ID: 562519
Cookbook: browseurl.jbs
Time: 00:02:02
Date: 29/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

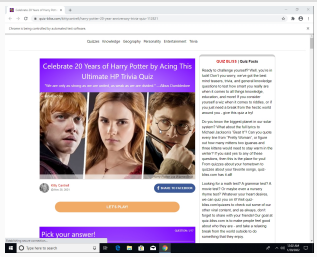
Windows Analysis Report

https://www.quiz-bliss.com/kittycantrell/harry-potter-20-year-anniversary-trivia-quiz-112821

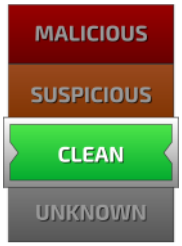
Overview

General Information

Sample URL:	http://https://www.quiz-bliss.com/kittycantrell/harry-potter-20-year-anniversary-trivia-quiz-112821
Analysis ID:	562519
Infos:	



Detection

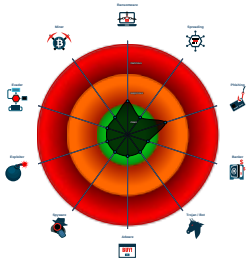


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Suspicious form URL found
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6516 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "https://www.quiz-bliss.com/kittycantrell/harry-potter-20-year-anniversary-trivia-quiz-112821 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6740 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1536,9302057933297055962,10316816090944240565,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1924 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

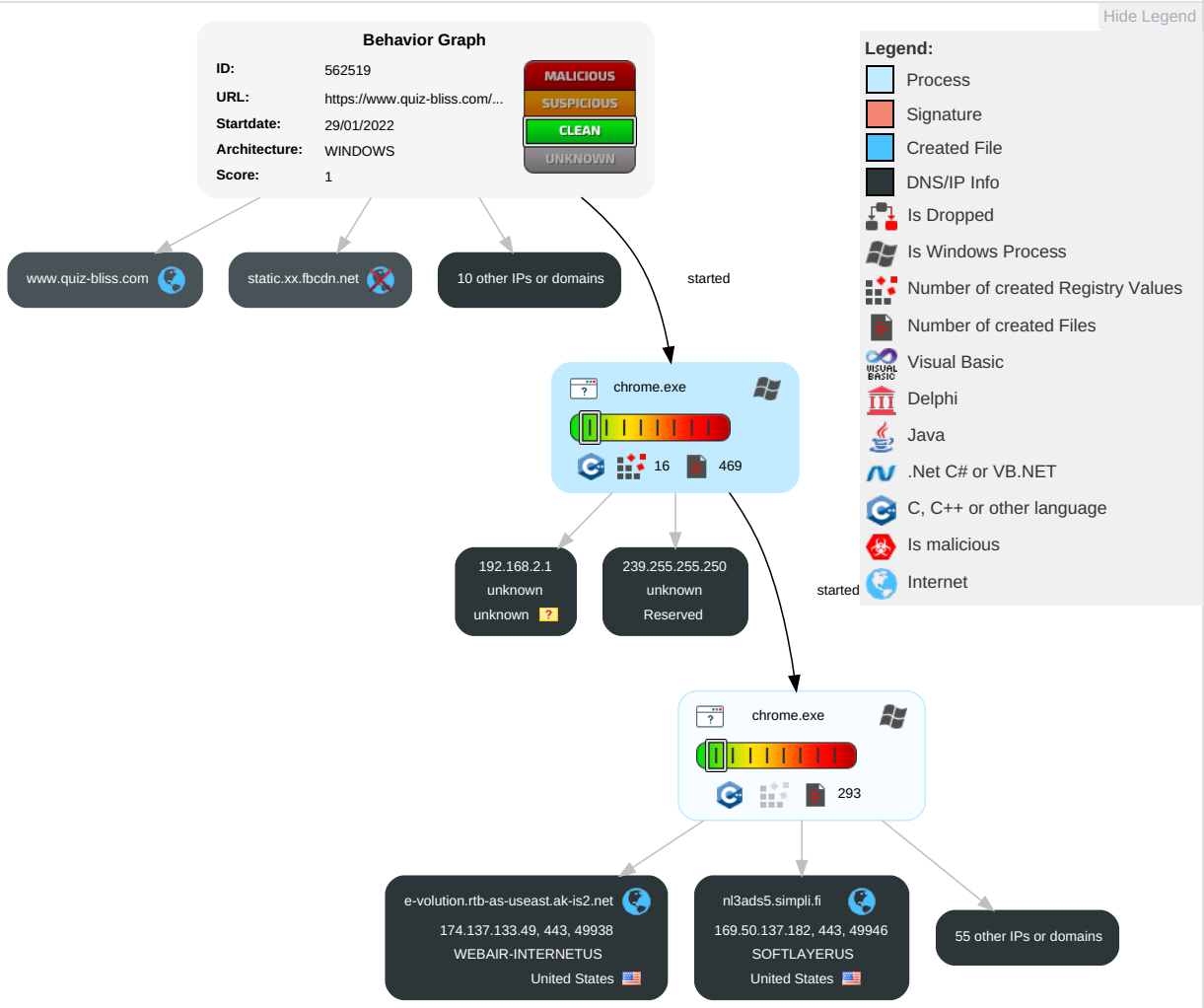
Jbx Signature Overview

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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)	1 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

