		13.224.96.4	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.568950891 CET	8.8.8.8	192.168.2.3	0xff	No error (0)	dxozrhxfn9 bwf.cloudf ront.net		13.224.96.73	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.568950891 CET	8.8.8.8	192.168.2.3	0xff	No error (0)	dxozrhxfn9 bwf.cloudf ront.net		13.224.96.89	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.568950891 CET	8.8.8.8	192.168.2.3	0xff	No error (0)	dxozrhxfn9 bwf.cloudf ront.net		13.224.96.71	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.594229937 CET	8.8.8.8	192.168.2.3	0xc0a7	Name error (3)	perf.logsss.com	none	none	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.622186899 CET	8.8.8.8	192.168.2.3	0x8ab1	No error (0)	review.gbt cdn.com	d2393mmhak2ysp.cloudfr ont.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 17:59:56.622186899 CET	8.8.8.8	192.168.2.3	0x8ab1	No error (0)	d2393mmhak 2ysp.cloud front.net		13.224.96.116	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.622186899 CET	8.8.8.8	192.168.2.3	0x8ab1	No error (0)	d2393mmhak 2ysp.cloud front.net		13.224.96.7	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.622186899 CET	8.8.8.8	192.168.2.3	0x8ab1	No error (0)	d2393mmhak 2ysp.cloud front.net		13.224.96.45	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.622186899 CET	8.8.8.8	192.168.2.3	0x8ab1	No error (0)	d2393mmhak 2ysp.cloud front.net		13.224.96.88	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.761271954 CET	8.8.8.8	192.168.2.3	0x59be	No error (0)	s.logsss.com	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 17:59:56.761271954 CET	8.8.8.8	192.168.2.3	0x59be	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.a mazonaws.com		54.174.190.185	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.761271954 CET	8.8.8.8	192.168.2.3	0x59be	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.a mazonaws.com		35.169.187.184	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.761271954 CET	8.8.8.8	192.168.2.3	0x59be	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.a mazonaws.com		34.230.152.110	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.761271954 CET	8.8.8.8	192.168.2.3	0x59be	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.a mazonaws.com		52.87.105.69	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.762145042 CET	8.8.8.8	192.168.2.3	0x1349	Name error (3)	rum.logsss.com	none	none	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.850853920 CET	8.8.8.8	192.168.2.3	0x1026	No error (0)	user.gearb est.com	d1s33wn15r3bpe.cloudfro nt.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 17:59:56.850853920 CET	8.8.8.8	192.168.2.3	0x1026	No error (0)	d1s33wn15r 3bpe.cloud front.net		13.224.96.124	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.850853920 CET	8.8.8.8	192.168.2.3	0x1026	No error (0)	d1s33wn15r 3bpe.cloud front.net		13.224.96.78	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.850853920 CET	8.8.8.8	192.168.2.3	0x1026	No error (0)	d1s33wn15r 3bpe.cloud front.net		13.224.96.123	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:56.850853920 CET	8.8.8.8	192.168.2.3	0x1026	No error (0)	d1s33wn15r 3bpe.cloud front.net		13.224.96.27	A (IP address)	IN (0x0001)
Jan 14, 2022 17:59:58.284739971 CET	8.8.8.8	192.168.2.3	0x28a5	No error (0)	cdntechone.com		172.67.131.171	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 17:59:58.284739971 CET	8.8.8.8	192.168.2.3	0x28a5	No error (0)	cdntechone.com		104.21.4.49	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:01.971491098 CET	8.8.8.8	192.168.2.3	0xaeb2	No error (0)	datatechone.com		37.48.68.71	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:01.975976944 CET	8.8.8.8	192.168.2.3	0xe190	No error (0)	www.google.com		142.250.185.164	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:02.167259932 CET	8.8.8.8	192.168.2.3	0xba46	No error (0)	stun.l.google.com		142.250.154.127	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:02.659307003 CET	8.8.8.8	192.168.2.3	0x24db	No error (0)	cur.gearbest.com	d3lp7swsejht2u.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:02.659307003 CET	8.8.8.8	192.168.2.3	0x24db	No error (0)	d3lp7swsejht2u.cloudfront.net		13.224.96.124	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:02.659307003 CET	8.8.8.8	192.168.2.3	0x24db	No error (0)	d3lp7swsejht2u.cloudfront.net		13.224.96.76	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:02.659307003 CET	8.8.8.8	192.168.2.3	0x24db	No error (0)	d3lp7swsejht2u.cloudfront.net		13.224.96.42	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:02.659307003 CET	8.8.8.8	192.168.2.3	0x24db	No error (0)	d3lp7swsejht2u.cloudfront.net		13.224.96.53	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:06.847296953 CET	8.8.8.8	192.168.2.3	0x79b1	No error (0)	www.cloud-security.xyz		172.67.215.223	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:06.847296953 CET	8.8.8.8	192.168.2.3	0x79b1	No error (0)	www.cloud-security.xyz		104.21.35.76	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:07.534049988 CET	8.8.8.8	192.168.2.3	0x93ed	No error (0)	nginx.1cros.net		18.184.39.239	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:07.534049988 CET	8.8.8.8	192.168.2.3	0x93ed	No error (0)	nginx.1cros.net		35.157.42.167	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:09.105751991 CET	8.8.8.8	192.168.2.3	0x1cb0	No error (0)	tpx.tesseradigital.com		35.157.179.180	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:09.110109091 CET	8.8.8.8	192.168.2.3	0xf826	No error (0)	www.adsaro.net		104.26.4.235	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:09.110109091 CET	8.8.8.8	192.168.2.3	0xf826	No error (0)	www.adsaro.net		172.67.68.31	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:09.110109091 CET	8.8.8.8	192.168.2.3	0xf826	No error (0)	www.adsaro.net		104.26.5.235	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:09.271856070 CET	8.8.8.8	192.168.2.3	0x9c4a	No error (0)	oneimpress.io		136.244.117.138	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:09.306399107 CET	8.8.8.8	192.168.2.3	0x1e69	No error (0)	www-google-analytics.l.google.com		142.250.186.110	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:09.880017042 CET	8.8.8.8	192.168.2.3	0xf051	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:10.627051115 CET	8.8.8.8	192.168.2.3	0xad30	No error (0)	goodnotification.net		172.67.138.139	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:10.627051115 CET	8.8.8.8	192.168.2.3	0xad30	No error (0)	goodnotification.net		104.21.46.120	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:10.755485058 CET	8.8.8.8	192.168.2.3	0x20b9	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:10.755485058 CET	8.8.8.8	192.168.2.3	0x20b9	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:11.153214931 CET	8.8.8.8	192.168.2.3	0x70c0	No error (0)	glsdk.logsss.com	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 18:00:11.153214931 CET	8.8.8.8	192.168.2.3	0x70c0	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		35.169.187.184	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:11.153214931 CET	8.8.8.8	192.168.2.3	0x70c0	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		54.174.190.185	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:11.153214931 CET	8.8.8.8	192.168.2.3	0x70c0	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		34.230.152.110	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:11.153214931 CET	8.8.8.8	192.168.2.3	0x70c0	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		52.87.105.69	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:11.160299063 CET	8.8.8.8	192.168.2.3	0xaa75	No error (0)	affiliate.gearbest.com	d28ndrjbfdkv0d.