ID: 562527
Cookbook: browseurl.jbs
Time: 00:28:49
Date: 29/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

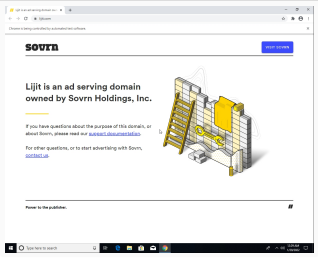
Windows Analysis Report

http://lijit.com

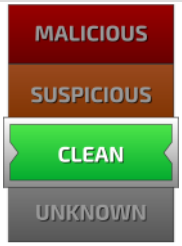
Overview

General Information

Sample URL:	http://lijit.com
Analysis ID:	562527
Infos:	



Detection

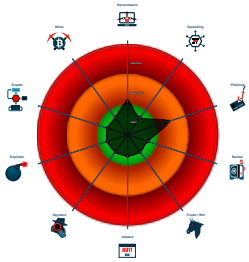


Score:	2
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Drops PE files
- Found iframes
- PE file contains sections with non-s…
- No HTML title found
- Form action URLs do not match ma…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6332 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "http://lijit.com MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6556 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1564,13595487648583302405,311083615002613945 9,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1932 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

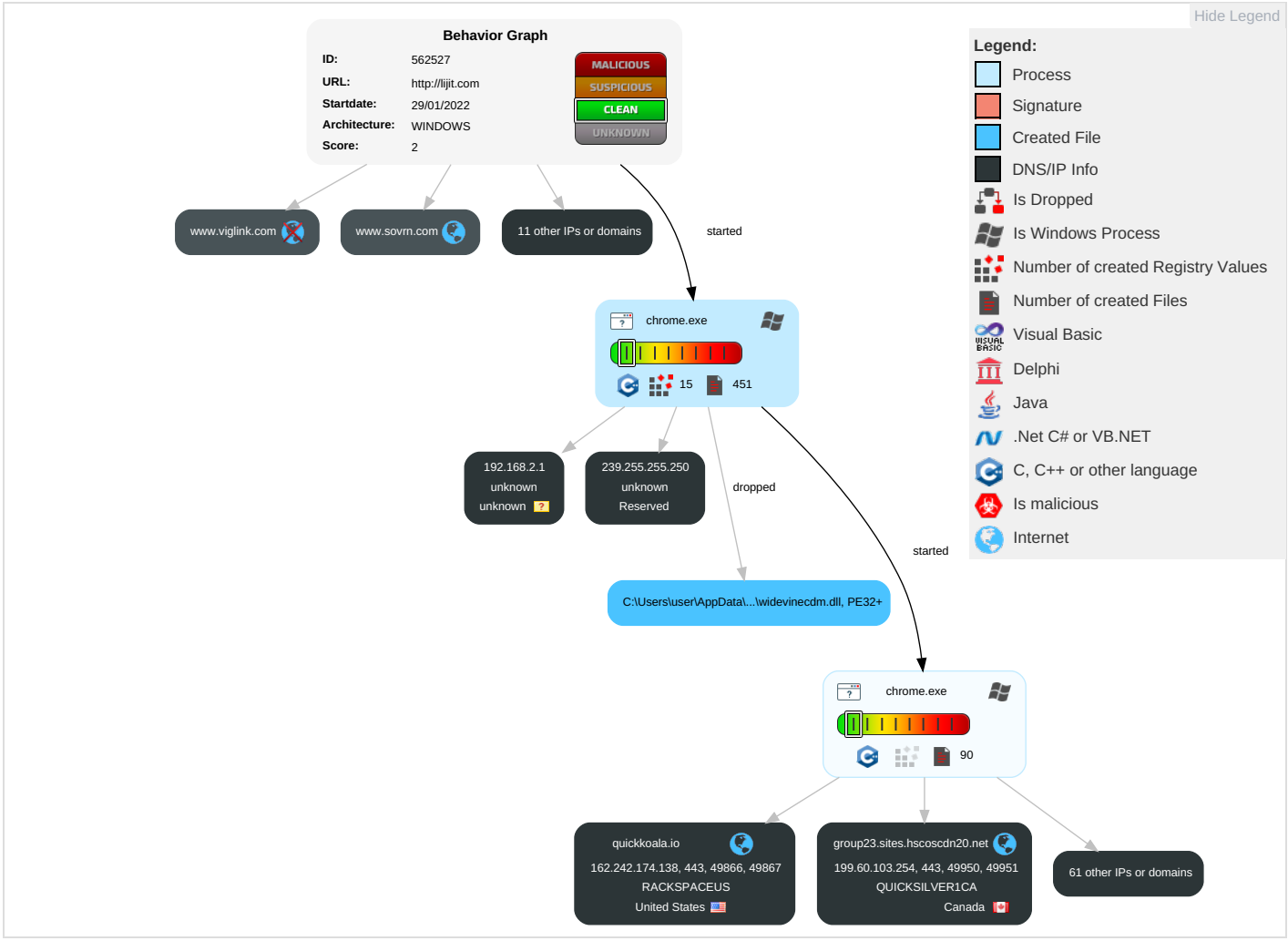
Jbx Signature Overview

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Drive-by Compromise	Windows Management Instrumentation	Path Interception	1 Process Injection	3 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

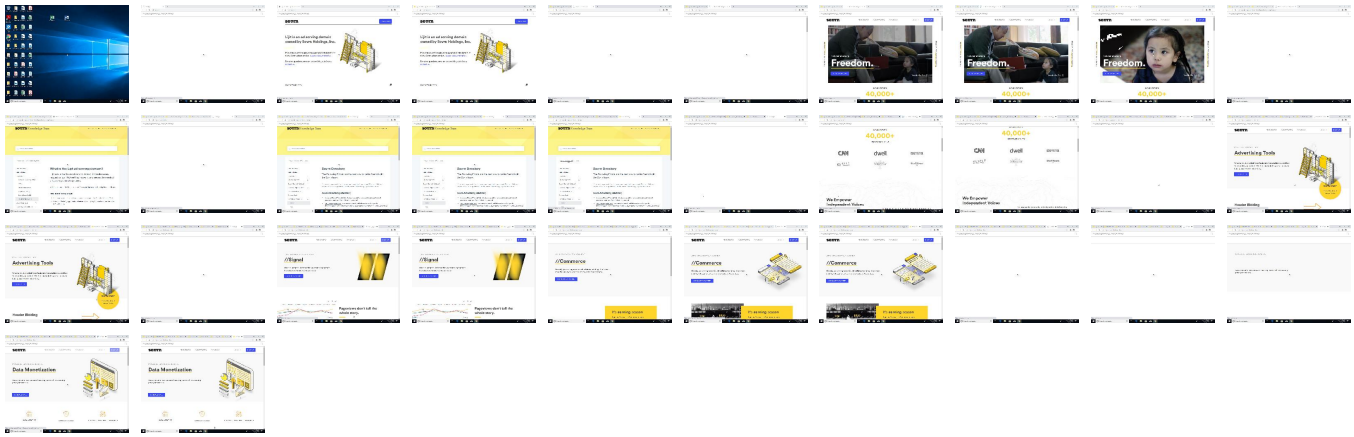
Behavior Graph

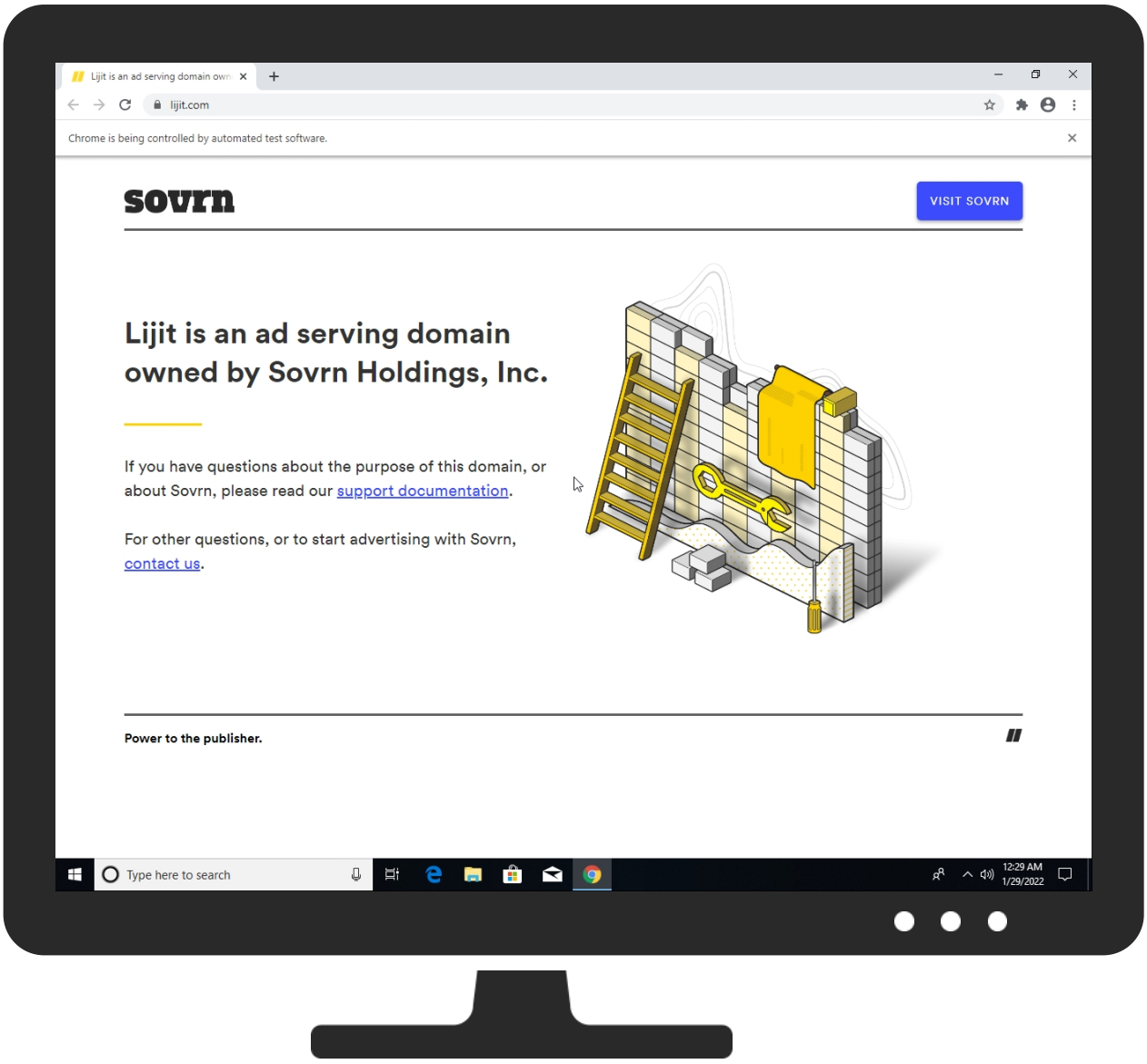


Screenshots

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
http://lijit.com	0%	Virustotal		Browse
http://lijit.com	0%	Avira URL Cloud	safe	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\6332_505347239_platform_specific\win_x64\widevinecdm.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\6332_505347239_platform_specific\win_x64\widevinecdm.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6332_505347239_platform_specific\win_x64\widevinecdm.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.googleoptimize.com	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
forms.hsforms.com	104.16.88.5	true	false		unknown
cdn2.hubspot.net	104.17.241.204	true	false		high
forms.hubspot.com	104.19.155.83	true	false		high
sovrn.com	34.135.254.63	true	false		high
d2mvl3dkxvehny.cloudfront.net	143.204.215.25	true	false		high
js.hs-analytics.net	104.17.68.176	true	false		unknown
1g3v9y2l2llh2lksnu1v316y-wpengine.netdna-ssl.com	94.31.29.99	true	false		high
ipapi.co	104.26.8.44	true	false		high
group23.sites.hscoscdn20.net	199.60.103.254	true	false		unknown
track.hubspot.com	104.19.155.83	true	false		high
fresnel.vimeocdn.com	34.120.202.204	true	false		high
js.hsforms.net	104.17.184.73	true	false		high
js.hs-scripts.com	104.17.210.204	true	false		high
web-2099239636.us-east-1.elb.amazonaws.com	3.227.218.120	true	false		high
js.hubspotfeedback.com	104.17.112.162	true	false		unknown
js.hs-banner.com	104.18.20.191	true	false		unknown
public.hubapi.com	104.17.201.204	true	false		high
a.nel.cloudflare.com	35.190.80.1	true	false		high
accounts.google.com	142.250.203.109	true	false		high
quickkoala.io	162.242.174.138	true	false		unknown
www-google-analytics.l.google.com	142.250.203.110	true	false		high
feedback.hubapi.com	104.17.200.204	true	false		high
app.hubspot.com	104.19.154.83	true	false		high
www-googletagmanager.l.google.com	172.217.168.8	true	false		high
vimeo.com	151.101.192.217	true	false		high
www.googleoptimize.com	142.250.203.110	true	false		unknown
vimeo.map.fastly.net	151.101.0.217	true	false		unknown
js.hsleadflows.net	104.17.231.204	true	false		unknown
js-na1.hs-scripts.com	104.17.211.204	true	false		high
f.hubspotusercontent20.net	104.16.187.114	true	false		unknown
clients.l.google.com	142.250.203.110	true	false		high
www.sovrn.com	34.135.254.63	true	false		high
googlehosted.l.googleusercontent.com	172.217.168.33	true	false		high
s.w.org	192.0.77.48	true	false		high
js.hscollectedforms.net	104.17.128.171	true	false		unknown
lijit.com	13.248.132.126	true	false		high
vimeo-video.map.fastly.net	151.101.114.109	true	false		unknown
v.pinimg.com	unknown	unknown	false		high
i.vimeocdn.com	unknown	unknown	false		high
ct.pinterest.com	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
use.fontawesome.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
www.viglink.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
f.vimeocdn.com	unknown	unknown	false		high
knowledge.sovrn.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
i.pinimg.com	unknown	unknown	false		high
assets.calendly.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
px.ads.linkedin.com	unknown	unknown	false		high
snap.licdn.com	unknown	unknown	false		high
s.pinimg.com	unknown	unknown	false		high
www.pinterest.ch	unknown	unknown	false		high
player.vimeo.com	unknown	unknown	false		high
www.pinterest.com	unknown	unknown	false		high