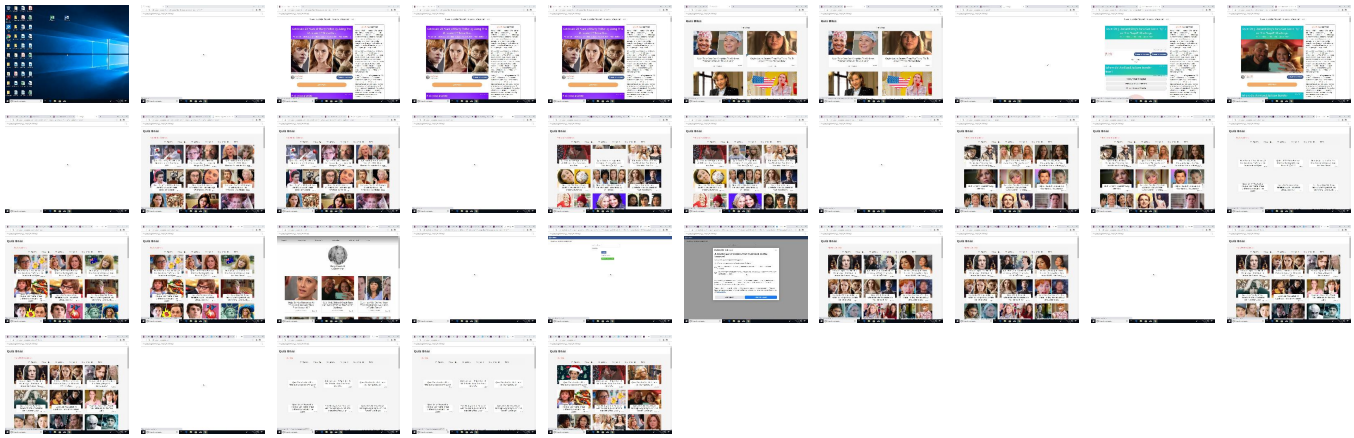
Behavior Graph

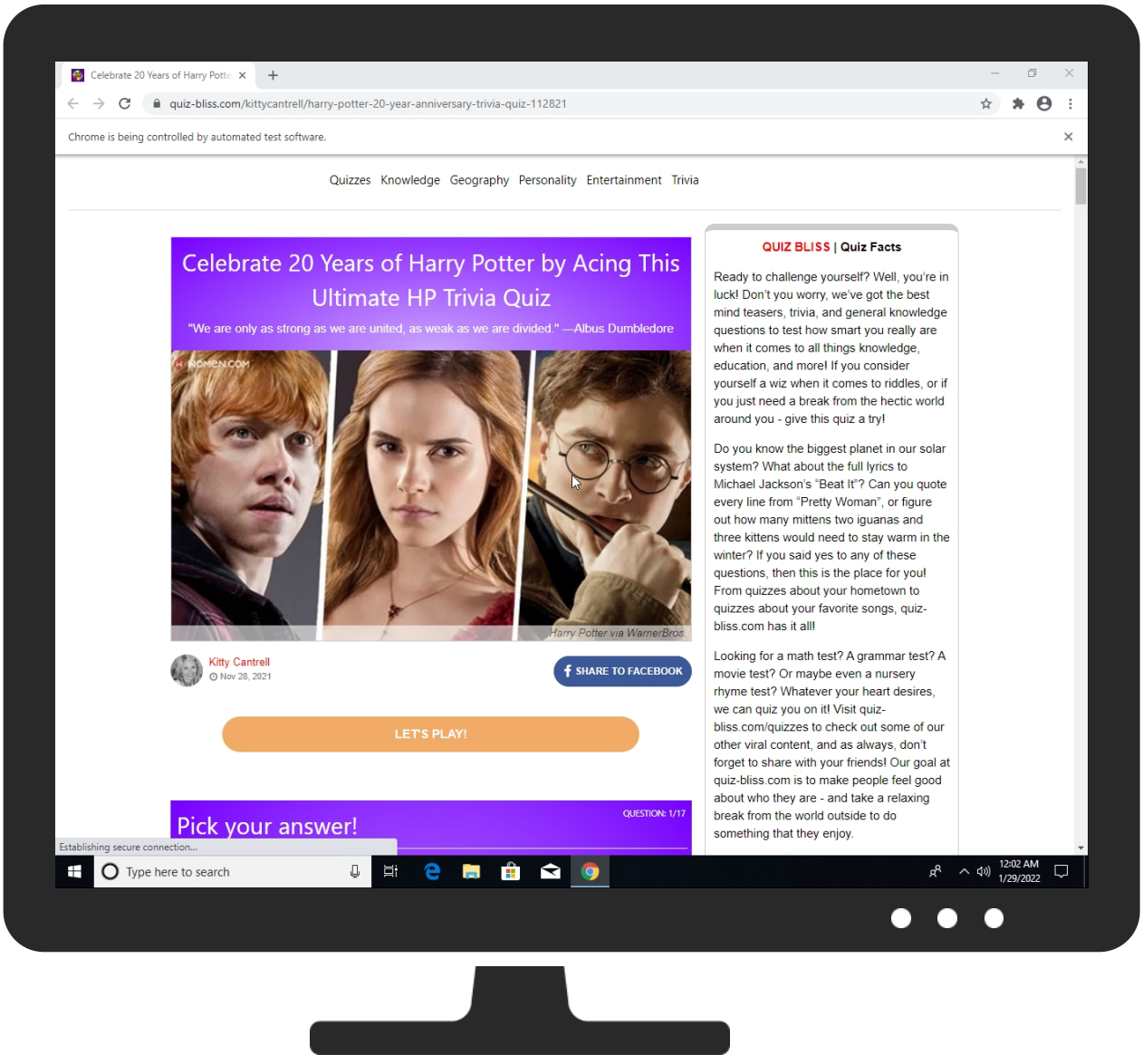


Screenshots

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://www.quiz-bliss.com/kittycantrell/harry-potter-20-year-anniversary-trivia-quiz-112821	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.quiz-bliss.com/	0%	Virustotal		Browse
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://www.quiz-bliss.com/kittycantrell/harry-potter-20-year-anniversary-trivia-quiz-1128212YCelebr	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	216.58.215.227	true	false		high
um.wbtrk.net	127.0.0.2	true	false		unknown
s.tribalfusion.com	104.18.13.5	true	false		high
tr.blismedia.com	34.96.105.8	true	false		unknown
media-gcp.women.com	35.186.224.64	true	false		high
www.googletagservices.com	172.217.168.2	true	false		high
www.quiz-bliss.com	130.211.6.0	true	false		unknown
adservice.google.com	142.250.203.98	true	false		high
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
cm.g.doubleclick.net	172.217.168.34	true	false		high
tg.dr.socdm.com	202.241.208.100	true	false		high
www.google.com	142.250.203.100	true	false		high
eu2-ice.360yield.com	18.197.199.94	true	false		high
e-volution.rtb-as-useast.ak-is2.net	174.137.133.49	true	false		unknown
star-mini.c10r.facebook.com	157.240.17.35	true	false		high
pagead46.l.doubleclick.net	142.250.203.98	true	false		high
pagead-googlehosted.l.google.com	172.217.168.65	true	false		high
accounts.google.com	142.250.203.109	true	false		high
www-google-analytics.l.google.com	142.250.203.110	true	false		high
googleads4.g.doubleclick.net	172.217.168.66	true	false		high
img.women.com	34.98.97.49	true	false		high
nl3ads5.simpli.fi	169.50.137.182	true	false		high
cs.media.net	184.87.212.24	true	false		high
partnerad.l.doubleclick.net	172.217.168.66	true	false		high
s0-2mdn-net.l.google.com	172.217.168.6	true	false		high
googleads.g.doubleclick.net	172.217.168.2	true	false		high
cs.emxdgt.com	18.195.155.181	true	false		unknown
s.ad.smaato.net	143.204.215.20	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
a.tribalfusion.com	104.18.12.5	true	false		high
sb.scorecardresearch.com	143.204.215.108	true	false		unknown
clients.l.google.com	142.250.203.110	true	false		high
ib.anycast.adnxs.com	185.33.221.13	true	false		high
googlehosted.l.googleusercontent.com	172.217.168.33	true	false		high