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:11.160299063 CET	8.8.8.8	192.168.2.3	0xaa75	No error (0)	d28ndrjbfdkv0d.cloudfront.net		13.224.96.45	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:11.160299063 CET	8.8.8.8	192.168.2.3	0xaa75	No error (0)	d28ndrjbfdkv0d.cloudfront.net		13.224.96.68	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:11.160299063 CET	8.8.8.8	192.168.2.3	0xaa75	No error (0)	d28ndrjbfdkv0d.cloudfront.net		13.224.96.81	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:11.160299063 CET	8.8.8.8	192.168.2.3	0xaa75	No error (0)	d28ndrjbfdkv0d.cloudfront.net		13.224.96.29	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:11.392321110 CET	8.8.8.8	192.168.2.3	0xcf3a	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:11.392321110 CET	8.8.8.8	192.168.2.3	0xcf3a	No error (0)	stats.l.doubleclick.net		108.177.15.154	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:11.392321110 CET	8.8.8.8	192.168.2.3	0xcf3a	No error (0)	stats.l.doubleclick.net		108.177.15.156	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:11.392321110 CET	8.8.8.8	192.168.2.3	0xcf3a	No error (0)	stats.l.doubleclick.net		108.177.15.157	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:11.392321110 CET	8.8.8.8	192.168.2.3	0xcf3a	No error (0)	stats.l.doubleclick.net		108.177.15.155	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:11.595793009 CET	8.8.8.8	192.168.2.3	0xf53d	No error (0)	googleads.g.doubleclick.net		142.250.185.226	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:17.305371046 CET	8.8.8.8	192.168.2.3	0x9666	No error (0)	360devtracking.com		37.230.138.66	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:17.436887026 CET	8.8.8.8	192.168.2.3	0xf510	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:17.436887026 CET	8.8.8.8	192.168.2.3	0xf510	No error (0)	googlehosted.l.googleusercontent.com		142.250.181.225	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:18.222779036 CET	8.8.8.8	192.168.2.3	0x3508	No error (0)	s.w.org		192.0.77.48	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:18.758706093 CET	8.8.8.8	192.168.2.3	0x9467	No error (0)	gstaticadssl.l.google.com		142.250.184.227	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:19.077955961 CET	8.8.8.8	192.168.2.3	0x6421	No error (0)	www.google.co.uk		142.250.186.99	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:19.473987103 CET	8.8.8.8	192.168.2.3	0xe25e	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:19.473987103 CET	8.8.8.8	192.168.2.3	0xe25e	No error (0)	star-mini.c10r.facebook.com		157.240.17.35	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 18:00:20.271117926 CET	8.8.8.8	192.168.2.3	0x3466	No error (0)	connectini.net		162.0.210.44	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:20.932301998 CET	8.8.8.8	192.168.2.3	0x6acd	No error (0)	ad.admitad.com		185.26.99.58	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:20.932301998 CET	8.8.8.8	192.168.2.3	0x6acd	No error (0)	ad.admitad.com		185.26.99.247	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:21.081909895 CET	8.8.8.8	192.168.2.3	0x3f15	No error (0)	ma.logsss.com	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:21.081909895 CET	8.8.8.8	192.168.2.3	0x3f15	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		54.174.190.185	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:21.081909895 CET	8.8.8.8	192.168.2.3	0x3f15	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		35.169.187.184	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:21.081909895 CET	8.8.8.8	192.168.2.3	0x3f15	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		34.230.152.110	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:21.081909895 CET	8.8.8.8	192.168.2.3	0x3f15	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		52.87.105.69	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:21.122626066 CET	8.8.8.8	192.168.2.3	0xaed4	No error (0)	global.zte devices.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:21.122626066 CET	8.8.8.8	192.168.2.3	0xaed4	No error (0)	shops.mysh opify.com		23.227.38.74	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:21.929944038 CET	8.8.8.8	192.168.2.3	0xd6ba	No error (0)	fonts.shop ifycdn.com		151.101.1.12	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:21.929944038 CET	8.8.8.8	192.168.2.3	0xd6ba	No error (0)	fonts.shop ifycdn.com		151.101.129.12	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:21.929944038 CET	8.8.8.8	192.168.2.3	0xd6ba	No error (0)	fonts.shop ifycdn.com		151.101.193.12	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:21.929944038 CET	8.8.8.8	192.168.2.3	0xd6ba	No error (0)	fonts.shop ifycdn.com		151.101.65.12	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:22.035773039 CET	8.8.8.8	192.168.2.3	0x948f	No error (0)	cdn.shopify.com		151.101.1.12	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:22.035773039 CET	8.8.8.8	192.168.2.3	0x948f	No error (0)	cdn.shopify.com		151.101.129.12	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:22.035773039 CET	8.8.8.8	192.168.2.3	0x948f	No error (0)	cdn.shopify.com		151.101.193.12	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:22.035773039 CET	8.8.8.8	192.168.2.3	0x948f	No error (0)	cdn.shopify.com		151.101.65.12	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:23.270862103 CET	8.8.8.8	192.168.2.3	0x7297	No error (0)	cdn.judge.me	judgeme-224d.kxcdn.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:23.270862103 CET	8.8.8.8	192.168.2.3	0x7297	No error (0)	judgeme-22 4d.kxcdn.com	p-chzh00.kxcdn.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:23.270862103 CET	8.8.8.8	192.168.2.3	0x7297	No error (0)	p-chzh00.k xcdn.com		94.126.16.223	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:24.661336899 CET	8.8.8.8	192.168.2.3	0xe527	No error (0)	s.yimg.com	edge.gycpi.b.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:24.661336899 CET	8.8.8.8	192.168.2.3	0xe527	No error (0)	edge.gycpi .b.yahoodns.net		87.248.118.23	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:24.661336899 CET	8.8.8.8	192.168.2.3	0xe527	No error (0)	edge.gycpi .b.yahoodns.net		87.248.118.22	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 18:00:25.321722031 CET	8.8.8.8	192.168.2.3	0x91a6	No error (0)	messengerview.1talking.net		52.38.191.23	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:26.271867990 CET	8.8.8.8	192.168.2.3	0xe3d	No error (0)	sp.analytics.yahoo.com	spdc-global.pbp.gysm.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:26.271867990 CET	8.8.8.8	192.168.2.3	0xe3d	No error (0)	spdc-global.pbp.gysm.yahoodns.net		212.82.100.181	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:26.430469036 CET	8.8.8.8	192.168.2.3	0x2b12	No error (0)	monorail-edge.shopifysvc.com	monorail-edge.tm.shopifysvc.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:26.430469036 CET	8.8.8.8	192.168.2.3	0x2b12	No error (0)	monorail-edge.tm.shopifysvc.com	monorail-edge.shopifycloud.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:26.430469036 CET	8.8.8.8	192.168.2.3	0x2b12	No error (0)	monorail-edge.shopifycloud.com	monorail-production-web-apps-a-us-east1-10.shopifycloud.