Contacted URLs

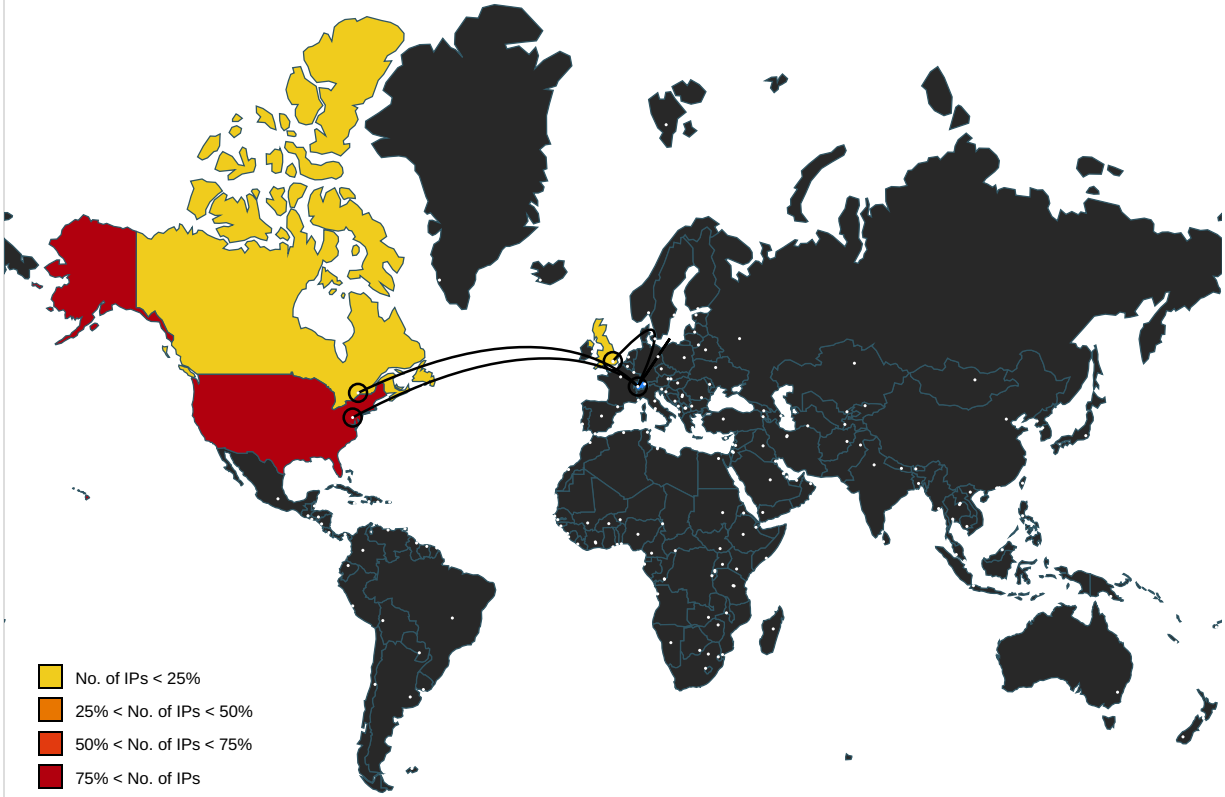
Name	Malicious	Antivirus Detection	Reputation
http://https://player.vimeo.com/video/180965741?color=5D9FE7&title=0&byline=0&portrait=0	false		high
http://https://lijit.com/	false		high
http://https://www.pinterest.ch/ct.html	false		high
http://https://www.sovrn.com/publishers/commerce/	false		high
http://https://knowledge.sovrn.com/what-is-the-lijit-ad-serving-domain	false		high
http://https://www.sovrn.com/	false		high
http://lijit.com/	false		high
http://https://www.sovrn.com/publishers/signal/	false		high
http://https://www.sovrn.com/publishers/data/	false		high
http://https://www.sovrn.com/advertising-tools/	false		high
http://https://www.sovrn.com/#content	false		high
http://https://player.vimeo.com/video/361117679?color=5D9FE7?color=5D9FE7&title=0&byline=0&portrait=0	false		high
http://https://knowledge.sovrn.com/contact-us	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://apis.google.com/js/client.js	mirroring_common.js.1.dr	false		high
http://https://www.google.com/images/cleardot.gif	craw_window.js.1.dr	false		high
http://https://play.google.com	2dd6a120-1e50-4e1c-9343-3106e141294e.tmp.3.dr, 8f53b7b9-af9d-41a5-aa8f-4d6a69835220.tmp.3.dr, 29df7120-4ea5-4e74-b7b4-fd59dfba73ed.tmp.3.dr	false		high
http://https://crash.corp.google.com/samples?reportid=&q=	common.js.1.dr, mirroring_cast_streaming.js.1.dr	false		high
http://https://www.google.com/log?format=json&hasfast=true	mirroring_hangouts.js.1.dr	false		high
http://https://sandbox.google.com/payments/v4/js/integrator.js	manifest.json0.1.dr, craw_window.js.1.dr	false		high
http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01	mirroring_hangouts.js.1.dr	false		high
http://https://accounts.google.com/MergeSession	craw_window.js.1.dr	false		high
http://https://preprod-hangouts-googleapis.sandbox.google.com	mirroring_hangouts.js.1.dr	false		high
http://https://lijit.com/2;Lijit	History Provider Cache.1.dr	false		high
http://https://www.google.com	2dd6a120-1e50-4e1c-9343-3106e141294e.tmp.3.dr, 8f53b7b9-af9d-41a5-aa8f-4d6a69835220.tmp.3.dr, manifest.json1.1.dr, 29df7120-4ea5-4e74-b7b4-fd59dfba73ed.tmp.3.dr	false		high
http://https://www.googleoptimize.com	2dd6a120-1e50-4e1c-9343-3106e141294e.tmp.3.dr, 29df7120-4ea5-4e74-b7b4-fd59dfba73ed.tmp.3.dr	false	• URL Reputation: safe	unknown
http://https://hangouts.clients6.google.com	mirroring_hangouts.js.1.dr	false		high
http://https://meet.google.com	mirroring_common.js.1.dr	false		high
http://https://hangouts.google.com/hangouts/_/logpref	mirroring_hangouts.js.1.dr	false		high
http://https://accounts.google.com	2dd6a120-1e50-4e1c-9343-3106e141294e.tmp.3.dr, 8f53b7b9-af9d-41a5-aa8f-4d6a69835220.tmp.3.dr, manifest.json1.1.dr, 29df7120-4ea5-4e74-b7b4-fd59dfba73ed.tmp.3.dr	false		high
http://https://clients2.google.com/cr/report	mirroring_hangouts.js.1.dr	false		high
http://angularjs.org	angular.js.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://creativecommons.org/publicdomain/zero/1.0/.	mirroring_hangouts.js.1.dr	false		high
http://https://github.com/angular/material	angular.js.1.dr, material_css_min.css.1.dr	false		high
http://https://apis.google.com	2dd6a120-1e50-4e1c-9343-3106e141294e.tmp.3.dr, 8f53b7b9-af9d-41a5-aa8f-4d6a69835220.tmp.3.dr, manifest.json1.1.dr, 29df7120-4ea5-4e74-b7b4-fd59dfba73ed.tmp.3.dr	false		high
http://https://www.google.com/accounts/OAuthLogin?issueuberauth=1	craw_window.js.1.dr	false		high
http://https://github.com/madler/zlib/blob/master/zlib.h	mirroring_hangouts.js.1.dr	false		high
http://https://www-googleapis-staging.sandbox.google.com	craw_background.js.1.dr, craw_window.js.1.dr	false		high
http://https://clients2.google.com	2dd6a120-1e50-4e1c-9343-3106e141294e.tmp.3.dr, 8f53b7b9-af9d-41a5-aa8f-4d6a69835220.tmp.3.dr, 29df7120-4ea5-4e74-b7b4-fd59dfba73ed.tmp.3.dr	false		high
http://https://www.google.com/tools/feedback	feedback_script.js.1.dr	false		high
http://www.apache.org/licenses/LICENSE-2.0	mirroring_hangouts.js.1.dr	false		high
http://https://dns.google	2dd6a120-1e50-4e1c-9343-3106e141294e.tmp.3.dr, 8f53b7b9-af9d-41a5-aa8f-4d6a69835220.tmp.3.dr, 29df7120-4ea5-4e74-b7b4-fd59dfba73ed.tmp.3.dr, d8d837a7-a1ab-4d3c-852b-02927a88920b.tmp.3.dr, 44f2ff87-727f-4f2c-8c13-d938c64150a1.tmp.3.dr	false	• URL Reputation: safe	unknown
http://https://github.com/google/closure-library/wiki/goog.module:-an-ES6-module-like-alternative-to-goog.p	craw_background.js.1.dr, craw_window.js.1.dr	false		high
http://https://www.google.com/intl/en-US/chrome/blank.html	craw_background.js.1.dr	false		high
http://https://ogs.google.com	2dd6a120-1e50-4e1c-9343-3106e141294e.tmp.3.dr, 8f53b7b9-af9d-41a5-aa8f-4d6a69835220.tmp.3.dr, 29df7120-4ea5-4e74-b7b4-fd59dfba73ed.tmp.3.dr	false		high
http://https://support.google.com/chromecast/troubleshooter/2995236	messages.json27.1.dr, messages.json83.1.dr, feedback.html.1.dr, messages.json28.1.dr, messages.json34.1.dr, messages.json17.1.dr, messages.json29.1.dr, messages.json48.1.dr, messages.json3.1.dr, messages.json62.1.dr, messages.json85.1.dr, messages.json4.1.dr, messages.json87.1.dr, messages.json86.1.dr, messages.json44.1.dr, messages.json69.1.dr, messages.json1.1.dr, messages.json18.1.dr, messages.json15.1.dr, messages.json33.1.dr, messages.json7.1.dr	false		high
http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions	mirroring_hangouts.js.1.dr	false		high
http://https://payments.google.com/payments/v4/js/integrator.js	manifest.json0.1.dr, craw_window.js.1.dr	false		high
http://https://www.google.com;	manifest.json1.1.dr	false	• Avira URL Cloud: safe	low
http://https://hangouts.google.com/	manifest.json1.1.dr	false		high
http://https://www.google.com/images/x2.gif	craw_window.js.1.dr	false		high
http://https://www.google.com/images/dot2.gif	craw_window.js.1.dr	false		high
http://https://meetings.clients6.google.com	mirroring_hangouts.js.1.dr	false		high
http://https://play.google.com/log?format=json&hasfast=true	mirroring_hangouts.js.1.dr	false		high
http://lijit.com/2;Lijit	History Provider Cache.1.dr	false		high
http://tools.ietf.org/html/rfc1950	mirroring_hangouts.js.1.dr	false		high
http://https://support.google.com/chromecast/answer/2998456	messages.json27.1.dr, messages.json83.1.dr, feedback.html.1.dr, messages.json28.1.dr, messages.json34.1.dr, messages.json17.1.dr, messages.json29.1.dr, messages.json48.1.dr, messages.json3.1.dr, messages.json62.1.dr, messages.json85.1.dr, messages.json4.1.dr, messages.json87.1.dr, messages.json86.1.dr, messages.json44.1.dr, messages.json69.1.dr, messages.json1.1.dr, messages.json18.1.dr, messages.json15.1.dr, messages.json33.1.dr, messages.json7.1.dr	false		high
http://https://clients2.googleusercontent.com	2dd6a120-1e50-4e1c-9343-3106e141294e.tmp.3.dr, 8f53b7b9-af9d-41a5-aa8f-4d6a69835220.tmp.3.dr, 29df7120-4ea5-4e74-b7b4-fd59dfba73ed.tmp.3.dr	false		high
http://https://docs.google.com	mirroring_common.js.1.dr	false		high
http://https://www.google.com/	manifest.json0.1.dr	false		high
http://https://feedback.googleusercontent.com	manifest.json1.1.dr	false		high
http://https://clients2.google.com/service/update2/crx	manifest.json0.1.dr, manifest.json.1.dr, manifest.json1.1.dr	false		high
http://https://clients6.google.com	mirroring_hangouts.js.1.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.26.8.44	ipapi.co	United States		13335	CLOUDFLARENETUS	false
104.19.155.83	forms.hubspot.com	United States		13335	CLOUDFLARENETUS	false
104.17.68.176	js.hs-analytics.net	United States		13335	CLOUDFLARENETUS	false
104.16.187.114	f.hubspotusercontent20.net	United States		13335	CLOUDFLARENETUS	false
104.18.20.191	js.hs-banner.com	United States		13335	CLOUDFLARENETUS	false
151.101.0.217	vimeo.map.fastly.net	United States		54113	FASTLYUS	false
199.60.103.254	group23.sites.hscoscdn20.net	Canada		23181	QUICKSILVER1CA	false
104.17.200.204	feedback.hubapi.com	United States		13335	CLOUDFLARENETUS	false
104.17.210.204	js.hs-scripts.com	United States		13335	CLOUDFLARENETUS	false
172.217.168.8	www-googletagmanager.l.google.com	United States		15169	GOOGLEUS	false
104.17.112.162	js.hubspotfeedback.com	United States		13335	CLOUDFLARENETUS	false
104.17.231.204	js.hsleadflows.net	United States		13335	CLOUDFLARENETUS	false
35.190.80.1	a.nel.cloudflare.com	United States		15169	GOOGLEUS	false
3.227.218.120	web-2099239636.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
104.17.128.171	js.hscollectedforms.net	United States		13335	CLOUDFLARENETUS	false
142.250.203.109	accounts.google.com	United States		15169	GOOGLEUS	false
104.17.201.204	public.hubapi.com	United States		13335	CLOUDFLARENETUS	false
94.31.29.99	1g3v9y2l2llh2lksnu1v316y-wpengine.netdna-ssl.com	United Kingdom		33438	HIGHWINDS2US	false
104.17.184.73	js.hsforms.net	United States		13335	CLOUDFLARENETUS	false
143.204.215.25	d2mvl3dkxvehny.cloudfront.net	United States		16509	AMAZON-02US	false
104.19.154.83	app.hubspot.com	United States		13335	CLOUDFLARENETUS	false
104.17.211.204	js-na1.hs-scripts.com	United States		13335	CLOUDFLARENETUS	false
162.242.174.138	quickkoala.io	United States		19994	RACKSPACEUS	false
151.101.114.109	vimeo-video.map.fastly.net	United States		54113	FASTLYUS	false
34.120.202.204	fresnel.vimeocdn.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
151.101.192.217	vimeo.com	United States		54113	FASTLYUS	false
34.135.254.63	sovrn.com	United States		2686	ATGS-MMD-ASUS	false
104.17.241.204	cdn2.hubspot.net	United States		13335	CLOUDFLARENETUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.217.168.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
104.16.88.5	forms.hsforms.com	United States		13335	CLOUDFLARENETUS	false
13.248.132.126	lijit.com	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562527
Start date:	29.01.2022
Start time:	00:28:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://lijit.com
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:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean2.win@46/200@56/34
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://www.sovrn.com/ • Browse: https://knowledge.sovrn.com/what-is-the-lijit-ad-serving-domain • Browse: https://www.sovrn.com/contact/ • Browse: https://www.sovrn.com/#content • Browse: https://www.sovrn.com/advertising-tools/ • Browse: https://www.sovrn.com/publishers/signal/ • Browse: https://www.sovrn.com/publishers/commerce/ • Browse: https://www.sovrn.com/publishers/data/

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WMIADAP.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 2.20.157.220, 2.20.156.69, 142.250.203.110, 173.194.182.73, 34.104.35.123, 142.250.203.99, 69.16.175.42, 69.16.175.10, 104.21.78.7, 172.67

.214.69, 2.20.156.249, 142.250.203.106, 104.18.14.176, 104.18.15.176, 92.123.101.114, 92.123.101.81, 95.101.180.83, 95.101.180.11, 13.107.42.14, 172.217.168.10, 172.217.168.42, 172.217.168.74

- Excluded domains from analysis (whitelisted): cds.s5x3j6q5.hwcdn.net, v.pinimg.com.edgesuite.net, e6449.dsca.akamaiedge.net, store-images.s-microsoft.com-c.edgekey.net, clientservices.googleapis.com, use.fontawesome.com.cdn.cloudflare.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, r4.sn-4g5e6ns7.gvt1.com, arc.msn.com, e12564.dspb.akamaiedge.net, 2-01-37d2-0006.cdx.cedexis.net, l-0005.l-msedge.net, redirector.gvt1.com, www.googletagmanager.com, 2-01-37d2-0018.cdx.cedexis.net, sovrnknowledge.wpengine.com, update.googleapis.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, e6449.a.akamaiedge.net, www.gstatic.com, prod.fs.microsoft.com.akadns.net, r4---sn-4g5e6ns7.gvt1.com, www.google-analytics.com, a1863.dscv.akamai.net, www-linkedin-com.l-0005.l-msedge.net, fs.microsoft.com, 2-01-37d2-0004.cdx.cedexis.net, content-autofill.googleapis.com, i-pinimg-com-cdn-cloudflare-net.pinimg.com.cdn.cloudflare.net, 2-01-37d2-0007.cdx.c
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA8321101
Malicious:	false
Reputation:	low
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:\Users\user\AppData\Local\Google\Chrome\User Data\0c14505d-0f2d-4fbf-9e74-8b568a2d0c1d.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):	198892
Entropy (8bit):	6.07410123231511
Encrypted:	false
SSDEEP:	6144:FFHm78s6OtziYLpDjqdHaqfIlUOoSiuR+:FFHFz4hLZSYo9
MD5:	BA6467EA2EACBF5065EE63B9A1139AC9
SHA1:	74B1A7199549D4EE5CB4627439E3D17FDEF83320
SHA-256:	7B10E6F448D11CC74E005AEDF0A8F0FC664DE897987C60810103D912F1F40099
SHA-512:	6A00A5EE8F798A0CD926D34026510C0661F68FC99590555E3B8A563D8D8F9E381E4DD0D30434ED5B8485B556A9A4DCE959DD5AE66C866E1E7058CAF730126C04
Malicious:	false
Reputation:	low
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":1.643444982326205e+12,"network":1.643412584e+12,"ticks":131326577.0,"uncertainty":4157582.0}},"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\234b1768-537f-4939-b41e-2731569afd32.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7454234657488144
Encrypted:	false
SSDEEP:	384:ZjO5lbcuXEbjVYeFgNNr+vRb36dbKHLGGuRr8/p1xivnfWrEJmUAi87VxFOO7Lx3:B6K1NqfkWEev9DLs/r+DKBfVRh
MD5:	3D70D0D13B5B1628A34647335335D53E
SHA1:	EF241E2B0BEA1BB4EFC18959438A685924508DE5
SHA-256:	489A45F65B1C97242473B00E19BF66145D7D9890AB971A6C8B48565A18DE3477
SHA-512:	DF04177ED166B0C4E9D1A5999547D1A117C508293E39596B60EB7240A543A9A0CF1C40EA2D6995A83CBC1A1E408B0C9D615B39872CB5988587656ED199514B65
Malicious:	false
Reputation:	low
Preview:	.t.....*...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...PR8.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\286b9a4f-04eb-4f26-9537-b4ee646db027.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):	190509
Entropy (8bit):	6.045384594781285
Encrypted:	false
SSDEEP:	3072:c/S1Cm78VKMvHOz5zXnZIFYLp964jYLftLt8aZpNPFcbXafIB0u1GOJmA3iuR+:WHm78s6OtziYLpDjqdHaqfIlUOoSiuR+

MD5:	A4B8C6B6B3F2CB1F1EA5D3ECB9AE805F
SHA1:	142357E174D8399296ABE9253917646617680034
SHA-256:	E143FE605F8EA847247AA08485A7A1E64303221D36B050AEE13B406D0A44A576
SHA-512:	58083D97510AFBEA98B6ED1B391CEB47E7F754095B882FCC4405F0A505081208A849287142D135CC9FE638424F3E12619AC356F2A4E9470C7D193AA2A27B78CA
Malicious:	false
Reputation:	low
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":1.643444982326205e+12,"network":1.643412584e+12,"ticks":131326577.0,"uncertainty":4157582.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799398844"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\72aad41b-6a0d-4dc3-b6d3-c649bd4f64dc.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):	198891
Entropy (8bit):	6.074102011842357
Encrypted:	false
SSDEEP:	6144:g/Hm78s6OtziYLpDjqdHaqfIlUOoSiuR+:g/HFz4hLZSYo9
MD5:	BC3C7AED1DA34204BE941C6BA1BF66CC
SHA1:	A988AED3AA3893D3F37676FF978A39506A8697CE
SHA-256:	73A8B3D0B8DE75648B31940667553123BE80EF6B17D5155A1FAD1EE2670E7CEF
SHA-512:	12DDF27EEB202FF4EC2FDCEC0866ECCFAD35783D01AD811B654D183031AF8AACDBC4199AB21CBCC6C2FE57C44DD1007B8E03E277AAC1E73FC8642DD3302(2DAE
Malicious:	false
Reputation:	low
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":1.643444982326205e+12,"network":1.643412584e+12,"ticks":131326577.0,"uncertainty":4157582.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+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\8c028a80-7257-4f23-aae9-e491b50354bd.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7450684000050636
Encrypted:	false
SSDEEP:	384:XjO5lbcuTbUFgNNr+vRb36dbKHLGGuRr8/p1xivnfWrEJmUX87VxFOO7LxNA1tsC:aK1NqfqWEev9DLs/r+DKBfVRy
MD5:	55B34D37EA1A686FBF47EDE525934CF1
SHA1:	81BF8BE86E19ABB519BFAEF1255D53F453B165B1
SHA-256:	B51D70EC350DEEF791C108E928C51BC2990085A7CCCB54DE0C93A049521440FC
SHA-512:	5CD03E95DC6F07879B7E838FD1001AB3D42D6CD03CD52169A2A99272493818E3F9BD4678AC0EB5525DEFFBE83E703257C65E30FE1D5BCF9D4AD0BFC4130E4I91
Malicious:	false
Reputation:	low
Preview:	0j.....*...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...PR8.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\92d025ba-bf1b-4223-9d91-acc100fd0c9b.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7453758716145127

