ID: 562123
Cookbook: browseurl.jbs
Time: 14:10:31
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

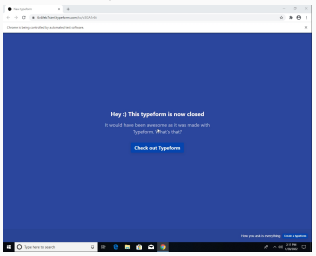
Windows Analysis Report

https://6v4feb7simf.typeform.com/to/v3GA1r6t

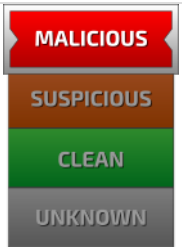
Overview

General Information

Sample URL:	http://https://6v4feb7simf.typeform.com/to/v3GA1r6t
Analysis ID:	562123
Infos:	



Detection



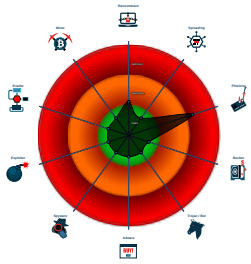
HTMLPhisher

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected HtmlPhish25
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6760 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "https://6v4feb7simf.typeform.com/to/v3GA1r6t MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6956 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1584,15928684533581983461,16347382913123571543,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1920 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6504 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1584,15928684533581983461,16347382913123571543,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=5536 /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

AV Detection

Antivirus / Scanner detection for submitted sample

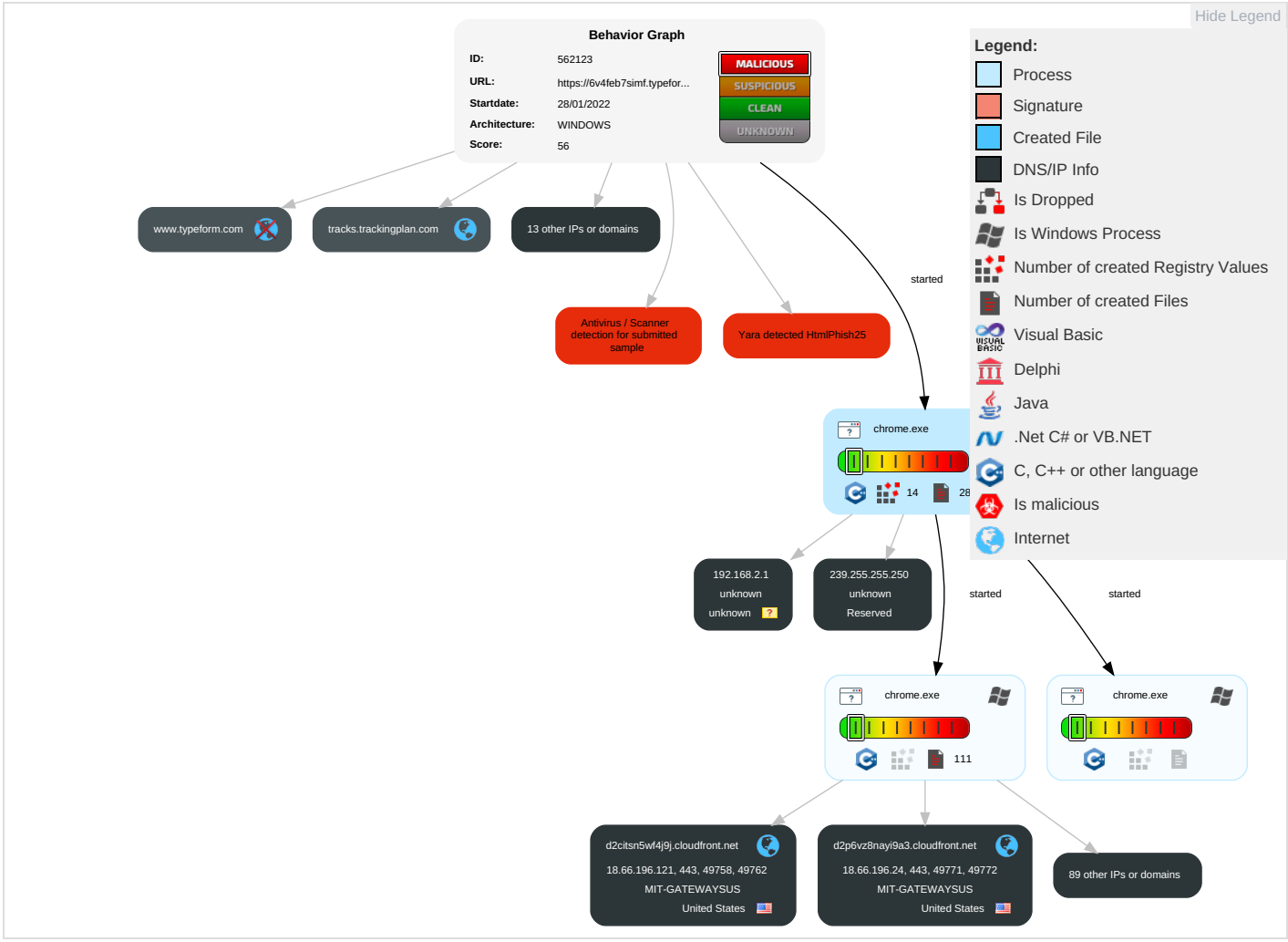
Phishing

Yara detected HtmlPhish25

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
Valid Accounts	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	1 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	2 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

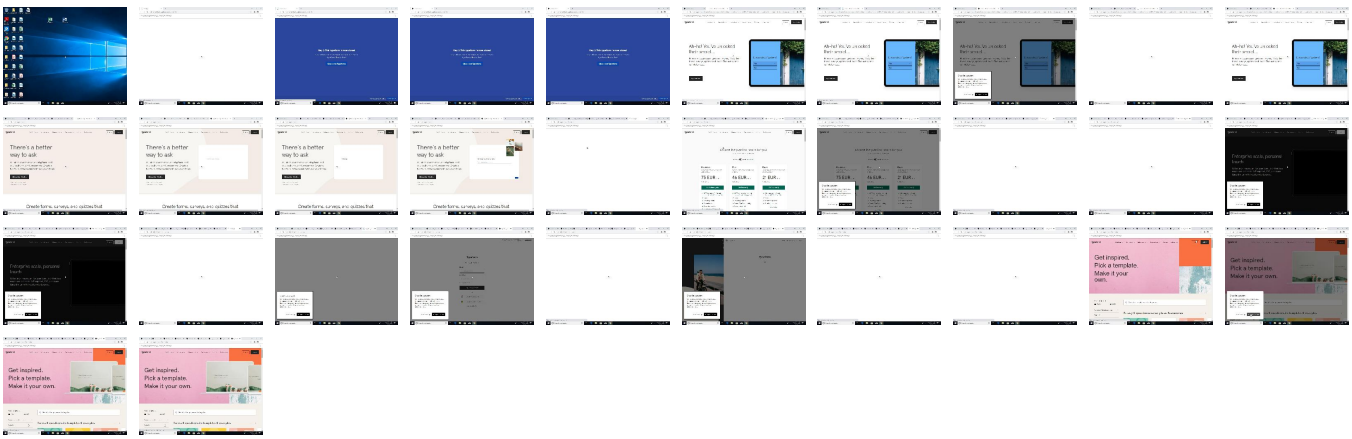
Behavior Graph

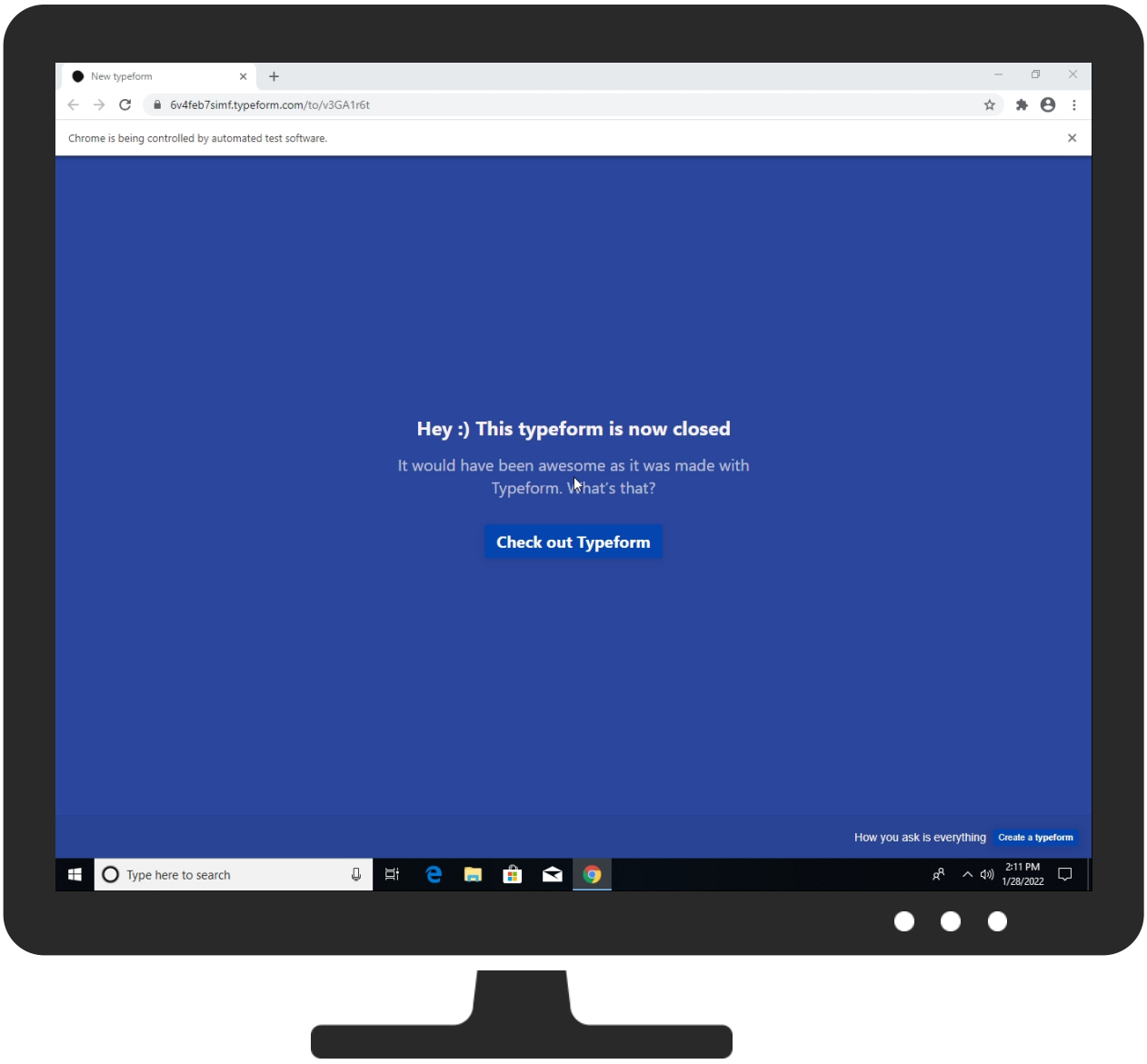


Screenshots

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://https://6v4feb7simf.typeform.com/to/v3GA1r6t	0%	Virustotal		Browse
http://https://6v4feb7simf.typeform.com/to/v3GA1r6t	0%	Avira URL Cloud	safe	
http://https://6v4feb7simf.typeform.com/to/v3GA1r6t	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
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
privacyportal-de.onetrust.com	104.20.184.68	true	false		high
d2citsn5wf4j9j.cloudfront.net	18.66.196.121	true	false		high
track.hubspot.com	104.19.155.83	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
js.hs-scripts.com	104.17.210.204	true	false		high
api.segment.io	54.149.50.128	true	false		high
www.google.com	172.217.168.68	true	false		high
polyfill.io	151.101.65.26	true	false		high
ok11-crtr-custom-domains-cd76c2bd4d92725a.elb.us-east-2.amazonaws.com	3.15.36.195	true	false		high
px.mountain.com	52.42.124.195	true	false		unknown
reveal.clearbit.com	52.56.230.239	true	false		high
match.adsrvr.org	52.223.40.198	true	false		high
px.steelhousemedia.com	44.237.157.168	true	false		high
js.hs-banner.com	104.18.20.191	true	false		unknown
star-mini.c10r.facebook.com	157.240.17.35	true	false		high
stats.l.doubleclick.net	108.177.127.155	true	false		high
dx.mountain.com	52.88.179.26	true	false		unknown
cdn.amplitude.com	108.156.0.174	true	false		high
dna8twue3dlxq.cloudfront.net	18.66.196.79	true	false		high
edge.fullstory.com	35.201.112.186	true	false		high
gs.mountain.com	34.212.4.35	true	false		unknown
d2q0tm6nh3syda.cloudfront.net	18.66.196.93	true	false		high
d1ftdm4q83us3q.cloudfront.net	18.66.218.92	true	false		high
googleads.g.doubleclick.net	172.217.168.66	true	false		high
api.amplitude.com	54.149.64.13	true	false		high
us2-events-2-1917544754.us-west-2.elb.amazonaws.com	52.26.89.215	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
unpkg.com	104.16.124.175	true	false		high
d2nvsmtq2poimt.cloudfront.net	18.66.218.95	true	false		high
cdn.cookielaw.org	104.16.149.64	true	false		high
googlehosted.l.googleusercontent.com	142.250.203.97	true	false		high
d3orhvfyxudxxq.cloudfront.net	108.139.243.33	true	false		high
dart.l.doubleclick.net	142.250.203.102	true	false		high
global-v2.clearbit.com	52.56.230.239	true	false		high
js.hs-analytics.net	104.17.68.176	true	false		unknown
adservice.google.com	172.217.168.2	true	false		high
x.clearbit.com	52.56.230.239	true	false		high
insight.adsrvr.org	52.223.40.198	true	false		high
d296je7bbdd650.cloudfront.net	108.139.240.122	true	false		high
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
prod-east-stats-tap-alb-627711272.us-east-1.elb.amazonaws.com	54.86.117.43	true	false		high
d2cjrwb117kaxb.cloudfront.net	18.66.218.54	true	false		high
tracks.trackingplan.com	3.224.204.97	true	false		unknown
accounts.google.com	172.217.168.45	true	false		high
www-google-analytics.l.google.com	216.58.215.238	true	false		high
ws.zoominfo.com	104.16.168.82	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www-googletagmanager.l.google.com	172.217.168.8	true	false		high
d19fvy74nkvmoz.cloudfront.net	18.66.218.11	true	false		high
p13nlog-1106815646.us-east-1.elb.amazonaws.com	52.2.252.209	true	false		high
d2p6vz8nayi9a3.cloudfront.net	18.66.196.24	true	false		high
pixel.streetmetrics.io	104.21.11.153	true	false		unknown
rs.fullstory.com	35.186.194.58	true	false		high
d3m6p8tvnbsibq.cloudfront.net	18.66.218.75	true	false		high
www.datadoghq-browser-agent.com	18.66.203.63	true	false		unknown
tags.srv.stackadapt.com	52.204.174.192	true	false		high
www.google.ch	172.217.168.35	true	false		high
geolocation.onetrust.com	104.20.185.68	true	false		high
cdn.rollbar.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
endpoint2.collection.us2.sumologic.com	unknown	unknown	false		high
logx.optimizely.com	unknown	unknown	false		high
admin.typeform.com	unknown	unknown	false		high
images.ctfassets.net	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
px.ads.linkedin.com	unknown	unknown	false		high
cdn.optimizely.com	unknown	unknown	false		high
public-assets.typeform.com	unknown	unknown	false		high
fast.wistia.com	unknown	unknown	false		high
10579985.fls.doubleclick.net	unknown	unknown	false		high
x.clearbitjs.com	unknown	unknown	false		unknown
cdn.segment.com	unknown	unknown	false		high
renderer-assets.typeform.com	unknown	unknown	false		high
www.typeform.com	unknown	unknown	false		high
distillery.wistia.com	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
images.typeform.com	unknown	unknown	false		high
public.profitwell.com	unknown	unknown	false		high
auth.typeform.com	unknown	unknown	false		high
config.trackingplan.com	unknown	unknown	false		unknown
embed-fastly.wistia.com	unknown	unknown	false		high
font.typeform.com	unknown	unknown	false		high
snap.licdn.com	unknown	unknown	false		high
6v4feb7simf.typeform.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://10579985.fls.doubleclick.net/activityi;dc_pre=CPac-YXD1PUCFTERBgAdHssPzQ;src=10579985;type=tf_visit;cat=pageview;ord=7023634409798;gtm=2wg1q0;gcs=G111;auiddc=101564392.1643407963;u17=www.typeform.com%2Ftemplates%2F;u18=(Non-Company);~oref=https%3A%2F%2Fwww.typeform.com%2Ftemplates%2F?	false		high
http://https://6v4feb7simf.typeform.com/to/v3GA1r6t	false		high
http://https://www.typeform.com/templates/	false		high
http://https://www.typeform.com/pricing/	false		high
http://https://www.typeform.com/enterprise/	false		high
http://https://www.typeform.com/	false		high
http://https://admin.typeform.com/login	false		high
http://https://admin.typeform.com/signup	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://stats.g.doubleclick.net	f72c4cd4-8ef2-4cbd-8ce2-c6de2c8d7e2a.tmp.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://apis.google.com/js/client.js	mirroring_common.js.0.dr	false		high
http://https://www.google.com/images/cleardot.gif	craw_window.js.0.dr	false		high
http://https://play.google.com	1dabbd6f-8aa7-4763-95a6-313f0fc53696.tmp.2.dr, 642debb1-2803-4aca-be10-e4e71a96b353.tmp.2.dr, f72c4cd4-8ef2-4cbd-8ce2-c6de2c8d7e2a.tmp.2.dr	false		high
http://https://crash.corp.google.com/samples?reportid=&q=	mirroring_cast_streaming.js.0.dr, common.js.0.dr	false		high
http://https://www.google.ch	f72c4cd4-8ef2-4cbd-8ce2-c6de2c8d7e2a.tmp.2.dr	false		high
http://https://www.google.com/log?format=json&hasfast=true	mirroring_hangouts.js.0.dr	false		high
http://https://easylist.to/)	LICENSE.txt.0.dr	false		high
http://https://sandbox.google.com/payments/v4/js/integrator.js	craw_window.js.0.dr, manifest.json.0.dr	false		high
http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01	mirroring_hangouts.js.0.dr	false		high
http://https://accounts.google.com/MergeSession	craw_window.js.0.dr	false		high
http://https://creativecommons.org/compatiblelicenses	LICENSE.txt.0.dr	false		high
http://https://preprod-hangouts-googleapis.sandbox.google.com	mirroring_hangouts.js.0.dr	false		high
http://https://www.google.com	1dabbd6f-8aa7-4763-95a6-313f0fc53696.tmp.2.dr, manifest.json0.0.dr, 642debb1-2803-4aca-be10-e4e71a96b353.tmp.2.dr, f72c4cd4-8ef2-4cbd-8ce2-c6de2c8d7e2a.tmp.2.dr	false		high
http://https://github.com/easylist)	LICENSE.txt.0.dr	false		high
http://https://creativecommons.org/.	LICENSE.txt.0.dr	false		high
http://https://hangouts.clients6.google.com	mirroring_hangouts.js.0.dr	false		high
http://https://meet.google.com	mirroring_common.js.0.dr	false		high
http://https://hangouts.google.com/hangouts/_/logpref	mirroring_hangouts.js.0.dr	false		high
http://https://accounts.google.com	1dabbd6f-8aa7-4763-95a6-313f0fc53696.tmp.2.dr, manifest.json0.0.dr, 642debb1-2803-4aca-be10-e4e71a96b353.tmp.2.dr, f72c4cd4-8ef2-4cbd-8ce2-c6de2c8d7e2a.tmp.2.dr	false		high
http://https://clients2.google.com/cr/report	mirroring_hangouts.js.0.dr, mirroring_cast_streaming.js.0.dr	false		high
http://angularjs.org	angular.js.0.dr	false		high
http://https://creativecommons.org/publicdomain/zero/1.0/.	mirroring_hangouts.js.0.dr	false		high
http://https://github.com/angular/material	material_css_min.css.0.dr, angular.js.0.dr	false		high
http://https://apis.google.com	1dabbd6f-8aa7-4763-95a6-313f0fc53696.tmp.2.dr, manifest.json0.0.dr, 642debb1-2803-4aca-be10-e4e71a96b353.tmp.2.dr, f72c4cd4-8ef2-4cbd-8ce2-c6de2c8d7e2a.tmp.2.dr	false		high
http://https://www.google.com/accounts/OAuthLogin?issueuberauth=1	craw_window.js.0.dr	false		high
http://https://github.com/madler/zlib/blob/master/zlib.h	mirroring_hangouts.js.0.dr	false		high
http://https://www-googleapis-staging.sandbox.google.com	craw_window.js.0.dr, craw_background.js.0.dr	false		high
http://https://clients2.google.com	1dabbd6f-8aa7-4763-95a6-313f0fc53696.tmp.2.dr, 642debb1-2803-4aca-be10-e4e71a96b353.tmp.2.dr, f72c4cd4-8ef2-4cbd-8ce2-c6de2c8d7e2a.tmp.2.dr	false		high
http://https://www.google.com/tools/feedback	feedback_script.js.0.dr	false		high
http://www.apache.org/licenses/LICENSE-2.0	mirroring_hangouts.js.0.dr	false		high
http://https://dns.google	db795b52-1412-40c6-a04c-0a4defb9463b.tmp.2.dr, 1dabbd6f-8aa7-4763-95a6-313f0fc53696.tmp.2.dr, 4ffc04b6-d8c0-4f67-ac72-40bcdc10607f.tmp.2.dr, 642debb1-2803-4aca-be10-e4e71a96b353.tmp.2.dr, f72c4cd4-8ef2-4cbd-8ce2-c6de2c8d7e2a.tmp.2.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_window.js.0.dr, craw_background.js.0.dr	false		high
http://https://www.google.com/intl/en-US/chrome/blank.html	craw_background.js.0.dr	false		high
http://https://ogs.google.com	1dabbd6f-8aa7-4763-95a6-313f0fc53696.tmp.2.dr, 642debb1-2803-4aca-be10-e4e71a96b353.tmp.2.dr, f72c4cd4-8ef2-4cbd-8ce2-c6de2c8d7e2a.tmp.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.google.com/chromecast/troubleshooter/2995236	messages.json29.0.dr, feedback.html.0.dr, messages.json61.0.dr, messages.json62.0.dr, messages.json75.0.dr, messages.json71.0.dr, messages.json73.0.dr, messages.json27.0.dr, messages.json83.0.dr, messages.json79.0.dr, messages.json82.0.dr, messages.json54.0.dr, messages.json44.0.dr, messages.json74.0.dr, messages.json39.0.dr, messages.json0.0.dr, messages.json85.0.dr, messages.json88.0.dr, messages.json14.0.dr, messages.json87.0.dr, messages.json76.0.dr	false		high
http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions	mirroring_hangouts.js.0.dr	false		high
http://https://payments.google.com/payments/v4/js/integrator.js	craw_window.js.0.dr, manifest.json.0.dr	false		high
http://https://adservice.google.com	f72c4cd4-8ef2-4cbd-8ce2-c6de2c8d7e2a.tmp.2.dr	false		high
http://https://www.google.com;	manifest.json0.0.dr	false	• Avira URL Cloud: safe	low
http://https://googleads.g.doubleclick.net	f72c4cd4-8ef2-4cbd-8ce2-c6de2c8d7e2a.tmp.2.dr	false		high
http://https://hangouts.google.com/	manifest.json0.0.dr	false		high
http://https://www.google.com/images/x2.gif	craw_window.js.0.dr	false		high
http://https://www.google.com/images/dot2.gif	craw_window.js.0.dr	false		high
http://https://meetings.clients6.google.com	mirroring_hangouts.js.0.dr	false		high
http://https://play.google.com/log?format=json&hasfast=true	mirroring_hangouts.js.0.dr	false		high
http://https://10579985.fls.doubleclick.net	f72c4cd4-8ef2-4cbd-8ce2-c6de2c8d7e2a.tmp.2.dr	false		high
http://tools.ietf.org/html/rfc1950	mirroring_hangouts.js.0.dr	false		high
http://https://6v4feb7simf.typeform.com/to/v3GA1r6t2	History Provider Cache.0.dr	false		high
http://https://support.google.com/chromecast/answer/2998456	messages.json29.0.dr, feedback.html.0.dr, messages.json61.0.dr, messages.json62.0.dr, messages.json75.0.dr, messages.json71.0.dr, messages.json73.0.dr, messages.json27.0.dr, messages.json83.0.dr, messages.json79.0.dr, messages.json82.0.dr, messages.json54.0.dr, messages.json44.0.dr, messages.json74.0.dr, messages.json39.0.dr, messages.json0.0.dr, messages.json85.0.dr, messages.json88.0.dr, messages.json14.0.dr, messages.json87.0.dr, messages.json76.0.dr	false		high
http://https://clients2.googleusercontent.com	1dabbd6f-8aa7-4763-95a6-313f0fc53696.tmp.2.dr, 642debb1-2803-4aca-be10-e4e71a96b353.tmp.2.dr, f72c4cd4-8ef2-4cbd-8ce2-c6de2c8d7e2a.tmp.2.dr	false		high
http://https://docs.google.com	mirroring_common.js.0.dr	false		high
http://https://www.google.com/	manifest.json.0.dr	false		high
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://clients2.google.com/service/update2/crx	manifest.json0.0.dr, manifest.json.0.dr	false		high
http://https://clients6.google.com	mirroring_hangouts.js.0.dr	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
18.66.196.93	d2q0tm6nh3syda.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
104.19.155.83	track.hubspot.com	United States		13335	CLOUDFLARENETUS	false
104.17.68.176	js.hs-analytics.net	United States		13335	CLOUDFLARENETUS	false
216.58.215.238	www-google-analytics.l.google.com	United States		15169	GOOGLEUS	false
35.186.194.58	rs.fullstory.com	United States		15169	GOOGLEUS	false
104.18.20.191	js.hs-banner.com	United States		13335	CLOUDFLARENETUS	false
157.240.17.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
18.66.218.92	d1ftdm4q83us3q.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
142.250.203.97	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
104.20.184.68	privacyportal-de.onetrust.com	United States		13335	CLOUDFLARENETUS	false
104.16.124.175	unpkg.com	United States		13335	CLOUDFLARENETUS	false
18.66.196.121	d2citsn5wf4j9j.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
18.66.218.11	d19fvy74nkvmoz.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
18.66.218.54	d2cjrwb117kaxb.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
18.66.218.95	d2nvsmtq2poimt.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
52.88.179.26	dx.mountain.com	United States		16509	AMAZON-02US	false
52.11.156.223	unknown	United States		16509	AMAZON-02US	false
108.177.127.155	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
172.217.168.2	adservice.google.com	United States		15169	GOOGLEUS	false
52.42.124.195	px.mountain.com	United States		16509	AMAZON-02US	false
18.66.218.127	unknown	United States		3	MIT-GATEWAYSUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
54.86.117.43	prod-east-stats-tap-alb-627711272.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.139.243.33	d3orhvfyxudxxq.cloudfront.net	United States		16509	AMAZON-02US	false
18.66.196.90	unknown	United States		3	MIT-GATEWAYSUS	false
34.212.4.35	gs.mountain.com	United States		16509	AMAZON-02US	false
18.66.196.79	dna8twue3dlxq.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
172.217.168.68	www.google.com	United States		15169	GOOGLEUS	false
104.17.210.204	js.hs-scripts.com	United States		13335	CLOUDFLARENETUS	false
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
172.217.168.8	www-googletagmanager.l.google.com	United States		15169	GOOGLEUS	false
104.21.11.153	pixel.streetmetrics.io	United States		13335	CLOUDFLARENETUS	false
172.217.168.66	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
108.139.240.122	d296je7bbdd650.cloudfront.net	United States		16509	AMAZON-02US	false
18.66.218.75	d3m6p8tvnbsibq.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
54.149.64.13	api.amplitude.com	United States		16509	AMAZON-02US	false
52.56.230.239	reveal.clearbit.com	United States		16509	AMAZON-02US	false
108.156.0.174	cdn.amplitude.com	United States		16509	AMAZON-02US	false
54.149.50.128	api.segment.io	United States		16509	AMAZON-02US	false
142.250.203.102	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false
18.66.196.24	d2p6vz8nayi9a3.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
52.26.89.215	us2-events-2-1917544754.us-west-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false
18.66.203.63	www.datadoghq-browser-agent.com	United States		3	MIT-GATEWAYSUS	false
18.66.196.29	unknown	United States		3	MIT-GATEWAYSUS	false
104.16.149.64	cdn.cookielaw.org	United States		13335	CLOUDFLARENETUS	false
172.217.168.35	www.google.ch	United States		15169	GOOGLEUS	false
151.101.65.26	polyfill.io	United States		54113	FASTLYUS	false
104.20.185.68	geolocation.onetrust.com	United States		13335	CLOUDFLARENETUS	false
35.201.112.186	edge.fullstory.com	United States		15169	GOOGLEUS	false
104.16.168.82	ws.zoominfo.com	United States		13335	CLOUDFLARENETUS	false
3.224.204.97	tracks.trackingplan.com	United States		14618	AMAZON-AESUS	false
52.2.252.209	p13nlog-1106815646.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
52.204.174.192	tags.srv.stackadapt.com	United States		14618	AMAZON-AESUS	false
3.15.36.195	ok11-crtr-custom-domains-cd76c2bd4d92725a.elb.us-east-2.amazonaws.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:	562123
Start date:	28.01.2022
Start time:	14:10:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 59s

Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://6v4feb7simf.typeform.com/to/v3GA1r6t
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:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.phis.win@35/201@80/59
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.typeform.com/explore/?utm_campaign=v3GA1r6t&utm_source=typeform.com-18086319-free&utm_medium=typeform&utm_content=typeform-closescreenbutton&utm_term=EN • Browse: https://www.typeform.com/explore/?utm_campaign=v3GA1r6t&utm_source=typeform.com-18086319-free&utm_medium=typeform&utm_content=typeform-closescreen&utm_term=EN • Browse: https://www.typeform.com/ • Browse: https://www.typeform.com/pricing/ • Browse: https://www.typeform.com/enterprise/ • Browse: https://admin.typeform.com/login • Browse: https://admin.typeform.com/signup • Browse: https://www.typeform.com/templates/

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.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): 23.211.6.115, 172.217.168.14, 104.18.27.71, 104.18.26.71, 74.125.100.73, 34.104.35.123, 172.217.168.67, 172.217.168.42, 151.101.2.110, 151.101.66.110, 151.101.130.110, 151.101.194.110, 151.101.2.133, 151.101.66.133, 151.101.130.133, 151.101.194.133, 23.211.5.34, 142.250.203.99, 80.67.82.240, 80.67.82.235, 13.107.42.14, 142.250.203.106, 216.58.215.234, 172.217.168.10, 172.217.168.74
- Excluded domains from analysis (whitelisted): store-images.s-microsoft.com-c.edgekey.net, clientservices.googleapis.com, arc.msn.com, e5048.dsca.akamaiedge.net, e12564.dspb.akamaiedge.net, l-0005.l-msedge.net, random.typeform.com.cdn.cloudflare.net, redirector.gvt1.com, www.googletagmanager.com, update.googleapis.com, dualstack.f4.shared.global.fastly.net, admin.typeform.com.cdn.cloudflare.net, displaycatalog.mp.microsoft.com, r4---sn-5hne6nsz.gvt1.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.gstatic.com, www.google-analytics.com, www-linkedin-com.l-0005.l-msedge.net, client.wns.windows.com, content-autofill.googleapis.com, ctldl.windowsupdate.com, d.sni.global.fastly.net, www.googleapis.com, od.linkedin.edgesuite.net, r4.sn-5hne6nsz.gvt1.com, ris.api.iris.microsoft.com, edgedl.me.gvt1.com, store-images.s-microsoft.com, cdn.o6.edgekey.net, a1916.dscg2.akamai.net
- 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 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 GMDS.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\12ebe537-a541-4bd9-b41d-6c0b2bda5bcf.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.743845978501557
Encrypted:	false
SSDEEP:	384:jLwPjByMFpuzqNbrAv393g/FAHZ4GM7rGRHzxAFlF0rOHmO5SdD3jYOtdXNy1b6H:sKF1u508AeP7p5EnbqhKHZz1x
MD5:	CCE5DF598D723D101FC17B7C1F606215
SHA1:	38A6E8BDF84D6D067E2FB64CE3A6FA304EA55B31
SHA-256:	321DCC9E71BA8F4457F606251D93BA75BC9F9C6F2D7DC908837A27C31604B5F9
SHA-512:	362702E1C50B525FE9C16465C5041278035045436A3760A2826496B7C522366AC50BA6648036F91220EA92A231A7995A4CDFA771217D1E6EB9D5A3DDD9D6565B
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...FR8.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\1a041006-3dfc-4366-84d5-a91d27e6c33c.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):	198652
Entropy (8bit):	6.0741214901815805
Encrypted:	false
SSDEEP:	6144:dr9407dorBtGzg4Kqkjc0maqfIlUOoSiuRU:durHG5WjZo3
MD5:	7A4D4ABB0A0DD3C1F3A4547855E4D99B
SHA1:	08DE6C8B39E6C98411E307772EF70DEBAF1FC187
SHA-256:	18C2C54ECF38A2019E008AF2BBAA5DA713AD6BA922C953F552585749B3BEE1EE
SHA-512:	FD70262D1DF9EE47499561C5C519B1480B74041CCE877063C8D162413B91705E1EA36CC65C883C5725EA740967D6FACB7600530C95B15E5D40CC8017BFC99BA
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":1.643407886424815e+12,"network":1.643375488e+12,"ticks":133402309.0,"uncertainty":3943022.0}},"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\25947faa-0cde-4b66-afb2-4abebcbf0cb3.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):	190280
Entropy (8bit):	6.0454734482002195
Encrypted:	false
SSDEEP:	3072:nydk+l20ee3L2oVJhynrpnbtpQVzg4d8qkwMc0YXFcbXafIB0u1GOJmA3iuRU:U9407dorBtGzg4Kqkjc0maqfIlUOoSiZ
MD5:	EA517C2F7AFCC8DBB5FAEA705547186B
SHA1:	F11838C8A97E9D01147AC76F804BAF83AA10C7F9
SHA-256:	8781ED4A36C60403472E69A418DABDFF91EE30B090865615E238892855FC7E87
SHA-512:	7D24BB73B8D4AA530F9EE5D7EEB0D6A8F7D8A1E92C08E19212D759BE36C1861E111DF90AE7856AA08FC103F3D0F62E3252D405D5B8B42C597B4DD761989CC9 7A
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":1.643407886424815e+12,"network":1.643375488e+12,"ticks":133402309.0,"uncertainty":3943022.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799438436"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\373f699c-7b68-4cae-9452-fa032ac6d88d.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.743909281442925
Encrypted:	false
SSDEEP:	384:1LwPjByMJGp1V+kzqNbrAv393g/FAHZ4GM7rGRHzxAFlF0rOHmO5SdD3jYOtdXNm:p+KF1u508AeP7p5EnbqhKHZz1G
MD5:	EB82BF5F4DE4799096964804BCB8817F
SHA1:	1005E0303833653A374FE48354842CE0EB3ED520
SHA-256:	4752FB44B52F211D74552BFA5010E993F99C4137E6926622B4F361C9B5A6BA46
SHA-512:	E33E7D326197AFFE38D0C17E547732580031BB441C693E0550F6E4F00A90581AC92C1A3C87C9C2F3360E370603CF2914C62B433157F5B7B350AB179F9476048E

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...FR8.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\525216c8-3d6a-4604-8930-cbdae6d14b05.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):	190176
Entropy (8bit):	6.045181024768099
Encrypted:	false
SSDEEP:	3072:itdk+l20ee3L2oVJhynrpnbtpQVzg4d8qkwMc0YXFcbXafIB0u1GOJmA3iuRU:o9407dorBtGzg4KqkjcOmaqfIlUOoSiZ
MD5:	976779E526BE2BAA2B654F4CBFF73E2D
SHA1:	4E6D60DE0680FDCF3DDF44EC6DE5B2CC0F1FBCB1
SHA-256:	009CBDCB14CFAE12DF545347AFE714E1D663A7182283C47D84F2EC7B953C521B
SHA-512:	B74D649393662FBB5EB67C2956B47F0657A5DC8258911FD7A384C5E3E77FAC8DD7064494FCFA2C214C7B6D5FEF251BD724BC3273E27A2C36EFD40EFA6A3FB263
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":1.643407886424815e+12,"network":1.643375488e+12,"ticks":133402309.0,"uncertainty":3943022.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799438436"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\693c4a5e-7f14-4b65-b101-7a8cc3bcf949.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):	190280
Entropy (8bit):	6.0454734482002195
Encrypted:	false
SSDEEP:	3072:nydk+l20ee3L2oVJhynrpnbtpQVzg4d8qkwMc0YXFcbXafIB0u1GOJmA3iuRU:U9407dorBtGzg4KqkjcOmaqfIlUOoSiZ
MD5:	EA517C2F7AFCC8DBB5FAEA705547186B
SHA1:	F11838C8A97E9D01147AC76F804BAF83AA10C7F9
SHA-256:	8781ED4A36C60403472E69A418DABDFF91EE30B090865615E238892855FC7E87
SHA-512:	7D24BB73B8D4AA530F9EE5D7EEB0D6A8F7D8A1E92C08E19212D759BE36C1861E111DF90AE7856AA08FC103F3D0F62E3252D405D5B8B42C597B4DD761989CC97A
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":1.643407886424815e+12,"network":1.643375488e+12,"ticks":133402309.0,"uncertainty":3943022.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799438436"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\7d5d8578-b03e-4611-a199-4200de553b52.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):	190280
Entropy (8bit):	6.045473191224309
Encrypted:	false
SSDEEP:	3072:4adk+l20ee3L2oVJhynrpnbtpQVzg4d8qkwMc0YXFcbXafIB0u1GOJmA3iuRU:J9407dorBtGzg4KqkjcOmaqfIlUOoSiZ
MD5:	97157D87FD68F9CB00F63F2ABFCBB958
SHA1:	3D7DEC5462FC290773F18E11F374F7140675958C

SHA-256:	FEC19CC2497186338560A01074E650020E0D770CA2AA98834AC5C978714D2AE5
SHA-512:	F5D4D42E79E3F139A63F7C951D446D747067C8E0127F1248D1350A1A6D540A1EF1ACBFCA6D823199E915BF229798EA87209AD7BFCB35BDB615B09C367A8EC38 6
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}}},"ne twork_time":{"network_time_mapping":{"local":1.643407886424815e+12,"network":1.643375488e+12,"ticks":133402309.0,"uncertainty":3943022.0}},"os_crypt":{"encrypte d_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrY iwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYq Qj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"pa ssword_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799438436"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\7fbf9687-5987-4d35-be15-4921cabca843.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):	190176
Entropy (8bit):	6.045182753980272
Encrypted:	false
SSDEEP:	3072:judk+l20ee3L2oVJhynrpnbtpQVzg4d8qkwMc0YXFcbXafIB0u1GOJmA3iuRU:E9407dorBtGzg4Kqkjc0maqfllUOoSiZ
MD5:	66989F922CEC0DC0F6F1F3E0DAEE6BA5
SHA1:	28B4A68FCD8A9547D389676ADDC2156B8D497126
SHA-256:	B26316E240F317EFFE6F0471C4C85A235B1A4DCFF8DEAECAA00A907B150389E1
SHA-512:	4A7E72B2A22F77A68EF8B72D33CFB0EEFC8000964AA9D7FB9CB094D4077B5E3A16D2DF9DA6385A16869BE7F7C9EB0149B1005CEA11408D7D78D547CA236232 15
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}}},"ne twork_time":{"network_time_mapping":{"local":1.643407886424815e+12,"network":1.643375488e+12,"ticks":133402309.0,"uncertainty":3943022.0}},"os_crypt":{"encrypte d_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrY iwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYq Qj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"pa ssword_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799438436"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\8b166c41-37b9-4be5-b433-3171eaaed10e.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):	198652
Entropy (8bit):	6.074122276993313
Encrypted:	false
SSDEEP:	6144:0f9407dorBtGzg4Kqkjc0maqfllUOoSiuRU:0arHG5WjZo3
MD5:	6F8FB10A4B7DB9449961069233FB60C9
SHA1:	0ACD7C37A7EA79AB3FC4AC653EAA9F215FDE6FAE
SHA-256:	58531515B7954AA53FAE076B3D6D357C2A8908DD185C75FC976D43CE924FC6F2
SHA-512:	054B8E74B626FA84BD4CC05E9DC9349C4051C5C296C74043717F8C95AAD2D0AF84817E7DE4E267E7DA9B459DFDEDD60E0ADD7C6BCFB718AA912929843A164 08
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}}},"ne twork_time":{"network_time_mapping":{"local":1.643407886424815e+12,"network":1.643375488e+12,"ticks":133402309.0,"uncertainty":3943022.0}},"os_crypt":{"encrypte d_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrY iwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYq Qj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"pa ssword_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799438436"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	3.254162526001658

Encrypted:	false
SSDEEP:	3:FkXft0xE1n:+ftlE1n
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\1dabbd6f-8aa7-4763-95a6-313f0fc53696.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):	2480
Entropy (8bit):	4.914701682809353
Encrypted:	false
SSDEEP:	48:Y2TntwCXGDH3qz5sLGscRLsW6WYr33sRyKs4MHHfsohKrs6QsQxbD:JTnOCXGDHazc6PbYrc9GH/hKToxH
MD5:	082B94D39E7E7DFE78A45A9B852E0FEF
SHA1:	153F45F0A48F058850FAD4D3B1FBFB34F2424F84
SHA-256:	DE13823759A644B95E03585186F38A660580D30F4554FB33417F8331074BA707
SHA-512:	A7A7EAFD173D127E142689EA9DF5640A0EB14796586F12B116E8652F3EF782271F5DB5A713CC4AFFDF6AC3C06BB56740D536D2DA5A5E0CED7A4CA8E1F03085 CC
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","supports_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.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13290473486557415","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13290473486580191","port":443,"protocol_str":"quic"}],"isol

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3986476a-79cf-4c77-824b-db73ebeb77e0.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):	5151
Entropy (8bit):	4.983788972745975
Encrypted:	false
SSDEEP:	96:nSpCsRX9pcKI+ZEok0JCKL8jkq7S1gbOTQVuwn:nSpCa9pco4KMkbw
MD5:	46F27CACE69C628F40B62D438868E60C
SHA1:	424119A81D61B140B5690E58196B4EE82035E06D
SHA-256:	F80D77B45310D234D6D627E675DAE31CB2F830B318EE59356221FA8909DE9266
SHA-512:	1CE841817874A4B43FB24EBD161E4A382DE490F2AA2307DEE6C65A9E2B46C4DDFD3D7EC5B0E06805DF9826ACE327F95674CA7B4A45EF288CC5DC62054735777 23
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287881484970204","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","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\51ea77e7-620f-4297-9607-dabfc578dd4b.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\5c82f211-e55c-4e29-824f-28b8b29a62f1.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):	5448
Entropy (8bit):	5.007432174203029
Encrypted:	false
SSDEEP:	96:nSpCiVZ9pcKI+ZYok0JCKL8jkq7S1JkqFjgbOTQVuwn:nSpC+9pcS4KMkbXkKG
MD5:	33E12CC0569B4F27769DE811DB8039F6
SHA1:	D578C4BE15E38CAE37887A9455F1131450162F27
SHA-256:	E83E962C2B62A4E169DC3555B18EF3591341CBD976F16F71022C000E045AD4E7
SHA-512:	FC0DFC4BF5B0835176AF0F71773B8ABFC07C5A65C22D1EDFC4D308E60EB649C476D18DAA647A7B70B4398A56DCC691627F59430B9D7BC6D8361C9540DCDEC DC
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287881484970204","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","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\642debb1-2803-4aca-be10-e4e71a96b353.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\798cba07-bd90-4bb5-80d5-7941f813ee2c.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):	5.5835133267250106
Encrypted:	false
SSDEEP:	384:mrRtiLlXuXR1kXqKf/pUZNCgVLH2HfDWrUHm+lc0f4QD:xLlER1kXqKf/pUZNCgVLH2HfyrUHk0fb
MD5:	5CC26CF9339B59CB3B56EE6D0F8B5A7B
SHA1:	E909D99AAE8D2DF4050DD0DF5F7972FCF20813CB

SHA-256:	E17512B998EE65145B41971E9F5B1C8F19F52AD129E4BC0A77970C6963C42A9A
SHA-512:	00829B3808E54C30F950E133AE99C9B179091A87889ABBEC0CFA4462335BCC0884DA0FCC1E9BFF4749B2E7246A6BA37413A5A9881ADA25685E7D5A98CB37CC 5
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13287881484400395","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8b74c677-fa94-4da0-9b5d-757b77c28285.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):	5.570454250151014
Encrypted:	false
SSDEEP:	384:mrRtiLlXuXR1kXqKf/pUZNCgVLH2HfDWrUNHGzm+l9f44w:xLlER1kXqKf/pUZNCgVLH2HfyrUxGzVo
MD5:	84371C7F87C8B40C4922CD9B356D12B4
SHA1:	E358D9E8E29D87630CD28364F75DCD001C5601C9
SHA-256:	0C9A12FD1ABB3F24021134845528778 72A2CA5D25DFF9863D2603571E89DA40D
SHA-512:	F42DDF752950FBEE3C164B824315AF678DF622A632F28A46365606DA8215BACE801460BE4F806F1B414BF128302A272C0CBD9226202393DBCEC204386350DC82
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13287881484400395","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8e9e6684-5fb9-4240-b614-1d2f540304a2.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):	5.570629826208175
Encrypted:	false
SSDEEP:	384:mrRtiLlXuXR1kXqKf/pUZNCgVLH2HfDWrUNHGQm+lef4C:xLlER1kXqKf/pUZNCgVLH2HfyrUxGQ2V
MD5:	491DA4201D32E6F60B45601105D3292B
SHA1:	887EEF634C44AFB39551619672C99C88B4E8ED92
SHA-256:	9DC30993B024361F325A79B1C7FCC43CA9E550199132D0C45541233E97787B1D
SHA-512:	648069E5370D64D4B08AF7E6D2B893E737ADE97613F70651FF4B9A161340E832676E793FCF2DDEC258D547E3937349F72A1074CC444F516A279E75D76B5847C6
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13287881484400395","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\980df397-b506-4ed6-bff7-b94330d0fc37.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	modified
Size (bytes):	203
Entropy (8bit):	5.36136427639681
Encrypted:	false
SSDEEP:	6:YAQNwR5Hy9RfSHJR8wXwlmUUAnIMp5V0SQ:Y6PHy9RAJ9+UAnIMHQ

MD5:	446D7B44685B649B9AEA4914A7C64CE3
SHA1:	4BEE245AFBB2075ABCE06B8E1C7F58266DDF45B7
SHA-256:	C7EA48C984336CA16FC50694B2E278CD69854F82EA523C08820850379449B756
SHA-512:	9A0575540E035BCF977025C94034272FACDCAD1FE7089E2B19A77145A2C814BF78163DB8DA0FE7D5388B130330AE794FFF55135DA84845C58B456C82A30DCD0
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1674943941.196854,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1643407941.196859}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9ab9e20a-4e94-4c98-bf90-88d78f8bc46b.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):	5199
Entropy (8bit):	4.983920669873034
Encrypted:	false
SSDEEP:	96:nSpCi5Z9pcKI+ZYok0JCKL8jkq7S1gbOTQVuwn:nSpC09pcS4KMkbw
MD5:	96F4FEB9DF2BE7ED58AF1524339189AB
SHA1:	514776F71AE1FD5B11E660A5B977E111E622A417
SHA-256:	8C88469355DAE2E9D781E36EE81DB571A20201601BFF54314F09E16B074B8E76
SHA-512:	1307FA84007531C9A1B9D0D6D116F872F90DF8DD71DB05250CF25ADAEC8D2230EA0E92154D50923896CE4D24EB0C942C137EA47107EEA3F2C1C65AD54954C33
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287881484970204","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","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:7dOscSRKc1nGRSklhEw6M1tf7SNyb
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):	5.195008286204894
Encrypted:	false
SSDEEP:	6:MBLcq2PWXp+N23iKKdK25+Xqx8chI+IFUtqVTBLcZZmwYVTBLJkwOWXp+N23iKKN:Myva5KkTXfchI3FUtuyZ/0j5f5KkTXfE
MD5:	C01502677E736A002B3DD7E00C2EA632
SHA1:	B5B7E10336FFA1CBC95FF216B20B1B1286F56D04
SHA-256:	E13616719BC73A46EBF6720F0EBB6A795EEEDE979F1A776218579D556CEB5E90
SHA-512:	89BB32047EFD0C0324F42C43F9BC88364D006FB8E6A28664B505FC3C02A890D1B7DDAF29609FDF6199ADCB83CFD856F8800BDFE350BCF6B97406644B35D21AF
Malicious:	false
Reputation:	low
Preview:	2022/01/28-14:11:42.128 1ac4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/01/28-14:11:42.130 1ac4 Recovering log #3.2022/01/28-14:11:42.131 1ac4 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):	5.195008286204894
Encrypted:	false
SSDEEP:	6:MBLcq2PWXp+N23iKKdK25+Xqx8chI+IFUtqVTBLcZZmwYVTBLJkwOWXp+N23iKKN:Myva5KkTXfchI3FUtuyZ/0j5f5KkTXfE
MD5:	C01502677E736A002B3DD7E00C2EA632
SHA1:	B5B7E10336FFA1CBC95FF216B20B1B1286F56D04