securepubads.g.doubleclick.net	unknown	unknown	false		high
um.simpli.fi	unknown	unknown	false		high
htlb.casalemedia.com	unknown	unknown	false		high
a.rfihub.com	unknown	unknown	false		high
fastlane.rubiconproject.com	unknown	unknown	false		high
adservice.google.co.uk	unknown	unknown	false		unknown
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
rtb2-useast.e-volution.ai	unknown	unknown	false		unknown
www.facebook.com	unknown	unknown	false		high
cdn-heroku.women.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
px.ads.linkedin.com	unknown	unknown	false		high
static.xx.fbcdn.net	unknown	unknown	false		high
tg.socdm.com	unknown	unknown	false		high
dsum-sec.casalemedia.com	unknown	unknown	false		high
s.pinimg.com	unknown	unknown	false		high
ib.adnxs.com	unknown	unknown	false		high
match.360yield.com	unknown	unknown	false		high
s0.2mdn.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://s0.2mdn.net/sadbundle/11288944710048972181/300x250-en/index.html	false		high
http://https://googleads.g.doubleclick.net/xbbe/pixel?d=CKi2gLICELWvmbICGJK0-78BMAE&v=APEucNU7Y7rRXHnNhkvcuUveQ6PCY04sEqUwGAnKQEIBoX3YcRtRU26fnK4nY9LHWgxgw9_EM4r5pUwMRrzveMSPRUUdUPew8g	false		high
http://https://www.quiz-bliss.com/quizzes/harry%20potter	false		unknown
http://https://googleads.g.doubleclick.net/xbbe/pixel?d=CKi2gLICELWvmbICGJK0-78BMAE&v=APEucNXD8VqIQag_88xrraiQBA3nM2WEC1ntwSS7HNbeN3Gtrz4q3swc61hzCRlP1vavH9n0GSNr1BGaaZUfuvqyyDUFEfi08w	false		high
http://https://www.quiz-bliss.com/kittycantrell/greys-anatomy-jackson-april-relaitonship-japril-trivia-quiz-121921	false		unknown
http://https://www.quiz-bliss.com/	false	• 0%, Virustotal, Browse	unknown
http://https://www.quiz-bliss.com/quizzes/movies	false		unknown
http://https://www.quiz-bliss.com/quizzes/knowledge?sort=recenthttps://www.quiz-bliss.com/quizzes/geography?sort=recent	false		unknown
http://https://www.quiz-bliss.com/kittycantrell	false		unknown
http://https://www.google.com/recaptcha/api2/aframe	false		high
http://https://www.quiz-bliss.com/kittycantrell/harry-potter-20-year-anniversary-trivia-quiz-112821	false		unknown
http://https://www.quiz-bliss.com/quizzes	false		unknown
http://https://www.quiz-bliss.com/quizzes/entertainment?sort=recent	false		unknown
http://https://www.quiz-bliss.com/quizzes/trivia?sort=recent	false		unknown
http://https://www.quiz-bliss.com/quizzes/personality?sort=recent	false		unknown