Encrypted:	false
SSDEEP:	384:pjO5lbcuXEbjVYeFgNNr+vRb36dbKHLGGuRr8/p1xivnfWrEJmUX87VxFOO7LxN1:x6K1NqfqWEev9DLs/r+DKBfVR5
MD5:	ED67A6F7695CA706CEAB7B5A7384AA80
SHA1:	7771577F49B618E87F12901C37FEA96478D38617
SHA-256:	F4056F3E6C25294801278FA8914D40F24AEDA54912AECA2E1136CCF83D0737EE
SHA-512:	17918C0325F2C7067B041E10620F44345893A1861AC717F78A3F501AD50A0868787735B7E57F84805A3BD1CAEA6D32D36041ADE9675C5F8E653A4BDD8F3178CD
Malicious:	false
Reputation:	low
Preview:	.q.............*...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...PR8.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\Crashpad\settings.dat

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1n:+ftIE1n
MD5:	BD4642AD6C750A12D912B20BCB92E14D
SHA1:	C549F0F48FDD4FBC62E51AC26D7E185160CE2123
SHA-256:	4FD71FE78DFE203137C89C9FB0734358FF432F2BC83338112DC7B830F9B30F2C
SHA-512:	04410D12EF327614C3AF1251C9906BFEB2977211A7F53CBB08A8C01F9465A382CD001E51AB936A0D196D359F1DECDDAEAF5E7D1DBD49CE5F4FF91BF5C332B6 CF
Malicious:	false
Reputation:	low
Preview:	sdPC...................s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\115b5a41-6e74-41a4-9117-9d5dc0e6f3fa.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):	5170
Entropy (8bit):	4.985582566995888
Encrypted:	false
SSDEEP:	96:nhCngw9pcKICok0JCKL8o6ki1abOTQVuwn:nhCR9pcv4KJ6kiG
MD5:	CD10B88E82743E7914780954488E4FA6
SHA1:	51AAA501694EF586F7922A0C235AA3EEA525C853
SHA-256:	235B0B8003D51B2FB0F1A0F883BB8600CB887F35EEAA69FF2D13FF52AE9CDEBB
SHA-512:	57B539F2CCABBBA37951ED980ED42359D350FAA91FC2CD7FD7B8AD525DD60C516645F0FD5DF0C692CA9E9AAEB07D618965FC7138318CFC5C001FF5A8A44FE 01C
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287918580796209","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":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"co untryid_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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\29df7120-4ea5-4e74-b7b4-fd59dfba73ed.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):	2902
Entropy (8bit):	4.915525305755444
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDHz5sgGsOZRLsj0rtdsGzyKs+MH+sW3zseMHTsNMH+suMH95s+MHFfH:JTnOCXGDHzPe9r/z7GMLGAGYG9VGFfH

MD5:	1C2942E91DC8A5F22AFAC303C35D7522
SHA1:	F27084AC7B3016A863C65BAA64E4DFC9BC6188D4
SHA-256:	D3DA4F493F89C84D088451C5CA4CBD8D2FF5BBAA5E228E9FEB36B93196D16DC7
SHA-512:	8151859108B9CAD1F2C3516E6B4B77B099DB7731835C6BC6210EA9EA5DC4BB69F19E471705DDF79150C4299C9D735A0B3CFB2B87275BEF5A39ADCADBBA68E(B5
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","s upports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.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.c om","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"1329051058 2561014","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13290 510582606823","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alt

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2dd6a120-1e50-4e1c-9343-3106e141294e.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):	2658
Entropy (8bit):	4.912052883995867
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDH3qz5sgGsOZRLsj0rtdsGzyKs+MH+se5sNKrsHI5sXwbD:JTnOCXGDHazPe9r/z7GUWKuIQwH
MD5:	516532F0334889E55308A75DB6298C22
SHA1:	025CC477842DD27D42EEADC7FC8FF4CE63B9DF92
SHA-256:	D58136DD9CD58805A8BE884675D0779830CD591BF358FF5836850B6F31860BBE
SHA-512:	F2E31FA5873274343E8A1BC430118A770725A0B93C79785E68294C48EDE3EF0A4148BF0EEF0D66B3D05D02EDBB6984057B83C4DBDE3FE999635514BE9DA459D 5
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.google.com","s upports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.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.c om","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":"13290510582561014","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"}, {"alternative_service":[{"advertised_versions":[50],"expiration":"13290510582606823","port":443,"protocol_str":"quic"}],"isol

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\34edbd4a-e245-44ec-9b06-d0da1331cb0a.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):	370
Entropy (8bit):	5.520578756771285
Encrypted:	false
SSDEEP:	6:YAQNwdM9XRm9RfSHJR8wXwlmUUAnIMp5lLwQcVdM9SPWZ3osHdOa8wXwlmUUAnIK:Y6O09RAJ9+UAnIOLBcVVOtlx+UAnIOLH
MD5:	440D614101AD9E2683D4FA36FBF88C30
SHA1:	C9CFD59377833EE059A9DA55D988B40CB0C1C399
SHA-256:	F7F1B9D4880768AE9602D2079391DFF08D12149E631F61F9F0882A6651205A91
SHA-512:	A71D9C72EDC80C5F43D9D0AC7E6160A3D80DCD60A3E416E0C46C6481824BEC28D3F321AE8EE9B20E13BD77127C15C6B656CCEF7BD24156CCA9DC061ADAE5 A39D
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1674981051.499697,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains" :true,"sts_observed":1643445051.499702},{"expiry":1674981051.782686,"host":"opXOuPncEqRjkYSjAgcGEU30CFS/DB8Obxt4KuKod80=","mode":"force-https","sts_in clude_subdomains":true,"sts_observed":1643445051.782691}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\55eb8d88-6d41-4fc5-abaf-4925f73264a4.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):	17091
Entropy (8bit):	5.583369769228121
Encrypted:	false
SSDEEP:	384:8dFt/Ll6TXc1kXqKf/pUZNCgVLH2HfDUrUTtV4D:eLl8c1kXqKf/pUZNCgVLH2HfYrUpVo

MD5:	9185000E1BF63D496A7811B4CDE42454
SHA1:	1B128F23DEF91F480FB9EBB0BE148E34D09A82BF
SHA-256:	1BABBFEEF5FBBB0B6AFA03DAF27F41382B5149844F6558FB98E9DCE1E31DC57A
SHA-512:	D805CDAD28D177100DC84C6431F8E07AFEFCB52FCC08858A02111E34DF27748E5CD41155366E0B45556A0CC3EC10F08D38BDBA1636F539448774473C49077D9
Malicious:	false
Reputation:	low
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":"13287918580297409","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/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\55f32e52-4f3c-4ad5-8109-805f2757a9e2.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):	369
Entropy (8bit):	5.528278751242751
Encrypted:	false
SSDEEP:	6:YAQNwdMCmitNm9RfSHJR8wXwlmUUAnIMp5qcFkY4mVdMCVQ73osHdOa8wXwlmUUf:Y6qito9RAJ9+UAnIzcd4mVijlx+UAnI1
MD5:	E0B2CAAFBCA8AF33442AF51BB22CEF84
SHA1:	7F7E54478C80D22F555E3F5AD9EAA17F4BB47095
SHA-256:	4961B8112A73175FBC6F5F2D02C4AFB45BC4CEE478C32CAE4681C753FD5E3434
SHA-512:	FAA31326600D70ABA4E032965203E1841717F5BE2DFC22B5A2F67791C19EBCB257706C52D97EFF445A14FF45B396B0FF061AD8CA7071D4F4619F86899F223A7A
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1674981027.069689,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1643445027.069695},{"expiry":1674981027.153254,"host":"opXOuPncEqRjkYSjAgcGEU30CFS/DB8Obxt4KuKod80=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1643445027.15326}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\75348905-db1f-43ce-9f48-bef33cb71b44.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):	369
Entropy (8bit):	5.508137897788713
Encrypted:	false
SSDEEP:	6:YAQNwdMS7m9RfSHJR8wXwlmUUAnIMp5XABVdMIPk3osHdOa8wXwlmUUAnIMp5Xky:Y689RAJ9+UAnI1BVhPYlx+UAnI/G+Q
MD5:	12CE1492E1B86C99E228577E549F5BE6
SHA1:	BBA596660D73336EB2086B7E7249651F421C671C
SHA-256:	7E7D246309802DCCDC9931665C41F69C59B836DDE8770BF71C57D60A1910DEA0
SHA-512:	396C47C79FBDB7822B5ECA12F88084925AC4A67731F0F94688A3A796B8D0C792110C34CCFEBF4FDFC052033A35DD655D1C05F496AC34B79E1F274F83B1F6C05E
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1674981039.455405,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1643445039.45541},{"expiry":1674981039.552126,"host":"opXOuPncEqRjkYSjAgcGEU30CFS/DB8Obxt4KuKod80=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1643445039.552131}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\879c9b2a-5e33-4e1b-b8b2-62a2d22f69d3.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):	5210
Entropy (8bit):	4.991417113366523
Encrypted:	false
SSDEEP:	96:nhCNuw9pcKIfok0JCKL8o6ki17bOTQVuwn:nhCp9pck4KJ6ki1
MD5:	115731201E925D3D0B8E42D1371E63AA
SHA1:	65442BACC1FD039D8E57993F869B879CA2AC22C9
SHA-256:	35EC8F25C437C249F21627CCD6510961ED087F6C924F86393DBCA183E55A54C5

SHA-512:	F040AD0B5FB4A94630EA5B6325C7AC80925954BBDA544CA5DF752570DA88EFB0C00B3A387C97972B9C7C05E18DC7EA836AC88BC91C6C5CC155EA4222B047D F8
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287918580796209","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8c1675ad-0bc3-450b-ad1f-9f7a538b3c94.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):	5.3450451235555985
Encrypted:	false
SSDEEP:	6:YAQNwdQE9RfSHJR8wXwlmUUAnIMp5IZ2SQ:Y639RAJ9+UAnIpZZQ
MD5:	C57E67D67C866D676F4F38EFE6E44FF5
SHA1:	6372C201A192152B616B31B189C91EB8CA9AB5D8
SHA-256:	761E49E1E7FBD87BFB8A6541E32BAC02F4D4E5D637ACE5500E1B9625B946466B
SHA-512:	FFB5E0582B5E34929ABD22EA6328D20A5BF96AFC172BE03563B342D0A8A4F30673C8CFF4E0D98F1ABC148E7E07369C25A9466766B48CEE3F539EA7B9EF024A6 C
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1674980998.229781,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1643444998.229786}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8f53b7b9-af9d-41a5-aa8f-4d6a69835220.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):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD160
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\90249c99-f1c4-47f4-baf6-f0f08927c3bd.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):	5210
Entropy (8bit):	4.991521497682733
Encrypted:	false
SSDEEP:	96:nhCNuw9pcKIaok0JCKL8o6ki17bOTQVuwn:nhCp9pcn4KJ6ki1
MD5:	F31B4C171380959025B2A4A471F0D0B1
SHA1:	CA562BF55913B75AA5050296F552EE9407C4341E
SHA-256:	647396A17A45B326246EFF2533778A7F328C457C2713279037957AF1ACF43B59
SHA-512:	DC04A3CF615D6726F48FE154535F93C0E7BC26E25691695FAED0BE66DD7F90FF6AF3A23128E5FC5102C9BC5AD970E9AD6B6C810758F7AD38DA5CC364DF7D9 9F

Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287918580796209","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

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:	low
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+e5QxYbUscllJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_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):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhIktCK62v2P3OZQAWupWsYzCnvk=","L

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:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985D
Malicious:	false
Reputation:	low
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):	5.239162787045311
Encrypted:	false
SSDEEP:	6:M0F6q2PWXp+N23iKKdK25+Xqx8chI+IFUtqVTTIZmwYVTTLvzkwOWXp+N23iKKdP:M0F6va5KkTXfchI3FUtuk/0n75f5KkTM
MD5:	2C3D059896782E870018D2E00740A2AC
SHA1:	01CE85AED7C07E5463CD7A1D6EF21B83466C9837
SHA-256:	FD0E12D7324E7B869DEC2C8CCAD53C1A66E96B3E58F6ED0D6CDC9EC0E313DA9D
SHA-512:	73CB808AC2E36E6B0851123D4C2FC766E7553D8CC59F865E927D558C64B7BB0C0637D631487678684D6B0E37B3D25C87B33CA8FA04BCAE6E1BADADED8F5A7 D0
Malicious:	false
Reputation:	low
Preview:	2022/01/29-00:29:48.279 1940 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MA NIFEST-000001.2022/01/29-00:29:48.307 1940 Recovering log #3.2022/01/29-00:29:48.308 1940 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):	5.239162787045311
Encrypted:	false
SSDEEP:	6:M0F6q2PWXp+N23iKKdK25+Xqx8chI+IFUtqVTTIZmwYVTTLvzkwOWXp+N23iKKdP:M0F6va5KkTXfchI3FUtuk/0n75f5KkTM
MD5:	2C3D059896782E870018D2E00740A2AC
SHA1:	01CE85AED7C07E5463CD7A1D6EF21B83466C9837
SHA-256:	FD0E12D7324E7B869DEC2C8CCAD53C1A66E96B3E58F6ED0D6CDC9EC0E313DA9D
SHA-512:	73CB808AC2E36E6B0851123D4C2FC766E7553D8CC59F865E927D558C64B7BB0C0637D631487678684D6B0E37B3D25C87B33CA8FA04BCAE6E1BADADED8F5A7 D0
Malicious:	false
Reputation:	low
Preview:	2022/01/29-00:29:48.279 1940 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MA NIFEST-000001.2022/01/29-00:29:48.307 1940 Recovering log #3.2022/01/29-00:29:48.308 1940 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\History Provider Cache

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	903
Entropy (8bit):	5.444778245750569
Encrypted:	false
SSDEEP:	24:twB8NkwvsorDBGXHdlEe0F9hDVp2dPTdV2az0z2Cd:twB82wkoObdmgdLdUK0CCd
MD5:	353D53A9CE12022034FE5D2EA086C51D
SHA1:	D4A69CC208FE396968A0C5A1CF88F2D3E2AB5E19
SHA-256:	1C38B9B700DAF8972C6BD411F17B4397CA2600F606A884EE41AC454C660451D4
SHA-512:	4342D1B883E22031792275EFF9ABA9A4D1C385B4E869C1DF3FD68A4A312F8EF5BA7ED28902896697AA821756F9B87B260CB43F389E3E0F187F80D0F4DF1103B9
Malicious:	false

Reputation:	low
Preview:	............"Y....ad..an..by..com..domain..holdings..http..inc..is..lijit..owned..serving..sovrn..https*........ad......an......by......com......domain......holdings......http......https......inc.... ..is......lijit......owned......serving......sovrn..2.........a..........b........c.........d...........e.........g.........h..........i............j........l.........m.........n.............o............p.........r.........s...........t ....v.........w........y...:..B.....p...... ....*.http://lijit.com/2;Lijit is an ad serving domain owned by Sovrn Holdings, Inc.:................v...... ....*.https://lijit.com/2;Lijit is an ad serving domain owned by Sovrn Holdings, Inc.:....................J....................$'-7... ....$'-7

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent StateMP (copy)

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):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD160
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advert ised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","support s_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration": "13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true}, {"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"1324854350 1454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)

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):	5210
Entropy (8bit):	4.991417113366523
Encrypted:	false
SSDEEP:	96:nhCNuw9pcKIfok0JCKL8o6ki17bOTQVuwn:nhCp9pck4KJ6ki1
MD5:	115731201E925D3D0B8E42D1371E63AA
SHA1:	65442BACC1FD039D8E57993F869B879CA2AC22C9
SHA-256:	35EC8F25C437C249F21627CCD6510961ED087F6C924F86393DBCA183E55A54C5
SHA-512:	F040AD0B5FB4A94630EA5B6325C7AC80925954BBDA544CA5DF752570DA88EFB0C00B3A387C97972B9C7C05E18DC7EA836AC88BC91C6C5CC155EA4222B047D F8
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287918580796209","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":{"default_browser _infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"co untryid_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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences38 (copy)

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):	5183
Entropy (8bit):	4.98748407347224
Encrypted:	false
SSDEEP:	96:nhCr5w9pcKIAok0JCKL8o6ki1abOTQVuwn:nhCy9pct4KJ6kiG
MD5:	1D968E90268F8A6E69E414D2C51DA0F7
SHA1:	D6D4E005792DACA9B41F2497C406D09902A016E1
SHA-256:	B8C564D415D96A8C45818536138C8FE25BF8028B9ABF2457F77A90320C874C58
SHA-512:	5D3CA53A4C99EB16DE21622B1086A5A03D5574D0774FFB65FAF114D53F58C295E5175C330F796F17A40340C1705BB6C826EC05051B6FB17339B027D0B2BAEA9
Malicious:	false

Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287918580796209","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\PreferencesMP (copy)	
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):	5183
Entropy (8bit):	4.987630782876119
Encrypted:	false
SSDEEP:	96:nhCN5w9pcKI5ok0JCKL8o6ki1abOTQVuwn:nhCc9pcu4KJ6kiG
MD5:	21C5064018F4CAFE4FFD3FD15DF195CE
SHA1:	76D06D83B4CDEE3344475E06B0E9B07A24E0DF9C
SHA-256:	7BB2CFE106AFB8BD838309FA4A7DBFAA698AE9268038E3749E01DE7037DBFD3A
SHA-512:	0DC16B528A96D3532CFB69AC00253F00CEB546C963AADE03B2D87CC7E27DD6D14D276EB8387D8152AAE9717BA168B426CDCC2BAD240EFF5B1DF1DC708579 21E
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287918580796209","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferencess (copy)	
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):	5170
Entropy (8bit):	4.985582566995888
Encrypted:	false
SSDEEP:	96:nhCngw9pcKICok0JCKL8o6ki1abOTQVuwn:nhCR9pcv4KJ6kiG
MD5:	CD10B88E82743E7914780954488E4FA6
SHA1:	51AAA501694EF586F7922A0C235AA3EEA525C853
SHA-256:	235B0B8003D51B2FB0F1A0F883BB8600CB887F35EEAA69FF2D13FF52AE9CDEBB
SHA-512:	57B539F2CCABBBA37951ED980ED42359D350FAA91FC2CD7FD7B8AD525DD60C516645F0FD5DF0C692CA9E9AAEB07D618965FC7138318CFC5C001FF5A8A44FE 01C
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287918580796209","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	
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):	19182
Entropy (8bit):	5.570603518074017
Encrypted:	false
SSDEEP:	384:8dFtGLl6TXc1kXqKf/pUZNCgVLH2HfDUrU9HG7XV4m:FLl8c1kXqKf/pUZNCgVLH2HfYrUhGzVB
MD5:	2504C521462FFA3F7650B0D123C95608
SHA1:	33759EF22B006C1D47D83CADA2007BA12D2A6A31
SHA-256:	F59AE21845342E88D28022A31180F132EC30E52ED29C65B316F60A4FAE433423
SHA-512:	655F1D21A19513DD5382C2776B3238BEA158A1EBBD0ED89FF53E59016041302FE6895F712AC5C43DC01BA9AAD56C976022489412AE542EE341860FA6D11F4C8

Malicious:	false
Reputation:	low
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":"13287918580297409","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/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences.~ (copy)

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):	17092
Entropy (8bit):	5.583358157619263
Encrypted:	false
SSDEEP:	384:8dFtGLl6TXc1kXqKf/pUZNCgVLH2HfDUrUptV4j:FLl8c1kXqKf/pUZNCgVLH2HfYrU/Vs
MD5:	528A21054B79FDC21A0BBBFFC2577098
SHA1:	B4490065BA9CD6DBE5E934DD395C24ECCE5553AE
SHA-256:	38417A8FFA70EA76EE5D908C751716A3A02B33A58161DAC505F04E9C2CE753E0
SHA-512:	3509D327405368C27ED7AFDF244FC71C66F984D62FE90DF1550EDE1D5B9F5EDA924CB88DAA26A24515FA2D6E4ECAB8E61D13C2961D82168F39C6176E34E6389
Malicious:	false
Reputation:	low
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":"13287918580297409","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/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure PreferencesMP (copy)

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):	19181
Entropy (8bit):	5.570401189533755
Encrypted:	false
SSDEEP:	384:8dFtGLl6TXc1kXqKf/pUZNCgVLH2HfDUrU9HGQIV48:FLl8c1kXqKf/pUZNCgVLH2HfYrUhGjV3
MD5:	E6678AB72311C5547272ACCA4A68A55E
SHA1:	DF4DF5E59C5C1F813FDF8782C613800FE2A2E906
SHA-256:	A69DBBA67489030918C90FD6AB798C8DF392AFFD48DB46704598901C19E28595
SHA-512:	0F54F079CDCD85121BE918888494CAB0213F0756830F5D30976ABDE987C13DD84390D44DB664112CC45C13D5B9E4398B7639B90D6FDE6277F5CD98AB979899E
Malicious:	false
Reputation:	low
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":"13287918580297409","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/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D

SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898D58
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy)

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):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\d8d837a7-a1ab-4d3c-852b-02927a88920b.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):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\44f2ff87-727f-4f2c-8c13-d938c64150a1.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):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0

SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BI
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898 D58
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\00000 3.log

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	80
Entropy (8bit):	3.4921535629071894
Encrypted:	false
SSDEEP:	3:S8ltHlS+QUl1ASEGhTFljl:S85aEFljl
MD5:	69449520FD9C139C534E2970342C6BD8
SHA1:	230FE369A09DEF748F8CC23AD70FD19ED8D1B885
SHA-256:	3F2E9648DFDB2DDB8E9D607E8802FEF05AFA447E17733DD3FD6D933E7CA49277
SHA-512:	EA34C39AEA13B281A6067DE20AD0CDA84135E70C97DB3CDD59E25E6536B19F7781E5FC0CA4A11C3618D43FC3BD3FBC120DD5C1C47821A248B8AD351F9F4E6 367
Malicious:	false
Reputation:	low
Preview:	*...#.....version.1..namespace-..&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.206287925268551
Encrypted:	false
SSDEEP:	12:MbBva5KkkGHArAFUtubx21/0bRz5f5KkkGHArfJ:Mbta5KkkGgkgubDbRlf5KkkGgV
MD5:	38B5AE598456A42C61BE0562ED55B7C1
SHA1:	3E3B5EDF2226CBF7C617DDCA27DDDD21C24EF038
SHA-256:	EE2AFD8D483C1AC99531EDA1A7979010FD646CBA71FAC01DCF330C024D5B8202
SHA-512:	B611AFD9E11DA6E7008895A12DB883706A9CB8263D1B67E216F759E8434BDF29543AC0F23A642F984FB1A9F83A4F046B6C0715D8E92BE89246ED43893392CCB
Malicious:	false
Reputation:	low

Preview:	2022/01/29-00:30:38.653 19e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2022/01/29-00:30:38.655 19e4 Recovering log #3.2022/01/29-00:30:38.656 19e4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG.old (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.206287925268551
Encrypted:	false
SSDEEP:	12:MbBva5KkkGHArAFUtubx21/0bRz5f5KkkGHArfJ:Mbta5KkkGgkgubDbRlf5KkkGgV
MD5:	38B5AE598456A42C61BE0562ED55B7C1
SHA1:	3E3B5EDF2226CBF7C617DDCA27DDDD21C24EF038
SHA-256:	EE2AFD8D483C1AC99531EDA1A7979010FD646CBA71FAC01DCF330C024D5B8202
SHA-512:	B611AFD9E11DA6E7008895A12DB883706A9CB8263D1B67E216F759E8434BDF29543AC0F23A642F984FB1A9F83A4F046B6C0715D8E92BE89246ED43893392CCB2
Malicious:	false
Reputation:	low
Preview:	2022/01/29-00:30:38.653 19e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2022/01/29-00:30:38.655 19e4 Recovering log #3.2022/01/29-00:30:38.656 19e4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.33852578318741
Encrypted:	false
SSDEEP:	12:MqQdSVva5KkkOrsFUtumg/0GGI5f5KkkOrzJ:MrdMa5Kk+guAKf5Kkn
MD5:	B662AA21ED4D1409A26C8C86085CB4DF
SHA1:	2C955961EF978A204F52090C36FE69A855AFB810
SHA-256:	E970857783A0660DC441924D48783EF7D4F2C0F775EB3B0133E3483C6D80E67F
SHA-512:	E453EE87F4F69BCF3176C4AEE4C454298B151DE99D539AEDACD9EF34D3B4EE3BAD11BDE9FA4BB9B360181FEE3D35571054EC8E0942C4F82951CC2DF8AF43753A
Malicious:	false
Reputation:	low
Preview:	2022/01/29-00:31:13.709 1658 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2022/01/29-00:31:13.710 1658 Recovering log #3.2022/01/29-00:31:13.711 1658 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity (copy)

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):	369
Entropy (8bit):	5.528278751242751
Encrypted:	false
SSDEEP:	6:YAQNwdMCmitNm9RfSHJR8wXwlmUUAnIMp5qcFkY4mVdMCVQ73osHdOa8wXwlmUUf:Y6qito9RAJ9+UAnIzcd4mVijlx+UAnI1
MD5:	E0B2CAAFBCA8AF33442AF51BB22CEF84
SHA1:	7F7E54478C80D22F555E3F5AD9EAA17F4BB47095
SHA-256:	4961B8112A73175FBC6F5F2D02C4AFB45BC4CEE478C32CAE4681C753FD5E3434
SHA-512:	FAA31326600D70ABA4E032965203E1841717F5BE2DFC22B5A2F67791C19EBCB257706C52D97EFF445A14FF45B396B0FF061AD8CA7071D4F4619F86899F223A7A
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1674981027.069689,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1643445027.069695},{"expiry":1674981027.153254,"host":"opXOuPncEqRjkYSjAgcGEU30CFS/DB8Obxt4KuKod80=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1643445027.15326}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\VideoDecodeStats\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:	low
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\VideoDecodeStats\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:	low
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\VideoDecodeStats\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 75B
Malicious:	false
Reputation:	low
Preview:	.|.."....leveldb.BytewiseComparator.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a0f57b7f-15a8-4add-9594-69752f8a6e7d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D

SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\acb9ba26-ce5a-4c54-a131-5cc6673182df.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):	22596
Entropy (8bit):	5.536073558320569
Encrypted:	false
SSDEEP:	384:8dFtGLl6TXc1kXqKf/pUZNCgVLH2HfDUrU9HG2nTvdV49:FLl8c1kXqKf/pUZNCgVLH2HfYrUhG2nO
MD5:	EEF22D72314DD66FEF5D60C2614CA488
SHA1:	C3105B252898E48B5C6FC2C6422834B93BB61971
SHA-256:	6969B054C3CE2BFA303CC95200FFE7882B81421A7F9C57D68B5F801CB1EE8943
SHA-512:	09BC33B63EBBA896F63211712EA9E307F82F73A0D8B9C94F5126D22CF116F197B2E0C197942F8149F2CD557ACC253C09EF04B77E3B139C5EFA89C184D844A5A
Malicious:	false
Reputation:	low
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":"13287918580297409","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\ad7e8658-d9c5-46ad-9493-759b6105bb5d.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):	5183
Entropy (8bit):	4.98748407347224
Encrypted:	false
SSDEEP:	96:nhCr5w9pcKIAok0JCKL8o6ki1abOTQVuwn:nhCy9pct4KJ6kiG
MD5:	1D968E90268F8A6E69E414D2C51DA0F7
SHA1:	D6D4E005792DACA9B41F2497C406D09902A016E1
SHA-256:	B8C564D415D96A8C45818536138C8FE25BF8028B9ABF2457F77A90320C874C58
SHA-512:	5D3CA53A4C99EB16DE21622B1086A5A03D5574D0774FFB65FAF114D53F58C295E5175C330F796F17A40340C1705BB6C826EC05051B6FB17339B027D0B2BAEA9
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287918580796209","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b28552ad-d5d2-4fe4-8523-4bb4a7975418.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):	19181
Entropy (8bit):	5.570401189533755
Encrypted:	false
SSDEEP:	384:8dFtGLl6TXc1kXqKf/pUZNCgVLH2HfDUrU9HGQIV48:FLl8c1kXqKf/pUZNCgVLH2HfYrUhGjV3
MD5:	E6678AB72311C5547272ACCA4A68A55E
SHA1:	DF4DF5E59C5C1F813FDF8782C613800FE2A2E906
SHA-256:	A69DBBA67489030918C90FD6AB798C8DF392AFFD48DB46704598901C19E28595

SHA-512:	0F54F079CDCD85121BE918888494CAB0213F0756830F5D30976ABDE987C13DD84390D44DB664112CC45C13D5B9E4398B7639B90D6FDE6277F5CD98AB979899E
Malicious:	false
Reputation:	low
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":"13287918580297409","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\c51c6840-f23d-4888-86b9-be19fa89c4dc.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):	5183
Entropy (8bit):	4.98749782271158
Encrypted:	false
SSDEEP:	96:nhCN5w9pcKIDok0JCKL8o6ki1abOTQVuwn:nhCc9pcI4KJ6kiG
MD5:	4262012BA8C8F6166399F96D84DE2C61
SHA1:	2D628930E83042821ABA12EE01BD8526B46C38AD
SHA-256:	80BCFABFD1B43088DC0074B712C444D4A51403F1EA5E99976CCECDD41334683C
SHA-512:	6A7347408DF0CA22E9F99CD729BEE2009E4935A994897516E8364874751E527F2B9040E20892CF0588552DCDEC938F07C07B834A9B879D27C825EC5D4A5DD50A
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287918580796209","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c6cb2a18-575d-4fbe-91e7-cd0057dfda43.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):	17092
Entropy (8bit):	5.583358157619263
Encrypted:	false
SSDEEP:	384:8dFtGLl6TXc1kXqKf/pUZNCgVLH2HfDUrUptV4j:FLl8c1kXqKf/pUZNCgVLH2HfYrU/Vs
MD5:	528A21054B79FDC21A0BBBFFC2577098
SHA1:	B4490065BA9CD6DBE5E934DD395C24ECCE5553AE
SHA-256:	38417A8FFA70EA76EE5D908C751716A3A02B33A58161DAC505F04E9C2CE753E0
SHA-512:	3509D327405368C27ED7AFDF244FC71C66F984D62FE90DF1550EDE1D5B9F5EDA924CB88DAA26A24515FA2D6E4ECAB8E61D13C2961D82168F39C6176E34E638 9
Malicious:	false
Reputation:	low
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":"13287918580297409","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\data_reduction_proxy_leveldb\000004.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//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F

SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\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//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e071d94e-6cd9-4683-8d62-2329de97e7ce.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):	6023
Entropy (8bit):	5.20392423663439
Encrypted:	false
SSDEEP:	96:nhCNlw996SJTBcKIaok0JCKL8o6ki1uk8XTbOTQVuwn:nhCk9ThBcn4KJ6kiok8X
MD5:	C0D98B904B99FA8A65B29CAAEC5D556F
SHA1:	0B3AF56B35FBCD7BA44AA257CB3287FD562F000C
SHA-256:	3EBB2A0FE6691BDD223FACE3A6297B37D4CA29022FEFE44A984703A67003DCDB
SHA-512:	1175A64603664BBE40995C47BD31A0C494D23D21B7BB925802A74A75441B23923294C8EEB79071D8C137AC756A79811C5B58F277199CF174CA87022A425B55AE
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287918580796209","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\fb7cb7a9-f8c6-45b8-9298-8059bfa3ad91.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):	5183
Entropy (8bit):	4.987630782876119
Encrypted:	false
SSDEEP:	96:nhCN5w9pcKI5ok0JCKL8o6ki1abOTQVuwn:nhCc9pcu4KJ6kiG
MD5:	21C5064018F4CAFE4FFD3FD15DF195CE
SHA1:	76D06D83B4CDEE3344475E06B0E9B07A24E0DF9C
SHA-256:	7BB2CFE106AFB8BD838309FA4A7DBFAA698AE9268038E3749E01DE7037DBFD3A
SHA-512:	0DC16B528A96D3532CFB69AC00253F00CEB546C963AADE03B2D87CC7E27DD6D14D276EB8387D8152AAE9717BA168B426CDCC2BAD240EFF5B1DF1DC708579 21E
Malicious:	false
Reputation:	low

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287918580796209","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\fc4ece92-4727-4a59-b762-69c3949c2315.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):	19182
Entropy (8bit):	5.570603518074017
Encrypted:	false
SSDEEP:	384:8dFtGLl6TXc1kXqKf/pUZNCgVLH2HfDUrU9HG7XV4m:FLl8c1kXqKf/pUZNCgVLH2HfYrUhGzVB
MD5:	2504C521462FFA3F7650B0D123C95608
SHA1:	33759EF22B006C1D47D83CADA2007BA12D2A6A31
SHA-256:	F59AE21845342E88D28022A31180F132EC30E52ED29C65B316F60A4FAE433423
SHA-512:	655F1D21A19513DD5382C2776B3238BEA158A1EBBD0ED89FF53E59016041302FE6895F712AC5C43DC01BA9AAD56C976022489412AE542EE341860FA6D11F4C8
Malicious:	false
Reputation:	low
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":"13287918580297409","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\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691 724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	13
Entropy (8bit):	2.8150724101159437
Encrypted:	false
SSDEEP:	3:Yx7:4
MD5:	C422F72BA41F662A919ED0B70E5C3289
SHA1:	AAD27C14B27F56B6E7C744A8EC5B1A7D767D7632
SHA-256:	02E71EB4C587FEB7EE00CE8600F97411C2774C2FC34CB95B92D5538E7F30DA59
SHA-512:	86010ED2B2EEBDCC5A8A076B37703669C294C6D1BFAAEA963E26A9C94B81B4C53EC765D9425E5B616159C43923F800A891F9B903659575DF02F8845521F8DC4
Malicious:	false
Reputation:	low
Preview:	85.0.4183.121