SHA-256:	E13616719BC73A46EBF6720F0EBB6A795EEEDE979F1A776218579D556CEB5E90
SHA-512:	89BB32047EFD0C0324F42C43F9BC88364D006FB8E6A28664B505FC3C02A890D1B7DDAF29609FDF6199ADCB83CFD856F8800BDFE350BCF6B97406644B35D21AF
Malicious:	false
Reputation:	low
Preview:	2022/01/28-14:11:42.128 1ac4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2022/01/28-14:11:42.130 1ac4 Recovering log #3.2022/01/28-14:11:42.131 1ac4 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):	1473
Entropy (8bit):	5.708454225002422
Encrypted:	false
SSDEEP:	24:XNeMgeMQp/Hw/hKnuDP+ngKhtZKkwag0jcsGSawNiyyxhFZQgCXWyUq6dCPj:XN7dpyUnuT+ngKXZfPdn7wbNLzyUTdc
MD5:	64BECC8A6B59FD0F73D99B773C6B29D7
SHA1:	7280A1FC9222A7CD46F2CC926FCEB666F79119D6
SHA-256:	67A21EC1EF6A5FEDA0019712EE557637E1475F6647ED570929AB46D15EC609A9
SHA-512:	7BF1BEAB02EF6A49767D78C6560888AAE9F7C74C58FA5A8FA5B492EFC2EA440A47B8B72576CABE6600F951258D19E00786D81E31097EB95F7DD4FE40C9756130
Malicious:	false
Reputation:	low
Preview:	.....".....18086319..campaign..closescreenbutton..com..content..discover..en..explore..forms..free..fun..https..medium..source..term..typeform..utm..v3ga1r6t..where..www..6v4feb7simf..new..to*.....18086319.....6v4feb7simf.....campaign.....closescreenbutton.....com.....content.....discover.....en.....explore.....forms.....free.....fun.....https.....medium.....new.....source.....term.....to.....typeform.....utm.....v3ga1r6t.....where.....www..2.....0.....1.....3.....4.....6.....7.....8.....9.....a.....b.....c.....d.....e.....f.....g.....h.....i.....l.....m.....n.....o.....p.....r.....s.....t.....u.....v.....w.....x.....y...:

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"},{"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\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):	5448
Entropy (8bit):	5.007432174203029
Encrypted:	false
SSDEEP:	96:nSpCiVZ9pcKI+ZYok0JCKL8jkq7S1JkqFjgbOTQVuwn:nSpC+9pcS4KMkbXkKG
MD5:	33E12CC0569B4F27769DE811DB8039F6
SHA1:	D578C4BE15E38CAE37887A9455F1131450162F27
SHA-256:	E83E962C2B62A4E169DC3555B18EF3591341CBD976F16F71022C000E045AD4E7

SHA-512:	FC0DFC4BF5B0835176AF0F71773B8ABFC07C5A65C22D1EDFC4D308E60EB649C476D18DAA647A7B70B4398A56DCC691627F59430B9D7BC6D8361C9540DCDEC DC
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287881484970204","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","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

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):	5199
Entropy (8bit):	4.983975138690969
Encrypted:	false
SSDEEP:	96:nSpCi5Z9pcKI+Z7ok0JCKL8jkq7S1gbOTQVuwn:nSpC09pc74KMkbw
MD5:	DF6B302E8C5317F711A9537E955B0D25
SHA1:	2206C9CBAD38B552455AFE4440ACEA9A2EE08C6C
SHA-256:	5A3851DCB3DCED98320AD5AE987D49C6EDED0C1EBF1FF298370A1450971D4EFF
SHA-512:	39155EA6AA408A4BCBBBFA2594B05D6250DA7A85376BA989056642BC8EEE586E86FEE11C1F1D6952BEEFDF2EF7229AB717ADBC975DA7D0F1333AD70ED4C27 013
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287881484970204","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","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferencese (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):	5151
Entropy (8bit):	4.983788972745975
Encrypted:	false
SSDEEP:	96:nSpCsRX9pcKI+ZEok0JCKL8jkq7S1gbOTQVuwn:nSpCa9pco4KMkbw
MD5:	46F27CACE69C628F40B62D438868E60C
SHA1:	424119A81D61B140B5690E58196B4EE82035E06D
SHA-256:	F80D77B45310D234D6D627E675DAE31CB2F830B318EE59356221FA8909DE9266
SHA-512:	1CE841817874A4B43FB24EBD161E4A382DE490F2AA2307DEE6C65A9E2B46C4DDFD3D7EC5B0E06805DF9826ACE327F95674CA7B4A45EF288CC5DC6205473577 23
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287881484970204","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","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferencesfn (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):	5199
Entropy (8bit):	4.983920669873034
Encrypted:	false
SSDEEP:	96:nSpCi5Z9pcKI+ZYok0JCKL8jkq7S1gbOTQVuwn:nSpC09pcS4KMkbw
MD5:	96F4FEB9DF2BE7ED58AF1524339189AB

SHA1:	514776F71AE1FD5B11E660A5B977E111E622A417
SHA-256:	8C88469355DAE2E9D781E36EE81DB571A20201601BFF54314F09E16B074B8E76
SHA-512:	1307FA84007531C9A1B9D0D6D116F872F90DF8DD71DB05250CF25ADAEC8D2230EA0E92154D50923896CE4D24EB0C942C137EA47107EEA3F2C1C65AD54954C3 3
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287881484970204","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\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):	5.5835133267250106
Encrypted:	false
SSDEEP:	384:mrRtiLlXuXR1kXqKf/pUZNCgVLH2HfDWrUHm+lc0f4QD:xLlER1kXqKf/pUZNCgVLH2HfyrUHk0fb
MD5:	5CC26CF9339B59CB3B56EE6D0F8B5A7B
SHA1:	E909D99AAE8D2DF4050DD0DF5F7972FCF20813CB
SHA-256:	E17512B998EE65145B41971E9F5B1C8F19F52AD129E4BC0A77970C6963C42A9A
SHA-512:	00829B3808E54C30F950E133AE99C9B179091A87889ABBEC0CFA4462335BCC0884DA0FCC1E9BFF4749B2E7246A6BA37413A5A9881ADA25685E7D5A98CB37CC 5
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":"13287881484400395","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\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\4ffc04b6-d8c0-4f67-ac72-40bcdc10607f.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\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\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:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898D58
Malicious:	false
Reputation:	low
Preview:	....

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.213140807252513
Encrypted:	false
SSDEEP:	12:MVva5KkkGHArBFUtuCX/0f5f5KkkGHAryJ:M5a5KkkGgPguC8xf5KkkGga
MD5:	20ED2B608D09D2591FD011FFE4298621

SHA1:	8974F4CD8E757B807ED2417AC67FE675059BC817
SHA-256:	BC17E147316EBE6D2211B15B4802B7A74B3CBB1DB6438153D9D80BFB8FB96FFA
SHA-512:	7F219799DB7D1DE86795453CD001E5F54CAF2B2C0F29331DDAB03A19BEFB0250718313E8211016BD2D8C974789988244EFF8166291FFA43F5D4E41C67B47DFE
Malicious:	false
Reputation:	low
Preview:	2022/01/28-14:12:41.679 1b80 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2022/01/28-14:12:41.682 1b80 Recovering log #3.2022/01/28-14:12:41.683 1b80 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.170142172149459
Encrypted:	false
SSDEEP:	12:Mdk+va5KkkGHArqiuFUtuQW/0nV5f5KkkGHArq2J:Mja5KkkGgCguQzHf5KkkGg7
MD5:	83938BDA10303A4870F7251BEB4AFC4A
SHA1:	AB803FAB5C11E18286DEED6B315E8730C89D171B
SHA-256:	10602BF703BBD18E3CE6FA0FD12EA632CEF43EDE5B937D7F8074F4128C647529
SHA-512:	0F043332DFD1B42863DC933D116D37EC21C839D6E4EAD367C51EC377976D3882CD3C1A93E677394625EBC9B2F7F83C73D2D2BA90F72860908F654213997ECF6
Malicious:	false
Reputation:	low
Preview:	2022/01/28-14:12:41.720 1aec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2022/01/28-14:12:41.723 1aec Recovering log #3.2022/01/28-14:12:41.723 1aec Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.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:	EA34C39AEA13B281A6067DE20AD0CDA84135E70C97DB3CDD59E25E6536B19F7781E5FC0CA4A11C3618D43FC3BD3FBC120DD5C1C47821A248B8AD351F9F4E6367
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):	5.200780925885529
Encrypted:	false
SSDEEP:	12:Md+va5KkkGHArAFUtuaZW/0WV5f5KkkGHArfJ:Mqa5KkkGgkguaZzQf5KkkGgV
MD5:	887C772CF9F1F59D939698AE733715F9
SHA1:	D647B30F33CBE36FB49E903F97420C4940F27F9A
SHA-256:	D26860E1391FE8E67F0B26FA465A1E7A1499325766E40850E979726ED48C94C2
SHA-512:	E39978963B490D9CAE62423B20347CEDBBAA36AC45C3737D2866663E75790167DA15A7505FDDF6E820F459101CB808CD6CAA39AABCCF31FC7C699B3DA98A27D9
Malicious:	false

Reputation:	low
Preview:	2022/01/28-14:12:56.963 1aec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2022/01/28-14:12:56.965 1aec Recovering log #3.2022/01/28-14:12:56.966 1aec 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\db795b52-1412-40c6-a04c-0a4defb9463b.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"},{"advertised_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\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):	5.3093529989049735
Encrypted:	false
SSDEEP:	12:Mcf+va5KkkOrsFUtucYW/0cfV5f5KkkOrzJ:Mcka5Kk+gucYzcff5Kkn
MD5:	90EC8E0E4DD0F8449AC6F85771E6F956
SHA1:	66A57BB7C3D6FCF393DB6D66080B5C02A13FF0BA
SHA-256:	62D3F9E2FAD702C86BC218DA5B8EAE77D17370E364B3D89812B0A6FD0776F802
SHA-512:	FC4EC83E96953B6A5A8F8E28A1B46313C83121F5B18D6569C7131B7E8860AD6C2EBDC44890A665F5529EB813166B202E4D3738D240CB91245D532D695B05BAB
Malicious:	false
Reputation:	low
Preview:	2022/01/28-14:13:50.417 1aec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2022/01/28-14:13:50.417 1aec Recovering log #3.2022/01/28-14:13:50.417 1aec 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 no line terminators
Category:	dropped
Size (bytes):	203
Entropy (8bit):	5.36136427639681
Encrypted:	false
SSDEEP:	6:YAQNwR5Hy9RfSHJR8wXwlmUUAnIMp5V0SQ:Y6PHy9RAJ9+UAnIMHQ
MD5:	446D7B44685B649B9AEA4914A7C64CE3
SHA1:	4BEE245AFBB2075ABCE06B8E1C7F58266DDF45B7
SHA-256:	C7EA48C984336CA16FC50694B2E278CD69854F82EA523C08820850379449B756
SHA-512:	9A0575540E035BCF977025C94034272FACDCAD1FE7089E2B19A77145A2C814BF78163DB8DA0FE7D5388B130330AE794FFF55135DA84845C58B456C82A30DCD0
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1674943941.196854,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1643407941.196859}],"version":2}

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.3412441691171475
Encrypted:	false
SSDEEP:	6:YAQNwRCLSSfE9RfSHJR8wXwlmUUAnIMp5VShqSQ:Y66VE9RAJ9+UAnIPQ
MD5:	CB1B710E288F91A5B225D87025A7298E
SHA1:	FB65999BFDE48C38F3D5FCFFB314F3AB135031F2
SHA-256:	252953DA8D2C8B6F001371FCF97F87BDAFB383F0F0E460A4D9512442C76CC5E5
SHA-512:	C6D3351C83B61E35D59CECACE337C66160CEC80937EFDD0ECB91109CC48775B62D3075E1A146CC09E77F7D81C27545D8298199656D5F2AB57BC32FB777B78E A
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1674943934.77648,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains": true,"sts_observed":1643407934.776485}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a8c076c5-e544-471f-af6b-3aaa1e4e8bea.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):	5.391904822900356
Encrypted:	false
SSDEEP:	6:YAQNwRQQXVS9RfSHJR8wXwlmUUAnIMp5TCQjKSQ:Y6zg9RAJ9+UAnIuj1Q
MD5:	CAED33D87ADEE47B66F30C7FFFFE6520
SHA1:	6F473587387275B0231167DF7B439C10D94B39FB
SHA-256:	B8D8AB71F3539630B75A67E722F49C2FAFED44B2252642B6F98AB5F47F71181A
SHA-512:	9F27475ACDC99DCCAAA3E3675DABBC41F14C8E8CC608B5F60AF70AB8CBD9F427979B01BD1C31227AA0A56DB6BFE0A150794AE0BD9E77CB0B0B5C9D5A2997 96C6
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1674943905.452806,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains" :true,"sts_observed":1643407905.452812}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\aa917eaa-189d-46cd-808f-edf3308cddf3.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):	16745
Entropy (8bit):	5.5777909323685115
Encrypted:	false
SSDEEP:	384:mrRtjLlXuXR1kXqKf/pUZNCgVLH2HfDWrURS+lcf4Bn:+LlER1kXqKf/pUZNCgVLH2HfyrURofMn
MD5:	F95515B981469839325C349466E305C8
SHA1:	FF1D6580E9528E4F2CF208CA7397E3DE59CF5881
SHA-256:	05F2DEF14E0B03988CA36F806669EE75153920B865E471AB65FA9CC3763C4DE4
SHA-512:	4F85F60CADB46E499CD4266BB47C637BF086BF9DDABB585D9D57F5B2DE205FB3D704EC35D20CAB0A681F65BEA89A4E346E2BA4A3FE86C0273C04B13C117A3 D3F
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13287881484400395","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b14865d2-598b-4ed1-a12c-7bd5da561001.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped

Size (bytes):	202
Entropy (8bit):	5.3412441691171475
Encrypted:	false
SSDEEP:	6:YAQNwRCLSSfE9RfSHJR8wXwlmUUAnIMp5VShqSQ:Y66VE9RAJ9+UAnIPQ
MD5:	CB1B710E288F91A5B225D87025A7298E
SHA1:	FB65999BFDE48C38F3D5FCFFB314F3AB135031F2
SHA-256:	252953DA8D2C8B6F001371FCF97F87BDAFB383F0F0E460A4D9512442C76CC5E5
SHA-512:	C6D3351C83B61E35D59CECACE337C66160CEC80937EFDD0ECB91109CC48775B62D3075E1A146CC09E77F7D81C27545D8298199656D5F2AB57BC32FB777B78E A
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1674943934.77648,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains": true,"sts_observed":1643407934.776485}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b9bc0aa4-71b1-45df-8714-2e278026136e.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):	5.536229513305132
Encrypted:	false
SSDEEP:	384:mrRtiLlXuXR1kXqKf/pUZNCgVLH2HfDWrUNHG4nT5m+lqxf4LD:xLlER1kXqKf/pUZNCgVLH2HfyrUxG4nl
MD5:	D7F6E9A7B58D42D276E531DA3E206C6B
SHA1:	C507BF7671879F8E99E50AA5BC256BF23516D832
SHA-256:	BD65568F0B66464D421A5540E9C22208C7084CF4DDE4229DC69EA1FC6AF542CB
SHA-512:	1C81FA04DAB3AE56122D2E6D35FAAD3FC6D4239F31CBA69B78764E0EA1A7908EF06034DC40295255A34CE12515F849BCA2C4F3230D153694E24DC817520A915
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":"13287881484400395","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":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c366ac19-2db8-47bc-ae5a-8013d7600b53.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):	6043
Entropy (8bit):	5.1975550747754005
Encrypted:	false
SSDEEP:	96:nSpCm/sZ95dfZCcKI+Zfok0JCKL8jkq7S1vkqu5fbOTQVuwn:nSpCt9bocP4KMkblkjd
MD5:	BB9D0B77AC8DE6F008096323CF31271D
SHA1:	455BD1215DF11B57F09AA2FDE4ACFEC559427AD7
SHA-256:	EABBFC628F7D147782E4108C4BCF92020E35221475FDDC6201B99A39AB8EC090
SHA-512:	A73228765E7C83994806AC01E550A2C26270451DF47968F113AE55432892FBC4273D7622F7DAE38DA9CAD6EB47439FFD16CA5373DE46E4F8D6632748DE51BCA
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287881484970204","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","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

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\dc89c097-f819-47b9-9858-132aac441971.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):	5.365860702320046
Encrypted:	false
SSDEEP:	6:YAQNwR6/E9RfSHJR8wXwlmUUAnIMp5p+hSQ:Y6uE9RAJ9+UAnI4Q
MD5:	9080E2AD668731D8DBFE52B8A4DFE452
SHA1:	B232440F263F116D45CAB1BCE83312704618BA89
SHA-256:	CBFB5DA74EB504A7F890EFC1B552A961B2C98FBE3C67E05F1451337B5E468B0A
SHA-512:	5412D07486B2AF29A1E1AA38DB83B47A8B97D0DC8FCE3FEDB342C6B8163CA03BDCD192CF9CF66437F0879DAACBD57FBAE522D113D08ECCDFDF4B83CB892E 4CDC
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1674943957.776858,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains" :true,"sts_observed":1643407957.776863}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ea2ef4d8-e23c-43e3-b650-d20fdaa619e3.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):	5.374123342730717
Encrypted:	false
SSDEEP:	6:YAQNwRRfNm9RfSHJR8wXwlmUUAnIMp5pZFd2SQ:Y6Po9RAJ9+UAnIg1ZQ
MD5:	1302284398E15C5863184E95E6AFC6FD
SHA1:	7D5E8687820C6BCE451C8613556289892B622DD8
SHA-256:	FA9CEBACFF8E1DD882891E1FB6C966D2754F4AD22F780D5A2E3CC839BBD4B623
SHA-512:	4D50AE6F7E60A2E107D0805D4793578DBB2FCA37AA03E92035CCA62EE9279E82D8A2C795DCD8E080B5FF35CE1640DA544D02B97E56FA215F3A9F2D0C007EBA E7
Malicious:	false

Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1674943917.543097,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1643407917.543102}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ea5aef07-dd87-4f20-b0ca-095724a3aeb0.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):	5449
Entropy (8bit):	5.008291247170403
Encrypted:	false
SSDEEP:	96:nSpCm/VZ9pcKI+Zfok0JCKL8jkq7S1UkqyCkbOTQVuwn:nSpCw9pcP4KMkb2kXv
MD5:	0FDC80B82A011B07742D663D12D3E07E
SHA1:	BE49BEC75739EC1B7DDCAA440FCEE5566C436371
SHA-256:	327C4F52302408F82DEF43D19CFE7420A11CE8FE5A55FD495B896EAF68FA1C22
SHA-512:	3221DF66DB6BE69E6F5AA2026AD2E0BD644081B36F44A43AFBCC54C98C4FE990B5AEB215E007B534A5CA7944D277A1B1DBF7637E4424B8D6633DD04B20B0B509
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287881484970204","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\f6a3fa6a-4330-4db7-9f19-26202fda87a1.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):	5199
Entropy (8bit):	4.983975138690969
Encrypted:	false
SSDEEP:	96:nSpCi5Z9pcKI+Z7ok0JCKL8jkq7S1gbOTQVuwn:nSpC09pc74KMkbw
MD5:	DF6B302E8C5317F711A9537E955B0D25
SHA1:	2206C9CBAD38B552455AFE4440ACEA9A2EE08C6C
SHA-256:	5A3851DCB3DCED98320AD5AE987D49C6EDED0C1EBF1FF298370A1450971D4EFF
SHA-512:	39155EA6AA408A4BCBBBFA2594B05D6250DA7A85376BA989056642BC8EEE586E86FEE11C1F1D6952BEEFDF2EF7229AB717ADBC975DA7D0F1333AD70ED4C27013
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287881484970204","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\f72c4cd4-8ef2-4cbd-8ce2-c6de2c8d7e2a.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):	3646
Entropy (8bit):	4.918201110513153
Encrypted:	false
SSDEEP:	96:JTOCXGDHazc6PbYrc9GH9d1EP6V68+GJGvGGGjmGD/H:JTOCXGDHazc60Y929dKP6V68+G8dv4P
MD5:	3BCA827722998DFBD9CD3EC485C4FFA5
SHA1:	60DACBDCEDBE007C629F097422A4BFED841141EF
SHA-256:	7EE06F931EB45541C6180278A360A3A593E45344D11B41BE090848D856BC38E5
SHA-512:	58C8753953435C235814E58030D0A85CE7C16227BFA12DC8DF0C9BA08BE1A1C146ADAA799D51A45ABCB70D021435F9E29EDD287D2F0C02253F5F65FFDE83684
Malicious:	false
Reputation:	low

Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://www.gstatic.com","supports_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.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13290473486557415","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13290473486580191","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f794f48d-9b99-4760-917b-7d6c7b9983fd.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):	538
Entropy (8bit):	5.516405248088698
Encrypted:	false
SSDEEP:	12:Y6uE9RAJ9+UAnIlmrFDMpL/fN+UAnIM2+pVnJN+UAnIsQ:YfE9RAeUXrfwUYwUmQ
MD5:	E0853AE21EE0DEE0EE1733B4D0DAB9C4
SHA1:	D12A728B0F0D0DF558A5E178A47FA1DD4B6788EA
SHA-256:	51775CF28202A5D178D474B2AD7A1E0E2EA6CB20C107A06533068614FF0820CE
SHA-512:	5B84F327B8488E361EB726D6A375F484628627326DECA1362A9435370F718A9CFC17D75BBCFE919D66C901D93576AB337770291B5758B553E5C1DEF32D958D29
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1674943957.776858,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1643407957.776863},{"expiry":1654294363.232731,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1643407963.232737},{"expiry":1643429564.084646,"host":"vzIWPxw7WTrYM5jSfFZaHars8cPVKgsDJJdvfJQVB6o=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1643407964.084651}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\fff4c294-8b77-40ed-af53-5562882e1b5c.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):	5199
Entropy (8bit):	4.983968531049477
Encrypted:	false
SSDEEP:	96:nSpCi5Z9pcKI+ZGok0JCKL8jkq7S1gbOTQVuwn:nSpC09pco4KMkbw
MD5:	351BD8EB0E2CE757F80C948F0BBB3A9E
SHA1:	9AC60DE8931838258C1E389B531FA6B3AE3D7784
SHA-256:	6871509726ED8EF662C7E2E3FEB375A5A54593C6AFD22D13402DF8EB32047F68
SHA-512:	42874190DFCE61065F86E8307B14F324B136D5A42B4F01F6DD8D0BE2E70014510DFB03DB5BBD490CFB954CF90F785C698842B04563969E59B29EDCDC90915C3
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287881484970204","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","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

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:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
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):	190176
Entropy (8bit):	6.045182753980272
Encrypted:	false
SSDEEP:	3072:judk+l20ee3L2oVJhynrpnbtpQVzg4d8qkwMc0YXFcbXafIB0u1GOJmA3iuRU:E9407dorBtGzg4Kqkjc0maqfIlUOoSiZ
MD5:	66989F922CEC0DC0F6F1F3E0DAEE6BA5
SHA1:	28B4A68FCD8A9547D389676ADDC2156B8D497126
SHA-256:	B26316E240F317EFFE6F0471C4C85A235B1A4DCFF8DEAECAA00A907B150389E1
SHA-512:	4A7E72B2A22F77A68EF8B72D33CFB0EEFC8000964AA9D7FB9CB094D4077B5E3A16D2DF9DA6385A16869BE7F7C9EB0149B1005CEA11408D7D78D547CA23623215
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":1.643407886424815e+12,"network":1.643375488e+12,"ticks":133402309.0,"uncertainty":3943022.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799438436"},"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):	198652
Entropy (8bit):	6.074121439148103
Encrypted:	false
SSDEEP:	6144:/R9407dorBtGzg4Kqkjc0maqfIlUOoSiuRU:/krHG5WjZo3
MD5:	C102A2251168308202B97590CA58C192
SHA1:	7FC180D3333F846F226C0DAADBB2560FCA0FBE96
SHA-256:	DE1D5141808AC959F2D94B0A86CDF205F691CE3C3B36381DCB1E11AD81C3F5BC
SHA-512:	6E43C41D977D4A9BCAA7ADA8685E42AE3988B4811E168940456678BB94045FCC5B1BE3223AFAC1D8B083E2A254D4E0CD554FBC19ED4DEFCFE4F4BAEE07407B9A
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":1.643407886424815e+12,"network":1.643375488e+12,"ticks":133402309.0,"uncertainty":3943022.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799438436"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local 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):	198651
Entropy (8bit):	6.074121683065808
Encrypted:	false
SSDEEP:	6144:2X9407dorBtGzg4Kqkjc0maqfIlUOoSiuRU:2yrHG5WjZo3
MD5:	6273EEDE77D6C1FB1025B0AA512FFEF0
SHA1:	C841FE43813D5F8C6B20BF4FCF11D8F0D4F0FEC0
SHA-256:	9EF4FCFC8E7814100F8335E37A63005A3358C09A81276F081460FF24EA5299A0
SHA-512:	63CF89B2913BB2E93C71DF65632DE1246F9BCFCBD1B4A285A101C854CA4BF126BE7BE0AD5E24D3380FFD5AAD5DF92233DB14897CBDDD8F45F587A86ED8054B70
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":1.643407886424815e+12,"network":1.643375488e+12,"ticks":133402309.0,"uncertainty":3943022.0}},"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\Module Info Cache (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.743904116578142
Encrypted:	false
SSDEEP:	384:lLwPjByMJGp1V+kzqNbrAv393g/FAHZ4GM7rGRHzxAFlF0rOHmOaoSdD3jYOtdXr:5+KF1u5g8AeP7p5EnbqhKHZz1p
MD5:	57AC1975B62CE04929A97C1FD025D761
SHA1:	AD60621644C42F87F48E77603EDD26265002393B
SHA-256:	792C7E95BE4BE8623E5BF1EC322AF3ECE6FF9E4582C66A763FE51F5313217BF3
SHA-512:	9ED82C7D5053BE7C5F50C4A15A5E3CF64396903B7AFD069BB8F36A66173CA3F1B26FA41D65ECE2C0BAE81B6D2936849B50802515BA0EA0BEE2304949C518933B
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...FR8.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 CacheFD (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.743845978501557
Encrypted:	false
SSDEEP:	384:jLwPjByMFpuzqNbrAv393g/FAHZ4GM7rGRHzxAFlF0rOHmO5SdD3jYOtdXNy1b6H:sKF1u508AeP7p5EnbqhKHZz1x
MD5:	CCE5DF598D723D101FC17B7C1F606215
SHA1:	38A6E8BDF84D6D067E2FB64CE3A6FA304EA55B31
SHA-256:	321DCC9E71BA8F4457F606251D93BA75BC9F9C6F2D7DC908837A27C31604B5F9
SHA-512:	362702E1C50B525FE9C16465C5041278035045436A3760A2826496B7C522366AC50BA6648036F91220EA92A231A7995A4CDFA771217D1E6EB9D5A3DDD9D6565B
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...FR8.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\Subresource Filter\Indexed Rules\27\scoped_dir6760_955344158\Ruleset Data