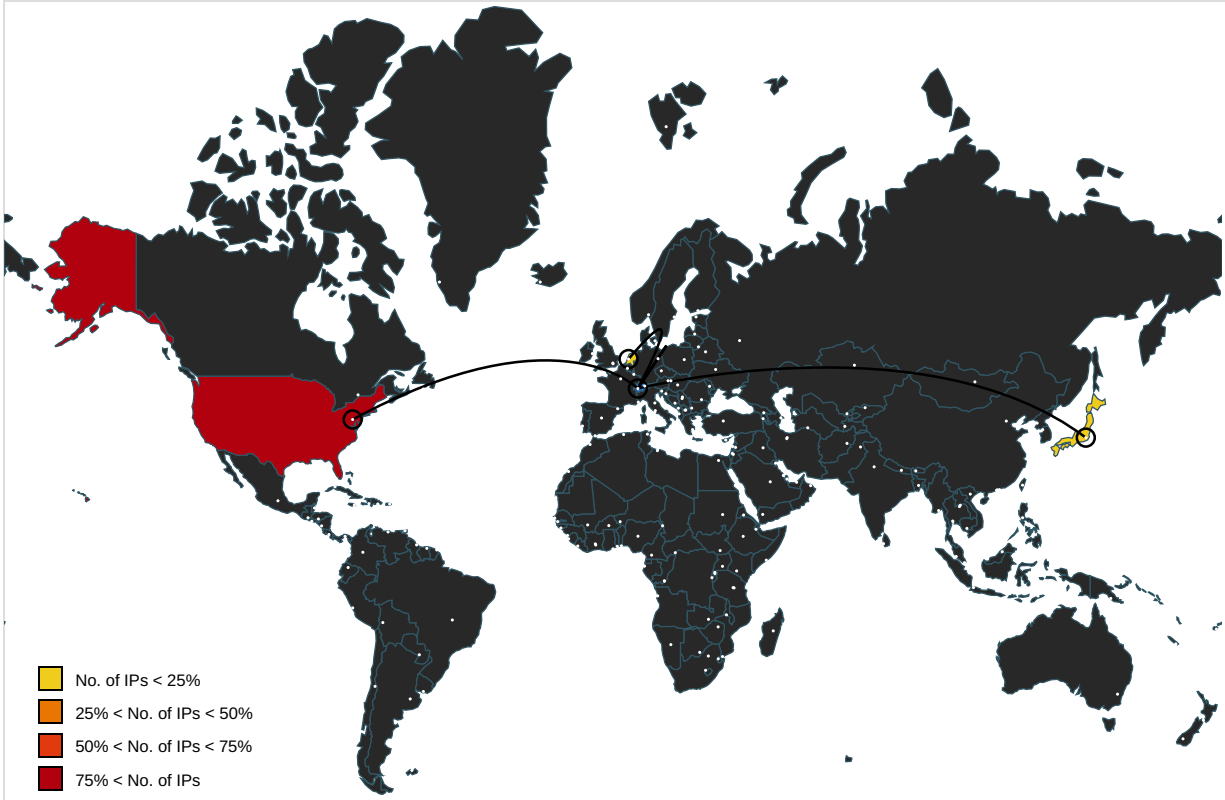
URLs from Memory and Binaries

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	d389d252-a51e-410a-befb-c0892fd8eb6f.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.com/log?format=json&hasfast=true	mirroring_hangouts.js.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
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://preprod-hangouts-googleapis.sandbox.google.com	mirroring_hangouts.js.0.dr	false		high
http://https://www.google.com	manifest.json2.0.dr, d389d252-a51e-410a-befb-c0892fd8eb6f.tmp.2.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	manifest.json2.0.dr, d389d252-a51e-410a-befb-c0892fd8eb6f.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	manifest.json2.0.dr, d389d252-a51e-410a-befb-c0892fd8eb6f.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	d389d252-a51e-410a-befb-c0892fd8eb6f.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	8d454001-03cc-42a8-ba1a-a4134cd05d7b.tmp.2.dr, 587ad5c5-835b-4e10-8cd7-57d6afe643ce.tmp.2.dr, d389d252-a51e-410a-befb-c0892fd8eb6f.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	d389d252-a51e-410a-befb-c0892fd8eb6f.tmp.2.dr	false		high
http://https://support.google.com/chromecast/troubleshooter/2995236	messages.json15.0.dr, messages.json5.0.dr, messages.json7.0.dr, messages.json49.0.dr, feedback.html.0.dr, messages.json61.0.dr, messages.json62.0.dr, messages.json75.0.dr, messages.json59.0.dr, messages.json27.0.dr, messages.json44.0.dr, messages.json46.0.dr, messages.json33.0.dr, messages.json0.0.dr, messages.json48.0.dr, messages.json88.0.dr, messages.json14.0.dr, messages.json87.0.dr, messages.json57.0.dr, messages.json76.0.dr, messages.json.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://www.google.com;	manifest.json2.0.dr	false	• Avira URL Cloud: safe	low
http://https://hangouts.google.com/	manifest.json2.0.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://tools.ietf.org/html/rfc1950	mirroring_hangouts.js.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://support.google.com/chromecast/answer/2998456	messages.json15.0.dr, messages.json5.0.dr, messages.json7.0.dr, messages.json49.0.dr, feedback.html.0.dr, messages.json61.0.dr, messages.json62.0.dr, messages.json75.0.dr, messages.json59.0.dr, messages.json27.0.dr, messages.json44.0.dr, messages.json46.0.dr, messages.json33.0.dr, messages.json0.0.dr, messages.json48.0.dr, messages.json88.0.dr, messages.json14.0.dr, messages.json87.0.dr, messages.json57.0.dr, messages.json76.0.dr, messages.json.0.dr	false		high
http://https://www.quiz-bliss.com/kittycantrell/harry-potter-20-year-anniversary-trivia-quiz-1128212YCelebr	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients2.googleusercontent.com	d389d252-a51e-410a-befb-c0892fd8eb6f.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.json2.0.dr	false		high
http://https://clients2.google.com/service/update2/crx	manifest.json.0.dr, manifest.json2.0.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
169.50.137.182	nl3ads5.simpli.fi	United States		36351	SOFTLAYERUS	false
157.240.17.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false
185.33.221.13	ib.anycast.adnxs.com	Netherlands		29990	ASN-APPNEXUS	false
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
18.197.199.94	eu2-ice.360yield.com	United States		16509	AMAZON-02US	false
172.217.168.65	pagead-googlehosted.l.google.com	United States		15169	GOOGLEUS	false
172.217.168.6	s0-2mdn-net.l.google.com	United States		15169	GOOGLEUS	false
34.96.105.8	tr.blismedia.com	United States		15169	GOOGLEUS	false
142.250.203.109	accounts.google.com	United States		15169	GOOGLEUS	false
143.204.215.108	sb.scorecardresearch.com	United States		16509	AMAZON-02US	false
174.137.133.49	e-volution.rtb-as-useast.ak-is2.net	United States		27257	WEBAIR-INTERNETUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
184.87.212.24	cs.media.net	United States		8529	OMANTEL-ASSultanateofOmanOM	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
202.241.208.100	tg.dr.socdm.com	Japan		4694	IDCFIDCFrontierIncJP	false
18.195.155.181	cs.emxdgt.com	United States		16509	AMAZON-02US	false
172.217.168.2	www.googletagservices.com	United States		15169	GOOGLEUS	false
34.98.97.49	img.women.com	United States		15169	GOOGLEUS	false
130.211.6.0	www.quiz-bliss.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
104.18.12.5	a.tribalfusion.com	United States		13335	CLOUDFLARENETUS	false
143.204.215.20	s.ad.smaato.net	United States		16509	AMAZON-02US	false
104.18.13.5	s.tribalfusion.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.2
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562519
Start date:	29.01.2022
Start time:	00:02:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://www.quiz-bliss.com/kittycantrell/harry-potter-20-year-anniversary-trivia-quiz-112821
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:	CLEAN
Classification:	clean1.win@46/203@48/25
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.quiz-bliss.com/ • Browse: https://www.quiz-bliss.com/quizzes?sort=recent • Browse: https://www.quiz-bliss.com/quizzes/knowledge?sort=recent • Browse: https://www.quiz-bliss.com/quizzes/geography?sort=recent • Browse: https://www.quiz-bliss.com/quizzes/personality?sort=recent • Browse: https://www.quiz-bliss.com/quizzes/entertainment?sort=recent • Browse: https://www.quiz-bliss.com/quizzes/trivia?sort=recent • Browse: https://www.quiz-bliss.com/kittycantrell • Browse: https://www.facebook.com/sharer.php?u=https%3A%2F%2Fwww.quiz-bliss.com%2Fkittycantrell%2Fharry-potter-20-year-anniversary-trivia-quiz-112821 • Browse: https://www.quiz-bliss.com/quizzes/movies • Browse: https://www.quiz-bliss.com/quizzes/harry%20potter • Browse: https://www.quiz-bliss.com/quizzes