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)	
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):	190416
Entropy (8bit):	6.045115893199996
Encrypted:	false
SSDEEP:	3072:T/S1Cm78VKMvHOz5zXnZlFYLp964jYLftLt8aZpNPFcbXafIB0u1GOJmA3iuR+:zHm78s6OtziYLpDjqdHaqfIlUOoSiuR+
MD5:	5833C6B53371CA24A1328DF0B9370DC7
SHA1:	093A4C42C9D9A030B064EDCB5748DD535515CA6A
SHA-256:	39A0BD5BC55E4CEA16CB0036700407ED536344479813D7734A1E43B09B8DFE1D
SHA-512:	787BD317A93026E3D0F98A190633196779759C04727132E8A3005EF8B5908BEE17AEEFE49AAB57CB516DE5D8C8919A77BA3E245AA621907B7503B4C88D6E310C
Malicious:	false
Reputation:	low
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":1.643444982326205e+12,"network":1.643412584e+12,"ticks":131326577.0,"uncertainty":4157582.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799398844"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State~ (copy)	
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):	198892
Entropy (8bit):	6.074102437533854
Encrypted:	false
SSDEEP:	6144:+gHm78s6OtziYLpDjqdHaqfIlUOoSiuR+:+gHFz4hLZSYo9
MD5:	FD2A59BCC436233E13CC33F42FD054D8
SHA1:	856B853E8F9BE96BD6CB70E398F27E881C918F4D
SHA-256:	E0328C9B2A5211D08296F41280B7BA0A0B80A2D9D94662D1778B59EEF606DEE1
SHA-512:	CB4BA1515F7A6A2F1CE7080E586A45E78D4F9557088D4927C5D26FE7A42E102F46DB67C7C07AD6DA2B935F49A4460B3BFBF73B7A23D56FE2B4BD4CE5962613EE
Malicious:	false
Reputation:	low
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":1.643444982326205e+12,"network":1.643412584e+12,"ticks":131326577.0,"uncertainty":4157582.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799398844"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7450684000050636
Encrypted:	false
SSDEEP:	384:XjO5lbcuTbUFgNNr+vRb36dbKHLGGuRr8/p1xivnfWrEJmUX87VxFOO7LxNA1tsC:aK1NqfqWEev9DLs/r+DKBfVRy
MD5:	55B34D37EA1A686FBF47EDE525934CF1
SHA1:	81BF8BE86E19ABB519BFAEF1255D53F453B165B1
SHA-256:	B51D70EC350DEEF791C108E928C51BC2990085A7CCCB54DE0C93A049521440FC
SHA-512:	5CD03E95DC6F07879B7E838FD1001AB3D42D6CD03CD52169A2A99272493818E3F9BD4678AC0EB5525DEFFBE83E703257C65E30FE1D5BCF9D4AD0BFC4130E4E91
Malicious:	false
Reputation:	low

Preview:	0j.....*...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...PR8.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\Module Info Cache\ (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7453758716145127
Encrypted:	false
SSDEEP:	384:pjO5lbcuXEbjVYeFgNNr+vRb36dbKHLGGuRr8/p1xivnfWrEJmUX87VxFOO7LxN1:x6K1NqfqWEev9DLs/r+DKBfVR5
MD5:	ED67A6F7695CA706CEAB7B5A7384AA80
SHA1:	7771577F49B618E87F12901C37FEA96478D38617
SHA-256:	F4056F3E6C25294801278FA8914D40F24AEDA54912AECA2E1136CCF83D0737EE
SHA-512:	17918C0325F2C7067B041E10620F44345893A1861AC717F78A3F501AD50A0868787735B7E57F84805A3BD1CAEA6D32D36041ADE9675C5F8E653A4BDD8F3178CD
Malicious:	false
Reputation:	low
Preview:	.q.....*...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...PR8.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\Module Info Cacheo (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7454234657488144
Encrypted:	false
SSDEEP:	384:ZjO5lbcuXEbjVYeFgNNr+vRb36dbKHLGGuRr8/p1xivnfWrEJmUAi87VxFOO7Lx3:B6K1NqfkWEev9DLs/r+DKBfVRh
MD5:	3D70D0D13B5B1628A34647335335D53E
SHA1:	EF241E2B0BEA1BB4EFC18959438A685924508DE5
SHA-256:	489A45F65B1C97242473B00E19BF66145D7D9890AB971A6C8B48565A18DE3477
SHA-512:	DF04177ED166B0C4E9D1A5999547D1A117C508293E39596B60EB7240A543A9A0CF1C40EA2D6995A83CBC1A1E408B0C9D615B39872CB5988587656ED199514B6
Malicious:	false
Reputation:	low
Preview:	.t.....*...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...PR8.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\bb43f43a-e858-421f-a169-1f3dbf2035c9.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):	190509
Entropy (8bit):	6.045384594781285
Encrypted:	false
SSDEEP:	3072:c/S1Cm78VKMvHOz5zXnZIFYLp964jYLftLt8aZpNPFcbXafIB0u1GOJmA3iuR+:WHm78s6OtziYLpDjqdHaqfIlUOoSiuR+
MD5:	A4B8C6B6B3F2CB1F1EA5D3ECB9AE805F
SHA1:	142357E174D8399296ABE9253917646617680034
SHA-256:	E143FE605F8EA847247AA08485A7A1E64303221D36B050AEE13B406D0A44A576
SHA-512:	58083D97510AFBEA98B6ED1B391CEB47E7F754095B882FCC4405F0A505081208A849287142D135CC9FE638424F3E12619AC356F2A4E9470C7D193AA2A27B78CA
Malicious:	false
Reputation:	low

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":1.643444982326205e+12,"network":1.643412584e+12,"ticks":131326577.0,"uncertainty":4157582.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799398844"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\c850b744-ce15-4a54-9799-52a0e4b547bd.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):	190509
Entropy (8bit):	6.045384594781285
Encrypted:	false
SSDEEP:	3072:c/S1Cm78VKMvHOz5zXnZIFYLp964jYLftLt8aZpNPFcbXafIB0u1GOJmA3iuR+:WHm78s6OtziYLpDjqdHaqfIlUOoSiuR+
MD5:	A4B8C6B6B3F2CB1F1EA5D3ECB9AE805F
SHA1:	142357E174D8399296ABE9253917646617680034
SHA-256:	E143FE605F8EA847247AA08485A7A1E64303221D36B050AEE13B406D0A44A576
SHA-512:	58083D97510AFBEA98B6ED1B391CEB47E7F754095B882FCC4405F0A505081208A849287142D135CC9FE638424F3E12619AC356F2A4E9470C7D193AA2A27B78CA
Malicious:	false
Reputation:	low
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":1.643444982326205e+12,"network":1.643412584e+12,"ticks":131326577.0,"uncertainty":4157582.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799398844"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\d3b0b81e-a8ca-4c5a-96ca-4654e0248975.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):	190416
Entropy (8bit):	6.045115893199996
Encrypted:	false
SSDEEP:	3072:T/S1Cm78VKMvHOz5zXnZIFYLp964jYLftLt8aZpNPFcbXafIB0u1GOJmA3iuR+:zHm78s6OtziYLpDjqdHaqfIlUOoSiuR+
MD5:	5833C6B53371CA24A1328DF0B9370DC7
SHA1:	093A4C42C9D9A030B064EDCB5748DD535515CA6A
SHA-256:	39A0BD5BC55E4CEA16CB0036700407ED536344479813D7734A1E43B09B8DFE1D
SHA-512:	787BD317A93026E3D0F98A190633196779759C04727132E8A3005EF8B5908BEE17AEEFE49AAB57CB516DE5D8C8919A77BA3E245AA621907B7503B4C88D6E310C
Malicious:	false
Reputation:	low
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":1.643444982326205e+12,"network":1.643412584e+12,"ticks":131326577.0,"uncertainty":4157582.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799398844"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\dbe4c257-2bcd-4a36-9233-536c8b695ddd.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):	198892
Entropy (8bit):	6.07410229907798
Encrypted:	false
SSDEEP:	6144:0IHm78s6OtziYLpDjqdHaqfIlUOoSiuR+:0IHFz4hLZSYo9
MD5:	4FE4AF6AFAEC856569F0250D3AA04116
SHA1:	AD552ADB85EFB723925170EC9952881C48136D10
SHA-256:	8EF93A8F44672D23A0A53423DD33B6F1388B062CA093F7BEF7E3B37D75FA7320
SHA-512:	E3E1CD1BE060F2F79DFF340296328094B4D31E45646381DE485CB9F7D3EA269E1A6095DEF9E1E876502BA49464CB1B4C647742A558709967D65E35EC2D39302D

Malicious:	false
Reputation:	low
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":1.643444982326205e+12,"network":1.643412584e+12,"ticks":131326577.0,"uncertainty":4157582.0}},"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\e17f27f0-d788-42ab-8861-2938d70bf031.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):	198892
Entropy (8bit):	6.074102437533854
Encrypted:	false
SSDEEP:	6144:+gHm78s6OtziYLpDjqdHaqfIlUOoSiuR+:+gHFz4hLZSYo9
MD5:	FD2A59BCC436233E13CC33F42FD054D8
SHA1:	856B853E8F9BE96BD6CB70E398F27E881C918F4D
SHA-256:	E0328C9B2A5211D08296F41280B7BA0A0B80A2D9D94662D1778B59EEF606DEE1
SHA-512:	CB4BA1515F7A6A2F1CE7080E586A45E78D4F9557088D4927C5D26FE7A42E102F46DB67C7C07AD6DA2B935F49A4460B3BFBF73B7A23D56FE2B4BD4CE5962613EE
Malicious:	false
Reputation:	low
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":1.643444982326205e+12,"network":1.643412584e+12,"ticks":131326577.0,"uncertainty":4157582.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799398844"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\e85783a3-90b8-42b0-9632-19fb70e02625.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):	190416
Entropy (8bit):	6.045114684171741
Encrypted:	false
SSDEEP:	3072:j/S1Cm78VKMvHOz5zXnZIFYLp964jYLftLt8aZpNPFcbXafIB0u1GOJmA3iuR+:jHm78s6OtziYLpDjqdHaqfIlUOoSiuR+
MD5:	0550FE96E3A19613C54CFB3A3E16BF64
SHA1:	29DC1F8FD6D39F8D8C0EF82F81C3EE5DC600D8AE
SHA-256:	936130630EDA6C93E35BA93D7DD98E4F1B6C2FC2BFC282121656AA3BE2B6C041
SHA-512:	39AABAD04226E48A17951FA37C725407FBC252D9F6769A2EF0586C488CD02F9AF0F7A0E7AF817712776A1D29C363E6AAA62215D968271BF00A84502496C82254
Malicious:	false
Reputation:	low
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":1.643444982326205e+12,"network":1.643412584e+12,"ticks":131326577.0,"uncertainty":4157582.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799398844"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\fb3337b7-89f6-45da-af06-ec730691aeb6.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):	190416
Entropy (8bit):	6.045114684171741
Encrypted:	false
SSDEEP:	3072:j/S1Cm78VKMvHOz5zXnZIFYLp964jYLftLt8aZpNPFcbXafIB0u1GOJmA3iuR+:jHm78s6OtziYLpDjqdHaqfIlUOoSiuR+
MD5:	0550FE96E3A19613C54CFB3A3E16BF64
SHA1:	29DC1F8FD6D39F8D8C0EF82F81C3EE5DC600D8AE

SHA-256:	936130630EDA6C93E35BA93D7DD98E4F1B6C2FC2BFC282121656AA3BE2B6C041
SHA-512:	39AABAD04226E48A17951FA37C725407FBC252D9F6769A2EF0586C488CD02F9AF0F7A0E7AF817712776A1D29C363E6AAA62215D968271BF00A84502496C82254
Malicious:	false
Reputation:	low
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":1.643444982326205e+12,"network":1.643412584e+12,"ticks":131326577.0,"uncertainty":4157582.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799398844"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\158a74fc-cbb2-4ca5-90d1-6a862d2eac42.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\6332_505347239_metadata\verified_contents.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):	1448
Entropy (8bit):	5.971745384085355
Encrypted:	false
SSDEEP:	24:pZRj/flTyyRTGYGRM86CAjkVmdZzUU7aoXtu0tSPqNnQoXCrBJr4k0UpLaahl6mc:p/hyyj7qAdZzUU7aktuLinQkCdJr70Uy
MD5:	3E59AFF1F633A40146220723D49FF69D
SHA1:	91114719E0FAE4D557857A57BFCEF4A621AAFAAA
SHA-256:	5EFF1D2049B3AFDB8F44C4C68DEB1B0F5081B43C9A1BE5AAC32B741CCC6016B3
SHA-512:	75E4EB0141E6E6F547E58D215DEDC2BFB7C9431015097859783302E9A770695AF9C4AC775101A2309468A1431D20483BCF4B204FC706CF5EBF605E6FD9E5864A
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMvd2luX3g2NC93aWRldmluZWNkbS5kbGwiLCJyb290X2hhc2giOiJUVWprbmV5ZDNlZmRVR0p0WnM0elNBbXRWLTREcEQ4TXM0UW5rZE1MVTBvIn0seyJwYXRoIjoiX3BsYXRmb3JtX3NwZWNpZmljL3dpbl94NjQvd2lkZXZpbmVjZG0uZGxsLnNpZyIsInJvb3RfaGFzaCI6IjJ3eXRkUHVFY3U1MDdJenRuN2VKOUNwQVd5ZVdXU0xoekdGQVlXQklfZkUifSx7InBhdGgiOiJtYW5pZmVzdC5qc29uIiwicm9vdF9oYXNoIjoicW9aS2xCRVJoTzIybXpwaEctZzFHNjQyc0pCRjNuN3laUzRWYlEwT3JZayJ9XSwiZm9ybWF0IjoidHJlZWhhc2giLCJoYXNoX2Jsb2NrX3NpemUiOjQwOTZ9XSwiaXRlbV9pZCI6Im9pbW9tcGVjYWduYWpkZWpnbm5qaWpvYmViYWVpZ2VrIiwiaXRlbV92ZXJzaW9uIjoiNC4xMC4yMzkxLjAiLCJwcm90b2NvbF92ZXJzaW9uIjoxfQ","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"J_varh3pbSCuoxRJJKBMABg5gxFq57n03z43XkUWJM7oy3eWRQ133bpCLFZB9QxF4hEr0j3QkT-oGRSGF8e2UNhauTxV8FmTjYoSF34D_idMe81x8xr_sKSshYV0BJC5VPDDw9-FcorpDHeeOmgpnBf

C:\Users\user\AppData\Local\Temp\6332_505347239_platform_specific\win_x64\widevinecdm.dll

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	10053976
Entropy (8bit):	7.433454408979122
Encrypted:	false
SSDEEP:	98304:sQ8AwzExgSMcgTnSUpCSDVLcyjbc2ZFWReP+klU/6CFNbnVzHyJJwN19hzjS1SJ:sQLw6Mce5p3VQyjbc0va/PFNzlyJahZJ
MD5:	55CE1BB968F23F546ED9E683050954A7
SHA1:	8088DED3DDF9D27700E470A75CFA7FA2EF565731
SHA-256:	6CB80D4B43B81D2C1DF133565638D3471E108702AE5FAED47300F3AE15BAA33D

SHA-512:	7F4F27EF9C7F571CD6C04305C6CE0A75CA0F7BDC4587A438133794418C530F0E95BF19B56DB120AA49DC96626E80058E567C47EC66B2813FD3A6A146AF1054A
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..d.....\`....." .....lS...E.....P.....2.....LS ....`A.....(.....x....02.....0.T....J..X....@2..;.....p..(.....0.....text....kS.....lS..... ..`.rdata...SD...S..T D..pS.....@..@.data...X.....2.....@....pdata..T.....0.....@..@.00cfg..(.....1.....@..@.rodata.....2..... ..`.tls....1....2.....@.. ._RDATA..... 2.....@..@.rsrc.....02.....@..@.reloc..;...@2..<.....@..B..... ....