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	142128
Entropy (8bit):	4.846664953094921
Encrypted:	false
SSDEEP:	3072:kYotddpTo2daWZy+CSzpjNTSha0NyruDcG4JCNDKR:kYoR+QNyYuDIL
MD5:	580DB025FA9444FBD3D00A0B7F4AEEE6
SHA1:	26BA225F9E58BA440E455B151AFA62E6DA71D052
SHA-256:	4DF7686CE689C87AE5AC45DE42E602ADB0AC316EE7C9F55717DEAD2509058ECC
SHA-512:	5940A7BA74606EC99BC366B42C47F32A89B11A6D1DF164C34BDE87241BE971BE81BC2762A6EACB5F58264573D1EDE7D233097D4A4CE6CBC033FA8B6507BE9D 9E
Malicious:	false
Reputation:	low
Preview:	.....$T..... ...X...l...h...d...0.....X...T...P...L...H.....@...<.....4...0.....\|...`...D..... ..... /.....ozama.....8/.....g.bat..... P/.....onwod.....h...h/.....ennab.....P..../.....nozam.....d..../.....geips...../.....rekoj...../.....lgoog.....@..../.....uotpo...../.....lreko.....H.../.....lR..... ...@R..$R...R...Q...Q...HR...Q..@R..<R..8R..4R...Q...R..(R..$R.. R...R..TQ...R...R..0Q...R...Q...R...P...Q...Q...P...Q...Q...Q...Q...Q...Q...P...Q..xP...Q...Q...Q..PP...Q...Q...Q... Q...Q...Q...Q...Q...Q...Q...Q...Q...P...O..\|Q..xQ..tQ..pQ..lQ..hQ..dQ..`Q..\Q...O..TQ...O..hO..HQ..DQ..@Q..@O..8Q..4Q..0Q..,Q..(Q..$Q.. Q...Q...Q...Q...Q...Q...Q...Q. ..Q...P...P...N...P...N...P...P...P...P...P...P...P...N..lN..PN...P...P...P...P...P...N...P...P...P...P...M...P...M...P...P...P..|P..xP..tP..pP..lP..hP..dP..`P..\P..XP..TP..PP..xM..HP..

C:\Users\user\AppData\Local\Google\Chrome\User Data\b19ff24c-8248-4f7d-9b7e-4ba4083bdb7a.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.743904116578142
Encrypted:	false
SSDEEP:	384:lLwPjByMJGp1V+kzqNbrAv393g/FAHZ4GM7rGRHzxAFlF0rOHmOaoSdD3jYOtdXr:5+KF1u5g8AeP7p5EnbqhKHZz1p
MD5:	57AC1975B62CE04929A97C1FD025D761
SHA1:	AD60621644C42F87F48E77603EDD26265002393B
SHA-256:	792C7E95BE4BE8623E5BF1EC322AF3ECE6FF9E4582C66A763FE51F5313217BF3
SHA-512:	9ED82C7D5053BE7C5F50C4A15A5E3CF64396903B7AFD069BB8F36A66173CA3F1B26FA41D65ECE2C0BAE81B6D2936849B50802515BA0EA0BEE2304949C518933 B
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...FR8.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\b823aa69-7386-4624-96fd-ce18c21d93a1.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):	190176
Entropy (8bit):	6.045181737579228
Encrypted:	false
SSDEEP:	3072:4Gdk+l20ee3L2oVJhynrpnbtpQVzg4d8qkwMc0YXFcbXafIB0u1GOJmA3iuRU:59407dorBtGzg4Kqkjc0maqfIlUOoSiZ
MD5:	3B0CB295B5A959BC433FA1C9582A562D
SHA1:	D1F34BEA125BE1BDD9A2F646A71AA38285616F7B
SHA-256:	AD42428AEDE70BEB752E39061FCD73C8214C1C211649AC6EACC565C6A4D2A083
SHA-512:	A1FAD431CCF9F0C967CD1114C9A499BDE0E5B508657C0553F2AA7397FA2DD7660FAF7DED58E5DD3C1D81128B93F48A31304400FE8FB710E84B1DAEEA031CA D3
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":1.643407886424815e+12,"network":1.643375488e+12,"ticks":133402309.0,"uncertainty":3943022.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799438436"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\b8925bb9-576f-423b-95fc-f4026e75719d.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97400
Entropy (8bit):	3.744309244980348
Encrypted:	false
SSDEEP:	384:oLwPjByMyCGp1V+kzqNbrAv393g/FAHZ4GM7rGRHp8xAFlF0rOHmOaoSdD3jYOtH:g+KF1uag8AePG5p5EnbqhKHZz1y
MD5:	116948FFDFB7D5F00C96C252FD8A1865
SHA1:	A4CA08716617185FAE10A972CCB3B4B16410DFFB
SHA-256:	0F18E009E37681966ACC84EA2BDE781C96E7D773619E41D2C0FAC3F28868A2C4
SHA-512:	4087E159664A44EB7B1200F26FE4C3DFF3C0581224B4606DDE5000B2B549B407F4117E6716F869D77624149BE941F743297E134D9AEC6F60A4D976DEB0A6C29C
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...FR8.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\e8c50bd3-7fa5-419b-87bd-69d770545d74.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):	198652
Entropy (8bit):	6.074121439148103
Encrypted:	false
SSDEEP:	6144:/R9407dorBtGzg4Kqkjc0maqfIlUOoSiuRU:/krHG5WjZo3
MD5:	C102A2251168308202B97590CA58C192
SHA1:	7FC180D3333F846F226C0DAADBB2560FCA0FBE96
SHA-256:	DE1D5141808AC959F2D94B0A86CDF205F691CE3C3B36381DCB1E11AD81C3F5BC
SHA-512:	6E43C41D977D4A9BCAA7ADA8685E42AE3988B4811E168940456678BB94045FCC5B1BE3223AFAC1D8B083E2A254D4E0CD554FBC19ED4DEFCFE4F4BAEE07407B9A
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":1.643407886424815e+12,"network":1.643375488e+12,"ticks":133402309.0,"uncertainty":3943022.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799438436"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\fc7b8661-0df4-466c-99b7-a87255d2838d.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):	198651
Entropy (8bit):	6.074121683065808
Encrypted:	false
SSDEEP:	6144:2X9407dorBtGzg4Kqkjc0maqfIlUOoSiuRU:2yrHG5WjZo3
MD5:	6273EEDE77D6C1FB1025B0AA512FFEF0
SHA1:	C841FE43813D5F8C6B20BF4FCF11D8F0D4F0FEC0
SHA-256:	9EF4FCFC8E7814100F8335E37A63005A3358C09A81276F081460FF24EA5299A0

SHA-512:	63CF89B2913BB2E93C71DF65632DE1246F9BCFCBD1B4A285A101C854CA4BF126BE7BE0AD5E24D3380FFD5AAD5DF92233DB14897CBDDD8F45F587A86ED8054B70
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":1.643407886424815e+12,"network":1.643375488e+12,"ticks":133402309.0,"uncertainty":3943022.0}},"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\Temp\4b36dbfb-df43-4f34-b401-572980654fc8.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\4d8ebc1e-4be5-4e4f-81b3-8aa89597a059.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:cK2ED9l48seur0/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\6760_1431660835\Filtering Rules

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	91283
Entropy (8bit):	5.445591581715125
Encrypted:	false
SSDEEP:	1536:FOONphT5b05W9w2ZH3HhahaHVFzIFSXkRrw8p1:HNNb0mwY3hpHVZIsX0d1
MD5:	492D833A4DACDC2843C7E1835DE22679
SHA1:	50461C265B3FF063690DFD7B5FDF742BA06DE36D
SHA-256:	081284C6EB49939EA138A836CD347C212E130266A4E0FAF3A5DF7C01F9F27E21
SHA-512:	9D82234FE1662226B348762028F7C2C9F0D36ACA06F758938ECE4F6D025FFCAA2FEC5D7A01E75B2156F914A7095E67EE3277B82DBF71445229121E4BBE779D13
Malicious:	false

Reputation:	low
Preview:	.....o0.8.@.R.-728x90.....o0.8.@.R.adtdp.com^.....o*...epaper.timesgroup.com*...nbcsports.com*...windalert.com*...kowb1290.com*...k2radio.com*...vimeo.com*.. .koel.com*...uefa.com0.8.@.R#googletagservices.com/tag/js/gpt.js.....o0.8.@.R./ad-inserter/.9.....o*...adcore.com.au..*...adcore.ch..0.8.@.R./adcore_.....o0.8.@.R. uwoaptee.com^.....o0.8.@.R._468_60..8.....o0.8.@.R)bancodevenezuela.com/imagenes/publicidad/.....o0.8.@.R..adbutler-.....o0.8.@.R.adrecover.com^.>.... ..o*...google.com0.8.@.R!developers.google.com/google-ads/.-.....o*...vk.com0.8.@.R.vk.me/css/al/ads.css.+.....o0.8.@.R.mysmth.net/nForum/*/ADAgent_.....o0 .8.@.R.indoleads.com^.%.....0.8.@.R.discordapp.com/banners/.D.....o*...daum.net0.8.@.R)daumcdn.net/adfit/static/ad-native.min.js.'.....o0.8.@.R.looker.com/ap i/internal/.".....o0.8.@.R.broadstreetads.com^.....o0.8.@.R./banner.cgi?.....o*...thefreedictionary.com*...downloads.codefi.re*...windows7themes.net*...smallseoto ols.com*..

C:\Users\user\AppData\Local\Temp\6760_1431660835\LICENSE.txt

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	24623
Entropy (8bit):	4.588307081140814
Encrypted:	false
SSDEEP:	384:mva5sf5dXrCN7tnBxpxkepTqzazijFgZk231Py9zD6WApYbm0:mvagXreRnTqzazWgj0v6XqD
MD5:	D33AAA5246E1CE0A94FA15BA0C407AE2
SHA1:	11D197ACB61361657D638154A9416DC3249EC9FB
SHA-256:	1D4FF95CE9C6E21FE4A4FF3B41E7A0DF88638DD449D909A7B46974D3DFAB7311
SHA-512:	98B1B12FF0991FD7A5612141F83F69B86BC5A89DD62FC472EE5971817B7BBB612A034C746C2D81AE58FDF6873129256A89AA8BB7456022246DC4515BAAE2454E
Malicious:	false
Reputation:	low
Preview:	EasyList Repository Licences.... Unless otherwise noted, the contents of the EasyList repository.. (https://github.com/easylist) is dual licensed under the GNU General.. Public License version 3 of the License, or (at your option) any later.. version, and Creative Commons Attribution-ShareAlike 3.0 Unported, or.. (at your option) any later version. You may use and/or modify the files.. as permitted by either licence; if required, "The EasyList authors.. (https://easylist.to/)" should be attributed as the source of the.. material. All relevant licence files are included in the repository..... Please be aware that files hosted externally and referenced in the.. repository, including but not limited to subscriptions other than.. EasyList, EasyPrivacy, EasyList Germany and EasyList Italy, may be.. available under other conditions; permission must be granted by the.. respective copyright holders to authorise the use of their material.....Creative Commons Attribut

C:\Users\user\AppData\Local\Temp\6760_1431660835_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):	1529
Entropy (8bit):	5.987722096297769
Encrypted:	false
SSDEEP:	24:pZRj/flTHYXKl0kYbKNzjeT3qzkaoXqyCUV0szeMXmx0eoXECqG3l0+3pGX8fpaj:p/h4X8ybKNOTqkak1CSyxtkJl00AXN
MD5:	531658FD4A53DCAA6706C4E299F7F321
SHA1:	30E6E2BBF0C17CDED7D479A14E96468B94B647C3
SHA-256:	99CFEEE3A649590AB00880AFF978CB3E9BE65302AE2CD60B134387D606F1C79A
SHA-512:	727967425E95B297071B293CE9E18A4F9D4851819E93EFE1D8670DED887270ADCC9BECA280687E1DCD3AA6EDCFDDBE61A7074B92CEC95656CB2BC5DD995F9 BF5
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiO lt7InBhdGgiOiJGaWx0ZXJpbmcgUnVsZXMiLCJyb290X2hhc2giOiJGb0toZEFTUTJiTGp4Mm9lODhqNnBVTTR4VF9aVDYwVWRvNGFvMEdQRW1rln0seyJwYXRoIoiTEl DRU5TRS50eHQiLCJyb290X2hhc2giOiIyaWswNmk0TFlCdVNHNWphRGFIS253NE9pdnVSRzZsQ0JKMVk0TGtzRFJJln0seyJwYXRoIjoibWFuaWZlc3QuanNvbiIsInJvb 3RfaGFzaCI6IlhZRXVyY2cyNUN3eVpKSmpVbDk4LWlfaEUtbkMwRTVEYnU0Yl81Zm5FMWsifV0sImZvcm1hdCI6InRyZWVoYXNoIiwiaGFzaF9ibG9ja19zaXplIjo0MDk 2fV0sIml0ZW1faWQiOiJnY21qa21nZGxnbmtrY29jbW9laW1pbmFpam1tam5paSIsIml0ZW1fdmVyc2lvbiI6IjkuMzIuMCIsInByb3RvY29sX3ZlcnNpb24iOjF9","signatures": [{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"yR3CR9-1WdhFXwIas-furfbkFjIT_vSCGmIc0g-d4snFbxb2ANfYiEM-CW7ZAilSpXLZEiY UxhrhtU6C-NbLrEfhyRxanHjYONy4YkWjp_VmS8dnZ1PAxC5KhmIOQoHRA4G4979n-OrSkHNubBTVntbKAdPl9YK0Wb6QBLBX_IFcvew8SKs2bhxb2SEf9PN AbM36eMVRZhTf6R7MfjxR-heObZwJJTnsgiqhOlldNjehhH2Pl

C:\Users\user\AppData\Local\Temp\6760_1431660835\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):	3.9462477267061056
Encrypted:	false
SSDEEP:	3:SxEQdYTVAUTVzDD4XScWGcY2R+Ql:SxElYxAobaSnOQl
MD5:	665E5819FD3845C8CF669B0FC7C35244
SHA1:	C807724385F53E2B2410E269CAEEA719ABB03F76
SHA-256:	317A5B0177F17156279688F1FEF1D2568AAEB975239BB48702C76E2C4EFCC050

SHA-512:	19820AC3AC8FE1615AC15804EC7F735F932A957C2CCE690145240D74686DCEF87A91B2F918291525E386EBD1FE50BD31E4A1DC9E1EE0DFDB6D690523B97FA03
Malicious:	false
Reputation:	low
Preview:	1.dbbba5869c1d8946e5e23215c0404619fe82793d60eb89489b345ef55023e077

C:\Users\user\AppData\Local\Temp\6760_1431660835\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	115
Entropy (8bit):	4.545910352797257
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFHXG7LGMdv5HcDKhtUJKS17vC:F6VlMZWuMt5SKPS1rC
MD5:	B0E35F2BE526F795B810BE0E88B72358
SHA1:	0C7CB5B9E7AF8DE8ABB306CFB722994820656A1A
SHA-256:	5D812EADC836E42C32649263525F7CFA2FE113E9C2D04E436EEE1BFF97E71359
SHA-512:	6C35C45F3524824DD5B2D9A571B36687E3CEE375723F5467FCE2BB9F743D88D16D9F07015772AD8736725EA5F6C3366F1671505FCA18B0CE3EB6EC21B0FC41A
Malicious:	false
Reputation:	low
Preview:	{. "manifest_version": 2,. "name": "Subresource Filtering Rules",. "ruleset_format": 1,. "version": "9.32.0".}.

C:\Users\user\AppData\Local\Temp\7317be36-9f82-462f-8ffd-03d633714428.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\d181d15e-928c-4b6e-a63d-3ea1a806682e.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..$.J....+M!.Hz.n`U.I)N.\|b.I....{.K@]6.LlP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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_dir6760_1072695678\4d8ebc1e-4be5-4e4f-81b3-8aa89597a059.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\scoped_dir6760_1072695678\CRX_INSTALL_locales\am\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17307
Entropy (8bit):	5.461848619761356
Encrypted:	false
SSDEEP:	384:arfbEVrFvMP4rMhuDopC3vUuFBYZV6uml:aHEVrFvMP4KuFvr6D6uml
MD5:	26330929DF0ED4E86F06C00C03F07CE3
SHA1:	478F3B7E7A7E007BEE182B89C2EF6FFE6045E92C
SHA-256:	621B5139ED199022BB6529AF18ED4DC312AE9F3E90ECAF3B2C9E1D12114F5B22
SHA-512:	0BE6183A1BF12575C0F99960705D4249E79CDB8528C55FF132BE99A111F09494231AD6A36CD61B090A3B34C6971D68A29373BA346888E852C52E05DC14380682
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "1282768764603190 75": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": ".... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "... ...".. },.. "180276274658945717 7": {.. "message": "...".. },.. "1850397500312020388": {.. "message": ".$START_LINK$Google Home .....END_LINK ... . Chromecast ....? $START_SPAN$*END_SPAN",.. "placeholde

C:\Users\user\AppData\Local\Temp\scoped_dir6760_1072695678\CRX_INSTALL_locales\ar\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16809
Entropy (8bit):	5.458147730761559
Encrypted:	false
SSDEEP:	192:0IprKC78JmUjk8RkeryFOYPATxLZ8fsbE3/IFV6c8TEKdl:Jrp8JjA8RkerK0lc3wFV6uml
MD5:	44325A88063573A4C77F6EF943B0FC3E
SHA1:	78908D766F3E7A0E4545E7BD823C8ED47C7164EB
SHA-256:	67A439A08804EF4BEF261BDBADD8F0FEFD51729167D01EDCA99DD4AF57D6108B
SHA-512:	889C02BC986794C58C76022E78F57F867DD1D5217687F12D679A33A2DB9E5A18F3A37CF94D8FE4585E747C78E4662EAB93361FF7D945990774C7CFCACCFB79D
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "....".. },.. "1213957982723875920": {.. "message": ".. .. ..".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "...".. },.. "1636686747687494376": {.. "message": "......".. },.. "1802762746589457177": {.. "message": "..... .....".. },.. "1850397500312020388": {.. "message": "... .... Chromecast .. $START_LINK$..... Google HomeEND_LINK. $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6760_1072695678\CRX_INSTALL_locales\bg\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18086
Entropy (8bit):	5.408731329060678
Encrypted:	false
SSDEEP:	192:4jjpr342SIwPIasR9VhMkACVmrv8evj+3eXivOMbb2vVzCkwRV6V6c8TEKdl:4ZrYo+rxT+qOV6V6uml
MD5:	6911CE87E8C47223F33BEF9488272E40
SHA1:	980398F076BB7D451B18D7FDE2DE09041B1F55AD
SHA-256:	273DEF0F67F0FA080802B85EF6F334DE50A19408F46BDF41F0F099B1F5501EEA
SHA-512:	CDB69405BB553E46DCF02F71B1A394307D0051E7FA662DFFEBA7888F30DD933F13C7FD6E32F1D7AEAEE8746316873B6E1D92029724ABDC75E49DCC092172EA22
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "......".. },.. "1213957982723875920": {.. "message": ".. .. ..-..... ....?".. },.. "12827687 6460319075": {.. "message": "..... .. ..".. },.. "1428448869078126731": {.. "message": "..... .. ..".. },.. "1522140683318860351": {.. "message": "..... .. .., ...".. },.. "1550904064710828958": {.. "message": "......".. },.. "1636686747687494376": {.. "message": "......".. },.. "18027627 46589457177": {.. "message": ".... .. ..".. },.. "1850397500312020388": {.. "message": "..... .. .. Chromecast . $START_LINK$..... Google Hom eEND_LINK? $START_SPAN$*END_SPAN",.. "p

C:\Users\user\AppData\Local\Temp\scoped_dir6760_1072695678\CRX_INSTALL_locales\bn\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19695
Entropy (8bit):	5.315564774032776
Encrypted:	false
SSDEEP:	384:PrUCrcTIOeswIW/Vre/sZn8TFfzheV6uml:lPswIWtoK8xfG6uml
MD5:	F9DDF525C07251282A3BFFCEE9A09ABB
SHA1:	A343A078E804AF400A8F3E1891E3390DA754A5CD
SHA-256:	C69C6C90F7EB8F10685CD815AF1F6F1B87CF30C4E8D95DF1D577DE1105AAD227
SHA-512:	EBD339C37162984672513019D470B92DF8B743DD69D4430361EF12D42FD1C208DBDE818A7BFE20BE8A7D63CD6E02B3F4344DEA1C4AEDB8719D789981A49DA4C
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".... ...".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128 276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... ....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": "......".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "$START_LINK$ Google

C:\Users\user\AppData\Local\Temp\scoped_dir6760_1072695678\CRX_INSTALL_locales\ca\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15518
Entropy (8bit):	5.242542310885
Encrypted:	false
SSDEEP:	384:drGUBKxMF2ayv8FrIccUVFmwf+7d9VKS3V6uml:dCUBKxMFBy0FE3UzmQ+zkSl6uml
MD5:	A90CF7930E7C3BEC61EE252DEFAD574A
SHA1:	F630CA01114A7BDD39607CB84B8280CCE218A5C6
SHA-256:	A533740E17559E2ADF40B4555C60F21EEC84E92C09CDBC19EED033A0B4DD2474
SHA-512:	598F991B344FA6724617D6CE57BB0D6D64EF86B4F5317BF6AD5EDF43E6B0A385094E7885F7A8FA2B107405B31C3D9F76E92315BC1D9BB52ACD4ECAD342917DE1
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Es congela".. },.. "1213957982723875920": {.. "message": "Quina de les opcions.seg.ents descriu millor la vostra xarxa?".. },.. "128276876460319075": {.. "message": "Detecci. de dispositius".. },.. "1428448869078126731": {.. "message": "Flu.desa del v.deo".. },.. "1522140683318860351": {.. "message": "S'ha produ.t un error en la connexi.. Torneu-ho a provar.".. },.. "1550904064710828958": {.. "message": "Correcta".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volum".. },.. "1850397500312020388": {.. "message": "Pots veure el Chromecast a l'$START_LINK$aplicaci. Google.HomeEND_LINK?$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "

C:\Users\user\AppData\Local\Temp\scoped_dir6760_1072695678\CRX_INSTALL_locales\cs\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15552
Entropy (8bit):	5.406413558584244
Encrypted:	false
SSDEEP:	192:eVdprJrG5efiTk93ebrxZR1fdc8VDCwT9fTV6c8TEKdl:2rMqiQerxQ88W7V6uml
MD5:	17E753EE877FDED25886D5F7925CA652
SHA1:	8E4EC969777CC0CEB7C12D0C1B9D87EBBB9C4678
SHA-256:	C562FCCFCE374D446BFAC30AC9B18FF17E7A3EF101C919FF857104917F300382
SHA-512:	33D61F6327FC81D7A45AA2CC97922DC527F5F43E54AA1A1638DA6EE407024A2F10CFD82CC5C3C581C2E7B216276987CB26C3FA95198572E139ACF29CC5B7AD B
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Video zamrz.".. },.. "1213957982723875920": {.. "message": "Kter. popis nejl.pe vystihuje va.i s..?".. },.. "128276876460319075": {.. "message": "Zji..ov.n. za..zen.".. },.. "1428448869078126731": {.. "message": "Plynulost videa".. },.. "1522140683318860351": {.. "message": "P.ipojen. se nezda.ilo. Zkuste to pros.m znovu.".. },.. "1550904064710828958": {.. "message": "Plynul.".. },.. "1636686747687494376": {.. "message": "Perfektn.".. },.. "1802762746589457177": {.. "message": "Hlasitost".. },.. "1850397500312020388": {.. "message": "Vid.te sv.j Chromecast v.$START_LINK$aplikaci Google Home END_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir6760_1072695678\CRX_INSTALL_locales\da\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15340
Entropy (8bit):	5.2479291792849105
Encrypted:	false
SSDEEP:	192:+Upr8XnI1MY2kPuir8j7Rd3kbTWc4QtV6c8TEKdl:FrJ1H9br8h6eZCV6uml
MD5:	F08A313C78454109B629B37521959B33
SHA1:	3D585D52EC8B4399F66D4BE88CED10F4A034FCCC
SHA-256:	23BF7E5EDF70291CA6D8F4A64788C5B86379EECB628E3DFA7DD83344612F7564
SHA-512:	9F2868AEBBF7F6167A7EA120FE65E752F9A65D1DC51072AA2413B2FDE374DA2D169D455A4788E341717F694179E6F1FA80413C080D9CD8CB397C3E84668CBFE C
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Fryser".. },.. "1213957982723875920": {.. "message": "Hvilket af f.lgende udsagn beskriver bedst dit netv.rk?".. },.. "128276876460319075": {.. "message": "Enhedsregistrering".. },.. "1428448869078126731": {.. "message": "Videostabilitet".. },.. "1522140683318860351": {.. "message": "Forbindelsen blev afbrudt. Pr.v igen.".. },.. "1550904064710828958": {.. "message": "Problemfri".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lydstyrke".. },.. "1850397500312020388": {.. "message": "Kan du se din Chromecast i $START_LINK$ Google Home-appenEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "STAR

C:\Users\user\AppData\Local\Temp\scoped_dir6760_1072695678\CRX_INSTALL_locales\de\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15555
Entropy (8bit):	5.258022363187752
Encrypted:	false
SSDEEP:	192:AJprM71A4qyJSwlk5KR5rtXsmvL0xhVw921YV6c8TEKdl:2re3jJS5A5rt8msA2KV6uml
MD5:	980FB419ED6ED94AD75686AFFB4E4C2E
SHA1:	871BFBCA6BCBA9197811883A93C50C0716562D57
SHA-256:	585C7814AFD2453232BC940252D4AE821D6E6CBCFD74A793F78E5DB8BA5342F1
SHA-512:	1681FA9C3BA882250A5005FB807D759EB8A634F1AA011725B1C865C0028BE7AB7BC16DC821A7F5BBFBA84C91E7D663ADE715284798E7E84E8FFF2D254488882 D
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "H.ngenbleiben".. },.. "1213957982723875920": {.. "message": "Welche dieser Aussagen beschreibt dein Netzwerk am besten?".. },.. "128276876460319075": {.. "message": "Ger.teerkennung".. },.. "1428448869078126731": {.. "message": "Videowiedergabequalit.t".. },.. "1522140683318860351": {.. "message": "Fehler beim Herstellen der Verbindung. Bitte versuche es noch einmal.".. },.. "1550904064710828958": {.. "message": "St.rungsfrei".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lautst.rke".. },.. "18503975003 12020388": {.. "message": "Siehst du deinen Chromecast in der $START_LINK$Google Home AppEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.