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:26.430469036 CET	8.8.8.8	192.168.2.3	0x2b12	No error (0)	monorail-production-web-apps-a-us-east1-10.shopifycloud.com		34.138.230.116	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:26.796889067 CET	8.8.8.8	192.168.2.3	0x9697	No error (0)	xhr.invl.co		18.136.177.10	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:26.796889067 CET	8.8.8.8	192.168.2.3	0x9697	No error (0)	xhr.invl.co		54.179.155.39	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:26.796889067 CET	8.8.8.8	192.168.2.3	0x9697	No error (0)	xhr.invl.co		52.77.107.31	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:26.900641918 CET	8.8.8.8	192.168.2.3	0xac85	No error (0)	chimpstatic.com		23.50.98.104	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:26.903731108 CET	8.8.8.8	192.168.2.3	0x2ef9	No error (0)	shopify.privy.com		104.22.21.108	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:26.903731108 CET	8.8.8.8	192.168.2.3	0x2ef9	No error (0)	shopify.privy.com		104.22.20.108	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:26.903731108 CET	8.8.8.8	192.168.2.3	0x2ef9	No error (0)	shopify.privy.com		172.67.36.106	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.134470940 CET	8.8.8.8	192.168.2.3	0x4225	No error (0)	product-labels-pro.bsscommerce.com		104.26.1.133	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.134470940 CET	8.8.8.8	192.168.2.3	0x4225	No error (0)	product-labels-pro.bsscommerce.com		172.67.69.178	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.134470940 CET	8.8.8.8	192.168.2.3	0x4225	No error (0)	product-labels-pro.bsscommerce.com		104.26.0.133	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.150697947 CET	8.8.8.8	192.168.2.3	0xb6d1	No error (0)	app.avada.io		151.101.1.195	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.150697947 CET	8.8.8.8	192.168.2.3	0xb6d1	No error (0)	app.avada.io		151.101.65.195	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.318660021 CET	8.8.8.8	192.168.2.3	0xfa51	No error (0)	api.privy.com		104.22.20.108	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.318660021 CET	8.8.8.8	192.168.2.3	0xfa51	No error (0)	api.privy.com		172.67.36.106	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.318660021 CET	8.8.8.8	192.168.2.3	0xfa51	No error (0)	api.privy.com		104.22.21.108	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.322449923 CET	8.8.8.8	192.168.2.3	0xeefd	No error (0)	widgets.automizely.com		104.19.168.102	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.322449923 CET	8.8.8.8	192.168.2.3	0xeefd	No error (0)	widgets.automizely.com		104.19.169.102	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 18:00:27.626979113 CET	8.8.8.8	192.168.2.3	0x1dfb	No error (0)	www.dwin1.com	d2pbcviywxotf2.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:27.626979113 CET	8.8.8.8	192.168.2.3	0x1dfb	No error (0)	d2pbcviywxotf2.cloudfront.net		13.224.96.72	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.626979113 CET	8.8.8.8	192.168.2.3	0x1dfb	No error (0)	d2pbcviywxotf2.cloudfront.net		13.224.96.52	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.626979113 CET	8.8.8.8	192.168.2.3	0x1dfb	No error (0)	d2pbcviywxotf2.cloudfront.net		13.224.96.124	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.626979113 CET	8.8.8.8	192.168.2.3	0x1dfb	No error (0)	d2pbcviywxotf2.cloudfront.net		13.224.96.107	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.710386038 CET	8.8.8.8	192.168.2.3	0xa37b	No error (0)	static.shareasale.com		104.16.227.72	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.710386038 CET	8.8.8.8	192.168.2.3	0xa37b	No error (0)	static.shareasale.com		104.16.226.72	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.719114065 CET	8.8.8.8	192.168.2.3	0xaf8d	No error (0)	cdn.langshop.app		104.21.51.248	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.719114065 CET	8.8.8.8	192.168.2.3	0xaf8d	No error (0)	cdn.langshop.app		172.67.192.67	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.749154091 CET	8.8.8.8	192.168.2.3	0x59a9	No error (0)	seo.apps.avada.io		151.101.1.195	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:27.749154091 CET	8.8.8.8	192.168.2.3	0x59a9	No error (0)	seo.apps.avada.io		151.101.65.195	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:28.163774014 CET	8.8.8.8	192.168.2.3	0x1095	No error (0)	cdn.pushowl.com	pushowl.imgkit.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:28.163774014 CET	8.8.8.8	192.168.2.3	0x1095	No error (0)	pushowl.imgkit.net	d2h3z7munabi1z.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:28.163774014 CET	8.8.8.8	192.168.2.3	0x1095	No error (0)	d2h3z7munabi1z.cloudfront.net		13.224.96.122	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:28.163774014 CET	8.8.8.8	192.168.2.3	0x1095	No error (0)	d2h3z7munabi1z.cloudfront.net		13.224.96.12	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:28.163774014 CET	8.8.8.8	192.168.2.3	0x1095	No error (0)	d2h3z7munabi1z.cloudfront.net		13.224.96.86	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:28.163774014 CET	8.8.8.8	192.168.2.3	0x1095	No error (0)	d2h3z7munabi1z.cloudfront.net		13.224.96.71	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:28.317300081 CET	8.8.8.8	192.168.2.3	0xa96a	No error (0)	static.zdassets.com		104.18.72.113	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:28.317300081 CET	8.8.8.8	192.168.2.3	0xa96a	No error (0)	static.zdassets.com		104.18.70.113	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:28.941593885 CET	8.8.8.8	192.168.2.3	0x7a0f	No error (0)	sdks.am-static.com		104.18.28.218	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:28.941593885 CET	8.8.8.8	192.168.2.3	0x7a0f	No error (0)	sdks.am-static.com		104.18.29.218	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:29.148611069 CET	8.8.8.8	192.168.2.3	0x46cc	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:29.148611069 CET	8.8.8.8	192.168.2.3	0x46cc	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:29.351161957 CET	8.8.8.8	192.168.2.3	0x53aa	No error (0)	dashboard.wheelio-app.com		52.173.139.125	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:29.468033075 CET	8.8.8.8	192.168.2.3	0x9228	No error (0)	ekr.zdassets.com		104.18.70.113	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:29.468033075 CET	8.8.8.8	192.168.2.3	0x9228	No error (0)	ekr.zdassets.com		104.18.72.113	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 18:00:29.857908010 CET	8.8.8.8	192.168.2.3	0x3571	No error (0)	api.pushowl.com	d8bc12a0-pushowlbackend-pu-0f8c-1616299444.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:29.857908010 CET	8.8.8.8	192.168.2.3	0x3571	No error (0)	d8bc12a0-pushowlbackend-pu-0f8c-1616299444.us-east-1.elb.amazonaws.com		34.196.60.195	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:29.857908010 CET	8.8.8.8	192.168.2.3	0x3571	No error (0)	d8bc12a0-pushowlbackend-pu-0f8c-1616299444.us-east-1.elb.amazonaws.com		54.163.255.81	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:29.857908010 CET	8.8.8.8	192.168.2.3	0x3571	No error (0)	d8bc12a0-pushowlbackend-pu-0f8c-1616299444.us-east-1.elb.amazonaws.com		54.152.99.78	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:29.990777016 CET	8.8.8.8	192.168.2.3	0xd758	No error (0)	static.addtoany.com		172.67.39.148	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:29.990777016 CET	8.8.8.8	192.168.2.3	0xd758	No error (0)	static.addtoany.com		104.22.71.197	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:29.990777016 CET	8.8.8.8	192.168.2.3	0xd758	No error (0)	static.addtoany.com		104.22.70.197	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:30.360325098 CET	8.8.8.8	192.168.2.3	0x3cef	No error (0)	cdn.admitad-connect.com		104.26.5.175	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:30.360325098 CET	8.8.8.8	192.168.2.3	0x3cef	No error (0)	cdn.admitad-connect.com		104.26.4.175	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:30.360325098 CET	8.8.8.8	192.168.2.3	0x3cef	No error (0)	cdn.admitad-connect.com		172.67.70.43	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:36.119179010 CET	8.8.8.8	192.168.2.3	0xc246	No error (0)	source3.boys4dayz.com		172.67.148.61	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:36.119179010 CET	8.8.8.8	192.168.2.3	0xc246	No error (0)	source3.boys4dayz.com		104.21.33.188	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:37.715714931 CET	8.8.8.8	192.168.2.3	0xba85	No error (0)	ztedevices.zendesk.com		104.16.51.111	