C:\Users\user\AppData\Local\Temp\6332_505347239_platform_specific\win_x64\widevinecdm.dll.sig

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1427
Entropy (8bit):	7.570377692439448
Encrypted:	false
SSDEEP:	24:38H/VZn47VBRxgCUQuODHBJeriJ8yojUdnkLvXWgl0oHLrUXAo8/f6Lu57x/:38HdurRxHSOlAiqYoXWVDX6XYu57x/
MD5:	EDEC647D2132F0F988F43BFCBA5932BA
SHA1:	3B16ABF4669A598A0095556D5DBBDCA0D448E654
SHA-256:	DB0CAD74FB8472EE74EC8CED9FB789F42A405B27965922E1CC6140616048FDF1
SHA-512:	005613A96CBE17C8482FBD973AFF8DF9D93C4D1BE8B9A01019E2436CDDF085BCD8748E1863221A3E15D541829C4BF81779F5A049255101F5CB7EA68DF92C773
Malicious:	false
Reputation:	low
Preview:	....0...0.....6cd/+J.v{..B...0...*.H.....0}1.0...U....US1.0...U....Washington1.0...U....Kirkland1.0...U....Google1.0...U....Widevine1"0 ..U....widevine-codesign-root-ca0.. .171013173909Z..271011173909Z0y1.0...U....US1.0...U....Washington1.0...U....Kirkland1.0...U....Google1.0...U....Widevine1.0...U....widevine-vmp-codesign0.."0...*.H..... .....0.....2F..8.e..-....$r...{^.....0.%.HA...sA"D.q.=6...#.J.N.....&..k;.+...<xF.....B8.)S....o..\|Ci.F.A6....J.....Y..4..{.5u.9N...=...#.M..s.F!j.f%&ld.R...?!Ot@.....#.f..O.. [.V.p0y....+...S.]....M.=.9...>.. .....>.:....1tl.....`D/c..j.....0..0...U.....L...cC.E..R.n...$.0...U.#..0....=..tW....!.B.#U).0...U....0.0...U.....0...U.%..0...+.....0...+.....y.....0...*.H. .....g..".[..t{.4~.,.G....4K.....(x$...} .*...N..b\|d.....h..u6?.L.(&.Oup...$!...4R. 5.-...s...K/..U[..[.+.sAX*.~...^0..ba>;.#....x...b.-1...E..l....S.n.a....)U .q..C>d:...<[..F5...7...[.-.l}.T Lc.X..Qf...z..:.Q..e.m

C:\Users\user\AppData\Local\Temp\6332_505347239\manifest.fingerprint

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.8618480997673856
Encrypted:	false
SSDEEP:	3:S4VW243EXtcQXQ8OUJGb00JpgUu:S7t3E+CLOZo0J6Uu
MD5:	9546E4EF0287DB27186BBCCF94ACA349
SHA1:	EB373F0CA09AE7EDF54E9637934B9E406F68BEE6
SHA-256:	08EBFF0F0F9DE95708F24ED2115634D44D8691648892D9BE449766F3677A0D8A
SHA-512:	ED90C91C641034BF6233BC442103988F5F685D0E1A6D84AEB6B67A2BFA6A4E99F48747B3C08C09A200C8487C461B0EB0D6AF68E54E4028EA611DE0EC24E401C 5
Malicious:	false
Reputation:	low
Preview:	1.e80345a4828e2b82d049520da48dc125df0c2600b1e4591cd05c71bb661231e5

C:\Users\user\AppData\Local\Temp\6332_505347239\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	825
Entropy (8bit):	4.819458905604673
Encrypted:	false
SSDEEP:	24:ulaihI11P1TRuRckckH3WoA0UNqLQxUNqmTb:C1hY91uRfckHksJ
MD5:	E15CE41AD7AB84F270A12DB01724A30D
SHA1:	DA82BF4C88965850A2EA06BC2E4A090F523D7DEA
SHA-256:	AA864A94111184EDB69B3A611BE8351BAE36B09045DE7EF2652E156D0D0EAD89
SHA-512:	51DA142996B586539DB044821E3D3FEA2A60D5F53F165976C770385B10B8B3A3A81078D8710F8984F45E7F09DC035296A7C6C7AA85791EF7BD2022AAC2DA0134

Malicious:	false
Reputation:	low
Preview:	{. "manifest_version": 2,. "update_url": "https://clients2.google.com/service/update2/crx",. "name": "WidevineCdm",. "description": "Widevine Content Decryption Module",. "version": "4.10.2391.0",. "minimum_chrome_version": "68.0.3430.0",. "x-cdm-module-versions": "4",. "x-cdm-interface-versions": "10",. "x-cdm-host-versions": "10",. "x-cdm-codecs": "vp8,vp09,avc1,av01",. "x-cdm-persistent-license-support": true,. "x-cdm-supported-encryption-schemes": [. "cenc",. "cbcs".],. "icons": {. "16": "imgs/icon-128x128.png",. "128": "imgs/icon-128x128.png". },. "platforms": [. {. "os": "win",. "arch": "x64",. "sub_package_path": "_platform_specific/win_x64/". },. {. "os": "win",. "arch": "x86",. "sub_package_path": "_platform_specific/win_x86/". }.].}

C:\Users\user\AppData\Local\Temp\6d5aad07-871e-4d9e-9989-f882409c40d9.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	768843
Entropy (8bit):	**7.992932603402907**
Encrypted:	**true**
SSDEEP:	12288:cK2ED9wjXNC1Gse83ru82/u0eKhgxuPFrDXgtbPz54Pm1D0fBmfH1sBrJ9mTiDga:cK2ED9I48seur0/uZKCuPNbgtbz6m1ob
MD5:	A11D5CAF6BF849AEB84B0C95B1C3B7CF
SHA1:	27F410CCBD75852C01C7464A1FD7EF8C29BE3916
SHA-256:	D0E62ACE64AFC334330A7AC3A2CC657914FEB321F1F89AEE11D2A6D0E7D81C31
SHA-512:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB590
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....6W..>Nuw9..R{c...Nq.H.K..A!....`v.k+..?.5.>v....;._~....tp....x.q.V...7.m.O.~.{!.o/q.'..BK..4./?'.....L..fH&.._<..&.p.k^..\s...:1y..F.N.+...X.PO@Mo....X.G1:..Y.@;..j.....=ae...0.....DU....n...n.;.lpr..Q....:... <....a.Y....{ei.....0..0...*.H.....0.....Mbh=.[O}.+..U.KHF(n3.\"...,g.c...6)..(.E...U...#.i.a.:...N.....P...x.O...(mC;|.5.S.{m.aEx...[..fP.i`.y..5..R....v.$.....l-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...l.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\d1213f0f-524a-4fc8-83bd-136685a7337d.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\f6798c58-db7e-406a-8b58-2d8eaa1e789b.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F332688
Malicious:	false
Reputation:	low

Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.| 1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u.. ..k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..)....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2.. ;...?.U,...W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....l...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z ....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir6332_1268641485\CRX_INSTALL_locales\bg\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F7700C
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6332_1268641485\CRX_INSTALL_locales\ca\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CB4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "Connecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6332_1268641485\CRX_INSTALL_locales\cs\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D8488CB
Malicious:	false
Reputation:	low

Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6332_1268641485\CRX_INSTALL_locales\da\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5E0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_unavailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6332_1268641485\CRX_INSTALL_locales\de\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB80552
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_unavailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6332_1268641485\CRX_INSTALL_locales\el\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOGAOf+XD:WguYpCZnpEZbGoD
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B40
Malicious:	false
Reputation:	low

Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavail able": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6332_1268641485\CRX_INSTALL_locales\en\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6332_1268641485\CRX_INSTALL_locales\en_GB\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unavailable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6332_1268641485\CRX_INSTALL_locales\es\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE0128
Malicious:	false
Reputation:	low

Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6332_1268641485\CRX_INSTALL_locales\es_419\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	637
Entropy (8bit):	4.47253983486615
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOGAOfvD
MD5:	6B2583D8D1C147E36A69A88009CBEBC7
SHA1:	4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937
SHA-256:	6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F
SHA-512:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA53
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6332_1268641485\CRX_INSTALL_locales\et\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	595
Entropy (8bit):	4.467205425399467
Encrypted:	false
SSDEEP:	12:1HEJfPGGGfPG+WYpU34Ze7z+dgrW9O8ZpU34ZwZz03OyZnLAOfTYgoLIR:1HEdvqlWYpTeObk8ZpT/OGAOfuLIR
MD5:	CFF6CB76EC724B17C1BC920726CB35A7
SHA1:	14ED068251D65A840F00C05409D705259D329FFC
SHA-256:	C85800BF45942FCC7FD6B1DF929C25F9CC2A977A6678966BD03D4B6B69889AFD
SHA-512:	53D7D01BB30C0306DE65A79FD9551D2E8C1F71F4F45F71906B009071CB3E0F231E6A50FDD78773E9B4DE94085BC7B97F829842FA21A89A2080D33458B745C46F
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome'i veebipoe maksed".. },.. "app_name": {.. "message": "Chrome'i veebipoe maksed".. },.. "craw_app_unavailable": {.. "message": "Rakendus pole praegu saadaval.".. },.. "craw_connect_to_network": {.. "message": "Looge .hendus v.rguga.".. },.. "iap_unavailable": {.. "message": "Rakendusesisesed maksed ei ole praegu saadaval.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logige Chrome'i sisse.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6332_1268641485\CRX_INSTALL_locales\fi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	4.595421267152647
Encrypted:	false
SSDEEP:	12:1HEJRuzGGRuz+WYpU34ujSBu+dgYO8ZpU34J+Bu03OyZnLAOfTY5HN:1HEFcWYpPNa8ZpD+FOGAOfEHN
MD5:	3A01FEE829445C482D1721FF63153D16
SHA1:	F3EAAADDC03F943FC88B30B67F534AA13E3336DD
SHA-256:	0BDE54B20845124113383B6EB81E43A0F05E4EB0C44BEE3C1DFAC4CC5FEC2836
SHA-512:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BED8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_unavailable": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. },.. "craw_connect_to_network": {.. "message": "Muodosta verkkoyhteys.".. },.. "iap_unavailable": {.. "message": "Sovelluksen sis.iset maksut eiv.t ole t.ll. hetkell. k.ytett.viss..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Kirjaudu sis..n Chromeen.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6332_1268641485\CRX_INSTALL_locales\fil\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	658
Entropy (8bit):	4.5231229502550745
Encrypted:	false
SSDEEP:	12:1HEJADlbGGADlb+WYpU34hTUT+dgHfZAFFZO8ZpU34hTjzeT03OyZnLAOfTYHfvF:1HEYah6WYp7TUSoxOS8Zp7TOsOGAOfqV
MD5:	57AF5B654270A945BDA8053A83353A06
SHA1:	EEEF7A4F869F97CF471A05D345E74F982D15E167
SHA-256:	EC002ED92359F67818B49455DFC579E140368E6A004080AF022FD4F57F6B03F2
SHA-512:	5F0AE839FCF3F4EA48FF41A76655AE0F3821564AFD5D42FBB9FBB9A38E8D8F7BB5E9B6F71064588CD441261F644095A44A755C134CE546D506D9A21E488BAF52
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "app_name": {.. "message": "Mga Pagbabayad sa Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Kasalukuyang hindi available ang app.".. },.. "craw_connect_to_network": {.. "message": "Mangyaring kumonekta sa isang network.".. },.. "iap_unavailable": {.. "message": "Kasalukuyang hindi available ang Mga Pagbabayad na In-App.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Mangyaring mag-sign in sa Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6332_1268641485\CRX_INSTALL_locales\fr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	677
Entropy (8bit):	4.552569602149629
Encrypted:	false
SSDEEP:	12:1HEJALf/nbGGALf/nb+WYpU34Owdgbyb+dgdQjO8ZpU34ITQpGnbyb03OyZnLAO8:1HE4Hna1Hn6WYpNdgpY8ZpSTQwnBOGAh
MD5:	8D11C90F44A6585B57B933AB38D1FFF8
SHA1:	3F9D44EA8807069A32AACA2AAAD02FD892E6CC90
SHA-256:	599491F8C52B945C16C441ADF45BFD45AFAE046DA07757D97C56AF4DE75ED3B5
SHA-512:	D7EF7F5AD7EF1A1595825D79B69E2B1E988AD3CF1F3881496FCCD30F241E4E9C6E457F9F5D0F855DE3536DB7A40C3E1C55946B50D3F556F4A35285066A0CD6F7
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "app_name": {.. "message": "Paiements via le Chrome.Web.Store".. },.. "craw_app_unavailable": {.. "message": "Application indisponible pour le moment.".. },.. "craw_connect_to_network": {.. "message": "Veuillez vous connecter . un r.seau.".. },.. "iap_unavailable": {.. "message": "Les paiements via l'application ne sont pas disponibles pour le moment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Veuillez vous connecter . Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6332_1268641485\CRX_INSTALL_locales\hi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.791154467711985
Encrypted:	false
SSDEEP:	24:1HEs07J0JWYp9vnCSVLP8Zp6CsOGAOf8SLm:Wh7qgYp1CMLUph1GiSLm
MD5:	E376D757C8FD66AC70A7D2D49760B94E
SHA1:	1525C5B1312D409604F097768503298EC440CC4D
SHA-256:	8106D98C4F8DA16DB698444409558E29CC96735E188BFA303C333A5D99231C1D
SHA-512:	673F3F259AF2946E4F49BBED14A2A70D44BF9FDA9D7A71DC9172BA9B7B3C7F7062B16D29682B638D485B0520ED6F99E7A735F28C7C719B539559005B69FA7555
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome ... .".. },.. "app_name": {.. "message": "Chrome ... .".. },.. "craw_app_unavailable": {.. "message": "......... .. ..".. },.. "craw_connect_to_network": {.. "message": "..... ....".. },.. "iap_unavailable": {.. "message": "..-.. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... Chrome ... .".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6332_1268641485\CRX_INSTALL_locales\hr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	618
Entropy (8bit):	4.56999230891419
Encrypted:	false
SSDEEP:	12:1HEJGiimxmbZGGGiimxmbZ+WYpU34OBOEuhopIO+dgcapZO8ZpU34GiiZrMrQphK:1HE4H4TH8WYpNjTta28ZpQVLP0SOGAOK
MD5:	8185D0490C86363602A137F9A261CC50
SHA1:	5BD933B874441CEACB9201CCC941FF67BAED6DC0
SHA-256:	A2B2EC359A9DD9DCCCE02859CE1E738BD30FAA4A05F1DC522893FFDF722BBC15
SHA-512:	D7629978FC031EA5F716F9C1065FB2FEAB48C15F10CD68830DC966FA1002C03DDC7ACDE314C7D075F9F3A0A68552A6ACBCCDEE24CF20B6C3DD1BCE6562D096E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "app_name": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "craw _app_unavailable": {.. "message": "Aplikacija trenuta.no nije dostupna.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se s mre.om.".. },.. "iap_unavailable": {.. "message": "Pla.anje u aplikaciji trenuta.no nije dostupno.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comple ted.".. },.. "please_sign_in": {.. "message": "Prijavite se na Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6332_1268641485\CRX_INSTALL_locales\hu\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	683
Entropy (8bit):	4.675370843321512
Encrypted:	false
SSDEEP:	12:1HEJVJiGGVJi+WYpU34Hpo9O+dgMmfgijO8ZpU34Huo9O03OyZnLAOfTYBIAYm:1HEVrk5WYpQzTUg/8ZpwoXOGAOfYIAd
MD5:	85609CF8623582A8376C206556ED2131
SHA1:	1E16EB70DB5E59BB684866FF3E3925C2DEF25A12
SHA-256:	32A249749F12ADB6A220BF9ADC272C7E5D9AD5497A38B0086D961E3ABA17FBC6
SHA-512:	27883430865D3CFA6EDFE8C6CE1442BD96150B5CE520CCF7D556A330CAA6392C712B47BD86F7350E174876BC681F6DEC94D1312402655B0AF90883A2899EC78
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. },.. "app_name": {.. "message": "Chrome Internetes .ruh.z Fizet.si r endszere".. },.. "craw_app_unavailable": {.. "message": "Az alkalmaz.s jelenleg nem .rhet. el.".. },.. "craw_connect_to_network": {.. "message": "K.rj.k, csatlako zzon egy h.l.zathoz.".. },.. "iap_unavailable": {.. "message": "Az alkalmaz.son bel.li fizet.s jelenleg nem .rhet. el.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Jelentkezzen be a Chrome-ba.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6332_1268641485\CRX_INSTALL_locales\id\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	604
Entropy (8bit):	4.465685261172395
Encrypted:	false
SSDEEP:	12:1HEJs25bGGs25b+WYpU34ORBHAeSJ+dgkmO8ZpU34s22C/SzFAs03OyZnLAOfTYR:1HEBaA6WYpaHFH8ZptOYOGAOf2D
MD5:	EAB2B946D1232AB98137E760954003AA
SHA1:	60BDC2937905B311D2C9844DF2D639D7AC9F7F67
SHA-256:	C6E8800450602DE0F39FE9F6854472383813FB454B08ABAE7E25A9167CE004C3
SHA-512:	970FEC9A9EF0BAF7F693C4C5977F3B47914579C5B5414FCE9DBB5E4574659A5BB9AD2DE0CC886B368F49C019785AF7D2D7FE82F71341F039EADC399ED776CA12
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pembayaran Chrome Webstore".. },.. "app_name": {.. "message": "Pembayaran Chrome Webstore".. },.. "cr aw_app_unavailable": {.. "message": "Aplikasi tidak tersedia saat ini.".. },.. "craw_connect_to_network": {.. "message": "Sambungkan ke jaringan.".. },.. "iap_unavailable": {.. "message": "Pembayaran Dalam Aplikasi saat ini tidak tersedia.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be co mpleted.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6332_1268641485\CRX_INSTALL_locales\it\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	603

Entropy (8bit):	4.479418964635223
Encrypted:	false
SSDEEP:	12:1HEJsqd/bGGsqd/b+WYpU34OcX4+dgUvIO8ZpU34vq703OyZnLAOfTYsD:1HEXd/aKd/6WYpZrv58ZpskOGAOfzD
MD5:	A328EEF5E841E0C72D3CD7366899C5C8
SHA1:	2851ED658385804E87911643F5A4200B1FB26E13
SHA-256:	CD891C45F7586FB4A2514205A11F260E4A6D4482FA03D901909DD9F57BE0536D
SHA-512:	E47297896E981774EC3B59D41B89D6BA9333F6B4435EB9727D8645A46B10C7D408ADE06844871FA757382FBE7E645276449DB7B1B23BC59C9A71A5CB5A5ECC5
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamenti Chrome Web Store".. },.. "app_name": {.. "message": "Pagamenti Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "App al momento non disponibile.".. },.. "craw_connect_to_network": {.. "message": "Collegati a una rete.".. },.. "iap_unavailable": {.. "message": "La funzione Pagamenti In-App non . al momento disponibile.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accedi a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6332_1268641485\CRX_INSTALL_locales\ja\messages.json

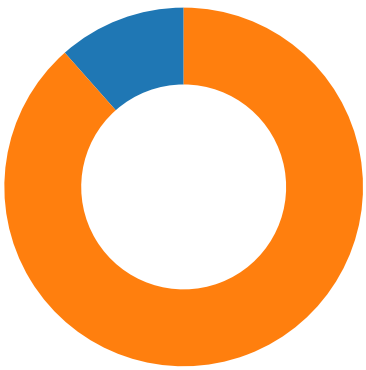
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	697
Entropy (8bit):	5.20469020877498
Encrypted:	false
SSDEEP:	12:1HEJ07uGG07u+WYpU34DB+dgnsVztO8ZpU34MwiB03OyZnLAOfTYmSH:1HEcnDNWYp1kxU8Zp2wiqOGAOfpSH
MD5:	9B3A5D473C3F2BBFAEECE94A07A940B8
SHA1:	61BACA342CF766BBA15C7B4D892A0E7DAC9405AA
SHA-256:	706312A4A2AEF3317223F141EB2B82685345B7EED444F16BB4DF3A272716DA1F
SHA-512:	94F6FEE9A11BD890AB8211C98D1CC142348961EBCF756F66477A3E3A76519804B70BE0AE4E551739F8AFE32D7ADE6EDE04EF6B9B9EED03E3A857E6058EEDD4C6
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome ....."... },.. "app_name": {.. "message": "Chrome ....."... },.. "craw_app_unavailable": {.. "message": "....."... },.. "craw_connect_to_network": {.. "message": "....."... },.. "iap_unavailable": {.. "message": "....."... },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed."... },.. "please_sign_in": {.. "message": "Chrome ....."... }..}..