C:\Users\user\AppData\Local\Temp\scoped_dir6760_1072695678\CRX_INSTALL_locales\el\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17941
Entropy (8bit):	5.465343004010711
Encrypted:	false
SSDEEP:	384:S0rDuhLh41cZrP3TzDBknbpgo6djlV6uml:S0fuBh46ZD3TzDinbpgoUK6uml
MD5:	40EB778339005A24FF9DA775D56E02B7
SHA1:	B00561CC7020F7FE717B5F692884253C689A7C61
SHA-256:	F56BF7C171AA20038EE30B754478B69A98F3014C89362779B0A8788C7B9BEEE1
SHA-512:	8BED281A33EC1E4E88A9F9D62BB13FE0266C0FAF8856D1DC2A843D26DD3CE5E7D1400FD3325ABD783B0364EC4FB1188AD941D56AEB9073BC365BE0D12DE6C013
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "......".. },.. "1213957982723875920": {.. "message": ".... ... .;".. },.. "1282768 76460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... .. ..".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": { .. "message": "..... ....".. },.. "1850397500312020388": {.. "message": "..... .. .. Chromecast .... $START_LINK$..... Google HomeEND_LINK; $ START_SPAN$*$END_SPAN$",.. "placeholders": {.. "END_LINK": {.. "content

C:\Users\user\AppData\Local\Temp\scoped_dir6760_1072695678\CRX_INSTALL_locales\en\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	14897
Entropy (8bit):	5.197356586852831
Encrypted:	false
SSDEEP:	96:2MKUOp5N7GTNMRuv6M0bIt3FXGkW6/5NkkQ9NJKJhnH3t9F410sUA+ISN6cGDSyR:VKzprogudTGkWqrKcJhdIR+V6c8TEKdl
MD5:	8351AF4EA9BDD9C09019BC85D25B0016
SHA1:	F6EC1FFD291C8632758E01C9EE837B1AD18D4DCF
SHA-256:	F41C82D8A4F0E9B645656D630C882BE94A0FB7F8CEC0FE864B57298F0312B212
SHA-512:	75672B57F21F38F97341AD76A199AD764E9FBAB2384D701BF6EB06CEFDE6C4F20F047F9051A4E30D99621E5C1FBBDB9E38E8D2B47470806704B38DA130A146CF
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Freezes".. },.. "1213957982723875920": {.. "message": "Which of the following best describes your network?".. },.. "128276876460319075": {.. "message": "Device Discovery".. },.. "1428448869078126731": {.. "message": "Video Smoothness".. },.. "1522140683318860 351": {.. "message": "Connection failed. Please try again.".. },.. "1550904064710828958": {.. "message": "Smooth".. },.. "1636686747687494376": {.. "message": "Perfect".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Are you able to see your Chrom ecast in the $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "START

C:\Users\user\AppData\Local\Temp\scoped_dir6760_1072695678\CRX_INSTALL_locales\es\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15560
Entropy (8bit):	5.236752363299121
Encrypted:	false
SSDEEP:	192:NAgprfy1pTCukFr+1DIyDRoanvV6c8TEKdl:KMrq6FrmvV6uml
MD5:	8A70C18BB1090AA4D500DE9E8E4A00EF
SHA1:	8AFC097FA956C1317DB0835348B2DA19F0789669
SHA-256:	FF173D1CEF665B1234E02F11070ABD2B65230318150734579A03C7F31B4AE3F4
SHA-512:	140BAF40A4ABE9B8AF0855B0EBB7DFDF17869EDFC4EE1037C5EA7FDD8EDEBD4850E055B6A4D7B8782657618BCE1517813779BA01BA993CC838BB43E0BE71EEEE
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Congelaci.n de im.genes".. },.. "1213957982723875920": {.. "message": ".Cu.l de las siguientes respuestas descr ibe mejor tu red?".. },.. "128276876460319075": {.. "message": "Detecci.n de dispositivo".. },.. "1428448869078126731": {.. "message": "Fluidez del v.deo".. },.. "1522140683318860351": {.. "message": "Error en la conexi.n. Vuelve a intentarlo.".. },.. "1550904064710828958": {.. "message": "V.deo fluido".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volumen".. },.. "1850397500312020388": {.. "messag e": ".Puedes ver tu Chromecast en la $START_LINK$aplicaci.n Google.HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6760_1072695678\CRX_INSTALL_locales\et\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15139
Entropy (8bit):	5.228213017029721
Encrypted:	false
SSDEEP:	96:Z48bxhWYp5Ny5M63niwAKD4rrJSJ2RkPXh9P5NFP2+NBMU01jewUEVez3QOiSevy:ikxprot3lYkf/rHBc0KsUV6c8TEKdl
MD5:	A62F12BCBA6D2C579212CA2FF90F8266
SHA1:	F7E964A2D9BBDA364252BCE5CFBA3FD34FDD825E
SHA-256:	3EB3EB0B3B4A8E5A477D1B3C3A3891CCC7DC6B8879ECE243A7BD7C478068273D
SHA-512:	E300201245C00ADEC8F39D586875F8FA4607AB203572BF3CE353C1CA7CDCA05B8786810CA0CEE27E4EA54A5EFD53690F1EA7AA4148CFF472A66BB1120272356
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Hangub".. },.. "1213957982723875920": {.. "message": "Milline j.rgmistest v.idetest kirjeldab k.ige paremini teie v.rku?".. },.. "128276876460319075": {.. "message": "Seadme tuvastamine".. },.. "1428448869078126731": {.. "message": "Video sujuvus".. },.. "1522140683318860351": {.. "message": ".hendamine eba.nnestus. Proovige uuesti.".. },.. "1550904064710828958": {.. "message": ".htlane".. },.. "1636686747687494376": {.. "message": "T.iuslik".. },.. "1802762746589457177": {.. "message": "Helitugevus".. },.. "1850397500312020388": {.. "message": "Kas n.ete oma Chromecasti $START_LINK$rakenduses Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir6760_1072695678\CRX_INSTALL_locales\fa\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17004
Entropy (8bit):	5.485874780010479
Encrypted:	false
SSDEEP:	192:rngaIprIX/t9wkjTJrs3hqaXxRQdiIMDnD+LhfHdoltV6c8TEKdl:4rin5rU1X7Qd0M9CtV6uml
MD5:	852BD3CFF960F1BC3A2AAB3CB3874EF9
SHA1:	C9F6F3C776542889FE3B67971D65ACFE048A3A0A
SHA-256:	D87597B6C10364501B98AA42524843F109009CCEF022D8E0170440D7F144F4C6
SHA-512:	2A7AE4D70E33E53EE31831CE2E61DD8DF103C4170EC483BDA14B8788E5DD536EEE84DBA340CACBDF16889C7E6465B48D82C4714E746E8A7B372D12CBDF371C95
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": ".... ... .".. },.. "1213957982723875920": {.. "message": ".... .. ..".. },.. "1282768764603190 75": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "....".. },.. "1802762746589457177": {.. "message": "..... ...".. },.. "1850397500312020388": {.. "message": ".... ..... Chromecast ... . $START_LINK$ ..... Google HomeEND_LINK ..... $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6760_1072695678\CRX_INSTALL_locales\fi\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15268
Entropy (8bit):	5.268402902466895
Encrypted:	false
SSDEEP:	192:efMprYXiYUNpj5Coik1tXxrUhvUzSPWV6c8TEKdl:eIrjbjosdrU5WV6uml
MD5:	3902581B6170D0CEA9B1ECF6CC82D669
SHA1:	C8208AC2B1DD6D4F8BDAAE01C8BD71FFFA5A732B
SHA-256:	D2A8180225A83A423BB6E17343DFA8F636D517154944002ED9240411B8C0C5E1
SHA-512:	612FDD8A3C5051F0A4F1E11E50B5D124B337C77D62D987D35C2AF9E08AFC6AFCEBAEE8D40FDFBCD1E1889F39758B96FAECBF6C6D1CF146C741A526195205021
Malicious:	false
Reputation:	low

Preview:	{.. "1018984561488520517": {.. "message": "Pys.htyy".. },.. "1213957982723875920": {.. "message": "Mik. seuraavista kuvaa parhaiten verkkoasi?".. },.. "128276876460319075": {.. "message": "Laitteiden tunnistaminen".. },.. "1428448869078126731": {.. "message": "Videon tasaisuus".. },.. "1522140683318860351": {.. "message": "Yhteys ep.onnistui. Yrit. uudelleen.".. },.. "1550904064710828958": {.. "message": "Tasainen".. },.. "1636686747687494376": {.. "message": "T.ydellinen".. },.. "1802762746589457177": {.. "message": "..nenvoimakkuus".. },.. "1850397500312020388": {.. "message": "N.etk. Chromec astisi $START_LINK$Google Home .sovelluksessaEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },..

C:\Users\user\AppData\Local\Temp\scoped_dir6760_1072695678\CRX_INSTALL_locales\fil\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15570
Entropy (8bit):	5.1924418176212646
Encrypted:	false
SSDEEP:	192:+esprzAsQp68wlJYkMyr2k0jR1/7Rr1uV6c8TEKdl:Gr78JDMyrR0tJuV6uml
MD5:	59483AD798347B291363327D446FA107
SHA1:	C069F29BB68FA7BA2631B0BF5BBF313346AC6736
SHA-256:	DD47530EAE96346CD4DC3267A0BB1091BB17B704803A93CDA2E3E81551B94F12
SHA-512:	091595CA135E965ED3DE376873541117F0E7A8EBDEB4714833EFDD6C820234373891BE5DEC437BA85CCB79CCCA053D407E6ADA17EBDAE7D313324A48775C0 10
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Hindi gumagalaw".. },.. "1213957982723875920": {.. "message": "Alin sa sumusunod ang pinakamahusay na naglalarawan sa iyong network?".. },.. "128276876460319075": {.. "message": "Pagtuklas ng Device".. },.. "1428448869078126731": {.. "message": "Pagka-s mooth ng Video".. },.. "1522140683318860351": {.. "message": "Hindi nakakonekta. Pakisubukang muli.".. },.. "1550904064710828958": {.. "message": "Smooth".. },.. "1636686747687494376": {.. "message": "Perpekto".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Nakikita mo ba ang iyong Chromecast sa $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$

C:\Users\user\AppData\Local\Temp\scoped_dir6760_1072695678\CRX_INSTALL_locales\fr\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15826
Entropy (8bit):	5.277877116547859
Encrypted:	false
SSDEEP:	192:nLZprAZg3EkV3sjrICe8L/1Va7lt1rlxLAkoYHHavV6c8TEKdl:vrW+2jrI7TdLAk3MV6uml
MD5:	9B416146FE4F1403C2AACAC4DCF1A5C3
SHA1:	616F055C9FAD4CE972DF82EC8A9B2F4EDA3E7FAD
SHA-256:	7C7F5758F54008190ACCDDBD1761CBD980FB5FE0847E992874498228D2571DBC
SHA-512:	6E8E70380A8C6E2C0587ADFF6AE36963EC76694904841CE1DFE4EEE215B917AD3E8AF727555627FBDF6B8BA6A4A0674D2B90AC4E9331B6628A32F4C4348FB51 B
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Se fige".. },.. "1213957982723875920": {.. "message": "Parmi les propositions suivantes, laquelle d.crit le mieux votre r.seau.?".. },.. "128276876460319075": {.. "message": "D.tection d'appareils".. },.. "1428448869078126731": {.. "message": "Fluidit. de la vid.o".. },.. "1522140683318860351": {.. "message": ".chec de la connexion. Veuillez r.essayer.".. },.. "1550904064710828958": {.. "message": "Fluide".. },.. "163 6686747687494376": {.. "message": "Parfaite".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Vo tre Chromecast est-il visible dans l'$START_LINK$application Google.HomeEND_LINK.? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir6760_1072695678\CRX_INSTALL_locales\gu\messages.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19255
Entropy (8bit):	5.32628732852814
Encrypted:	false
SSDEEP:	384:Hq2Mr+qPlJKYMdzKgXr3dGsGF+yAK37Wf7Cy/V6uml:KxzTVgX7ykj6uml
MD5:	68B03519786F71A426BAC24DECA2DD52
SHA1:	B8E6608932EC5CEC4BC3C5475BFC3E312D2E2E7D
SHA-256:	C77A4D27E9E6CA25B9290056D93A656E3EBE975957E4C2EE9F0FB11B133D5CD4
SHA-512:	5FFE06A10774877AF25E05BA07F3032CC52F874896D67E320F4EF9D524A22E40B462CC6206700E9557EB354FA2730172DC6912EBCA49C671FB0EF155B17F9EFF
Malicious:	false

Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "....".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "... ... $START_LINK$ Google Home ..END_LINK... Chromecast..

C:\Users\user\AppData\Local\Temp\scoped_dir6760_1072695678\CRX_INSTALL_locales\hi\messages.json

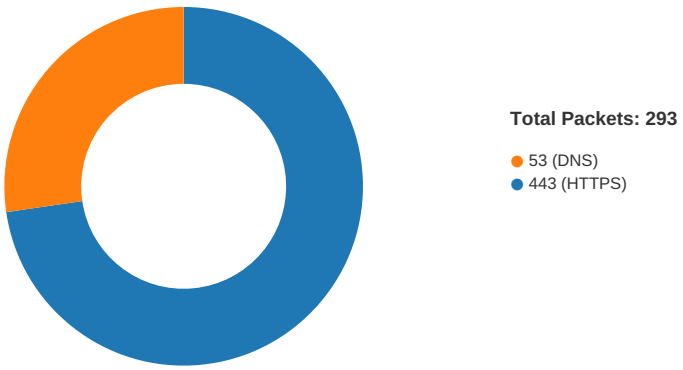
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19381
Entropy (8bit):	5.328912995891658
Encrypted:	false
SSDEEP:	384:zrGrSmhKy7KyY+bNEDqlQdrMEPxtShJV6uml:zBqG6QdwEPrW6uml
MD5:	20C86E04B1833EA7F21C07361061420A
SHA1:	617C0D70E162CF380005E9780B61F650B7A39F9B
SHA-256:	C2C27CA242DBDE600BA3AA7782156BC2B190A64D8A1B51EDC8007BDECA139553
SHA-512:	9FB91AA8E0226519E298B1136E8A1A3C1879DB7F0E6052AF1BFD55921CD698346278D04602510680A9695A76DD5C96D9665380580044C50D81392BB2CB3E8E95
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "128276876460319075": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": ".... .. $START_LINK$ Google Home .....END_LINK ... . Ch

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:11:26.654328108 CET	49750	443	192.168.2.3	172.217.168.45
Jan 28, 2022 14:11:26.654381037 CET	443	49750	172.217.168.45	192.168.2.3
Jan 28, 2022 14:11:26.654484987 CET	49750	443	192.168.2.3	172.217.168.45
Jan 28, 2022 14:11:26.654900074 CET	49751	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:26.654942036 CET	443	49751	142.250.203.110	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:11:26.655309916 CET	49751	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:26.656575918 CET	49750	443	192.168.2.3	172.217.168.45
Jan 28, 2022 14:11:26.656605959 CET	443	49750	172.217.168.45	192.168.2.3
Jan 28, 2022 14:11:26.656799078 CET	49751	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:26.656817913 CET	443	49751	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:26.712713957 CET	443	49751	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:26.713632107 CET	443	49750	172.217.168.45	192.168.2.3
Jan 28, 2022 14:11:26.722846031 CET	49751	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:26.722882986 CET	443	49751	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:26.722955942 CET	49750	443	192.168.2.3	172.217.168.45
Jan 28, 2022 14:11:26.723001957 CET	443	49750	172.217.168.45	192.168.2.3
Jan 28, 2022 14:11:26.723504066 CET	443	49751	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:26.723684072 CET	49751	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:26.724193096 CET	443	49750	172.217.168.45	192.168.2.3
Jan 28, 2022 14:11:26.724333048 CET	49750	443	192.168.2.3	172.217.168.45
Jan 28, 2022 14:11:26.725064039 CET	443	49751	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:26.725579977 CET	49751	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:26.997797012 CET	49750	443	192.168.2.3	172.217.168.45
Jan 28, 2022 14:11:26.998168945 CET	443	49750	172.217.168.45	192.168.2.3
Jan 28, 2022 14:11:26.998495102 CET	49751	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:26.999089956 CET	443	49751	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:27.004359007 CET	49750	443	192.168.2.3	172.217.168.45
Jan 28, 2022 14:11:27.004396915 CET	443	49750	172.217.168.45	192.168.2.3
Jan 28, 2022 14:11:27.004466057 CET	49751	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:27.004506111 CET	443	49751	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:27.041632891 CET	443	49751	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:27.041821003 CET	443	49751	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:27.041873932 CET	49751	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:27.041887045 CET	49751	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:27.043162107 CET	49751	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:27.043181896 CET	443	49751	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:27.059231043 CET	443	49750	172.217.168.45	192.168.2.3
Jan 28, 2022 14:11:27.059397936 CET	49750	443	192.168.2.3	172.217.168.45
Jan 28, 2022 14:11:27.060723066 CET	49750	443	192.168.2.3	172.217.168.45
Jan 28, 2022 14:11:27.060750008 CET	443	49750	172.217.168.45	192.168.2.3
Jan 28, 2022 14:11:27.614048004 CET	49757	443	192.168.2.3	18.66.218.95
Jan 28, 2022 14:11:27.614092112 CET	443	49757	18.66.218.95	192.168.2.3
Jan 28, 2022 14:11:27.614176035 CET	49757	443	192.168.2.3	18.66.218.95
Jan 28, 2022 14:11:27.614365101 CET	49757	443	192.168.2.3	18.66.218.95
Jan 28, 2022 14:11:27.614381075 CET	443	49757	18.66.218.95	192.168.2.3
Jan 28, 2022 14:11:27.694955111 CET	443	49757	18.66.218.95	192.168.2.3
Jan 28, 2022 14:11:27.697196960 CET	49757	443	192.168.2.3	18.66.218.95
Jan 28, 2022 14:11:27.697240114 CET	443	49757	18.66.218.95	192.168.2.3
Jan 28, 2022 14:11:27.698405981 CET	443	49757	18.66.218.95	192.168.2.3
Jan 28, 2022 14:11:27.698513031 CET	49757	443	192.168.2.3	18.66.218.95
Jan 28, 2022 14:11:27.700500011 CET	49757	443	192.168.2.3	18.66.218.95
Jan 28, 2022 14:11:27.700608015 CET	443	49757	18.66.218.95	192.168.2.3
Jan 28, 2022 14:11:27.700860023 CET	49757	443	192.168.2.3	18.66.218.95
Jan 28, 2022 14:11:27.700886965 CET	443	49757	18.66.218.95	192.168.2.3
Jan 28, 2022 14:11:27.783263922 CET	49757	443	192.168.2.3	18.66.218.95
Jan 28, 2022 14:11:27.783518076 CET	49758	443	192.168.2.3	18.66.196.121
Jan 28, 2022 14:11:27.783551931 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.783653975 CET	49758	443	192.168.2.3	18.66.196.121
Jan 28, 2022 14:11:27.783900023 CET	49758	443	192.168.2.3	18.66.196.121
Jan 28, 2022 14:11:27.783914089 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.845432997 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.845922947 CET	49758	443	192.168.2.3	18.66.196.121
Jan 28, 2022 14:11:27.845952988 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.846982002 CET	443	49758	18.66.196.121	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:11:27.847064018 CET	49758	443	192.168.2.3	18.66.196.121
Jan 28, 2022 14:11:27.849756956 CET	49758	443	192.168.2.3	18.66.196.121
Jan 28, 2022 14:11:27.849884033 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.849940062 CET	49758	443	192.168.2.3	18.66.196.121
Jan 28, 2022 14:11:27.893928051 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.929358006 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.929379940 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.929492950 CET	49758	443	192.168.2.3	18.66.196.121
Jan 28, 2022 14:11:27.929517984 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.929537058 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.929590940 CET	49758	443	192.168.2.3	18.66.196.121
Jan 28, 2022 14:11:27.929590940 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.929615974 CET	49758	443	192.168.2.3	18.66.196.121
Jan 28, 2022 14:11:27.929661036 CET	49758	443	192.168.2.3	18.66.196.121
Jan 28, 2022 14:11:27.934101105 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.934112072 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.934125900 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.934178114 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.934223890 CET	49758	443	192.168.2.3	18.66.196.121
Jan 28, 2022 14:11:27.934232950 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.934283972 CET	49758	443	192.168.2.3	18.66.196.121
Jan 28, 2022 14:11:27.934302092 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.934318066 CET	49758	443	192.168.2.3	18.66.196.121
Jan 28, 2022 14:11:27.934401989 CET	49758	443	192.168.2.3	18.66.196.121
Jan 28, 2022 14:11:27.956042051 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.956053972 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.956218004 CET	49758	443	192.168.2.3	18.66.196.121
Jan 28, 2022 14:11:27.956218958 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.956274033 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.956322908 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.956343889 CET	49758	443	192.168.2.3	18.66.196.121
Jan 28, 2022 14:11:27.956374884 CET	49758	443	192.168.2.3	18.66.196.121
Jan 28, 2022 14:11:27.960654974 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.960691929 CET	443	49758	18.66.196.121	192.168.2.3
Jan 28, 2022 14:11:27.960788965 CET	49758	443	192.168.2.3	18.66.196.121
Jan 28, 2022 14:11:27.960809946 CET	443	49758	18.66.196.121	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:11:26.614268064 CET	53910	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:26.622510910 CET	64021	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:26.624651909 CET	60784	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:26.633502007 CET	53	53910	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:26.642139912 CET	53	64021	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:27.589205027 CET	49572	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:27.612962008 CET	53	49572	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:27.747873068 CET	60823	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:27.782454967 CET	53	60823	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:28.599059105 CET	55102	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:28.622694016 CET	53	55102	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:29.618362904 CET	56236	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:29.631606102 CET	56527	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:29.637316942 CET	53	56236	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:29.658797026 CET	53	56527	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:30.891089916 CET	49559	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:30.917804956 CET	53	49559	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:36.279155016 CET	57106	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:36.312275887 CET	53	57106	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:11:36.543761969 CET	60352	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:36.546597004 CET	56773	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:36.564910889 CET	53	60352	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:36.567703962 CET	53	56773	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:36.614010096 CET	60982	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:36.636920929 CET	53	60982	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:36.893440008 CET	58058	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:36.915905952 CET	64367	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:36.934633017 CET	53	58058	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:36.950077057 CET	53	64367	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:37.263056040 CET	55393	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:37.279689074 CET	53	55393	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:37.444833994 CET	50585	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:37.467516899 CET	53	50585	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:37.739039898 CET	50586	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:37.768590927 CET	443	50586	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:37.814085007 CET	50586	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:37.844420910 CET	443	50586	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:37.844474077 CET	443	50586	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:37.844502926 CET	443	50586	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:37.844531059 CET	443	50586	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:37.961175919 CET	50586	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:37.964965105 CET	50586	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:37.970776081 CET	443	50586	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:37.970818996 CET	443	50586	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:37.970840931 CET	443	50586	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:37.970863104 CET	443	50586	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:37.971551895 CET	50586	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:37.971626043 CET	50586	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:38.013577938 CET	50586	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:38.014298916 CET	50586	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:38.056354046 CET	443	50586	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:38.072350979 CET	443	50586	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:38.076138973 CET	50586	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:38.076203108 CET	50586	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:38.094374895 CET	443	50586	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:38.106857061 CET	443	50586	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:38.106892109 CET	443	50586	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:38.108270884 CET	50586	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:38.179215908 CET	443	50586	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:38.179491997 CET	443	50586	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:38.179513931 CET	443	50586	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:38.182358027 CET	50586	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:38.342400074 CET	50586	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:38.356460094 CET	443	50586	142.250.203.110	192.168.2.3
Jan 28, 2022 14:11:38.433348894 CET	50586	443	192.168.2.3	142.250.203.110
Jan 28, 2022 14:11:38.495250940 CET	63456	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:38.516864061 CET	53	63456	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:38.594053984 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:38.596025944 CET	58540	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:38.618048906 CET	53	58540	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:38.624842882 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:38.624871016 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:38.624888897 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:38.626096964 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:38.652316093 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:38.708600998 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:38.816595078 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.030740976 CET	443	63457	172.217.168.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:11:39.089584112 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.092700958 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.092833042 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.101588011 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.101927996 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.144234896 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.144789934 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.145600080 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.160495043 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.160516977 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.160531998 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.160547972 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.160569906 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.160584927 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.160600901 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.160617113 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.160631895 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.160646915 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.160662889 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.160926104 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.161004066 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.161075115 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.161165953 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.161250114 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.161665916 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.161825895 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.161912918 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.161933899 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.162091970 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.162910938 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.162930012 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.163124084 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.164215088 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.164238930 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.164256096 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.164447069 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.165838003 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.165874004 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.165890932 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.166423082 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.166502953 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.168003082 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.168023109 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.168039083 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.168054104 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.169001102 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.169071913 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.170644999 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.170670033 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.170685053 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.170700073 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.170716047 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.170846939 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.170922995 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.172312975 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.172333956 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.172349930 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.172480106 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.172566891 CET	63457	443	192.168.2.3	172.217.168.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:11:39.174391031 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.174417019 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.174428940 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.174444914 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.175681114 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.175790071 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.175909042 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.175930023 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.175945997 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.176121950 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.177582026 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.177602053 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.178152084 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.178169012 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.178710938 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.178796053 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.179064035 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.179085970 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.179243088 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.180334091 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:39.183676004 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:39.218801022 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:40.667515039 CET	58942	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:40.691313028 CET	53	58942	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:41.998745918 CET	49250	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:42.016252995 CET	53	49250	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:42.041488886 CET	63490	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:42.075723886 CET	53	63490	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:42.119020939 CET	65110	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:42.125231981 CET	61120	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:42.136338949 CET	53	65110	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:42.147732973 CET	53	61120	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:42.956993103 CET	53079	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:42.984280109 CET	53	53079	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:43.863256931 CET	50824	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:43.888356924 CET	53	50824	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:44.149133921 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:44.181617975 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:44.181647062 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:44.182862043 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:45.914968967 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:45.951723099 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.951754093 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.951766968 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.951778889 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.951791048 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.951803923 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.951822996 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.951841116 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.951857090 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.951874018 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.951890945 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.951904058 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.952173948 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:45.952204943 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:45.952259064 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:45.952315092 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:45.952372074 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:45.952428102 CET	63457	443	192.168.2.3	172.217.168.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:11:45.952852964 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.952872992 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.952886105 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.952903986 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.952922106 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.952939034 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.952956915 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.952972889 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.953020096 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:45.953080893 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:45.953136921 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:45.953195095 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:45.954121113 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.954140902 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.954154015 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.954173088 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.954186916 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.954298019 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:45.954355001 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:45.954652071 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.954670906 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.954688072 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.954705000 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.954721928 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.954739094 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.954755068 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.954777002 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:45.954777002 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.954839945 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:45.954899073 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:45.954955101 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:45.956398964 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.956422091 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.956439018 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.956455946 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.956470966 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.956486940 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.956504107 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.956521034 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.956542015 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.956542969 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:45.956559896 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.956577063 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.956593037 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.956605911 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:45.956669092 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:45.957279921 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:45.958472967 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.958493948 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.958506107 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.958518982 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.958533049 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:45.958792925 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:46.000088930 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:46.066176891 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:11:46.097403049 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:11:46.097430944 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:11:46.097449064 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:11:46.104772091 CET	50827	443	192.168.2.3	216.58.215.238