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:37.715714931 CET	8.8.8.8	192.168.2.3	0xba85	No error (0)	ztedevices.zendesk.com		104.16.53.111	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:39.520040035 CET	8.8.8.8	192.168.2.3	0xdda5	No error (0)	korolova.s3.nl-ams.scw.cloud	s3.nl-ams.scw.cloud		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:39.520040035 CET	8.8.8.8	192.168.2.3	0xdda5	No error (0)	s3.nl-ams.scw.cloud		163.172.208.8	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:43.144484043 CET	8.8.8.8	192.168.2.3	0xa63a	No error (0)	diromalxx.com		62.122.170.197	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:47.342961073 CET	8.8.8.8	192.168.2.3	0xb5e9	No error (0)	widget-mediator.zopim.com		3.120.252.147	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:47.342961073 CET	8.8.8.8	192.168.2.3	0xb5e9	No error (0)	widget-mediator.zopim.com		18.193.13.198	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:47.342961073 CET	8.8.8.8	192.168.2.3	0xb5e9	No error (0)	widget-mediator.zopim.com		35.156.198.62	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:47.342961073 CET	8.8.8.8	192.168.2.3	0xb5e9	No error (0)	widget-mediator.zopim.com		3.65.119.100	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:47.342961073 CET	8.8.8.8	192.168.2.3	0xb5e9	No error (0)	widget-mediator.zopim.com		18.185.160.226	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:47.342961073 CET	8.8.8.8	192.168.2.3	0xb5e9	No error (0)	widget-mediator.zopim.com		18.197.230.19	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 18:00:47.342961073 CET	8.8.8.8	192.168.2.3	0xb5e9	No error (0)	widget-mediator.zopim.com		18.185.191.77	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:47.342961073 CET	8.8.8.8	192.168.2.3	0xb5e9	No error (0)	widget-mediator.zopim.com		18.157.227.136	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:52.985104084 CET	8.8.8.8	192.168.2.3	0xbd5d	No error (0)	myhypeposts.com		139.45.197.139	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:52.988718033 CET	8.8.8.8	192.168.2.3	0xef35	No error (0)	vexacion.com		139.45.197.236	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:52.992381096 CET	8.8.8.8	192.168.2.3	0xc06c	No error (0)	propeller-tracking.com		139.45.197.240	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:53.027823925 CET	8.8.8.8	192.168.2.3	0x99a8	No error (0)	my.rtmark.net		139.45.195.8	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:54.685396910 CET	8.8.8.8	192.168.2.3	0xacc1	No error (0)	affiliates.abebooks.com	affiliates-abebooks-com.customtraffic.impactradius.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:54.685396910 CET	8.8.8.8	192.168.2.3	0xacc1	No error (0)	affiliates-abebooks-com.customtraffic.impactradius.com		35.244.197.23	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:54.807816982 CET	8.8.8.8	192.168.2.3	0x8d88	No error (0)	www.ojrq.net		34.95.127.121	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:55.046559095 CET	8.8.8.8	192.168.2.3	0x861d	No error (0)	www.abebooks.com	tp.0b4c9a994-frontier.abebooks.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:55.046559095 CET	8.8.8.8	192.168.2.3	0x861d	No error (0)	tp.0b4c9a994-frontier.abebooks.com	dr35amawwlvaz.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:55.046559095 CET	8.8.8.8	192.168.2.3	0x861d	No error (0)	dr35amawwlvaz.cloudfront.net		13.224.96.15	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:55.046559095 CET	8.8.8.8	192.168.2.3	0x861d	No error (0)	dr35amawwlvaz.cloudfront.net		13.224.96.68	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:55.046559095 CET	8.8.8.8	192.168.2.3	0x861d	No error (0)	dr35amawwlvaz.cloudfront.net		13.224.96.30	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:55.046559095 CET	8.8.8.8	192.168.2.3	0x861d	No error (0)	dr35amawwlvaz.cloudfront.net		13.224.96.104	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:55.400245905 CET	8.8.8.8	192.168.2.3	0xb0ba	No error (0)	www.directdexchange.com	directdexchange.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:55.400245905 CET	8.8.8.8	192.168.2.3	0xb0ba	No error (0)	directdexchange.com		35.201.70.46	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:56.316418886 CET	8.8.8.8	192.168.2.3	0x96dd	No error (0)	assets.prod.abebookscdn.com		13.224.96.28	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:56.316418886 CET	8.8.8.8	192.168.2.3	0x96dd	No error (0)	assets.prod.abebookscdn.com		13.224.96.72	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:56.316418886 CET	8.8.8.8	192.168.2.3	0x96dd	No error (0)	assets.prod.abebookscdn.com		13.224.96.13	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:56.316418886 CET	8.8.8.8	192.168.2.3	0x96dd	No error (0)	assets.prod.abebookscdn.com		13.224.96.126	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:56.322531939 CET	8.8.8.8	192.168.2.3	0x1764	No error (0)	littlecdn.com		104.22.25.116	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:56.322531939 CET	8.8.8.8	192.168.2.3	0x1764	No error (0)	littlecdn.com		172.67.10.98	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:56.322531939 CET	8.8.8.8	192.168.2.3	0x1764	No error (0)	littlecdn.com		104.22.24.116	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:56.369102001 CET	8.8.8.8	192.168.2.3	0x498d	No error (0)	mc.yandex.ru		93.158.134.119	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 18:00:56.369102001 CET	8.8.8.8	192.168.2.3	0x498d	No error (0)	mc.yandex.ru		87.250.250.119	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:56.369102001 CET	8.8.8.8	192.168.2.3	0x498d	No error (0)	mc.yandex.ru		77.88.21.119	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:56.369102001 CET	8.8.8.8	192.168.2.3	0x498d	No error (0)	mc.yandex.ru		87.250.251.119	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:56.429987907 CET	8.8.8.8	192.168.2.3	0x77fe	No error (0)	assets.brightspot.abebooks.a2z.com	cdn.abebooks.psdops.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:56.429987907 CET	8.8.8.8	192.168.2.3	0x77fe	No error (0)	cdn.abebooks.psdops.com	d1qcny5kzqmo9s.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:56.429987907 CET	8.8.8.8	192.168.2.3	0x77fe	No error (0)	d1qcny5kzqmo9s.cloudfront.net		13.224.96.6	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:56.429987907 CET	8.8.8.8	192.168.2.3	0x77fe	No error (0)	d1qcny5kzqmo9s.cloudfront.net		13.224.96.5	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:56.429987907 CET	8.8.8.8	192.168.2.3	0x77fe	No error (0)	d1qcny5kzqmo9s.cloudfront.net		13.224.96.91	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:56.429987907 CET	8.8.8.8	192.168.2.3	0x77fe	No error (0)	d1qcny5kzqmo9s.cloudfront.net		13.224.96.99	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:57.455707073 CET	8.8.8.8	192.168.2.3	0x5e08	No error (0)	yonhelioliskor.com		139.45.197.251	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:57.516067982 CET	8.8.8.8	192.168.2.3	0xf16d	No error (0)	atzekromchan.com		139.45.197.238	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:58.635418892 CET	8.8.8.8	192.168.2.3	0x829f	No error (0)	cdntechone.com		172.67.131.171	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:58.635418892 CET	8.8.8.8	192.168.2.3	0x829f	No error (0)	cdntechone.com		104.21.4.49	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:59.239145994 CET	8.8.8.8	192.168.2.3	0x964e	No error (0)	360devtracking.com		37.230.138.66	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:59.253182888 CET	8.8.8.8	192.168.2.3	0x82f2	No error (0)	libs.coremetrics.com	wildcard.coremetrics.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:00:59.301009893 CET	8.8.8.8	192.168.2.3	0xe0c4	No error (0)	data.abeboks.com		3.86.136.12	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:59.301009893 CET	8.8.8.8	192.168.2.3	0xe0c4	No error (0)	data.abeboks.com		54.144.151.173	A (IP address)	IN (0x0001)