Static File Info

No static file info

Network Behavior

Network Port Distribution



Total Packets: 52

- 443 (HTTPS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 29, 2022 00:29:42.454762936 CET	49741	80	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:42.455347061 CET	49742	80	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:42.463313103 CET	49745	443	192.168.2.3	142.250.203.109
Jan 29, 2022 00:29:42.463355064 CET	443	49745	142.250.203.109	192.168.2.3
Jan 29, 2022 00:29:42.463427067 CET	49745	443	192.168.2.3	142.250.203.109
Jan 29, 2022 00:29:42.463674068 CET	49745	443	192.168.2.3	142.250.203.109
Jan 29, 2022 00:29:42.463692904 CET	443	49745	142.250.203.109	192.168.2.3
Jan 29, 2022 00:29:42.474363089 CET	80	49741	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:42.474494934 CET	49741	80	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:42.474772930 CET	49741	80	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:42.474905968 CET	80	49742	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:42.474983931 CET	49742	80	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:42.494002104 CET	80	49741	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:42.525341988 CET	443	49745	142.250.203.109	192.168.2.3
Jan 29, 2022 00:29:42.550637960 CET	49745	443	192.168.2.3	142.250.203.109
Jan 29, 2022 00:29:42.550663948 CET	443	49745	142.250.203.109	192.168.2.3
Jan 29, 2022 00:29:42.552819014 CET	443	49745	142.250.203.109	192.168.2.3
Jan 29, 2022 00:29:42.552889109 CET	49745	443	192.168.2.3	142.250.203.109
Jan 29, 2022 00:29:42.676275015 CET	80	49741	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:42.772212029 CET	49746	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:42.772265911 CET	443	49746	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:42.772358894 CET	49746	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:42.772716045 CET	49746	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:42.772757053 CET	443	49746	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:42.804512024 CET	49741	80	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:42.818788052 CET	49745	443	192.168.2.3	142.250.203.109
Jan 29, 2022 00:29:42.819020033 CET	49745	443	192.168.2.3	142.250.203.109
Jan 29, 2022 00:29:42.819051027 CET	443	49745	142.250.203.109	192.168.2.3
Jan 29, 2022 00:29:42.819104910 CET	443	49745	142.250.203.109	192.168.2.3
Jan 29, 2022 00:29:42.897985935 CET	443	49745	142.250.203.109	192.168.2.3
Jan 29, 2022 00:29:42.898091078 CET	49745	443	192.168.2.3	142.250.203.109
Jan 29, 2022 00:29:42.899545908 CET	49745	443	192.168.2.3	142.250.203.109
Jan 29, 2022 00:29:42.899569988 CET	443	49745	142.250.203.109	192.168.2.3
Jan 29, 2022 00:29:43.123717070 CET	443	49746	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.124039888 CET	49746	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.124069929 CET	443	49746	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.125965118 CET	443	49746	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.126069069 CET	49746	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.128418922 CET	49746	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.128619909 CET	443	49746	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.128801107 CET	49746	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.128832102 CET	443	49746	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.168530941 CET	49746	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.260524988 CET	443	49746	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.260560989 CET	443	49746	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.260639906 CET	49746	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.260659933 CET	443	49746	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.260711908 CET	49746	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.260739088 CET	443	49746	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.260790110 CET	49746	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.262219906 CET	49746	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.262243032 CET	443	49746	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.332777023 CET	49749	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.332830906 CET	443	49749	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.332917929 CET	49749	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.333178997 CET	49749	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.333199978 CET	443	49749	13.248.132.126	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 29, 2022 00:29:43.333789110 CET	49750	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.333830118 CET	443	49750	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.333961010 CET	49750	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.334147930 CET	49750	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.334176064 CET	443	49750	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.334789038 CET	49751	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.334841013 CET	443	49751	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.334949970 CET	49751	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.335117102 CET	49751	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.335139990 CET	443	49751	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.351675987 CET	49752	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.351748943 CET	443	49752	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.351881027 CET	49752	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.352065086 CET	49752	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.352091074 CET	443	49752	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.352576971 CET	49753	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.352643967 CET	443	49753	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.352745056 CET	49753	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.352972984 CET	49754	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.353017092 CET	443	49754	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.353104115 CET	49754	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.353228092 CET	49753	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.353257895 CET	443	49753	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.353389025 CET	49754	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.353413105 CET	443	49754	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.553831100 CET	443	49749	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.555155039 CET	49749	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.555185080 CET	443	49749	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.556066036 CET	443	49749	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.556721926 CET	49749	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.556876898 CET	49749	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.556950092 CET	443	49749	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.571952105 CET	443	49753	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.572135925 CET	443	49752	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.572350979 CET	49753	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.572408915 CET	443	49753	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.572534084 CET	49752	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.572607040 CET	443	49752	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.573367119 CET	443	49754	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.573723078 CET	49754	443	192.168.2.3	13.248.132.126
Jan 29, 2022 00:29:43.573755026 CET	443	49754	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.574232101 CET	443	49753	13.248.132.126	192.168.2.3
Jan 29, 2022 00:29:43.574378014 CET	49753	443	192.168.2.3	13.248.132.126