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 2.20.156.69, 142.250.203.110, 173.194.182.73, 34.104.35.123, 172.217.168.10, 2.20.156.249, 172.217.168.33, 142.250.203.99, 104.83.145.243, 213.19.162.21, 213.19.162.41, 213.19.162.61, 213.19.162.51, 213.19.162.31, 172.217.168.66, 142.250.203.98, 2.20.157.55, 13.107.42.14, 193.0.160.128, 172.217.168.34, 142.250.203.106, 172.217.168.74, 216.58.215.234, 172.217.168.42
- Excluded domains from analysis (whitelisted): e6449.dsca.akamaiedge.net, clientservices.googleapis.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, r4.sn-4g5e6ns7.gvt1.com, htlb.casalemedia.com.edgekey.net, arc.msn.com, tagged-by.rubiconproject.net.akadns.net, 2-01-37d2-0006.cdx.cedexis.net, l-0005.l-msedge.net, e8037.g.akamaiedge.net, ade.googlesyndication.com, redirector.gvt1.com, a.rfihub.com.akadns.net, update.googleapis.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.gstatic.com, prod.fs.microsoft.com.akadns.net, r4---sn-4g5e6ns7.gvt1.com, www.google-analytics.com, www-linkedin-com.l-0005.l-msedge.net, fonts.googleapis.com, fs.microsoft.com, content-autofill.googleapis.com, fonts.gstatic.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a-emea.rfihub.com.akadns.net, pagead2.googlesyndication.com, www.googleapis.com, e8037.i.akamaiedge.net, ris.api.iris.microsoft.com, edgedl.me.gvt1.com, s.pinimg.com.edgeke
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA8321101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GM DS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS .AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\0d89be2c-c67f-4ac3-af1f-e4fdb6b59dbb.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	96680
Entropy (8bit):	3.7451830208493018
Encrypted:	false
SSDEEP:	384:GjO5lbcukoEbjVYeFgNNr+vRb36dbKHLGGuRr8/pfqxivnfWrEJmUX87VxFOO7LZ:A6K1NqKqWEevorDLs/r+DKBfVRG
MD5:	6AADEEC9ACB7BF2E5A914EF9851E3C4C
SHA1:	004F73547DB16F9322A11E953FC1C06034FEEF42
SHA-256:	861A013FA591C0030FF27E00BC38E340BC08FEF7A4A2CF6249C20FBD3D813E8F
SHA-512:	D94076BBF1963A4EB15A23350EA08D664E09F097EAB7FBE7D6F2179EADB4FF82989ECC446EC05F4BCDEBBA26A7688F9F6A469404B8EEE0C84BDF5FE29CCA7AB0
Malicious:	false
Reputation:	low
Preview:	.y.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{}...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...PR8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\1a562cb5-0812-4f19-9097-f6d520d52b4d.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):	190587
Entropy (8bit):	6.045374131274452
Encrypted:	false
SSDEEP:	3072:I/S1Cm78VKMvHOz5zXnZIFYLp964jYLftLt8aZpNkFcbXafIB0u1GOJmA3iuR6:aHm78s6OtziYLpDjqd8aqfIlUOoSiuR6
MD5:	0D3970E906DB6DA971BDF7FDC78B4142
SHA1:	110A5F9F8341059D565AFB1438BE0229EF8412B2
SHA-256:	7B75884CE8EC25392494A93A075AD582B3FCC6074ACA5B38E6B0BCC19D1E9E4E
SHA-512:	2760BDBF864EA20250EC03286BF3A896D15AD18FE7B34309EF668EB8174962C65FC80D9A80C53BEC07BDCC39DF18933D27B3CA2FE3142C013EED9D8B65661E1E
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":1.643443374882769e+12,"network":1.643410977e+12,"ticks":131913429.0,"uncertainty":3949173.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799825646"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\307dde0a-2e97-4879-a241-be417a7b78ec.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):	190418
Entropy (8bit):	6.045049120946776
Encrypted:	false
SSDEEP:	3072:a/S1Cm78VKMvHOz5zXnZIFYLp964jYLftLt8aZpNkFcbXafIB0u1GOJmA3iuR6:UHm78s6OtziYLpDjqd8aqfIlUOoSiuR6
MD5:	9E546C39AA0C6FB41A9EA20ED630CE6A
SHA1:	49DD79F8E1D478355898D0AF356D0F90D0CB1A4E
SHA-256:	F181AD50FCC4FD87250F6A2C258CD097750884E579C206004A79A49BCD080BF6
SHA-512:	572AB1D62231F3179D5672895BBFF13D990EDA4F5AEFF72FD908AB7DCA37ECCFD2C38D579FC3A8AD64771899C1748E70117FC1B30C1592E994E35C43F98BC6F
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":1.643443374882769e+12,"network":1.643410977e+12,"ticks":131913429.0,"uncertainty":3949173.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799825646"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\423be078-73c9-4de3-aff9-b40c512c2b7f.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	198892
Entropy (8bit):	6.074045797159456
Encrypted:	false
SSDEEP:	6144:yNHm78s6OtziYLpDjqd8aqfIlUOoSiuR6:yNHFz4hLZS7o1
MD5:	09C423DAA76EEEF38BCA9F98CD9603A5
SHA1:	0A8520BE30ADAA9DB9E288AE633373F2DF89338E
SHA-256:	11218B28F707E21BB3778643565CDF9F7AE024767647E1F094E22CF7E59F1B5F
SHA-512:	F3874A2C468C7CEB38002D38466E03FBF4B95D17B964348269DB57E37B13EC253C171340009DA73521BABBA7B9E87F00F7505689A1C4299CE6FE4BD5BC937AD4
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":1.643443374882769e+12,"network":1.643410977e+12,"ticks":131913429.0,"uncertainty":3949173.0}},"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\7d231985-b690-48d5-a60b-d1352d300427.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):	190504
Entropy (8bit):	6.0452121245640615
Encrypted:	false
SSDEEP:	3072:r/S1Cm78VKMvHOz5zXnZIFYLp964jYLftLt8aZpNkFcbXafIB0u1GOJmA3iuR6:7Hm78s6OtziYLpDjqd8aqfIlUOoSiuR6
MD5:	A03C7D28CB03014B29998AF169EC0312
SHA1:	359D10FC04DA69B535DC97B3CE08D06178E5F131