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:11:46.128681898 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:11:46.135199070 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:11:46.161751032 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:11:46.172182083 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:11:46.172396898 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:11:46.172797918 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:11:46.173060894 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:11:46.205935001 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:11:46.205954075 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:11:46.206549883 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:11:55.484805107 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:55.486511946 CET	53569	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:55.507631063 CET	53	53569	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:55.516458035 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:55.516491890 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:55.524815083 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:57.990530014 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:58.024034023 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.024055958 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.024072886 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.024086952 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.024101973 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.024118900 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.024135113 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.024149895 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.024163961 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.024178982 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.024194002 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.024205923 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.024621964 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:58.025095940 CET	62855	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:11:58.025521040 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.025541067 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.025557995 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.025573015 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.025590897 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.025607109 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.025623083 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.025640011 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.026092052 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:58.027369976 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.027390003 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.027405977 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.027421951 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.027435064 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.027450085 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.027466059 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.027482033 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.027498007 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.027513027 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.027529001 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.027544022 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.028397083 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:58.029041052 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.029062033 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.029089928 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.029104948 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.029120922 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.029131889 CET	443	63457	172.217.168.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:11:58.029148102 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.029160023 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.029175043 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.029190063 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.029203892 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.029218912 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.029232979 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.029669046 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:58.030514956 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.030534983 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.030553102 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.030570984 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.030581951 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:11:58.031143904 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:11:58.048718929 CET	53	62855	8.8.8.8	192.168.2.3
Jan 28, 2022 14:11:58.085937977 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:11:58.117230892 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:11:58.117459059 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:11:58.117702007 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:03.943784952 CET	51046	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:03.967839956 CET	53	51046	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:06.020170927 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:06.052706003 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.053584099 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.056512117 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:06.099842072 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.156861067 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:06.190253973 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.190278053 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.190293074 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.190310001 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.190327883 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.190342903 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.190360069 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.190375090 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.190391064 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.190406084 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.190468073 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.190480947 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.190949917 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:06.191068888 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.191090107 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.191107035 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.191123962 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.191139936 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.191155910 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.191170931 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.191186905 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.191416979 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:06.192600012 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.192620993 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.192653894 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.192671061 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.192687035 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.192702055 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.192718983 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.192733049 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.192749023 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.192766905 CET	443	63457	172.217.168.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:12:06.194309950 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.194334030 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.194349051 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.194365025 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.194380045 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.194396973 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.194411993 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.194427013 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.194442987 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.194458008 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.195246935 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.195266962 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.195281029 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.195292950 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.195305109 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.195318937 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.195339918 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.195354939 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.196247101 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:06.196458101 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:06.196559906 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:06.204896927 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:06.533720016 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:06.565186024 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:06.565202951 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:06.565635920 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:15.205322027 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:15.238257885 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:15.238306999 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:15.251071930 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:15.831559896 CET	59754	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:16.096627951 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:16.130425930 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.130484104 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.130527020 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.130564928 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.130604982 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.130641937 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.130681992 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.130719900 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.130757093 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.130795956 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.130832911 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.130858898 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.131167889 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:16.133202076 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.133243084 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.133280993 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.133320093 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.133356094 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.133393049 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.133430958 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.133469105 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.134071112 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:16.134857893 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.134901047 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.134938002 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.134974957 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.135004997 CET	443	63457	172.217.168.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:12:16.136064053 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.136101961 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.136138916 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.136178017 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.136214018 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.136250973 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.136286974 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.136322975 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.136372089 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:16.138062000 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.138104916 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.138144016 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.138180017 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.138210058 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.138977051 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.139017105 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.139055014 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.139091015 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.139131069 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.139182091 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.139219999 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.139254093 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:16.139260054 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.141197920 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.141237974 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.141277075 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.141307116 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:16.141711950 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:16.213123083 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:16.245090008 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:16.245281935 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:16.247929096 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:17.477580070 CET	49234	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:17.497668028 CET	53	49234	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:17.709533930 CET	58720	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:21.104784012 CET	63583	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:21.647464991 CET	64099	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:21.664484024 CET	64610	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:21.675234079 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:21.680389881 CET	51989	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:21.680571079 CET	53	64099	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:21.686961889 CET	53	64610	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:21.704523087 CET	53	51989	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:21.709817886 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.709871054 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.709935904 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.709959984 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.709976912 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.710000038 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.710017920 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.710074902 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.710098028 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.710119963 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.710136890 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.710155010 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.710454941 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:21.711287975 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.711375952 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.711421967 CET	443	63457	172.217.168.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:12:21.711446047 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.711468935 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.711534023 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.711559057 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.711580992 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.712219000 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.712363005 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.712388992 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.712415934 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.712436914 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.712460041 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.712481976 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.712505102 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.712527037 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.712594032 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.712618113 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.712641954 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.713264942 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:21.713515043 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:21.713754892 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.713778019 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.713793039 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.713808060 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.713826895 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.713906050 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.713924885 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.714057922 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.714077950 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.714092016 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.714106083 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.714416027 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:21.718075991 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.718097925 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.718131065 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.718144894 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.718163967 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.718203068 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.718218088 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.719496965 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:21.725517988 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.725775957 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.725866079 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.725887060 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.725905895 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.725925922 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.725991964 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.726035118 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.727123976 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.729285955 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.729305983 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.729326010 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.729345083 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.729366064 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.729384899 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.729403973 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.729448080 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.729463100 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:21.730509043 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:21.739144087 CET	63457	443	192.168.2.3	172.217.168.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:12:22.223210096 CET	53152	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:28.944674015 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:28.976367950 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:28.976401091 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:28.985502005 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:30.954277992 CET	60253	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:30.954988003 CET	58706	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:30.978835106 CET	53	58706	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:30.990870953 CET	53	60253	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:31.346537113 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:31.389738083 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:36.372591972 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:36.405314922 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:36.405338049 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:36.443046093 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:36.480962992 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:36.680085897 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:36.680110931 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:37.080775023 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:37.080805063 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:37.358963013 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:37.366750956 CET	62677	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:37.392621040 CET	53	62677	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:37.762331009 CET	62595	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:37.786091089 CET	53	62595	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:38.037000895 CET	51189	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:38.054856062 CET	53	51189	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:38.213845015 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:38.247405052 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.247426987 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.247442961 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.247459888 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.247476101 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.247492075 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.247509003 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.247524977 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.247540951 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.247556925 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.247570992 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.247582912 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.248868942 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.248888016 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.248904943 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.248920918 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.248936892 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.248953104 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.248967886 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.248984098 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.249361038 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:38.250093937 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.250113010 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.250128031 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.250144005 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.250157118 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.250384092 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:38.250531912 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.250550985 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.250566959 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.250582933 CET	443	63457	172.217.168.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:12:38.250597954 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.250613928 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.251915932 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.251933098 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.251950026 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.251966000 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.251981974 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.251997948 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.252010107 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.252557993 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:38.252752066 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.252768993 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.252784967 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.252800941 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.252818108 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.252831936 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.252847910 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.252862930 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.253446102 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:38.253998995 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.254018068 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.254034042 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.254045010 CET	443	63457	172.217.168.8	192.168.2.3
Jan 28, 2022 14:12:38.254502058 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:38.437800884 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:38.469026089 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:38.469062090 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:38.469547987 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:39.663017035 CET	51454	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:39.701322079 CET	53	51454	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:43.608031988 CET	57163	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:43.627573967 CET	53	57163	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:43.706100941 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:43.710771084 CET	56360	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:43.710833073 CET	49258	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:43.711147070 CET	56195	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:43.711225986 CET	53021	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:43.724092960 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:43.724123955 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:43.724143982 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:43.724162102 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:43.724183083 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:43.724203110 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:43.724221945 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:43.724241972 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:43.724260092 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:43.724278927 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:43.724298000 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:43.724317074 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:43.725464106 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:43.725527048 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:43.725599051 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:43.725677013 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:43.725745916 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:43.726120949 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:43.726238012 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:43.726283073 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:43.726304054 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:43.727777958 CET	50827	443	192.168.2.3	216.58.215.238