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 29, 2022 00:29:42.428852081 CET	192.168.2.3	8.8.8.8	0xf9b2	Standard query (0)	lijit.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:42.431309938 CET	192.168.2.3	8.8.8.8	0x1d5f	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:42.433576107 CET	192.168.2.3	8.8.8.8	0xcca5	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:46.096728086 CET	192.168.2.3	8.8.8.8	0x62fd	Standard query (0)	lijit.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:48.525435925 CET	192.168.2.3	8.8.8.8	0x115	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:52.207479954 CET	192.168.2.3	8.8.8.8	0x5c07	Standard query (0)	www.sovrn.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 29, 2022 00:29:53.176026106 CET	192.168.2.3	8.8.8.8	0xc8b1	Standard query (0)	1g3v9y2l2l lh2lksnu1v316y-wpengine.netdna-ssl.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:53.393491030 CET	192.168.2.3	8.8.8.8	0xdfcb	Standard query (0)	s.w.org	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:53.394804001 CET	192.168.2.3	8.8.8.8	0x6c67	Standard query (0)	use.fontawesome.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:53.395776987 CET	192.168.2.3	8.8.8.8	0x5f67	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:54.722853899 CET	192.168.2.3	8.8.8.8	0xeee	Standard query (0)	s.pinimg.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:56.185457945 CET	192.168.2.3	8.8.8.8	0xe31	Standard query (0)	js.hs-analytics.net	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:56.844579935 CET	192.168.2.3	8.8.8.8	0xa7e2	Standard query (0)	ct.pinterest.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:57.311920881 CET	192.168.2.3	8.8.8.8	0x8b19	Standard query (0)	ipapi.co	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:57.412606955 CET	192.168.2.3	8.8.8.8	0x47ad	Standard query (0)	quickkoala.io	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:57.459466934 CET	192.168.2.3	8.8.8.8	0x3206	Standard query (0)	www.pinterest.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:57.460170031 CET	192.168.2.3	8.8.8.8	0x8664	Standard query (0)	track.hubspot.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:57.711396933 CET	192.168.2.3	8.8.8.8	0x1dc9	Standard query (0)	player.vimeo.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:57.844914913 CET	192.168.2.3	8.8.8.8	0x2a38	Standard query (0)	www.pinterest.ch	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.220007896 CET	192.168.2.3	8.8.8.8	0x71ba	Standard query (0)	f.vimeocdn.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.220696926 CET	192.168.2.3	8.8.8.8	0xf1ef	Standard query (0)	i.vimeocdn.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.221251011 CET	192.168.2.3	8.8.8.8	0xc02b	Standard query (0)	fresnel.vimeocdn.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.493005991 CET	192.168.2.3	8.8.8.8	0x31e6	Standard query (0)	i.pinimg.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.500835896 CET	192.168.2.3	8.8.8.8	0x62ea	Standard query (0)	v.pinimg.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.566663980 CET	192.168.2.3	8.8.8.8	0xc3c8	Standard query (0)	js.hs-scripts.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.609992981 CET	192.168.2.3	8.8.8.8	0x8e2	Standard query (0)	www.googleoptimize.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.731519938 CET	192.168.2.3	8.8.8.8	0x4630	Standard query (0)	js.hs-banner.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.732362032 CET	192.168.2.3	8.8.8.8	0x94d1	Standard query (0)	js.hsleadflows.net	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.733036995 CET	192.168.2.3	8.8.8.8	0x55e	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.733418941 CET	192.168.2.3	8.8.8.8	0x34ec	Standard query (0)	js.hscollectedforms.net	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.891930103 CET	192.168.2.3	8.8.8.8	0xc32a	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:59.145191908 CET	192.168.2.3	8.8.8.8	0x59fa	Standard query (0)	forms.hubspot.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:59.190097094 CET	192.168.2.3	8.8.8.8	0x2a90	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:59.398159981 CET	192.168.2.3	8.8.8.8	0x517a	Standard query (0)	forms.hsforms.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:00.667028904 CET	192.168.2.3	8.8.8.8	0xd174	Standard query (0)	f.hubspotusercontent20.net	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:00.804867029 CET	192.168.2.3	8.8.8.8	0xfdc1	Standard query (0)	1g3v9y2l2l lh2lksnu1v316y-wpengine.netdna-ssl.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:01.324475050 CET	192.168.2.3	8.8.8.8	0x1f4d	Standard query (0)	vimeo.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:02.810867071 CET	192.168.2.3	8.8.8.8	0xb5bb	Standard query (0)	knowledge.sovrn.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:03.204438925 CET	192.168.2.3	8.8.8.8	0x5f4e	Standard query (0)	i.vimeocdn.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.407047987 CET	192.168.2.3	8.8.8.8	0xb996	Standard query (0)	cdn2.hubspot.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 29, 2022 00:30:04.583996058 CET	192.168.2.3	8.8.8.8	0xe17d	Standard query (0)	js.hubspot feedback.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.793917894 CET	192.168.2.3	8.8.8.8	0x12c1	Standard query (0)	feedback.h ubapi.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.794595003 CET	192.168.2.3	8.8.8.8	0x8775	Standard query (0)	public.hub api.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.829551935 CET	192.168.2.3	8.8.8.8	0x63d5	Standard query (0)	app.hubspo t.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:06.413559914 CET	192.168.2.3	8.8.8.8	0x892e	Standard query (0)	knowledge. sovrn.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:10.488104105 CET	192.168.2.3	8.8.8.8	0xb840	Standard query (0)	f.hubspotu sercontent20.net	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:26.257399082 CET	192.168.2.3	8.8.8.8	0x4bd1	Standard query (0)	js.hsforms.net	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:28.310538054 CET	192.168.2.3	8.8.8.8	0xec37	Standard query (0)	a.nel.clou dflare.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:38.484894991 CET	192.168.2.3	8.8.8.8	0x3170	Standard query (0)	www.viglink.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:39.533302069 CET	192.168.2.3	8.8.8.8	0xe516	Standard query (0)	sovrn.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:40.857727051 CET	192.168.2.3	8.8.8.8	0x451a	Standard query (0)	js-na1.hs-scripts.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:42.582561016 CET	192.168.2.3	8.8.8.8	0xafef	Standard query (0)	www.viglink.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:43.247199059 CET	192.168.2.3	8.8.8.8	0x4c92	Standard query (0)	sovrn.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:44.094639063 CET	192.168.2.3	8.8.8.8	0xdeaf	Standard query (0)	www.sovrn.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:46.252686977 CET	192.168.2.3	8.8.8.8	0x62fd	Standard query (0)	assets.cal endly.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:31:00.288830042 CET	192.168.2.3	8.8.8.8	0xd84e	Standard query (0)	quickkoala.io	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 29, 2022 00:29:42.449615002 CET	8.8.8.8	192.168.2.3	0xf9b2	No error (0)	lijit.com		13.248.132.126	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:42.449615002 CET	8.8.8.8	192.168.2.3	0xf9b2	No error (0)	lijit.com		76.223.8.20	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:42.459904909 CET	8.8.8.8	192.168.2.3	0x1d5f	No error (0)	clients2.g oogle.com	clients.l.google.co m		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:42.459904909 CET	8.8.8.8	192.168.2.3	0x1d5f	No error (0)	clients.l. google.com		142.250.203.110	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:42.462558985 CET	8.8.8.8	192.168.2.3	0xcca5	No error (0)	accounts.g oogle.com		142.250.203.109	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:46.115904093 CET	8.8.8.8	192.168.2.3	0x62fd	No error (0)	lijit.com		13.248.132.126	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:46.115904093 CET	8.8.8.8	192.168.2.3	0x62fd	No error (0)	lijit.com		76.223.8.20	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:48.552690983 CET	8.8.8.8	192.168.2.3	0x115	No error (0)	clients2.g oogleuserc ontent.com	googlehosted.l.goo gleusercontent.co m		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:48.552690983 CET	8.8.8.8	192.168.2.3	0x115	No error (0)	googlehost ed.l.googl euserconte nt.com		172.217.168.33	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:52.238142967 CET	8.8.8.8	192.168.2.3	0x5c07	No error (0)	www.sovrn.com		34.135.254.63	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:53.196795940 CET	8.8.8.8	192.168.2.3	0xc8b1	No error (0)	1g3v9y2l2l lh2lksnu1v316y-wpengine.netdna-ssl.com		94.31.29.99	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:53.411807060 CET	8.8.8.8	192.168.2.3	0xdfcb	No error (0)	s.w.org		192.0.77.48	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:53.413795948 CET	8.8.8.8	192.168.2.3	0x5f67	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcd n.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:53.415165901 CET	8.8.8.8	192.168.2.3	0x6c67	No error (0)	use.fontaw esome.com	use.fontawesome. com.cdn.cloudflare .net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 29, 2022 00:29:54.746495008 CET	8.8.8.8	192.168.2.3	0xeee	No error (0)	s.pinimg.com	s-pinimg-com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:54.746495008 CET	8.8.8.8	192.168.2.3	0xeee	No error (0)	s-pinimg-com.gslb.pinterest.com	2-01-37d2-0006.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:56.207274914 CET	8.8.8.8	192.168.2.3	0xe31	No error (0)	js.hs-analytics.net		104.17.68.176	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:56.207274914 CET	8.8.8.8	192.168.2.3	0xe31	No error (0)	js.hs-analytics.net		104.17.70.176	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:56.207274914 CET	8.8.8.8	192.168.2.3	0xe31	No error (0)	js.hs-analytics.net		104.17.71.176	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:56.207274914 CET	8.8.8.8	192.168.2.3	0xe31	No error (0)	js.hs-analytics.net		104.17.69.176	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:56.207274914 CET	8.8.8.8	192.168.2.3	0xe31	No error (0)	js.hs-analytics.net		104.17.67.176	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:56.865768909 CET	8.8.8.8	192.168.2.3	0xa7e2	No error (0)	ct.pinterest.com	www.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:56.865768909 CET	8.8.8.8	192.168.2.3	0xa7e2	No error (0)	www.pinterest.com	www-pinterest-com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:56.865768909 CET	8.8.8.8	192.168.2.3	0xa7e2	No error (0)	www-pinterest-com.gslb.pinterest.com	2-01-37d2-0018.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:57.331176996 CET	8.8.8.8	192.168.2.3	0x8b19	No error (0)	ipapi.co		104.26.8.44	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:57.331176996 CET	8.8.8.8	192.168.2.3	0x8b19	No error (0)	ipapi.co		104.26.9.44	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:57.331176996 CET	8.8.8.8	192.168.2.3	0x8b19	No error (0)	ipapi.co		172.67.69.226	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:57.428908110 CET	8.8.8.8	192.168.2.3	0x47ad	No error (0)	quickkoala.io		162.242.174.138	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:57.428908110 CET	8.8.8.8	192.168.2.3	0x47ad	No error (0)	quickkoala.io		23.253.207.75	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:57.428908110 CET	8.8.8.8	192.168.2.3	0x47ad	No error (0)	quickkoala.io		23.253.41.115	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:57.428908110 CET	8.8.8.8	192.168.2.3	0x47ad	No error (0)	quickkoala.io		198.61.165.71	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:57.482016087 CET	8.8.8.8	192.168.2.3	0x8664	No error (0)	track.hubspot.com		104.19.155.83	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:57.482016087 CET	8.8.8.8	192.168.2.3	0x8664	No error (0)	track.hubspot.com		104.19.154.83	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:57.482213974 CET	8.8.8.8	192.168.2.3	0x3206	No error (0)	www.pinterest.com	www-pinterest-com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:57.482213974 CET	8.8.8.8	192.168.2.3	0x3206	No error (0)	www-pinterest-com.gslb.pinterest.com	www.gslb.pinterest.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:57.482213974 CET	8.8.8.8	192.168.2.3	0x3206	No error (0)	www.gslb.pinterest.net	www.pinterest.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:57.729836941 CET	8.8.8.8	192.168.2.3	0x1dc9	No error (0)	player.vimeo.com	vimeo.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:57.729836941 CET	8.8.8.8	192.168.2.3	0x1dc9	No error (0)	vimeo.map.fastly.net		151.101.0.217	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:57.729836941 CET	8.8.8.8	192.168.2.3	0x1dc9	No error (0)	vimeo.map.fastly.net		151.101.64.217	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:57.729836941 CET	8.8.8.8	192.168.2.3	0x1dc9	No error (0)	vimeo.map.fastly.net		151.101.128.217	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:57.729836941 CET	8.8.8.8	192.168.2.3	0x1dc9	No error (0)	vimeo.map.fastly.net		151.101.192.217	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:57.752068043 CET	8.8.8.8	192.168.2.3	0xf8cc	No error (0)	www-google tagmanager.l.google.com		172.217.168.8	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:57.861375093 CET	8.8.8.8	192.168.2.3	0x2a38	No error (0)	www.pinterest.ch	www.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:57.861375093 CET	8.8.8.8	192.168.2.3	0x2a38	No error (0)	www.pinterest.com	www-pinterest-com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 29, 2022 00:29:57.861375093 CET	8.8.8.8	192.168.2.3	0x2a38	No error (0)	www-pinterest-com.gslb.pinterest.com	www.gslb.pinterest.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:57.861375093 CET	8.8.8.8	192.168.2.3	0x2a38	No error (0)	www.gslb.pinterest.net	www.pinterest.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:57.997180939 CET	8.8.8.8	192.168.2.3	0x3909	No error (0)	www-google-analytics.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.239196062 CET	8.8.8.8	192.168.2.3	0x71ba	No error (0)	f.vimeocdn.com	vimeo-video.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:58.239196062 CET	8.8.8.8	192.168.2.3	0x71ba	No error (0)	vimeo-video.map.fastly.net		151.101.114.109	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.239238977 CET	8.8.8.8	192.168.2.3	0xf1ef	No error (0)	i.vimeocdn.com	vimeo-video.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:58.239238977 CET	8.8.8.8	192.168.2.3	0xf1ef	No error (0)	vimeo-video.map.fastly.net		151.101.114.109	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.239337921 CET	8.8.8.8	192.168.2.3	0xc02b	No error (0)	fresnel.vimeocdn.com		34.120.202.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.521274090 CET	8.8.8.8	192.168.2.3	0x31e6	No error (0)	i.pinimg.com	i.pinimg.com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:58.521274090 CET	8.8.8.8	192.168.2.3	0x31e6	No error (0)	i.pinimg.com.gslb.pinterest.com	2-01-37d2-0004.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:58.529515028 CET	8.8.8.8	192.168.2.3	0x62ea	No error (0)	v.pinimg.com	v.pinimg.com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:58.529515028 CET	8.8.8.8	192.168.2.3	0x62ea	No error (0)	v.pinimg.com.gslb.pinterest.com	2-01-37d2-0007.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:58.588438988 CET	8.8.8.8	192.168.2.3	0xc3c8	No error (0)	js.hs-scripts.com		104.17.210.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.588438988 CET	8.8.8.8	192.168.2.3	0xc3c8	No error (0)	js.hs-scripts.com		104.17.211.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.588438988 CET	8.8.8.8	192.168.2.3	0xc3c8	No error (0)	js.hs-scripts.com		104.17.212.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.588438988 CET	8.8.8.8	192.168.2.3	0xc3c8	No error (0)	js.hs-scripts.com		104.17.213.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.588438988 CET	8.8.8.8	192.168.2.3	0xc3c8	No error (0)	js.hs-scripts.com		104.17.214.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.636674881 CET	8.8.8.8	192.168.2.3	0x8e2	No error (0)	www.googleoptimize.com		142.250.203.110	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.753504038 CET	8.8.8.8	192.168.2.3	0x4630	No error (0)	js.hs-banner.com		104.18.20.191	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.753504038 CET	8.8.8.8	192.168.2.3	0x4630	No error (0)	js.hs-banner.com		104.18.21.191	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.753552914 CET	8.8.8.8	192.168.2.3	0x94d1	No error (0)	js.hsleadflows.net		104.17.231.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.753552914 CET	8.8.8.8	192.168.2.3	0x94d1	No error (0)	js.hsleadflows.net		104.17.234.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.753552914 CET	8.8.8.8	192.168.2.3	0x94d1	No error (0)	js.hsleadflows.net		104.17.230.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.753552914 CET	8.8.8.8	192.168.2.3	0x94d1	No error (0)	js.hsleadflows.net		104.17.232.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.753552914 CET	8.8.8.8	192.168.2.3	0x94d1	No error (0)	js.hsleadflows.net		104.17.233.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.753956079 CET	8.8.8.8	192.168.2.3	0x55e	No error (0)	snap.licdn.com	od.linkedin.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:58.754889965 CET	8.8.8.8	192.168.2.3	0x34ec	No error (0)	js.hscollectedforms.net		104.17.128.171	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.754889965 CET	8.8.8.8	192.168.2.3	0x34ec	No error (0)	js.hscollectedforms.net		104.17.127.171	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.754889965 CET	8.8.8.8	192.168.2.3	0x34ec	No error (0)	js.hscollectedforms.net		104.17.131.171	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.754889965 CET	8.8.8.8	192.168.2.3	0x34ec	No error (0)	js.hscollectedforms.net		104.17.130.171	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:58.754889965 CET	8.8.8.8	192.168.2.3	0x34ec	No error (0)	js.hscollectedforms.net		104.17.129.171	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 29, 2022 00:29:58.912754059 CET	8.8.8.8	192.168.2.3	0xc32a	No error (0)	px.ads.linkedin.com	www.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:58.912754059 CET	8.8.8.8	192.168.2.3	0xc32a	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:59.166301966 CET	8.8.8.8	192.168.2.3	0x59fa	No error (0)	forms.hubspot.com		104.19.155.83	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:59.166301966 CET	8.8.8.8	192.168.2.3	0x59fa	No error (0)	forms.hubspot.com		104.19.154.83	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:59.206170082 CET	8.8.8.8	192.168.2.3	0x2a90	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:29:59.419800997 CET	8.8.8.8	192.168.2.3	0x517a	No error (0)	forms.hsforms.com		104.16.88.5	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:59.419800997 CET	8.8.8.8	192.168.2.3	0x517a	No error (0)	forms.hsforms.com		104.16.86.5	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:59.419800997 CET	8.8.8.8	192.168.2.3	0x517a	No error (0)	forms.hsforms.com		104.16.89.5	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:59.419800997 CET	8.8.8.8	192.168.2.3	0x517a	No error (0)	forms.hsforms.com		104.16.87.5	A (IP address)	IN (0x0001)
Jan 29, 2022 00:29:59.419800997 CET	8.8.8.8	192.168.2.3	0x517a	No error (0)	forms.hsforms.com		104.16.85.5	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:00.688991070 CET	8.8.8.8	192.168.2.3	0xd174	No error (0)	f.hubspotusercontent20.net		104.16.187.114	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:00.688991070 CET	8.8.8.8	192.168.2.3	0xd174	No error (0)	f.hubspotusercontent20.net		104.16.186.114	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:00.823438883 CET	8.8.8.8	192.168.2.3	0xfdc1	No error (0)	1g3v9y2l2llh2lksnu1v316y-wpengine.netdna-ssl.com		94.31.29.99	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:01.340570927 CET	8.8.8.8	192.168.2.3	0x1f4d	No error (0)	vimeo.com		151.101.192.217	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:01.340570927 CET	8.8.8.8	192.168.2.3	0x1f4d	No error (0)	vimeo.com		151.101.128.217	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:01.340570927 CET	8.8.8.8	192.168.2.3	0x1f4d	No error (0)	vimeo.com		151.101.64.217	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:01.340570927 CET	8.8.8.8	192.168.2.3	0x1f4d	No error (0)	vimeo.com		151.101.0.217	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:02.838562965 CET	8.8.8.8	192.168.2.3	0xb5bb	No error (0)	knowledge.sovrn.com	7216873.group23.sites.hubspot.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:30:02.838562965 CET	8.8.8.8	192.168.2.3	0xb5bb	No error (0)	7216873.group23.sites.hubspot.net	group23.sites.hscoscdn20.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:30:02.838562965 CET	8.8.8.8	192.168.2.3	0xb5bb	No error (0)	group23.sites.hscoscdn20.net		199.60.103.254	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:02.838562965 CET	8.8.8.8	192.168.2.3	0xb5bb	No error (0)	group23.sites.hscoscdn20.net		199.60.103.2	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:03.223275900 CET	8.8.8.8	192.168.2.3	0x5f4e	No error (0)	i.vimeocdn.com	vimeo-video.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:30:03.223275900 CET	8.8.8.8	192.168.2.3	0x5f4e	No error (0)	vimeo-video.map.fastly.net		151.101.114.109	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.427525997 CET	8.8.8.8	192.168.2.3	0xb996	No error (0)	cdn2.hubspot.net		104.17.241.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.427525997 CET	8.8.8.8	192.168.2.3	0xb996	No error (0)	cdn2.hubspot.net		104.17.244.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.427525997 CET	8.8.8.8	192.168.2.3	0xb996	No error (0)	cdn2.hubspot.net		104.17.243.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.427525997 CET	8.8.8.8	192.168.2.3	0xb996	No error (0)	cdn2.hubspot.net		104.17.242.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.427525997 CET	8.8.8.8	192.168.2.3	0xb996	No error (0)	cdn2.hubspot.net		104.17.240.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.605407000 CET	8.8.8.8	192.168.2.3	0xe17d	No error (0)	js.hubspotfeedback.com		104.17.112.162	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.605407000 CET	8.8.8.8	192.168.2.3	0xe17d	No error (0)	js.hubspotfeedback.com		104.17.116.162	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.605407000 CET	8.8.8.8	192.168.2.3	0xe17d	No error (0)	js.hubspotfeedback.com		104.17.115.162	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 29, 2022 00:30:04.605407000 CET	8.8.8.8	192.168.2.3	0xe17d	No error (0)	js.hubspot feedback.com		104.17.113.162	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.605407000 CET	8.8.8.8	192.168.2.3	0xe17d	No error (0)	js.hubspot feedback.com		104.17.114.162	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.813494921 CET	8.8.8.8	192.168.2.3	0x12c1	No error (0)	feedback.hubapi.com		104.17.200.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.813494921 CET	8.8.8.8	192.168.2.3	0x12c1	No error (0)	feedback.hubapi.com		104.17.203.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.813494921 CET	8.8.8.8	192.168.2.3	0x12c1	No error (0)	feedback.hubapi.com		104.17.202.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.813494921 CET	8.8.8.8	192.168.2.3	0x12c1	No error (0)	feedback.hubapi.com		104.17.204.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.813494921 CET	8.8.8.8	192.168.2.3	0x12c1	No error (0)	feedback.hubapi.com		104.17.201.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.816113949 CET	8.8.8.8	192.168.2.3	0x8775	No error (0)	public.hubapi.com		104.17.201.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.816113949 CET	8.8.8.8	192.168.2.3	0x8775	No error (0)	public.hubapi.com		104.17.203.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.816113949 CET	8.8.8.8	192.168.2.3	0x8775	No error (0)	public.hubapi.com		104.17.202.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.816113949 CET	8.8.8.8	192.168.2.3	0x8775	No error (0)	public.hubapi.com		104.17.204.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.816113949 CET	8.8.8.8	192.168.2.3	0x8775	No error (0)	public.hubapi.com		104.17.200.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.848596096 CET	8.8.8.8	192.168.2.3	0x63d5	No error (0)	app.hubspot.com		104.19.154.83	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:04.848596096 CET	8.8.8.8	192.168.2.3	0x63d5	No error (0)	app.hubspot.com		104.19.155.83	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:06.443361998 CET	8.8.8.8	192.168.2.3	0x892e	No error (0)	knowledge.sovrn.com	7216873.group23.sites.hubspot.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:30:06.443361998 CET	8.8.8.8	192.168.2.3	0x892e	No error (0)	7216873.group23.sites.hubspot.net	group23.sites.hscoscdn20.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:30:06.443361998 CET	8.8.8.8	192.168.2.3	0x892e	No error (0)	group23.sites.hscoscdn20.net		199.60.103.2	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:06.443361998 CET	8.8.8.8	192.168.2.3	0x892e	No error (0)	group23.sites.hscoscdn20.net		199.60.103.254	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:10.506777048 CET	8.8.8.8	192.168.2.3	0xb840	No error (0)	f.hubspotusercontent20.net		104.16.187.114	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:10.506777048 CET	8.8.8.8	192.168.2.3	0xb840	No error (0)	f.hubspotusercontent20.net		104.16.186.114	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:26.277014017 CET	8.8.8.8	192.168.2.3	0x4bd1	No error (0)	js.hsforms.net		104.17.184.73	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:26.277014017 CET	8.8.8.8	192.168.2.3	0x4bd1	No error (0)	js.hsforms.net		104.17.186.73	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:26.277014017 CET	8.8.8.8	192.168.2.3	0x4bd1	No error (0)	js.hsforms.net		104.17.183.73	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:26.277014017 CET	8.8.8.8	192.168.2.3	0x4bd1	No error (0)	js.hsforms.net		104.17.182.73	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:26.277014017 CET	8.8.8.8	192.168.2.3	0x4bd1	No error (0)	js.hsforms.net		104.17.185.73	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:28.329967976 CET	8.8.8.8	192.168.2.3	0xec37	No error (0)	a.nel.cloudflare.com		35.190.80.1	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:38.516840935 CET	8.8.8.8	192.168.2.3	0x3170	No error (0)	www.viglink.com	web-2099239636.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:30:38.516840935 CET	8.8.8.8	192.168.2.3	0x3170	No error (0)	web-2099239636.us-east-1.elb.amazonaws.com		3.227.218.120	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:38.516840935 CET	8.8.8.8	192.168.2.3	0x3170	No error (0)	web-2099239636.us-east-1.elb.amazonaws.com		3.221.39.9	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:39.551585913 CET	8.8.8.8	192.168.2.3	0xe516	No error (0)	sovrn.com		34.135.254.63	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:40.881351948 CET	8.8.8.8	192.168.2.3	0x451a	No error (0)	js-na1.hs-scripts.com		104.17.211.204	A (IP address)	IN (0x0001)

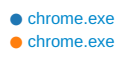
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 29, 2022 00:30:40.881351948 CET	8.8.8.8	192.168.2.3	0x451a	No error (0)	js-na1.hs-scripts.com		104.17.213.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:40.881351948 CET	8.8.8.8	192.168.2.3	0x451a	No error (0)	js-na1.hs-scripts.com		104.17.214.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:40.881351948 CET	8.8.8.8	192.168.2.3	0x451a	No error (0)	js-na1.hs-scripts.com		104.17.210.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:40.881351948 CET	8.8.8.8	192.168.2.3	0x451a	No error (0)	js-na1.hs-scripts.com		104.17.212.204	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:42.603255033 CET	8.8.8.8	192.168.2.3	0xafef	No error (0)	www.viglink.com	web-2099239636.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:30:42.603255033 CET	8.8.8.8	192.168.2.3	0xafef	No error (0)	web-2099239636.us-east-1.elb.amazonaws.com		3.221.39.9	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:42.603255033 CET	8.8.8.8	192.168.2.3	0xafef	No error (0)	web-2099239636.us-east-1.elb.amazonaws.com		3.227.218.120	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:43.269644976 CET	8.8.8.8	192.168.2.3	0x4c92	No error (0)	sovrn.com		34.135.254.63	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:44.117263079 CET	8.8.8.8	192.168.2.3	0xdeaf	No error (0)	www.sovrn.com		34.135.254.63	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:46.278851032 CET	8.8.8.8	192.168.2.3	0x62fd	No error (0)	assets.calendly.com	d2mvl3dkxvehny.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:30:46.278851032 CET	8.8.8.8	192.168.2.3	0x62fd	No error (0)	d2mvl3dkxvehny.cloudfront.net		143.204.215.25	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:46.278851032 CET	8.8.8.8	192.168.2.3	0x62fd	No error (0)	d2mvl3dkxvehny.cloudfront.net		143.204.215.128	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:46.278851032 CET	8.8.8.8	192.168.2.3	0x62fd	No error (0)	d2mvl3dkxvehny.cloudfront.net		143.204.215.101	A (IP address)	IN (0x0001)
Jan 29, 2022 00:30:46.278851032 CET	8.8.8.8	192.168.2.3	0x62fd	No error (0)	d2mvl3dkxvehny.cloudfront.net		143.204.215.110	A (IP address)	IN (0x0001)
Jan 29, 2022 00:31:00.307787895 CET	8.8.8.8	192.168.2.3	0xd84e	No error (0)	quickkoala.io		162.242.174.138	A (IP address)	IN (0x0001)
Jan 29, 2022 00:31:00.307787895 CET	8.8.8.8	192.168.2.3	0xd84e	No error (0)	quickkoala.io		23.253.207.75	A (IP address)	IN (0x0001)
Jan 29, 2022 00:31:00.307787895 CET	8.8.8.8	192.168.2.3	0xd84e	No error (0)	quickkoala.io		23.253.41.115	A (IP address)	IN (0x0001)
Jan 29, 2022 00:31:00.307787895 CET	8.8.8.8	192.168.2.3	0xd84e	No error (0)	quickkoala.io		198.61.165.71	A (IP address)	IN (0x0001)

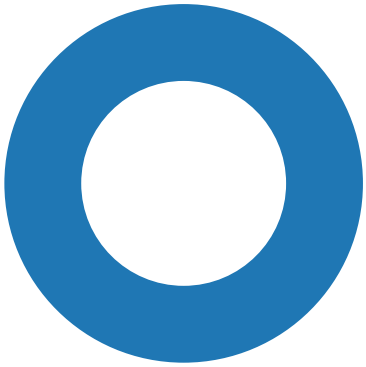
HTTP Request Dependency Graph

- lijit.com

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6332, Parent PID: 3312

General

Target ID:	1
Start time:	00:29:38
Start date:	29/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "http://lijit.com
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:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF68B0DFC4B	RegSetValueExW

Analysis Process: chrome.exe PID: **6556**, Parent PID: **6332**

General

Target ID:	3
Start time:	00:29:40
Start date:	29/01/2022
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=1564,13595487648583302405,3110836150026139459,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1932 /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
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly

No disassembly