Jan 14, 2022 18:00:59.301009893 CET	8.8.8.8	192.168.2.3	0xe0c4	No error (0)	data.abeboks.com		54.224.36.233	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:02.246078968 CET	8.8.8.8	192.168.2.3	0x64c8	No error (0)	datatechone.com		37.48.68.71	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:02.798759937 CET	8.8.8.8	192.168.2.3	0x2235	No error (0)	stun.l.google.com		142.250.154.127	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:04.386529922 CET	8.8.8.8	192.168.2.3	0xaae6	No error (0)	pictures.abebooks.com	d6gl2ual1jt2h.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:01:04.386529922 CET	8.8.8.8	192.168.2.3	0xaae6	No error (0)	d6gl2ual1jt2h.cloudfront.net		13.224.96.80	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:04.386529922 CET	8.8.8.8	192.168.2.3	0xaae6	No error (0)	d6gl2ual1jt2h.cloudfront.net		13.224.96.45	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:04.386529922 CET	8.8.8.8	192.168.2.3	0xaae6	No error (0)	d6gl2ual1jt2h.cloudfront.net		13.224.96.54	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:04.386529922 CET	8.8.8.8	192.168.2.3	0xaae6	No error (0)	d6gl2ual1jt2h.cloudfront.net		13.224.96.44	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.005476952 CET	8.8.8.8	192.168.2.3	0xd079	No error (0)	www.gearbest.com	d1lytq8w52fohg.cloudfront.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 18:01:06.005476952 CET	8.8.8.8	192.168.2.3	0xd079	No error (0)	d1lytq8w52fohg.cloudfront.net		13.224.96.84	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.005476952 CET	8.8.8.8	192.168.2.3	0xd079	No error (0)	d1lytq8w52fohg.cloudfront.net		13.224.96.39	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.005476952 CET	8.8.8.8	192.168.2.3	0xd079	No error (0)	d1lytq8w52fohg.cloudfront.net		13.224.96.29	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.005476952 CET	8.8.8.8	192.168.2.3	0xd079	No error (0)	d1lytq8w52fohg.cloudfront.net		13.224.96.43	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.724971056 CET	8.8.8.8	192.168.2.3	0xb0cb	No error (0)	analytics.logsss.com	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:01:06.724971056 CET	8.8.8.8	192.168.2.3	0xb0cb	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		52.87.105.69	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.724971056 CET	8.8.8.8	192.168.2.3	0xb0cb	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		35.169.187.184	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.724971056 CET	8.8.8.8	192.168.2.3	0xb0cb	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		34.230.152.110	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.724971056 CET	8.8.8.8	192.168.2.3	0xb0cb	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		54.174.190.185	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.728334904 CET	8.8.8.8	192.168.2.3	0x8870	No error (0)	cart.gearbest.com	d2ovawmze1vtgu.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:01:06.728334904 CET	8.8.8.8	192.168.2.3	0x8870	No error (0)	d2ovawmze1vtgu.cloudfront.net		13.224.96.116	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.728334904 CET	8.8.8.8	192.168.2.3	0x8870	No error (0)	d2ovawmze1vtgu.cloudfront.net		13.224.96.2	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.728334904 CET	8.8.8.8	192.168.2.3	0x8870	No error (0)	d2ovawmze1vtgu.cloudfront.net		13.224.96.27	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.728334904 CET	8.8.8.8	192.168.2.3	0x8870	No error (0)	d2ovawmze1vtgu.cloudfront.net		13.224.96.120	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.729296923 CET	8.8.8.8	192.168.2.3	0xf764	No error (0)	css.gbtcdn.com	dyjtibcz3b48v.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:01:06.729296923 CET	8.8.8.8	192.168.2.3	0xf764	No error (0)	dyjtibcz3b48v.cloudfront.net		13.224.96.86	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.729296923 CET	8.8.8.8	192.168.2.3	0xf764	No error (0)	dyjtibcz3b48v.cloudfront.net		13.224.96.29	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.729296923 CET	8.8.8.8	192.168.2.3	0xf764	No error (0)	dyjtibcz3b48v.cloudfront.net		13.224.96.33	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.729296923 CET	8.8.8.8	192.168.2.3	0xf764	No error (0)	dyjtibcz3b48v.cloudfront.net		13.224.96.95	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.741488934 CET	8.8.8.8	192.168.2.3	0x9cca	No error (0)	order.gearbest.com	di7rtopbiewfz.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:01:06.741488934 CET	8.8.8.8	192.168.2.3	0x9cca	No error (0)	di7rtopbiewfz.cloudfront.net		13.224.96.106	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.741488934 CET	8.8.8.8	192.168.2.3	0x9cca	No error (0)	di7rtopbiewfz.cloudfront.net		13.224.96.31	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.741488934 CET	8.8.8.8	192.168.2.3	0x9cca	No error (0)	di7rtopbiewfz.cloudfront.net		13.224.96.103	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:06.741488934 CET	8.8.8.8	192.168.2.3	0x9cca	No error (0)	di7rtopbiewfz.cloudfront.net		13.224.96.79	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 18:01:07.051917076 CET	8.8.8.8	192.168.2.3	0x2ce4	No error (0)	des.gbtcdn.com	d155tv9w8vktl.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:01:07.051917076 CET	8.8.8.8	192.168.2.3	0x2ce4	No error (0)	d155tv9w8vktl.cloudfront.net		13.224.96.7	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.051917076 CET	8.8.8.8	192.168.2.3	0x2ce4	No error (0)	d155tv9w8vktl.cloudfront.net		13.224.96.124	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.051917076 CET	8.8.8.8	192.168.2.3	0x2ce4	No error (0)	d155tv9w8vktl.cloudfront.net		13.224.96.88	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.051917076 CET	8.8.8.8	192.168.2.3	0x2ce4	No error (0)	d155tv9w8vktl.cloudfront.net		13.224.96.71	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.064466000 CET	8.8.8.8	192.168.2.3	0x9ffe	No error (0)	gloimg.gbtcdn.com	d1h4d6cj0c830c.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:01:07.064466000 CET	8.8.8.8	192.168.2.3	0x9ffe	No error (0)	d1h4d6cj0c830c.cloudfront.net		13.224.96.41	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.064466000 CET	8.8.8.8	192.168.2.3	0x9ffe	No error (0)	d1h4d6cj0c830c.cloudfront.net		13.224.96.122	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.064466000 CET	8.8.8.8	192.168.2.3	0x9ffe	No error (0)	d1h4d6cj0c830c.cloudfront.net		13.224.96.51	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.064466000 CET	8.8.8.8	192.168.2.3	0x9ffe	No error (0)	d1h4d6cj0c830c.cloudfront.net		13.224.96.30	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.085930109 CET	8.8.8.8	192.168.2.3	0x7986	No error (0)	login.gearbest.com	dxozrhxfn9bwf.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:01:07.085930109 CET	8.8.8.8	192.168.2.3	0x7986	No error (0)	dxozrhxfn9bwf.cloudfront.net		13.224.96.71	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.085930109 CET	8.8.8.8	192.168.2.3	0x7986	No error (0)	dxozrhxfn9bwf.cloudfront.net		13.224.96.89	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.085930109 CET	8.8.8.8	192.168.2.3	0x7986	No error (0)	dxozrhxfn9bwf.cloudfront.net		13.224.96.73	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.085930109 CET	8.8.8.8	192.168.2.3	0x7986	No error (0)	dxozrhxfn9bwf.cloudfront.net		13.224.96.4	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.120990038 CET	8.8.8.8	192.168.2.3	0xac8b	Name error (3)	perf.logsss.com	none	none	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.142317057 CET	8.8.8.8	192.168.2.3	0x9219	No error (0)	review.gbtcdn.com	d2393mmhak2ysp.