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:12:43.727857113 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:43.727874994 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:43.728319883 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:43.731688023 CET	53	56360	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:43.732825041 CET	53	56195	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:43.741009951 CET	53	53021	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:43.752752066 CET	52618	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:43.753905058 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:43.755583048 CET	51633	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:43.755649090 CET	64383	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:43.757698059 CET	50346	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:43.773293018 CET	53	52618	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:43.774442911 CET	53	64383	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:43.777220964 CET	50281	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:43.779556990 CET	53	50346	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:43.780919075 CET	56328	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:43.781688929 CET	53	51633	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:43.798604012 CET	53	50281	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:43.800209999 CET	53	56328	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:43.822449923 CET	56921	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:43.823324919 CET	59529	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:43.840259075 CET	53	56921	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:43.849050045 CET	53	59529	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:43.905333996 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:43.935996056 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:43.936197996 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:43.936342001 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:43.937796116 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:43.954241037 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:43.954262018 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:43.957870960 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:43.966489077 CET	64853	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:43.967531919 CET	56317	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:43.992690086 CET	53	64853	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:44.180449009 CET	51570	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:44.183784008 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:44.201726913 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:44.201795101 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:44.202342987 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:44.207829952 CET	53	51570	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:44.217012882 CET	53663	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:44.218043089 CET	60070	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:44.219264030 CET	60071	443	192.168.2.3	172.217.168.68
Jan 28, 2022 14:12:44.223288059 CET	58750	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:44.238337994 CET	53	60070	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:44.239109993 CET	53	53663	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:44.248382092 CET	443	60071	172.217.168.68	192.168.2.3
Jan 28, 2022 14:12:44.248919010 CET	53	58750	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:44.249507904 CET	60071	443	192.168.2.3	172.217.168.68
Jan 28, 2022 14:12:44.255769014 CET	60727	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:44.279323101 CET	443	60071	172.217.168.68	192.168.2.3
Jan 28, 2022 14:12:44.279344082 CET	443	60071	172.217.168.68	192.168.2.3
Jan 28, 2022 14:12:44.279360056 CET	443	60071	172.217.168.68	192.168.2.3
Jan 28, 2022 14:12:44.279375076 CET	443	60071	172.217.168.68	192.168.2.3
Jan 28, 2022 14:12:44.280558109 CET	60071	443	192.168.2.3	172.217.168.68
Jan 28, 2022 14:12:44.281745911 CET	60071	443	192.168.2.3	172.217.168.68
Jan 28, 2022 14:12:44.307174921 CET	60071	443	192.168.2.3	172.217.168.68
Jan 28, 2022 14:12:44.307467937 CET	60071	443	192.168.2.3	172.217.168.68
Jan 28, 2022 14:12:44.337630033 CET	443	60071	172.217.168.68	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:12:44.352319002 CET	60071	443	192.168.2.3	172.217.168.68
Jan 28, 2022 14:12:44.362306118 CET	443	60071	172.217.168.68	192.168.2.3
Jan 28, 2022 14:12:44.364197016 CET	443	60071	172.217.168.68	192.168.2.3
Jan 28, 2022 14:12:44.364288092 CET	60728	443	192.168.2.3	142.250.203.102
Jan 28, 2022 14:12:44.366703987 CET	443	60071	172.217.168.68	192.168.2.3
Jan 28, 2022 14:12:44.367141008 CET	60071	443	192.168.2.3	172.217.168.68
Jan 28, 2022 14:12:44.368009090 CET	443	60071	172.217.168.68	192.168.2.3
Jan 28, 2022 14:12:44.393840075 CET	443	60728	142.250.203.102	192.168.2.3
Jan 28, 2022 14:12:44.393883944 CET	443	60728	142.250.203.102	192.168.2.3
Jan 28, 2022 14:12:44.393902063 CET	443	60728	142.250.203.102	192.168.2.3
Jan 28, 2022 14:12:44.394186974 CET	60728	443	192.168.2.3	142.250.203.102
Jan 28, 2022 14:12:44.394747972 CET	60071	443	192.168.2.3	172.217.168.68
Jan 28, 2022 14:12:44.419634104 CET	443	60728	142.250.203.102	192.168.2.3
Jan 28, 2022 14:12:44.420418024 CET	60728	443	192.168.2.3	142.250.203.102
Jan 28, 2022 14:12:44.433984995 CET	63753	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:44.435240984 CET	60728	443	192.168.2.3	142.250.203.102
Jan 28, 2022 14:12:44.435647964 CET	60728	443	192.168.2.3	142.250.203.102
Jan 28, 2022 14:12:44.454586983 CET	53	63753	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:44.478306055 CET	443	60728	142.250.203.102	192.168.2.3
Jan 28, 2022 14:12:44.479190111 CET	60728	443	192.168.2.3	142.250.203.102
Jan 28, 2022 14:12:44.489886999 CET	443	60728	142.250.203.102	192.168.2.3
Jan 28, 2022 14:12:44.491908073 CET	60728	443	192.168.2.3	142.250.203.102
Jan 28, 2022 14:12:44.492016077 CET	60728	443	192.168.2.3	142.250.203.102
Jan 28, 2022 14:12:44.496553898 CET	443	60728	142.250.203.102	192.168.2.3
Jan 28, 2022 14:12:44.509403944 CET	443	60728	142.250.203.102	192.168.2.3
Jan 28, 2022 14:12:44.522241116 CET	443	60728	142.250.203.102	192.168.2.3
Jan 28, 2022 14:12:44.522557974 CET	443	60728	142.250.203.102	192.168.2.3
Jan 28, 2022 14:12:44.523452044 CET	60728	443	192.168.2.3	142.250.203.102
Jan 28, 2022 14:12:44.577049971 CET	443	60728	142.250.203.102	192.168.2.3
Jan 28, 2022 14:12:44.577435017 CET	443	60728	142.250.203.102	192.168.2.3
Jan 28, 2022 14:12:44.578412056 CET	60728	443	192.168.2.3	142.250.203.102
Jan 28, 2022 14:12:44.766376972 CET	54609	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:44.785737038 CET	53	54609	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:44.889327049 CET	52405	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:44.906059027 CET	53	52405	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:44.940455914 CET	56219	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:44.943962097 CET	52312	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:44.947818995 CET	64731	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:44.963460922 CET	53	52312	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:44.963494062 CET	53	56219	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:44.967375040 CET	53	64731	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:45.191989899 CET	59130	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:45.213989973 CET	53	59130	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:45.255640984 CET	51636	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:45.275006056 CET	53	51636	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:45.702687979 CET	60432	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:45.720405102 CET	53	60432	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:45.755034924 CET	64271	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:45.777513981 CET	53	64271	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:45.916944027 CET	51973	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:45.935868025 CET	53	51973	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:47.452997923 CET	63193	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:47.453852892 CET	53946	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:47.470156908 CET	53	63193	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:47.472815037 CET	53	53946	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:48.021871090 CET	61244	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:48.043325901 CET	53	61244	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:53.223828077 CET	63457	443	192.168.2.3	172.217.168.8
Jan 28, 2022 14:12:53.266561985 CET	443	63457	172.217.168.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:12:56.012693882 CET	55029	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:56.038065910 CET	53	55029	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:58.823024035 CET	51235	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:12:58.845690966 CET	53	51235	8.8.8.8	192.168.2.3
Jan 28, 2022 14:12:58.906924963 CET	50827	443	192.168.2.3	216.58.215.238
Jan 28, 2022 14:12:58.950189114 CET	443	50827	216.58.215.238	192.168.2.3
Jan 28, 2022 14:12:59.438533068 CET	60728	443	192.168.2.3	142.250.203.102
Jan 28, 2022 14:12:59.483319998 CET	443	60728	142.250.203.102	192.168.2.3
Jan 28, 2022 14:13:17.528856993 CET	56240	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:13:17.548682928 CET	53	56240	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 14:11:26.614268064 CET	192.168.2.3	8.8.8.8	0xeb35	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:26.622510910 CET	192.168.2.3	8.8.8.8	0x180	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:26.624651909 CET	192.168.2.3	8.8.8.8	0x535	Standard query (0)	6v4feb7simf.typeform.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:27.589205027 CET	192.168.2.3	8.8.8.8	0x6581	Standard query (0)	images.typeform.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:27.747873068 CET	192.168.2.3	8.8.8.8	0x5e21	Standard query (0)	renderer-assets.typeform.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:28.599059105 CET	192.168.2.3	8.8.8.8	0x8b12	Standard query (0)	cdn.segment.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:29.618362904 CET	192.168.2.3	8.8.8.8	0x5db4	Standard query (0)	api.segment.io	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:29.631606102 CET	192.168.2.3	8.8.8.8	0x13e9	Standard query (0)	public-assets.typeform.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:30.891089916 CET	192.168.2.3	8.8.8.8	0xb071	Standard query (0)	public-assets.typeform.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.279155016 CET	192.168.2.3	8.8.8.8	0xe9d6	Standard query (0)	www.typeform.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.543761969 CET	192.168.2.3	8.8.8.8	0x97c7	Standard query (0)	cdn.cookielaw.org	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.546597004 CET	192.168.2.3	8.8.8.8	0x282a	Standard query (0)	font.typeform.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.614010096 CET	192.168.2.3	8.8.8.8	0x2a29	Standard query (0)	images.ctfassets.net	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.893440008 CET	192.168.2.3	8.8.8.8	0xa9ac	Standard query (0)	cdn.rollbar.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.915905952 CET	192.168.2.3	8.8.8.8	0xa1be	Standard query (0)	www.datadoghq-browser-agent.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:37.263056040 CET	192.168.2.3	8.8.8.8	0xf7c1	Standard query (0)	polyfill.io	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:37.444833994 CET	192.168.2.3	8.8.8.8	0xc412	Standard query (0)	d3m6p8tvnbsibq.cloudfront.net	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:38.495250940 CET	192.168.2.3	8.8.8.8	0xab3	Standard query (0)	geolocation.onetrust.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:38.596025944 CET	192.168.2.3	8.8.8.8	0xeb86	Standard query (0)	unpkg.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:40.667515039 CET	192.168.2.3	8.8.8.8	0x2994	Standard query (0)	config.trackingplan.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:41.998745918 CET	192.168.2.3	8.8.8.8	0x2730	Standard query (0)	www.typeform.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:42.041488886 CET	192.168.2.3	8.8.8.8	0xad7	Standard query (0)	images.ctfassets.net	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:42.119020939 CET	192.168.2.3	8.8.8.8	0xa85e	Standard query (0)	d3m6p8tvnbsibq.cloudfront.net	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:42.125231981 CET	192.168.2.3	8.8.8.8	0x7683	Standard query (0)	cdn.cookielaw.org	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:42.956993103 CET	192.168.2.3	8.8.8.8	0xe43a	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 14:11:43.863256931 CET	192.168.2.3	8.8.8.8	0x80e2	Standard query (0)	tracks.trackingplan.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:55.486511946 CET	192.168.2.3	8.8.8.8	0x6322	Standard query (0)	public.profitwell.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:58.025095940 CET	192.168.2.3	8.8.8.8	0xb43c	Standard query (0)	pixel.stretmetrics.io	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:03.943784952 CET	192.168.2.3	8.8.8.8	0xd444	Standard query (0)	pixel.stretmetrics.io	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:15.831559896 CET	192.168.2.3	8.8.8.8	0x7b60	Standard query (0)	fast.wistia.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:17.477580070 CET	192.168.2.3	8.8.8.8	0xf261	Standard query (0)	distillery.wistia.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:17.709533930 CET	192.168.2.3	8.8.8.8	0x1c52	Standard query (0)	embed-fastly.wistia.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:21.104784012 CET	192.168.2.3	8.8.8.8	0x7550	Standard query (0)	admin.typeform.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:21.647464991 CET	192.168.2.3	8.8.8.8	0xfc1c	Standard query (0)	d2cjrwb117kaxb.cloudfront.net	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:21.664484024 CET	192.168.2.3	8.8.8.8	0xc5fd	Standard query (0)	endpoint2.collection.us2.sumologic.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:21.680389881 CET	192.168.2.3	8.8.8.8	0x9829	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:22.223210096 CET	192.168.2.3	8.8.8.8	0x395	Standard query (0)	cdn.optimizely.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:30.954277992 CET	192.168.2.3	8.8.8.8	0x1b6	Standard query (0)	public-assets.typeform.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:30.954988003 CET	192.168.2.3	8.8.8.8	0x6d69	Standard query (0)	auth.typeform.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:37.366750956 CET	192.168.2.3	8.8.8.8	0x9c89	Standard query (0)	www.typeform.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:37.762331009 CET	192.168.2.3	8.8.8.8	0xca24	Standard query (0)	images.ctfassets.net	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:38.037000895 CET	192.168.2.3	8.8.8.8	0xe057	Standard query (0)	cdn.cookielaw.org	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:39.663017035 CET	192.168.2.3	8.8.8.8	0xd123	Standard query (0)	font.typeform.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.608031988 CET	192.168.2.3	8.8.8.8	0xcaec	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.710771084 CET	192.168.2.3	8.8.8.8	0xce8	Standard query (0)	js.hs-scripts.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.710833073 CET	192.168.2.3	8.8.8.8	0xf97f	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.711147070 CET	192.168.2.3	8.8.8.8	0x4858	Standard query (0)	reveal.clearbit.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.711225986 CET	192.168.2.3	8.8.8.8	0x7c5f	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.752752066 CET	192.168.2.3	8.8.8.8	0xda49	Standard query (0)	dx.mountain.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.755583048 CET	192.168.2.3	8.8.8.8	0x8f0f	Standard query (0)	ws.zoominfo.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.755649090 CET	192.168.2.3	8.8.8.8	0xd030	Standard query (0)	tags.srv.stackadapt.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.757698059 CET	192.168.2.3	8.8.8.8	0xfd2	Standard query (0)	cdn.segment.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.777220964 CET	192.168.2.3	8.8.8.8	0xf521	Standard query (0)	privacyportal-de.onetrust.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.780919075 CET	192.168.2.3	8.8.8.8	0xee2e	Standard query (0)	logx.optimizely.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.822449923 CET	192.168.2.3	8.8.8.8	0x3068	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.823324919 CET	192.168.2.3	8.8.8.8	0xea87	Standard query (0)	x.clearbitjs.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.966489077 CET	192.168.2.3	8.8.8.8	0x5ac2	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.967531919 CET	192.168.2.3	8.8.8.8	0x1f72	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.180449009 CET	192.168.2.3	8.8.8.8	0xb835	Standard query (0)	10579985.fls.doubleclick.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 14:12:44.217012882 CET	192.168.2.3	8.8.8.8	0x40e2	Standard query (0)	js.hs-banner.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.218043089 CET	192.168.2.3	8.8.8.8	0x467b	Standard query (0)	js.hs-analytics.net	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.223288059 CET	192.168.2.3	8.8.8.8	0xcc84	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.255769014 CET	192.168.2.3	8.8.8.8	0x240	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.433984995 CET	192.168.2.3	8.8.8.8	0x9496	Standard query (0)	track.hubspot.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.766376972 CET	192.168.2.3	8.8.8.8	0x3a37	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.889327049 CET	192.168.2.3	8.8.8.8	0xe3d4	Standard query (0)	api.segment.io	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.940455914 CET	192.168.2.3	8.8.8.8	0xe603	Standard query (0)	cdn.amplitude.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.943962097 CET	192.168.2.3	8.8.8.8	0xe17c	Standard query (0)	edge.fullstory.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.947818995 CET	192.168.2.3	8.8.8.8	0xf557	Standard query (0)	px.mountain.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:45.191989899 CET	192.168.2.3	8.8.8.8	0x3c3b	Standard query (0)	x.clearbit.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:45.255640984 CET	192.168.2.3	8.8.8.8	0xd048	Standard query (0)	rs.fullstory.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:45.702687979 CET	192.168.2.3	8.8.8.8	0x7c8c	Standard query (0)	adservice.google.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:45.755034924 CET	192.168.2.3	8.8.8.8	0x1da8	Standard query (0)	gs.mountain.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:45.916944027 CET	192.168.2.3	8.8.8.8	0x287b	Standard query (0)	api.amplitude.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:47.452997923 CET	192.168.2.3	8.8.8.8	0xc2c9	Standard query (0)	match.adsrvr.org	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:47.453852892 CET	192.168.2.3	8.8.8.8	0x455	Standard query (0)	insight.adsrvr.org	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:48.021871090 CET	192.168.2.3	8.8.8.8	0xf899	Standard query (0)	px.steelhousemedia.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:56.012693882 CET	192.168.2.3	8.8.8.8	0x8e17	Standard query (0)	adservice.google.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:58.823024035 CET	192.168.2.3	8.8.8.8	0x78b7	Standard query (0)	tracks.trackingplan.com	A (IP address)	IN (0x0001)
Jan 28, 2022 14:13:17.528856993 CET	192.168.2.3	8.8.8.8	0x80d1	Standard query (0)	distillery.wistia.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 14:11:26.633502007 CET	8.8.8.8	192.168.2.3	0xeb35	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:26.642139912 CET	8.8.8.8	192.168.2.3	0x180	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:11:26.642139912 CET	8.8.8.8	192.168.2.3	0x180	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:26.652848959 CET	8.8.8.8	192.168.2.3	0x535	No error (0)	6v4feb7simf.typeform.com	random.typeform.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:11:27.612962008 CET	8.8.8.8	192.168.2.3	0x6581	No error (0)	images.typeform.com	d2nvsmtq2poimt.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:11:27.612962008 CET	8.8.8.8	192.168.2.3	0x6581	No error (0)	d2nvsmtq2poimt.cloudfront.net		18.66.218.95	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:27.612962008 CET	8.8.8.8	192.168.2.3	0x6581	No error (0)	d2nvsmtq2poimt.cloudfront.net		18.66.218.129	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:27.612962008 CET	8.8.8.8	192.168.2.3	0x6581	No error (0)	d2nvsmtq2poimt.cloudfront.net		18.66.218.9	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:27.612962008 CET	8.8.8.8	192.168.2.3	0x6581	No error (0)	d2nvsmtq2poimt.cloudfront.net		18.66.218.54	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 14:11:27.782454967 CET	8.8.8.8	192.168.2.3	0x5e21	No error (0)	renderer-assets.typeform.com	d2citsn5wf4j9j.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:11:27.782454967 CET	8.8.8.8	192.168.2.3	0x5e21	No error (0)	d2citsn5wf4j9j.cloudfront.net		18.66.196.121	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:27.782454967 CET	8.8.8.8	192.168.2.3	0x5e21	No error (0)	d2citsn5wf4j9j.cloudfront.net		18.66.196.27	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:27.782454967 CET	8.8.8.8	192.168.2.3	0x5e21	No error (0)	d2citsn5wf4j9j.cloudfront.net		18.66.196.80	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:27.782454967 CET	8.8.8.8	192.168.2.3	0x5e21	No error (0)	d2citsn5wf4j9j.cloudfront.net		18.66.196.78	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:28.622694016 CET	8.8.8.8	192.168.2.3	0x8b12	No error (0)	cdn.segment.com	d296je7bbdd650.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:11:28.622694016 CET	8.8.8.8	192.168.2.3	0x8b12	No error (0)	d296je7bbdd650.cloudfront.net		108.139.240.122	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:29.637316942 CET	8.8.8.8	192.168.2.3	0x5db4	No error (0)	api.segment.io		54.149.50.128	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:29.637316942 CET	8.8.8.8	192.168.2.3	0x5db4	No error (0)	api.segment.io		54.71.252.35	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:29.637316942 CET	8.8.8.8	192.168.2.3	0x5db4	No error (0)	api.segment.io		100.20.244.74	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:29.637316942 CET	8.8.8.8	192.168.2.3	0x5db4	No error (0)	api.segment.io		54.149.179.129	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:29.637316942 CET	8.8.8.8	192.168.2.3	0x5db4	No error (0)	api.segment.io		52.33.186.161	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:29.637316942 CET	8.8.8.8	192.168.2.3	0x5db4	No error (0)	api.segment.io		54.69.52.31	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:29.637316942 CET	8.8.8.8	192.168.2.3	0x5db4	No error (0)	api.segment.io		34.223.143.252	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:29.637316942 CET	8.8.8.8	192.168.2.3	0x5db4	No error (0)	api.segment.io		52.35.195.250	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:29.658797026 CET	8.8.8.8	192.168.2.3	0x13e9	No error (0)	public-assets.typeform.com	d2p6vz8nayi9a3.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:11:29.658797026 CET	8.8.8.8	192.168.2.3	0x13e9	No error (0)	d2p6vz8nayi9a3.cloudfront.net		18.66.196.24	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:29.658797026 CET	8.8.8.8	192.168.2.3	0x13e9	No error (0)	d2p6vz8nayi9a3.cloudfront.net		18.66.196.29	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:29.658797026 CET	8.8.8.8	192.168.2.3	0x13e9	No error (0)	d2p6vz8nayi9a3.cloudfront.net		18.66.196.55	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:29.658797026 CET	8.8.8.8	192.168.2.3	0x13e9	No error (0)	d2p6vz8nayi9a3.cloudfront.net		18.66.196.31	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:30.917804956 CET	8.8.8.8	192.168.2.3	0xb071	No error (0)	public-assets.typeform.com	d2p6vz8nayi9a3.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:11:30.917804956 CET	8.8.8.8	192.168.2.3	0xb071	No error (0)	d2p6vz8nayi9a3.cloudfront.net		18.66.196.55	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:30.917804956 CET	8.8.8.8	192.168.2.3	0xb071	No error (0)	d2p6vz8nayi9a3.cloudfront.net		18.66.196.29	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:30.917804956 CET	8.8.8.8	192.168.2.3	0xb071	No error (0)	d2p6vz8nayi9a3.cloudfront.net		18.66.196.24	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:30.917804956 CET	8.8.8.8	192.168.2.3	0xb071	No error (0)	d2p6vz8nayi9a3.cloudfront.net		18.66.196.31	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.312275887 CET	8.8.8.8	192.168.2.3	0xe9d6	No error (0)	www.typeform.com	d2q0tm6nh3syda.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:11:36.312275887 CET	8.8.8.8	192.168.2.3	0xe9d6	No error (0)	d2q0tm6nh3syda.cloudfront.net		18.66.196.93	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 14:11:36.312275887 CET	8.8.8.8	192.168.2.3	0xe9d6	No error (0)	d2q0tm6nh3syda.cloudfront.net		18.66.196.9	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.312275887 CET	8.8.8.8	192.168.2.3	0xe9d6	No error (0)	d2q0tm6nh3syda.cloudfront.net		18.66.196.47	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.312275887 CET	8.8.8.8	192.168.2.3	0xe9d6	No error (0)	d2q0tm6nh3syda.cloudfront.net		18.66.196.90	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.564910889 CET	8.8.8.8	192.168.2.3	0x97c7	No error (0)	cdn.cookielaw.org		104.16.149.64	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.564910889 CET	8.8.8.8	192.168.2.3	0x97c7	No error (0)	cdn.cookielaw.org		104.16.148.64	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.567703962 CET	8.8.8.8	192.168.2.3	0x282a	No error (0)	font.typeform.com	d3m6p8tvnbsibq.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:11:36.567703962 CET	8.8.8.8	192.168.2.3	0x282a	No error (0)	d3m6p8tvnbsibq.cloudfront.net		18.66.218.75	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.567703962 CET	8.8.8.8	192.168.2.3	0x282a	No error (0)	d3m6p8tvnbsibq.cloudfront.net		18.66.218.56	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.567703962 CET	8.8.8.8	192.168.2.3	0x282a	No error (0)	d3m6p8tvnbsibq.cloudfront.net		18.66.218.15	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.567703962 CET	8.8.8.8	192.168.2.3	0x282a	No error (0)	d3m6p8tvnbsibq.cloudfront.net		18.66.218.127	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.636920929 CET	8.8.8.8	192.168.2.3	0x2a29	No error (0)	images.ctfassets.net	d3orhvfyxudxxq.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:11:36.636920929 CET	8.8.8.8	192.168.2.3	0x2a29	No error (0)	d3orhvfyxudxxq.cloudfront.net		108.139.243.33	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.636920929 CET	8.8.8.8	192.168.2.3	0x2a29	No error (0)	d3orhvfyxudxxq.cloudfront.net		108.139.243.42	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.636920929 CET	8.8.8.8	192.168.2.3	0x2a29	No error (0)	d3orhvfyxudxxq.cloudfront.net		108.139.243.97	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.636920929 CET	8.8.8.8	192.168.2.3	0x2a29	No error (0)	d3orhvfyxudxxq.cloudfront.net		108.139.243.45	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.934633017 CET	8.8.8.8	192.168.2.3	0xa9ac	No error (0)	cdn.rollbar.com	d1ftdm4q83us3q.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:11:36.934633017 CET	8.8.8.8	192.168.2.3	0xa9ac	No error (0)	d1ftdm4q83us3q.cloudfront.net		18.66.218.92	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.934633017 CET	8.8.8.8	192.168.2.3	0xa9ac	No error (0)	d1ftdm4q83us3q.cloudfront.net		18.66.218.35	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.934633017 CET	8.8.8.8	192.168.2.3	0xa9ac	No error (0)	d1ftdm4q83us3q.cloudfront.net		18.66.218.40	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.934633017 CET	8.8.8.8	192.168.2.3	0xa9ac	No error (0)	d1ftdm4q83us3q.cloudfront.net		18.66.218.117	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:36.950077057 CET	8.8.8.8	192.168.2.3	0xa1be	No error (0)	www.datadoghq-browser-agent.com		18.66.203.63	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:37.036259890 CET	8.8.8.8	192.168.2.3	0xdba0	No error (0)	www-google tagmanager.l.google.com		172.217.168.8	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:37.279689074 CET	8.8.8.8	192.168.2.3	0xf7c1	No error (0)	polyfill.io		151.101.65.26	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:37.279689074 CET	8.8.8.8	192.168.2.3	0xf7c1	No error (0)	polyfill.io		151.101.1.26	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:37.279689074 CET	8.8.8.8	192.168.2.3	0xf7c1	No error (0)	polyfill.io		151.101.193.26	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:37.279689074 CET	8.8.8.8	192.168.2.3	0xf7c1	No error (0)	polyfill.io		151.101.129.26	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:37.467516899 CET	8.8.8.8	192.168.2.3	0xc412	No error (0)	d3m6p8tvnbsibq.cloudfront.net		18.66.218.127	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 14:11:37.467516899 CET	8.8.8.8	192.168.2.3	0xc412	No error (0)	d3m6p8tvnbsibq.cloudfront.net		18.66.218.75	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:37.467516899 CET	8.8.8.8	192.168.2.3	0xc412	No error (0)	d3m6p8tvnbsibq.cloudfront.net		18.66.218.56	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:37.467516899 CET	8.8.8.8	192.168.2.3	0xc412	No error (0)	d3m6p8tvnbsibq.cloudfront.net		18.66.218.15	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:38.516864061 CET	8.8.8.8	192.168.2.3	0xab3	No error (0)	geolocation.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:38.516864061 CET	8.8.8.8	192.168.2.3	0xab3	No error (0)	geolocation.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:38.618048906 CET	8.8.8.8	192.168.2.3	0xeb86	No error (0)	unpkg.com		104.16.124.175	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:38.618048906 CET	8.8.8.8	192.168.2.3	0xeb86	No error (0)	unpkg.com		104.16.125.175	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:38.618048906 CET	8.8.8.8	192.168.2.3	0xeb86	No error (0)	unpkg.com		104.16.122.175	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:38.618048906 CET	8.8.8.8	192.168.2.3	0xeb86	No error (0)	unpkg.com		104.16.126.175	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:38.618048906 CET	8.8.8.8	192.168.2.3	0xeb86	No error (0)	unpkg.com		104.16.123.175	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:39.504476070 CET	8.8.8.8	192.168.2.3	0xe745	No error (0)	www-google-analytics.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:40.691313028 CET	8.8.8.8	192.168.2.3	0x2994	No error (0)	config.trackingplan.com	d19fvy74nkvmoz.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:11:40.691313028 CET	8.8.8.8	192.168.2.3	0x2994	No error (0)	d19fvy74nkvmoz.cloudfront.net		18.66.218.11	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:40.691313028 CET	8.8.8.8	192.168.2.3	0x2994	No error (0)	d19fvy74nkvmoz.cloudfront.net		18.66.218.4	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:40.691313028 CET	8.8.8.8	192.168.2.3	0x2994	No error (0)	d19fvy74nkvmoz.cloudfront.net		18.66.218.80	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:40.691313028 CET	8.8.8.8	192.168.2.3	0x2994	No error (0)	d19fvy74nkvmoz.cloudfront.net		18.66.218.2	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:42.016252995 CET	8.8.8.8	192.168.2.3	0x2730	No error (0)	www.typeform.com	d2q0tm6nh3syda.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:11:42.016252995 CET	8.8.8.8	192.168.2.3	0x2730	No error (0)	d2q0tm6nh3syda.cloudfront.net		18.66.196.93	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:42.016252995 CET	8.8.8.8	192.168.2.3	0x2730	No error (0)	d2q0tm6nh3syda.cloudfront.net		18.66.196.9	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:42.016252995 CET	8.8.8.8	192.168.2.3	0x2730	No error (0)	d2q0tm6nh3syda.cloudfront.net		18.66.196.47	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:42.016252995 CET	8.8.8.8	192.168.2.3	0x2730	No error (0)	d2q0tm6nh3syda.cloudfront.net		18.66.196.90	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:42.075723886 CET	8.8.8.8	192.168.2.3	0xad7	No error (0)	images.ctfassets.net	d3orhvfyxudxxq.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:11:42.075723886 CET	8.8.8.8	192.168.2.3	0xad7	No error (0)	d3orhvfyxudxxq.cloudfront.net		108.139.243.42	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:42.075723886 CET	8.8.8.8	192.168.2.3	0xad7	No error (0)	d3orhvfyxudxxq.cloudfront.net		108.139.243.33	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:42.075723886 CET	8.8.8.8	192.168.2.3	0xad7	No error (0)	d3orhvfyxudxxq.cloudfront.net		108.139.243.97	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:42.075723886 CET	8.8.8.8	192.168.2.3	0xad7	No error (0)	d3orhvfyxudxxq.cloudfront.net		108.139.243.45	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:42.136338949 CET	8.8.8.8	192.168.2.3	0xa85e	No error (0)	d3m6p8tvnbsibq.cloudfront.net		18.66.218.127	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 14:11:42.136338949 CET	8.8.8.8	192.168.2.3	0xa85e	No error (0)	d3m6p8tvnbsibq.cloudfront.net		18.66.218.75	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:42.136338949 CET	8.8.8.8	192.168.2.3	0xa85e	No error (0)	d3m6p8tvnbsibq.cloudfront.net		18.66.218.56	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:42.136338949 CET	8.8.8.8	192.168.2.3	0xa85e	No error (0)	d3m6p8tvnbsibq.cloudfront.net		18.66.218.15	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:42.147732973 CET	8.8.8.8	192.168.2.3	0x7683	No error (0)	cdn.cookielaw.org		104.16.149.64	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:42.147732973 CET	8.8.8.8	192.168.2.3	0x7683	No error (0)	cdn.cookielaw.org		104.16.148.64	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:42.984280109 CET	8.8.8.8	192.168.2.3	0xe43a	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:11:42.984280109 CET	8.8.8.8	192.168.2.3	0xe43a	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:43.888356924 CET	8.8.8.8	192.168.2.3	0x80e2	No error (0)	tracks.trackingplan.com		3.224.204.97	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:43.888356924 CET	8.8.8.8	192.168.2.3	0x80e2	No error (0)	tracks.trackingplan.com		52.207.36.48	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:55.507631063 CET	8.8.8.8	192.168.2.3	0x6322	No error (0)	public.profitwell.com	dna8twue3dlxq.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:11:55.507631063 CET	8.8.8.8	192.168.2.3	0x6322	No error (0)	dna8twue3dlxq.cloudfront.net		18.66.196.79	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:55.507631063 CET	8.8.8.8	192.168.2.3	0x6322	No error (0)	dna8twue3dlxq.cloudfront.net		18.66.196.119	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:55.507631063 CET	8.8.8.8	192.168.2.3	0x6322	No error (0)	dna8twue3dlxq.cloudfront.net		18.66.196.74	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:55.507631063 CET	8.8.8.8	192.168.2.3	0x6322	No error (0)	dna8twue3dlxq.cloudfront.net		18.66.196.10	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:58.048718929 CET	8.8.8.8	192.168.2.3	0xb43c	No error (0)	pixel.stretmetrics.io		104.21.11.153	A (IP address)	IN (0x0001)
Jan 28, 2022 14:11:58.048718929 CET	8.8.8.8	192.168.2.3	0xb43c	No error (0)	pixel.stretmetrics.io		172.67.166.95	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:03.967839956 CET	8.8.8.8	192.168.2.3	0xd444	No error (0)	pixel.stretmetrics.io		104.21.11.153	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:03.967839956 CET	8.8.8.8	192.168.2.3	0xd444	No error (0)	pixel.stretmetrics.io		172.67.166.95	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:15.849034071 CET	8.8.8.8	192.168.2.3	0x7b60	No error (0)	fast.wistia.com	dualstack.f4.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:12:17.497668028 CET	8.8.8.8	192.168.2.3	0xf261	No error (0)	distillery.wistia.com	prod-east-stats-tap-alb-627711272.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:12:17.497668028 CET	8.8.8.8	192.168.2.3	0xf261	No error (0)	prod-east-stats-tap-alb-627711272.us-east-1.elb.amazonaws.com		54.86.117.43	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:17.497668028 CET	8.8.8.8	192.168.2.3	0xf261	No error (0)	prod-east-stats-tap-alb-627711272.us-east-1.elb.amazonaws.com		52.86.94.156	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:17.729088068 CET	8.8.8.8	192.168.2.3	0x1c52	No error (0)	embed-fastly.wistia.com	d.sni.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:12:21.132042885 CET	8.8.8.8	192.168.2.3	0x7550	No error (0)	admin.typeform.com	admin.typeform.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:12:21.680571079 CET	8.8.8.8	192.168.2.3	0xfc1c	No error (0)	d2cjrwb117kaxb.cloudfront.net		18.66.218.54	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:21.680571079 CET	8.8.8.8	192.168.2.3	0xfc1c	No error (0)	d2cjrwb117kaxb.cloudfront.net		18.66.218.37	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 14:12:21.680571079 CET	8.8.8.8	192.168.2.3	0xfc1c	No error (0)	d2cjrwb117kaxb.cloudfront.net		18.66.218.97	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:21.680571079 CET	8.8.8.8	192.168.2.3	0xfc1c	No error (0)	d2cjrwb117kaxb.cloudfront.net		18.66.218.32	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:21.686961889 CET	8.8.8.8	192.168.2.3	0xc5fd	No error (0)	endpoint2.collection.us2.sumologic.com	us2-events-2-1917544754.us-west-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:12:21.686961889 CET	8.8.8.8	192.168.2.3	0xc5fd	No error (0)	us2-events-2-1917544754.us-west-2.elb.amazonaws.com		52.26.89.215	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:21.686961889 CET	8.8.8.8	192.168.2.3	0xc5fd	No error (0)	us2-events-2-1917544754.us-west-2.elb.amazonaws.com		35.81.60.248	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:21.686961889 CET	8.8.8.8	192.168.2.3	0xc5fd	No error (0)	us2-events-2-1917544754.us-west-2.elb.amazonaws.com		54.201.153.89	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:21.686961889 CET	8.8.8.8	192.168.2.3	0xc5fd	No error (0)	us2-events-2-1917544754.us-west-2.elb.amazonaws.com		35.83.133.155	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:21.686961889 CET	8.8.8.8	192.168.2.3	0xc5fd	No error (0)	us2-events-2-1917544754.us-west-2.elb.amazonaws.com		52.34.151.97	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:21.686961889 CET	8.8.8.8	192.168.2.3	0xc5fd	No error (0)	us2-events-2-1917544754.us-west-2.elb.amazonaws.com		35.167.144.138	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:21.686961889 CET	8.8.8.8	192.168.2.3	0xc5fd	No error (0)	us2-events-2-1917544754.us-west-2.elb.amazonaws.com		52.12.231.71	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:21.686961889 CET	8.8.8.8	192.168.2.3	0xc5fd	No error (0)	us2-events-2-1917544754.us-west-2.elb.amazonaws.com		35.161.190.194	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:21.704523087 CET	8.8.8.8	192.168.2.3	0x9829	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:21.704523087 CET	8.8.8.8	192.168.2.3	0x9829	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:22.244441986 CET	8.8.8.8	192.168.2.3	0x395	No error (0)	cdn.optimizely.com	cdn.o6.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:12:30.978835106 CET	8.8.8.8	192.168.2.3	0x6d69	No error (0)	auth.typeform.com	typeform.customdomains.okta.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:12:30.978835106 CET	8.8.8.8	192.168.2.3	0x6d69	No error (0)	typeform.customdomains.okta.com	ok11-custom-crtrs.okta.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:12:30.978835106 CET	8.8.8.8	192.168.2.3	0x6d69	No error (0)	ok11-custom-crtrs.okta.com	ok11-crtr-custom-domains-cd76c2bd4d92725a.elb.us-east-2.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:12:30.978835106 CET	8.8.8.8	192.168.2.3	0x6d69	No error (0)	ok11-crtr-custom-domains-cd76c2bd4d92725a.elb.us-east-2.amazonaws.com		3.15.36.195	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:30.978835106 CET	8.8.8.8	192.168.2.3	0x6d69	No error (0)	ok11-crtr-custom-domains-cd76c2bd4d92725a.elb.us-east-2.amazonaws.com		3.15.36.196	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 14:12:30.978835106 CET	8.8.8.8	192.168.2.3	0x6d69	No error (0)	ok11-crtr-custom-domains-cd76c2bd4d92725a.elb.us-east-2.amazonaws.com		3.15.36.199	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:30.990870953 CET	8.8.8.8	192.168.2.3	0x1b6	No error (0)	public-assets.typeform.com	d2p6vz8nayi9a3.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:12:30.990870953 CET	8.8.8.8	192.168.2.3	0x1b6	No error (0)	d2p6vz8nayi9a3.cloudfront.net		18.66.196.29	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:30.990870953 CET	8.8.8.8	192.168.2.3	0x1b6	No error (0)	d2p6vz8nayi9a3.cloudfront.net		18.66.196.24	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:30.990870953 CET	8.8.8.8	192.168.2.3	0x1b6	No error (0)	d2p6vz8nayi9a3.cloudfront.net		18.66.196.55	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:30.990870953 CET	8.8.8.8	192.168.2.3	0x1b6	No error (0)	d2p6vz8nayi9a3.cloudfront.net		18.66.196.31	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:37.392621040 CET	8.8.8.8	192.168.2.3	0x9c89	No error (0)	www.typeform.com	d2q0tm6nh3syda.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:12:37.392621040 CET	8.8.8.8	192.168.2.3	0x9c89	No error (0)	d2q0tm6nh3syda.cloudfront.net		18.66.196.90	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:37.392621040 CET	8.8.8.8	192.168.2.3	0x9c89	No error (0)	d2q0tm6nh3syda.cloudfront.net		18.66.196.9	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:37.392621040 CET	8.8.8.8	192.168.2.3	0x9c89	No error (0)	d2q0tm6nh3syda.cloudfront.net		18.66.196.93	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:37.392621040 CET	8.8.8.8	192.168.2.3	0x9c89	No error (0)	d2q0tm6nh3syda.cloudfront.net		18.66.196.47	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:37.786091089 CET	8.8.8.8	192.168.2.3	0xca24	No error (0)	images.ctfassets.net	d3orhvfyxudxxq.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:12:37.786091089 CET	8.8.8.8	192.168.2.3	0xca24	No error (0)	d3orhvfyxudxxq.cloudfront.net		108.139.243.33	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:37.786091089 CET	8.8.8.8	192.168.2.3	0xca24	No error (0)	d3orhvfyxudxxq.cloudfront.net		108.139.243.45	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:37.786091089 CET	8.8.8.8	192.168.2.3	0xca24	No error (0)	d3orhvfyxudxxq.cloudfront.net		108.139.243.97	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:37.786091089 CET	8.8.8.8	192.168.2.3	0xca24	No error (0)	d3orhvfyxudxxq.cloudfront.net		108.139.243.42	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:38.054856062 CET	8.8.8.8	192.168.2.3	0xe057	No error (0)	cdn.cookielaw.org		104.16.149.64	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:38.054856062 CET	8.8.8.8	192.168.2.3	0xe057	No error (0)	cdn.cookielaw.org		104.16.148.64	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:39.701322079 CET	8.8.8.8	192.168.2.3	0xd123	No error (0)	font.typeform.com	d3m6p8tvnbsibq.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:12:39.701322079 CET	8.8.8.8	192.168.2.3	0xd123	No error (0)	d3m6p8tvnbsibq.cloudfront.net		18.66.218.127	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:39.701322079 CET	8.8.8.8	192.168.2.3	0xd123	No error (0)	d3m6p8tvnbsibq.cloudfront.net		18.66.218.15	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:39.701322079 CET	8.8.8.8	192.168.2.3	0xd123	No error (0)	d3m6p8tvnbsibq.cloudfront.net		18.66.218.56	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:39.701322079 CET	8.8.8.8	192.168.2.3	0xd123	No error (0)	d3m6p8tvnbsibq.cloudfront.net		18.66.218.75	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.627573967 CET	8.8.8.8	192.168.2.3	0xcaec	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.731513977 CET	8.8.8.8	192.168.2.3	0xf97f	No error (0)	snap.licdn.com	od.linkedin.edgesuite.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 14:12:43.731688023 CET	8.8.8.8	192.168.2.3	0xce8	No error (0)	js.hs-scripts.com		104.17.210.204	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.731688023 CET	8.8.8.8	192.168.2.3	0xce8	No error (0)	js.hs-scripts.com		104.17.211.204	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.731688023 CET	8.8.8.8	192.168.2.3	0xce8	No error (0)	js.hs-scripts.com		104.17.214.204	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.731688023 CET	8.8.8.8	192.168.2.3	0xce8	No error (0)	js.hs-scripts.com		104.17.212.204	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.731688023 CET	8.8.8.8	192.168.2.3	0xce8	No error (0)	js.hs-scripts.com		104.17.213.204	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.732825041 CET	8.8.8.8	192.168.2.3	0x4858	No error (0)	reveal.clearbit.com		52.56.230.239	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.732825041 CET	8.8.8.8	192.168.2.3	0x4858	No error (0)	reveal.clearbit.com		18.135.20.243	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.741009951 CET	8.8.8.8	192.168.2.3	0x7c5f	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:12:43.741009951 CET	8.8.8.8	192.168.2.3	0x7c5f	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.773293018 CET	8.8.8.8	192.168.2.3	0xda49	No error (0)	dx.mountain.com		52.88.179.26	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.773293018 CET	8.8.8.8	192.168.2.3	0xda49	No error (0)	dx.mountain.com		35.83.209.52	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.773293018 CET	8.8.8.8	192.168.2.3	0xda49	No error (0)	dx.mountain.com		44.238.33.223	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.773293018 CET	8.8.8.8	192.168.2.3	0xda49	No error (0)	dx.mountain.com		54.69.255.140	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.773293018 CET	8.8.8.8	192.168.2.3	0xda49	No error (0)	dx.mountain.com		44.240.152.58	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.773293018 CET	8.8.8.8	192.168.2.3	0xda49	No error (0)	dx.mountain.com		54.190.217.118	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.774442911 CET	8.8.8.8	192.168.2.3	0xd030	No error (0)	tags.srv.stackadapt.com		52.204.174.192	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.774442911 CET	8.8.8.8	192.168.2.3	0xd030	No error (0)	tags.srv.stackadapt.com		50.16.242.140	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.774442911 CET	8.8.8.8	192.168.2.3	0xd030	No error (0)	tags.srv.stackadapt.com		44.193.136.195	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.774442911 CET	8.8.8.8	192.168.2.3	0xd030	No error (0)	tags.srv.stackadapt.com		54.162.122.226	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.779556990 CET	8.8.8.8	192.168.2.3	0xfd2	No error (0)	cdn.segment.com	d296je7bbdd650.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:12:43.779556990 CET	8.8.8.8	192.168.2.3	0xfd2	No error (0)	d296je7bbdd650.cloudfront.net		108.139.240.122	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.781688929 CET	8.8.8.8	192.168.2.3	0x8f0f	No error (0)	ws.zoominfo.com		104.16.168.82	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.781688929 CET	8.8.8.8	192.168.2.3	0x8f0f	No error (0)	ws.zoominfo.com		104.16.101.12	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.798604012 CET	8.8.8.8	192.168.2.3	0xf521	No error (0)	privacyportal-de.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.798604012 CET	8.8.8.8	192.168.2.3	0xf521	No error (0)	privacyportal-de.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.800209999 CET	8.8.8.8	192.168.2.3	0xee2e	No error (0)	logx.optimizely.com	p13nlog-1106815646.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:12:43.800209999 CET	8.8.8.8	192.168.2.3	0xee2e	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		52.2.252.209	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.800209999 CET	8.8.8.8	192.168.2.3	0xee2e	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		52.201.68.224	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.800209999 CET	8.8.8.8	192.168.2.3	0xee2e	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		52.23.68.152	A (IP address)	IN (0x0001)