SHA-256:	110A22607664437860BD3D59D25D5D3B349CD15CB5C0697F1F240F29DA1EBBFF
SHA-512:	B3584AB3A0554DD3A35A7EDD28319DAEE841FEF03DCF23FCF3E4E509967184A54DC49A4F421E6043753765ADFF06A04C1699C54251BF71570F11C86EB07DC94 0
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":1.643443374882769e+12,"network":1.643410977e+12,"ticks":131913429.0,"uncertainty":3949173.0}},"os_crypt":{"encrypte d_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrY iwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYq Qj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"pa ssword_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799825646"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\94a0eef0-8ae2-46b6-bf60-7ee9c026ed7d.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):	190418
Entropy (8bit):	6.045047793347654
Encrypted:	false
SSDEEP:	3072:f/S1Cm78VKMvHOz5zXnZIFYLp964jYLftLt8aZpNkFcbXafIB0u1GOJmA3iuR6:nHm78s6OtziYLpDjqd8aqfIlUOoSiuR6
MD5:	24B8A57078E8728F3924515B0BF032A5
SHA1:	03607EE44FE4CCB872C021768BE88AD6AFC9F82E
SHA-256:	08D1B5072D333508CB800223DBEDB7D825F243600D798BE673269D31B7E50028
SHA-512:	102AB360D3562B89A1A84BAED026BB6B6FE4F7F36D24F2A7D686605C29930748F5997A2A58B395AC9E8220C550C7B8D0CF54183E36BC94036D882339728FCF3F
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":1.643443374882769e+12,"network":1.643410977e+12,"ticks":131913429.0,"uncertainty":3949173.0}},"os_crypt":{"encrypte d_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrY iwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYq Qj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"pa ssword_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799825646"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\94fa266f-7893-4111-92ad-11bfc0ecc68d.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):	190587
Entropy (8bit):	6.045374131274452
Encrypted:	false
SSDEEP:	3072:I/S1Cm78VKMvHOz5zXnZIFYLp964jYLftLt8aZpNkFcbXafIB0u1GOJmA3iuR6:aHm78s6OtziYLpDjqd8aqfIlUOoSiuR6
MD5:	0D3970E906DB6DA971BDF7FDC78B4142
SHA1:	110A5F9F8341059D565AFB1438BE0229EF8412B2
SHA-256:	7B75884CE8EC25392494A93A075AD582B3FCC6074ACA5B38E6B0BCC19D1E9E4E
SHA-512:	2760BDBF864EA20250EC03286BF3A896D15AD18FE7B34309EF668EB8174962C65FC80D9A80C53BEC07BDCC39DF18933D27B3CA2FE3142C013EED9D8B65661E 1E
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":1.643443374882769e+12,"network":1.643410977e+12,"ticks":131913429.0,"uncertainty":3949173.0}},"os_crypt":{"encrypte d_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrY iwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYq Qj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"pa ssword_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799825646"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\9525774e-c1d6-4de6-8976-9c350704412c.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97400
Entropy (8bit):	3.745238339289495
Encrypted:	false

SSDEEP:	384:8jO5lbcukoEbjVYeFgNNr+vRb36dbKHLGGuRr8/pfqxivnfWrEJmUAi87VxFOO7h:W6K1NqKkWEevorDLs/r+DKBfVRe
MD5:	6DA0394760B5BA505907FE85AF0E3BD9
SHA1:	5D18E60E4C5782602C9EA9DB04DD4B65B4E5B54A
SHA-256:	AF9DB2FCC54A221E4F81C3622B1423A10560DF86C4AA283672748AEF031AC9AE
SHA-512:	C5C1E2455841B31162BE1C4A3683749E432AF7E6EEDD7850BDB9DB3CB01866507A36E2279AFBD5DA4481984E0D39608D6E24FD91E8E078DA61EB4198E0A1FF 0
Malicious:	false
Reputation:	low
Preview:	t|.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...PR8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\954a132f-0918-417e-9cea-b3b83028ec01.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	198892
Entropy (8bit):	6.074046396986606
Encrypted:	false
SSDEEP:	6144:L8Hm78s6OtziYLpDjqd8aqfIlUOoSiuR6:L8HFz4hLZS7o1
MD5:	3CF821A128656F43D3D6D7700270321A
SHA1:	C965692F1FF149F229903B044EDC5B62D8827EA6
SHA-256:	FCD988E68126502A90F0F7C0FF77BDAC73E73422D58F162153FD33D5AD55197D
SHA-512:	8EF495AA7386196F146BDA868759F37E928BDF195E846A98F6D83A6F2FCCB8B79B6ED2B29BCD95E55601739EB49D0DE653B339E9585A8F2FFF5E5BA6B8C2DD 68
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":1.643443374882769e+12,"network":1.643410977e+12,"ticks":131913429.0,"uncertainty":3949173.0}},"os_crypt":{"encrypte d_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrY iwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYq Qj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"pa ssword_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799825646"},"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\05428b73-4cb8-4796-b9e1-2cd593eab456.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):	5192
Entropy (8bit):	4.9883221476349355
Encrypted:	false
SSDEEP:	96:nWCA5e9pcKIr8ok0JCKL8/XWUSkDU1xLbOTQVuwn:nWC99pcx4KQhSkDULf

MD5:	19AF7DAEBDB9C62B614E6ABE7AC05C14
SHA1:	B397C963664716831B270CF3D47D22BD5BF00836
SHA-256:	8340D4B166C6739D980A6FC807F107365488E1A6C77B49EC0EEB91E9572EE2AA
SHA-512:	D6A0C554AE1BA170C09CD5E7CAE3A56D985A3B335A100AE2E8B98C9F2178700C19C83294DD64FEF087A28DB87B940C3AC8422C13A9925B0E3355C784770719I B
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287916973390501","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\13fd322a-ac75-438f-8fc2-71de8b0141ab.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F2 5F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\148d7455-1a88-4ca1-8bda-e08352ca313c.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):	5179
Entropy (8bit):	4.986436828149611
Encrypted:	false
SSDEEP:	96:nWCAge9pcKIrZok0JCKL8/XWUSkDU1xLbOTQVuwn:nWCM9pc24KQhSkDULf
MD5:	C25B28E61B041832FCF8AB482B2C588F
SHA1:	6DE2E9C849C315A75AD8017BB7B84FC64E36997C
SHA-256:	F3EEBD210CCF73E2F7A02F6A508FB22149A535ECD8F3F82A85174D3326A0000A
SHA-512:	0C184FBC9EA6EAD7805984C210E5173FD7BF2A0918EC32767D7A908B617B5AEF138F7D1216C193139AD24EAD571655859760E4EC002469B0466D055AD4FE0B8
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287916973390501","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\175faa00-cdfd-4a9d-a7b6-6fb864491171.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):	5.570301461964212
Encrypted:	false
SSDEEP:	384:kKKtoLlLPX91kXqKf/pUZNCgVLH2HfDprUNHGUkBzD4N:9LlD91kXqKf/pUZNCgVLH2HflrUxGbvW
MD5:	F6B1C1C9E63E0C0BA4E3AA4B67BC62A9
SHA1:	2CFCCBA891F57ECB7045C447FAA93328C1192410