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:01:07.142317057 CET	8.8.8.8	192.168.2.3	0x9219	No error (0)	d2393mmhak2ysp.cloudfront.net		13.224.96.116	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.142317057 CET	8.8.8.8	192.168.2.3	0x9219	No error (0)	d2393mmhak2ysp.cloudfront.net		13.224.96.7	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.142317057 CET	8.8.8.8	192.168.2.3	0x9219	No error (0)	d2393mmhak2ysp.cloudfront.net		13.224.96.45	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.142317057 CET	8.8.8.8	192.168.2.3	0x9219	No error (0)	d2393mmhak2ysp.cloudfront.net		13.224.96.88	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.142467022 CET	8.8.8.8	192.168.2.3	0x7976	Name error (3)	rum.logsss.com	none	none	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.149975061 CET	8.8.8.8	192.168.2.3	0x5752	No error (0)	s.logsss.com	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:01:07.149975061 CET	8.8.8.8	192.168.2.3	0x5752	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		52.87.105.69	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.149975061 CET	8.8.8.8	192.168.2.3	0x5752	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		54.174.190.185	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 18:01:07.149975061 CET	8.8.8.8	192.168.2.3	0x5752	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		35.169.187.184	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.149975061 CET	8.8.8.8	192.168.2.3	0x5752	No error (0)	cloudmonitor-logsss-com-1570812809.us-east-1.elb.amazonaws.com		34.230.152.110	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.174689054 CET	8.8.8.8	192.168.2.3	0xe3a4	No error (0)	user.gearbest.com	d1s33wn15r3bpe.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:01:07.174689054 CET	8.8.8.8	192.168.2.3	0xe3a4	No error (0)	d1s33wn15r3bpe.cloudfront.net		13.224.96.123	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.174689054 CET	8.8.8.8	192.168.2.3	0xe3a4	No error (0)	d1s33wn15r3bpe.cloudfront.net		13.224.96.27	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.174689054 CET	8.8.8.8	192.168.2.3	0xe3a4	No error (0)	d1s33wn15r3bpe.cloudfront.net		13.224.96.78	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.174689054 CET	8.8.8.8	192.168.2.3	0xe3a4	No error (0)	d1s33wn15r3bpe.cloudfront.net		13.224.96.124	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.176999092 CET	8.8.8.8	192.168.2.3	0xb28f	No error (0)	uidesign.gbtcdn.com	d21fnsp1pg8r6b.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 18:01:07.176999092 CET	8.8.8.8	192.168.2.3	0xb28f	No error (0)	d21fnsp1pg8r6b.cloudfront.net		13.224.96.58	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.176999092 CET	8.8.8.8	192.168.2.3	0xb28f	No error (0)	d21fnsp1pg8r6b.cloudfront.net		13.224.96.11	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.176999092 CET	8.8.8.8	192.168.2.3	0xb28f	No error (0)	d21fnsp1pg8r6b.cloudfront.net		13.224.96.18	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:07.176999092 CET	8.8.8.8	192.168.2.3	0xb28f	No error (0)	d21fnsp1pg8r6b.cloudfront.net		13.224.96.69	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:08.290028095 CET	8.8.8.8	192.168.2.3	0x65	No error (0)	c.xyzgamec.com		172.67.143.225	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:08.290028095 CET	8.8.8.8	192.168.2.3	0x65	No error (0)	c.xyzgamec.com		104.21.71.70	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:08.788780928 CET	8.8.8.8	192.168.2.3	0xd0dd	No error (0)	google.com		142.250.186.110	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:09.053558111 CET	8.8.8.8	192.168.2.3	0xcb38	No error (0)	htagzdownload.pw		35.205.61.67	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:09.144165993 CET	8.8.8.8	192.168.2.3	0x9e0d	No error (0)	b.dxyzgame.com		172.67.164.165	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:09.144165993 CET	8.8.8.8	192.168.2.3	0x9e0d	No error (0)	b.dxyzgame.com		104.21.74.240	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:09.198246002 CET	8.8.8.8	192.168.2.3	0x664f	No error (0)	connectini.net		162.0.210.44	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:09.201986074 CET	8.8.8.8	192.168.2.3	0xab06	No error (0)	www.google.com		142.250.185.164	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:09.631330967 CET	8.8.8.8	192.168.2.3	0x4e8	No error (0)	connectini.net		162.0.210.44	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:12.735085964 CET	8.8.8.8	192.168.2.3	0x5121	No error (0)	360devtracking.com		37.230.138.66	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:13.244292021 CET	8.8.8.8	192.168.2.3	0x2d8a	No error (0)	www.profitabletrustednetwork.com		192.243.59.12	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:13.244292021 CET	8.8.8.8	192.168.2.3	0x2d8a	No error (0)	www.profitabletrustednetwork.com		192.243.59.13	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:13.255242109 CET	8.8.8.8	192.168.2.3	0xba2b	No error (0)	source3.boys4dayz.com		104.21.33.188	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 18:01:13.255242109 CET	8.8.8.8	192.168.2.3	0xba2b	No error (0)	source3.boys4dayz.com		172.67.148.61	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:14.226411104 CET	8.8.8.8	192.168.2.3	0xbaa5	No error (0)	htagzdownload.pw		35.205.61.67	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:14.766592026 CET	8.8.8.8	192.168.2.3	0x36ac	No error (0)	c.xyzgamec.com		104.21.71.70	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:14.766592026 CET	8.8.8.8	192.168.2.3	0x36ac	No error (0)	c.xyzgamec.com		172.67.143.225	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:15.366584063 CET	8.8.8.8	192.168.2.3	0x6726	No error (0)	b.dxyzgame.com		104.21.74.240	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:15.366584063 CET	8.8.8.8	192.168.2.3	0x6726	No error (0)	b.dxyzgame.com		172.67.164.165	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:15.806950092 CET	8.8.8.8	192.168.2.3	0x260a	No error (0)	iplogger.org		148.251.234.83	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:17.200695038 CET	8.8.8.8	192.168.2.3	0xc8d	No error (0)	gp.gamebuy768.com		172.67.143.210	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:17.200695038 CET	8.8.8.8	192.168.2.3	0xc8d	No error (0)	gp.gamebuy768.com		104.21.27.252	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:18.169684887 CET	8.8.8.8	192.168.2.3	0x2fde	No error (0)	curtainshare.su		172.67.133.243	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:18.169684887 CET	8.8.8.8	192.168.2.3	0x2fde	No error (0)	curtainshare.su		104.21.5.229	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:24.179886103 CET	8.8.8.8	192.168.2.3	0xb349	No error (0)	iplogger.org		148.251.234.83	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:24.580885887 CET	8.8.8.8	192.168.2.3	0xc405	No error (0)	gp.gamebuy768.com		172.67.143.210	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:24.580885887 CET	8.8.8.8	192.168.2.3	0xc405	No error (0)	gp.gamebuy768.com		104.21.27.252	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:27.202059031 CET	8.8.8.8	192.168.2.3	0x4137	No error (0)	curtainshare.su		104.21.5.229	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:27.202059031 CET	8.8.8.8	192.168.2.3	0x4137	No error (0)	curtainshare.su		172.67.133.243	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:30.246517897 CET	8.8.8.8	192.168.2.3	0x6b0e	No error (0)	gp.gamebuy768.com		104.21.27.252	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:30.246517897 CET	8.8.8.8	192.168.2.3	0x6b0e	No error (0)	gp.gamebuy768.com		172.67.143.210	A (IP address)	IN (0x0001)
Jan 14, 2022 18:01:31.581506968 CET	8.8.8.8	192.168.2.3	0x67a8	No error (0)	toa.mygametoa.com		34.64.183.91	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- onepiece.s3.pl-waw.scw.cloud
- www.google.com
- 360devtracking.com
- vexacion.com
- www.directdexchange.com
- www.abebooks.com
- htagzdownload.pw