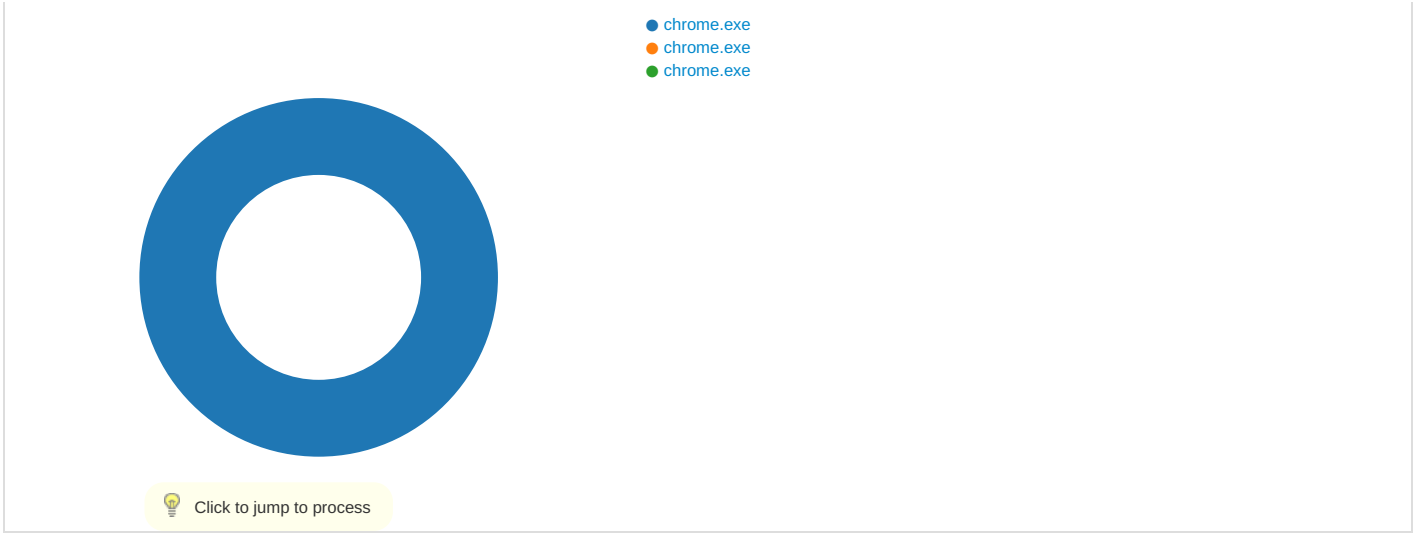
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 14:12:43.800209999 CET	8.8.8.8	192.168.2.3	0xee2e	No error (0)	p13nlog-11 06815646.us-east-1.e lb.amazona ws.com		54.210.193.118	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.800209999 CET	8.8.8.8	192.168.2.3	0xee2e	No error (0)	p13nlog-11 06815646.us-east-1.e lb.amazona ws.com		52.2.215.210	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.800209999 CET	8.8.8.8	192.168.2.3	0xee2e	No error (0)	p13nlog-11 06815646.us-east-1.e lb.amazona ws.com		18.214.155.228	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.800209999 CET	8.8.8.8	192.168.2.3	0xee2e	No error (0)	p13nlog-11 06815646.us-east-1.e lb.amazona ws.com		34.199.209.94	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.800209999 CET	8.8.8.8	192.168.2.3	0xee2e	No error (0)	p13nlog-11 06815646.us-east-1.e lb.amazona ws.com		54.90.25.171	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.840259075 CET	8.8.8.8	192.168.2.3	0x3068	No error (0)	googleads. g.doubleclick.net		172.217.168.66	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.849050045 CET	8.8.8.8	192.168.2.3	0xea87	No error (0)	x.clearbitjs.com	global-v2.clearbit.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:12:43.849050045 CET	8.8.8.8	192.168.2.3	0xea87	No error (0)	global-v2. clearbit.com		52.56.230.239	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.849050045 CET	8.8.8.8	192.168.2.3	0xea87	No error (0)	global-v2. clearbit.com		18.135.20.243	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.984332085 CET	8.8.8.8	192.168.2.3	0x1f72	No error (0)	px.ads.lin kedin.com	www.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:12:43.984332085 CET	8.8.8.8	192.168.2.3	0x1f72	No error (0)	www.linked in.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:12:43.992690086 CET	8.8.8.8	192.168.2.3	0x5ac2	No error (0)	stats.g.do ubleclick.net	stats.l.doubleclick. net		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:12:43.992690086 CET	8.8.8.8	192.168.2.3	0x5ac2	No error (0)	stats.l.do ubleclick.net		108.177.127.155	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.992690086 CET	8.8.8.8	192.168.2.3	0x5ac2	No error (0)	stats.l.do ubleclick.net		108.177.127.157	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.992690086 CET	8.8.8.8	192.168.2.3	0x5ac2	No error (0)	stats.l.do ubleclick.net		108.177.127.156	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:43.992690086 CET	8.8.8.8	192.168.2.3	0x5ac2	No error (0)	stats.l.do ubleclick.net		108.177.127.154	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.207829952 CET	8.8.8.8	192.168.2.3	0xb835	No error (0)	10579985.f ls.doubleclick.net	dart.l.doubleclick.n et		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:12:44.207829952 CET	8.8.8.8	192.168.2.3	0xb835	No error (0)	dart.l.dou bleclick.net		142.250.203.102	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.238337994 CET	8.8.8.8	192.168.2.3	0x467b	No error (0)	js.hs-anal ytics.net		104.17.68.176	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.238337994 CET	8.8.8.8	192.168.2.3	0x467b	No error (0)	js.hs-anal ytics.net		104.17.67.176	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.238337994 CET	8.8.8.8	192.168.2.3	0x467b	No error (0)	js.hs-anal ytics.net		104.17.69.176	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.238337994 CET	8.8.8.8	192.168.2.3	0x467b	No error (0)	js.hs-anal ytics.net		104.17.70.176	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.238337994 CET	8.8.8.8	192.168.2.3	0x467b	No error (0)	js.hs-anal ytics.net		104.17.71.176	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.239109993 CET	8.8.8.8	192.168.2.3	0x40e2	No error (0)	js.hs-bann er.com		104.18.20.191	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.239109993 CET	8.8.8.8	192.168.2.3	0x40e2	No error (0)	js.hs-bann er.com		104.18.21.191	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.248919010 CET	8.8.8.8	192.168.2.3	0xcc84	No error (0)	www.google.ch		172.217.168.35	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.275022984 CET	8.8.8.8	192.168.2.3	0x240	No error (0)	www.linked in.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 14:12:44.454586983 CET	8.8.8.8	192.168.2.3	0x9496	No error (0)	track.hubspot.com		104.19.155.83	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.454586983 CET	8.8.8.8	192.168.2.3	0x9496	No error (0)	track.hubspot.com		104.19.154.83	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.785737038 CET	8.8.8.8	192.168.2.3	0x3a37	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:12:44.785737038 CET	8.8.8.8	192.168.2.3	0x3a37	No error (0)	star-mini.c10r.facebook.com		157.240.17.35	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.906059027 CET	8.8.8.8	192.168.2.3	0xe3d4	No error (0)	api.segment.io		52.11.156.223	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.906059027 CET	8.8.8.8	192.168.2.3	0xe3d4	No error (0)	api.segment.io		52.88.208.102	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.906059027 CET	8.8.8.8	192.168.2.3	0xe3d4	No error (0)	api.segment.io		52.43.15.143	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.906059027 CET	8.8.8.8	192.168.2.3	0xe3d4	No error (0)	api.segment.io		52.89.95.104	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.906059027 CET	8.8.8.8	192.168.2.3	0xe3d4	No error (0)	api.segment.io		54.201.25.196	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.906059027 CET	8.8.8.8	192.168.2.3	0xe3d4	No error (0)	api.segment.io		35.164.88.121	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.906059027 CET	8.8.8.8	192.168.2.3	0xe3d4	No error (0)	api.segment.io		54.71.192.93	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.906059027 CET	8.8.8.8	192.168.2.3	0xe3d4	No error (0)	api.segment.io		52.38.212.85	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.963460922 CET	8.8.8.8	192.168.2.3	0xe17c	No error (0)	edge.fullstory.com		35.201.112.186	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.963494062 CET	8.8.8.8	192.168.2.3	0xe603	No error (0)	cdn.amplitude.com		108.156.0.174	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.963494062 CET	8.8.8.8	192.168.2.3	0xe603	No error (0)	cdn.amplitude.com		108.156.0.206	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.963494062 CET	8.8.8.8	192.168.2.3	0xe603	No error (0)	cdn.amplitude.com		108.156.0.53	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.963494062 CET	8.8.8.8	192.168.2.3	0xe603	No error (0)	cdn.amplitude.com		108.156.0.133	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.967375040 CET	8.8.8.8	192.168.2.3	0xf557	No error (0)	px.mountain.com		52.42.124.195	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.967375040 CET	8.8.8.8	192.168.2.3	0xf557	No error (0)	px.mountain.com		35.81.173.170	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.967375040 CET	8.8.8.8	192.168.2.3	0xf557	No error (0)	px.mountain.com		44.235.191.156	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.967375040 CET	8.8.8.8	192.168.2.3	0xf557	No error (0)	px.mountain.com		34.210.219.79	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.967375040 CET	8.8.8.8	192.168.2.3	0xf557	No error (0)	px.mountain.com		52.89.99.220	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.967375040 CET	8.8.8.8	192.168.2.3	0xf557	No error (0)	px.mountain.com		35.85.106.161	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:44.967375040 CET	8.8.8.8	192.168.2.3	0xf557	No error (0)	px.mountain.com		52.37.218.4	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:45.213989973 CET	8.8.8.8	192.168.2.3	0x3c3b	No error (0)	x.clearbit.com		52.56.230.239	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:45.213989973 CET	8.8.8.8	192.168.2.3	0x3c3b	No error (0)	x.clearbit.com		18.135.20.243	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:45.275006056 CET	8.8.8.8	192.168.2.3	0xd048	No error (0)	rs.fullstory.com		35.186.194.58	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:45.720405102 CET	8.8.8.8	192.168.2.3	0x7c8c	No error (0)	adservice.google.com		172.217.168.2	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:45.777513981 CET	8.8.8.8	192.168.2.3	0x1da8	No error (0)	gs.mountain.com		34.212.4.35	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:45.777513981 CET	8.8.8.8	192.168.2.3	0x1da8	No error (0)	gs.mountain.com		35.81.162.201	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:45.777513981 CET	8.8.8.8	192.168.2.3	0x1da8	No error (0)	gs.mountain.com		52.12.117.226	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:45.935868025 CET	8.8.8.8	192.168.2.3	0x287b	No error (0)	api.amplitude.com		54.149.64.13	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:45.935868025 CET	8.8.8.8	192.168.2.3	0x287b	No error (0)	api.amplitude.com		52.25.249.66	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:45.935868025 CET	8.8.8.8	192.168.2.3	0x287b	No error (0)	api.amplitude.com		54.148.216.244	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 14:12:45.935868025 CET	8.8.8.8	192.168.2.3	0x287b	No error (0)	api.amplitude.com		35.83.9.142	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:45.935868025 CET	8.8.8.8	192.168.2.3	0x287b	No error (0)	api.amplitude.com		44.235.17.170	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:45.935868025 CET	8.8.8.8	192.168.2.3	0x287b	No error (0)	api.amplitude.com		44.229.21.222	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:45.935868025 CET	8.8.8.8	192.168.2.3	0x287b	No error (0)	api.amplitude.com		52.26.226.86	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:45.935868025 CET	8.8.8.8	192.168.2.3	0x287b	No error (0)	api.amplitude.com		52.10.133.216	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:47.470156908 CET	8.8.8.8	192.168.2.3	0xc2c9	No error (0)	match.adsrvr.org		52.223.40.198	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:47.470156908 CET	8.8.8.8	192.168.2.3	0xc2c9	No error (0)	match.adsrvr.org		35.71.131.137	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:47.470156908 CET	8.8.8.8	192.168.2.3	0xc2c9	No error (0)	match.adsrvr.org		15.197.193.217	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:47.470156908 CET	8.8.8.8	192.168.2.3	0xc2c9	No error (0)	match.adsrvr.org		3.33.220.150	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:47.472815037 CET	8.8.8.8	192.168.2.3	0x455	No error (0)	insight.adsrvr.org		52.223.40.198	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:47.472815037 CET	8.8.8.8	192.168.2.3	0x455	No error (0)	insight.adsrvr.org		35.71.131.137	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:47.472815037 CET	8.8.8.8	192.168.2.3	0x455	No error (0)	insight.adsrvr.org		15.197.193.217	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:47.472815037 CET	8.8.8.8	192.168.2.3	0x455	No error (0)	insight.adsrvr.org		3.33.220.150	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:48.043325901 CET	8.8.8.8	192.168.2.3	0xf899	No error (0)	px.steelhousemedia.com		44.237.157.168	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:48.043325901 CET	8.8.8.8	192.168.2.3	0xf899	No error (0)	px.steelhousemedia.com		44.225.29.129	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:48.043325901 CET	8.8.8.8	192.168.2.3	0xf899	No error (0)	px.steelhousemedia.com		44.233.136.7	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:48.043325901 CET	8.8.8.8	192.168.2.3	0xf899	No error (0)	px.steelhousemedia.com		35.82.204.11	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:48.043325901 CET	8.8.8.8	192.168.2.3	0xf899	No error (0)	px.steelhousemedia.com		54.244.159.189	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:48.043325901 CET	8.8.8.8	192.168.2.3	0xf899	No error (0)	px.steelhousemedia.com		52.10.121.135	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:48.043325901 CET	8.8.8.8	192.168.2.3	0xf899	No error (0)	px.steelhousemedia.com		54.245.46.233	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:56.038065910 CET	8.8.8.8	192.168.2.3	0x8e17	No error (0)	adservice.google.com		142.250.203.98	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:58.845690966 CET	8.8.8.8	192.168.2.3	0x78b7	No error (0)	tracks.trackingplan.com		34.226.250.102	A (IP address)	IN (0x0001)
Jan 28, 2022 14:12:58.845690966 CET	8.8.8.8	192.168.2.3	0x78b7	No error (0)	tracks.trackingplan.com		52.207.126.81	A (IP address)	IN (0x0001)
Jan 28, 2022 14:13:17.548682928 CET	8.8.8.8	192.168.2.3	0x80d1	No error (0)	distillery.wistia.com	prod-east-stats-tap-alb-627711272.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 14:13:17.548682928 CET	8.8.8.8	192.168.2.3	0x80d1	No error (0)	prod-east-stats-tap-alb-627711272.us-east-1.elb.amazonaws.com		52.86.94.156	A (IP address)	IN (0x0001)
Jan 28, 2022 14:13:17.548682928 CET	8.8.8.8	192.168.2.3	0x80d1	No error (0)	prod-east-stats-tap-alb-627711272.us-east-1.elb.amazonaws.com		54.86.117.43	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **6760**, Parent PID: **3312**

General

Target ID:	0
Start time:	14:11:22
Start date:	28/01/2022
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 "https://6v4feb7simf.typeform.com/to/v3GA1r6t
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: **6956**, Parent PID: **6760**

General

Target ID:	2
Start time:	14:11:24
Start date:	28/01/2022
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=1584,15928684533581983461,16347382913123571543,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1920 /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

Analysis Process: chrome.exe PID: **6504**, Parent PID: **6760**

General

Target ID:	11
Start time:	14:12:17
Start date:	28/01/2022
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=audio.mojom.AudioService --field-trial-handle=1584,15928684533581983461,16347382913123571543,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=5536 /prefetch:8
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

No disassembly