SHA-256:	74B4CEF11C8F5E1F9D10CDB64D4E39506A2D64652EA956C92C500DFA4BB1AECE
SHA-512:	119F92D8B6DF5764A432828613803F6C167BD06527A8C9F835E3DA54D4F643854AFD9A0218638A2222E005116447B41B319E09A36321FFF459F5E51C4632BBCD
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":"13287916972879370","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2993e2a7-2707-42c1-859c-7fe1cd2db6f8.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):	5.583194549225984
Encrypted:	false
SSDEEP:	384:kKKtoLlLPX91kXqKf/pUZNCgVLH2HfDprUPkCzD4L:9LlD91kXqKf/pUZNCgVLH2HflrU1vs
MD5:	47AC5CD463EBE01D0F1EC97B593F322A
SHA1:	8E39E67FCB90868254FFD9282EBAE73A5FB34D26
SHA-256:	7DEE4B80114BAF622DD83E62E0DBA1A4A2F3C7A6961AA33D25BB5A4CB3097C38
SHA-512:	89FBE34C6A8A0DB730BF255882872332A4F2EB277BDC6C63427712EC3CE93AD1DD26FD3436B2045A5CE2E55E4D773700D932B068B3A806EC3E1AF9112E77423F
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":"13287916972879370","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2ce8f007-444e-40d8-affd-13dc05ea164e.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):	5031
Entropy (8bit):	4.92494163817205
Encrypted:	false
SSDEEP:	96:JTOCXGDHazlMyrmYBKfFExJOBH01EsabAWpbBXabfGWpi/G3GHWKfH:JTOCXGDHazlMySYBKixJOBH0KsabAWp1
MD5:	8305D9822098EF7930492F63282FA31A
SHA1:	282D477DE3D19458B6D7A7595C58EC8ED97A2EE0
SHA-256:	C206409654C123377752C3006C06A7762071D88CF0F23EB2BBC5CC6BCEAFEE8A
SHA-512:	BF7B0F8C6E3D084D9DBF1D5FBAFBA721157FD142D99EEB3C5673FDB1794A951962DD7CF2C09403B7E6B29D0A25496832072F1C5FB9E71BE72B1772499FA562D
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":"13290508974844485","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13290508974868506","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\375d7f13-a7a2-4af8-8bed-ccd1a5af138c.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):	5.577896196686978
Encrypted:	false
SSDEEP:	384:kKKt5LlLPX91kXqKf/pUZNCgVLH2HfDprUaSzD4i:CLlD91kXqKf/pUZNCgVLH2HflrUHvp

MD5:	78098DF603B3D8F3B4020EA94455B97C
SHA1:	170EE4C6F4E2D49DE5704A49094783FD1DC9F2E0
SHA-256:	E519CF3228D51BE92E04C15823947B07BE77DC6A3AE47A51D26702606F86492A
SHA-512:	89961150C4D59D4DBB6F3C35966AE9B9160225943E5804D79194F8A493D2133974F5275E2BAB0C69DD6046E8D69E5372B08F7A2054FF7D1F8FBB310F07D1324B
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":"13287916972879370","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\3a821e45-dc15-41c3-b8e4-19e10a7b3511.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):	5.570263437175062
Encrypted:	false
SSDEEP:	384:kKKtoLlLPX91kXqKf/pUZNCgVLH2HfDprUNHGpkgzD44:9LlD91kXqKf/pUZNCgVLH2HflrUxGdv/
MD5:	92788CA84D3FA5F7E3EE859B9BF3FCFB
SHA1:	4702B993F2F098782D241E6211C8F8A023E9E7D9
SHA-256:	D39F236B3F1DCCAE1678DBCACAA4079FDC14A7B873AEE0A88ABEA637E34CAD19
SHA-512:	0FBEB3DFE4F1FEE1D94C49B2C14B4A0E2C897DC4864A3AACDF929B87FD6F31022B3C8BEC530951B0613B9E9037043C1D66454AD1BAEE4C0243372ECF086E1 E5
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":"13287916972879370","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\47199a30-ed52-49d7-83f3-4621f5d65015.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):	5179
Entropy (8bit):	4.986237699347827
Encrypted:	false
SSDEEP:	96:nWCAWe9pcKIrUok0JCKL8/XWUSkDU1xLbOTQVuwn:nWCK9pc54KQhSkDULf
MD5:	D240558DB05D9268D0D5115E672D96B1
SHA1:	0EE732F6281E8043D77275C6AD8B151890E04E9E
SHA-256:	6D151FCBFB358399EAC3A30D31B6BA0325EA03E4F663151FC032D3089F369B3B
SHA-512:	429ED9B6729E4E0A11737B0C095115CB3DDE82845D757C42C7E4B0F4643B4976D9013D38052960C4EE4AABBCDD8220E31ED274D59FAE3A6118664A8FB02D72 5
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287916973390501","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\4abad8f5-01a5-4ae1-babd-bade8a1d0101.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):	5220
Entropy (8bit):	4.992700842128553

Encrypted:	false
SSDEEP:	96:nWCrVe9pcKIreok0JCKL8/XWUSkDU1x9bOTQVuwn:nWC89pcP4KQhSkDULl
MD5:	0BE5CE133EAFBC085E57E34D1EE46BFC
SHA1:	0D551D1318CEE2EF1758906E0D336E8ED2B50918
SHA-256:	B6036D5E25E24E489D860480E77004962A1BBDFA21C8B5EE72F35C2EE4ECB1B2
SHA-512:	457D6347F5127D996282D52C13DBD1BCBE14B615A74C5C5D321F79CA8B1DCDF9495B3C466F26A358083E497417A517A7283415FCB22CEF735291B5ADE0B6AB5 1
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287916973390501","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\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUscllJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=","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):	5.171867000171164
Encrypted:	false
SSDEEP:	6:Mc9v+q2PWXp+N23iKKdK25+Xqx8chI+IFUtqVTc9yZmwYVTc9hVkwOWXp+N23iKG:Mc92va5KkTXfchI3FUtuc9y/0c9v5f5G
MD5:	964EA19CD32FF28A02D63F42EB95F935
SHA1:	89A0D76AD4DF3EC48B701CC625484CDF398BCCF8
SHA-256:	9A0C6C5CD74E760584563FDDBBB036683895D35FDE9479D0C9F7AA6A7F3EA7C2
SHA-512:	C7E3A2DDFAFB50162C6DB7D6BDD5A74C6C0E5A7A1238D50E1F40C10C7AE3A985F63A8CFEC96F5FDAC888612479472477A4684886E0F804F32EC68587194031 6
Malicious:	false
Reputation:	low
Preview:	2022/01/29-00:03:02.911 19e8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MA NIFEST-000001.2022/01/29-00:03:02.912 19e8 Recovering log #3.2022/01/29-00:03:02.913 19e8 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"0 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.171867000171164
Encrypted:	false
SSDEEP:	6:Mc9v+q2PWXp+N23iKKdK25+Xqx8chI+IFUtqVTc9yZmwYVTc9hVkwOWXp+N23iKG:Mc92va5KkTXfchI3FUtuc9y/0c9v5f5G
MD5:	964EA19CD32FF28A02D63F42EB95F935
SHA1:	89A0D76AD4DF3EC48B701CC625484CDF398BCCF8
SHA-256:	9A0C6C5CD74E760584563FDDBBB036683895D35FDE9479D0C9F7AA6A7F3EA7C2
SHA-512:	C7E3A2DDFAFB50162C6DB7D6BDD5A74C6C0E5A7A1238D50E1F40C10C7AE3A985F63A8CFEC96F5FDAC888612479472477A4684886E0F804F32EC68587194031 6
Malicious:	false
Reputation:	low
Preview:	2022/01/29-00:03:02.911 19e8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MA NIFEST-000001.2022/01/29-00:03:02.912 19e8 Recovering log #3.2022/01/29-00:03:02.913 19e8 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):	1184
Entropy (8bit):	5.54289371047801