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 1nJGU59JPU.exe PID: 6704 Parent PID: 3044

General

Start time:	17:59:03
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\1nJGU59JPU.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\1nJGU59JPU.exe"
Imagebase:	0x400000
File size:	767327 bytes
MD5 hash:	AEA21AB88CCA720A34EC1C9C4794F82A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: 1nJGU59JPU.tmp PID: 6680 Parent PID: 6704

General

Start time:	17:59:04
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\is-5FEVP.tmp\1nJGU59JPU.tmp
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\is-5FEVP.tmp\1nJGU59JPU.tmp" /SL5="$22016E,506086,422400,C:\Users\user\Desktop\1nJGU59JPU.exe"
Imagebase:	0x400000
File size:	1076736 bytes
MD5 hash:	91D64D52451891441D23398DD3A6E05E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: 7((_8888YTR(.exe PID: 1364 Parent PID: 6680

General

Start time:	17:59:06
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\is-H3FQR.tmp\7((_8888YTR(.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\is-H3FQR.tmp\7((_8888YTR(.exe" /S /UID=rec7
Imagebase:	0x600000
File size:	571904 bytes
MD5 hash:	F97D18BAE067594234DC3EA8E06D10A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: Vahutuqeke.exe PID: 7024 Parent PID: 1364

General

Start time:	17:59:17
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\32-0401d-119-d44a2-34100e2dbea8e\Vahutuqeke.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\32-0401d-119-d44a2-34100e2dbea8e\Vahutuqeke.exe"
Imagebase:	0xf0000
File size:	589824 bytes
MD5 hash:	7F9B48E1096C162D3D0615E43D935A04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities — Show Windows behavior

File Created

File Read

Registry Activities — Show Windows behavior

Analysis Process: Kixysyshysy.exe PID: 5256 Parent PID: 1364

General

Start time:	17:59:19
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\8e-e5544-da4-a2b8a-aabe03824c51e\Kixysyshysy.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\8e-e5544-da4-a2b8a-aabe03824c51e\Kixysyshysy.exe"
Imagebase:	0xef0000
File size:	686080 bytes
MD5 hash:	D63BDAFB7AAA3B7C513EB42F1A867157
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities — Show Windows behavior

File Created

File Read

Registry Activities — Show Windows behavior

Analysis Process: irecord.exe PID: 4932 Parent PID: 1364

General

Start time:	17:59:24
Start date:	14/01/2022
Path:	C:\Program Files\internet explorer\ROOKKLCFJB\irecord.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\internet explorer\ROOKKLCFJB\irecord.exe" /VERYSILENT
Imagebase:	0x400000
File size:	6055915 bytes
MD5 hash:	F3E69396BFCB70EE59A828705593171A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: irecord.tmp PID: 6708 Parent PID: 4932

General

Start time:	17:59:26
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\is-2M9B3.tmp\irecord.tmp" /SL5="$50038,5808768,66560,C:\Program Files\internet explorer\ROOKKLCFJB\irecord.exe" /VERYSILENT
Imagebase:	0x400000
File size:	720896 bytes
MD5 hash:	B5FFB69C517BD2EE5411F7A24845C829
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: ZHunuhebaqu.exe PID: 6892 Parent PID: 3352

General

Start time:	17:59:31
Start date:	14/01/2022
Path:	C:\Program Files (x86)\Windows Multimedia Platform\ZHunuhebaqu.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files (x86)\windows multimedia platform\ZHunuhebaqu.exe"
Imagebase:	0x400000
File size:	34304 bytes
MD5 hash:	9D8A50291AF41031974A371A0F8C5601
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 34%, Metadefender, Browse • Detection: 78%, ReversingLabs
Reputation:	low

Analysis Process: ZHunuhebaqu.exe PID: 6916 Parent PID: 3352

General

General

Start time:	17:59:35
Start date:	14/01/2022
Path:	C:\Program Files (x86)\Windows Multimedia Platform\ZHunuhebaqu.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files (x86)\windows multimedia platform\ZHunuhebaqu.exe"
Imagebase:	0x510000
File size:	34304 bytes
MD5 hash:	9D8A50291AF41031974A371A0F8C5601
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: chrome.exe PID: 4864 Parent PID: 7024

General

Start time:	17:59:36
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.profitabletrustednetwork.com/e2q8zu9hu?key=a971bbe4a40a7216a1a87d8f455f71e6
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: I-Record.exe PID: 6244 Parent PID: 6708

General

Start time:	17:59:37
Start date:	14/01/2022
Path:	C:\Program Files (x86)\i-record\I-Record.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\i-record\I-Record.exe" -silent -desktopShortcut -programMenu
Imagebase:	0x780000
File size:	893952 bytes
MD5 hash:	13C3BA689A19B325A19AB62CBE4C313C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: chrome.exe PID: 6784 Parent PID: 7024

General

Start time:	17:59:39
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false

Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.profitabletrustednetwork.com/b1fsmdd9m?key=7e872dab99d78bffc4aa0c1e6b062dad
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: chrome.exe PID: 6868 Parent PID: 7024

General

Start time:	17:59:40
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1851483
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: chrome.exe PID: 3572 Parent PID: 7024

General

Start time:	17:59:42
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1851513
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Windows Update.exe PID: 5188 Parent PID: 6916

General

Start time:	17:59:42
Start date:	14/01/2022
Path:	C:\Program Files (x86)\Windows Multimedia Platform\Windows Update.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files (x86)\windows multimedia platform\Windows Update.exe"
Imagebase:	0xf60000
File size:	592384 bytes
MD5 hash:	D7CC834FB3ED6B3F67C017CD8FAA920C
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 20%, Metadefender, Browse • Detection: 79%, ReversingLabs
Reputation:	low

Analysis Process: chrome.exe PID: 4068 Parent PID: 7024

General

Start time:	17:59:43
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" http://www.directdexchange.com/jump/next.php?r=2087215
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: chrome.exe PID: 7020 Parent PID: 7024

General

Start time:	17:59:44
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.directdexchange.com/jump/next.php?r=4263119
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 4168 Parent PID: 4864

General

Start time:	17:59:45
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1556,9627623661114225042,16842326924946872670,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1908 /prefetch:8
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 7200 Parent PID: 7024

General

Start time:	17:59:46
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?id=1294231
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 7376 Parent PID: 7024

General

Start time:	17:59:47
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1492888&var=3
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 7648 Parent PID: 6784

General

Start time:	17:59:48
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1564,16917623383291386263,6472938917553362493,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1856 /prefetch:8
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 7768 Parent PID: 7024

General

Start time:	17:59:49
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1343177&var=3
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 5544 Parent PID: 6868

General

Start time:	17:59:51
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1536,6457543823163007411,15253291914772866949,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1728 /prefetch:8
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 8224 Parent PID: 7024

General

Start time:	17:59:51
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?id=1339680
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 8560 Parent PID: 3572

General

Start time:	17:59:53
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false

Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1532,10546296038144766013,8885457530477492480,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1852 /prefetch:8
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 9180 Parent PID: 7024

General

Start time:	17:59:55
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1620783&var=3
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 4456 Parent PID: 7024

General

Start time:	17:59:58
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?id=1343178
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 2948 Parent PID: 7024

General

Start time:	18:00:01
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.cloud-security.xyz/u/script/redirect.php?zoneid=465
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 6944 Parent PID: 7024

General

Start time:	18:00:03
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.cloud-security.xyz/u/script/redirect.php?zoneid=466
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 9188 Parent PID: 4068

General

Start time:	18:00:04
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1536,5678826982049071516,14035945569805029 64,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1860 /prefetch:8
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 8612 Parent PID: 7024

General

Start time:	18:00:05
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.profitabletrustednetwork.com/e2q8zu9hu?key=a971bbe4a40a7216a1a87d8f455f71e6
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 9420 Parent PID: 7024

General

Start time:	18:00:08
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.profitabletrustednetwork.com/b1fsmdd9m?key=7e872dab99d78bffc4aa0c1e6b062dad
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 9968 Parent PID: 7024

General

Start time:	18:00:10
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1851483
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 3244 Parent PID: 7024

General

Start time:	18:00:13
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1851513
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 4908 Parent PID: 7024

General

Start time:	18:00:16
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" http://www.directdexchange.com/jump/next.php?r=2087215

Imagebase:	0x7ff71aa50000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 5224 Parent PID: 7024

General

Start time:	18:00:19
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.directdexchange.com/jump/next.php?r=4263119
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 7620 Parent PID: 7024

General

Start time:	18:00:21
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?id=1294231
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 8032 Parent PID: 7024

General

Start time:	18:00:23
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1492888&var=3
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 10004 Parent PID: 7024

General

Start time:	18:00:25
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1343177&var=3
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 7800 Parent PID: 7024

General

Start time:	18:00:27
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?id=1339680
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 10324 Parent PID: 7024

General

Start time:	18:00:29
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?zoneid=1620783&var=3
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 10548 Parent PID: 7024

General

Start time:	18:00:31
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe

Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" http://vexacion.com/afu.php?id=1343178
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 10948 Parent PID: 7024

General

Start time:	18:00:36
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.cloud-security.xyz/u/script/redirect.php?zoneid=465
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 11136 Parent PID: 7024

General

Start time:	18:00:38
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.cloud-security.xyz/u/script/redirect.php?zoneid=466
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: chrome.exe PID: 6280 Parent PID: 7024

General

Start time:	18:00:41
Start date:	14/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" https://www.profitabletrustednetwork.com/e2q8zu9hu?key=a971bbe4a40a7216a1a87d8f455f71e6
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Disassembly

Code Analysis