Encrypted:	false
SSDEEP:	24:zebwLeaeYFeBQBlSoY1rHTYMSftI5TjzEY78BJgskfa9yBDOxo7nQBrxzkr2iXLA:zekLeae64ql/Y1bUf+ZzSU8JFYXLDr3Y
MD5:	A6FA05F12568E60DDCE879668674A1E1
SHA1:	AAE2F3A408DAC9B269E8A80A1FD86532524EFD9F
SHA-256:	6F115294E706EA2D28B78D237145A9CD5A976F45A88BC61290D6751A7167489D
SHA-512:	ED0152FAE0A9BABE24CC130598AB1EB8F4E832C7BFABD22E4908F9D91E8E05A7F8E90E497FDE4D0102170BA9CA6781EAA935C2AE30D612311F2E8B086EFDF807
Malicious:	false
Reputation:	low
Preview:	............"......112821..20..acing..anniversary..bliss..by..celebrate..com..harry..hp..https..kittycantrell..of..potter..quiz..this..trivia..ultimate..www..year..years*........112821......20......acing......anniversary......bliss......by......celebrate......com......harry......hp......https......kittycantrell......of......potter......quiz......this......trivia......ultimate......www......year......years..2........0........1........2........8........a...............b.........c..........e.............f........g........h..........i..............k........l..........m.........n.........o..........p..........q........r..............s...........t.............u.........v.........w........y............z...:...B............ ......*\https://www.quiz-bliss.com/kittycantrell/harry-potter-20-y

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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):	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):	5220
Entropy (8bit):	4.992700842128553
Encrypted:	false
SSDEEP:	96:nWCrVe9pcKIreok0JCKL8/XWUSkDU1x9bOTQVuwn:nWC89pcP4KQhSkDULl
MD5:	0BE5CE133EAFBC085E57E34D1EE46BFC
SHA1:	0D551D1318CEE2EF1758906E0D336E8ED2B50918
SHA-256:	B6036D5E25E24E489D860480E77004962A1BBDFA21C8B5EE72F35C2EE4ECB1B2
SHA-512:	457D6347F5127D996282D52C13DBD1BCBE14B615A74C5C5D321F79CA8B1DCDF9495B3C466F26A358083E497417A517A7283415FCB22CEF735291B5ADE0B6AB51
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287916973390501","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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5179

Entropy (8bit):	4.9864997753703
Encrypted:	false
SSDEEP:	96:nWCAge9pcKIr1ok0JCKL8/XWUSkDU1xLbOTQVuwn:nWCM9pci4KQhSkDULf
MD5:	E8B10EDA5C76C9501FC287E38AF73C04
SHA1:	C9D31654D3ACA03F9AC489EA209964C4B6291770
SHA-256:	4E269E9CEAAC53BD8C2BCD896407427AA2D78DAEAAE020242339F5B43D8DCACD
SHA-512:	9F795011F189D6AF100F8945F22160292146D2C2855E1C9AF5A802C97684DA52E00B041789046B48D508E67EC6F71CB73DD2BC331E8C69C2D059A98710A4BAE3
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287916973390501","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\Preferences\ (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	14773
Entropy (8bit):	5.670562029027517
Encrypted:	false
SSDEEP:	192:hppr6VVD8/LkiQKrTV2U00jT25kNV6c8TEKdl:hr88/YOrTjF2GV6uml
MD5:	D4513639FFC58664556B4607BF8A3F19
SHA1:	65629BC4CBBACA498F4082DD5884C8D3D7DDDC8A
SHA-256:	C6D49997A9B4FF7FE701EC3644B1A523679A27778FB4BD39B7DBCA9F1ACCE595
SHA-512:	16260FAC30D57EBFD577833F45D52FEA446ABE877D0D4015EF47C5C9072B81DDA71ED4E5E7DAFDEBE82B26556A4477EA4BFCDEC227058E381B9812DAB1F4379B
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 ..$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "START_SPAN": {.

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19182
Entropy (8bit):	5.570301461964212
Encrypted:	false
SSDEEP:	384:kKKtoLlLPX91kXqKf/pUZNCgVLH2HfDprUNHGUkBzD4N:9LlD91kXqKf/pUZNCgVLH2HflrUxGbvW
MD5:	F6B1C1C9E63E0C0BA4E3AA4B67BC62A9
SHA1:	2CFCCBA891F57ECB7045C447FAA93328C1192410
SHA-256:	74B4CEF11C8F5E1F9D10CDB64D4E39506A2D64652EA956C92C500DFA4BB1AECE
SHA-512:	119F92D8B6DF5764A432828613803F6C167BD06527A8C9F835E3DA54D4F643854AFD9A0218638A2222E005116447B41B319E09A36321FFF459F5E51C4632BBCD
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":"13287916972879370","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\Secure PreferencesMP (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745

Entropy (8bit):	5.577896196686978
Encrypted:	false
SSDEEP:	384:kKKt5LlLPX91kXqKf/pUZNCgVLH2HfDprUaSzD4i:CLlD91kXqKf/pUZNCgVLH2HflrUHvp
MD5:	78098DF603B3D8F3B4020EA94455B97C
SHA1:	170EE4C6F4E2D49DE5704A49094783FD1DC9F2E0
SHA-256:	E519CF3228D51BE92E04C15823947B07BE77DC6A3AE47A51D26702606F86492A
SHA-512:	89961150C4D59D4DBB6F3C35966AE9B9160225943E5804D79194F8A493D2133974F5275E2BAB0C69DD6046E8D69E5372B08F7A2054FF7D1F8FBB310F07D1324B
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":"13287916972879370","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferencess- (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):	5.583194549225984
Encrypted:	false
SSDEEP:	384:kKKtoLlLPX91kXqKf/pUZNCgVLH2HfDprUPkCzD4L:9LlD91kXqKf/pUZNCgVLH2HflrU1vs
MD5:	47AC5CD463EBE01D0F1EC97B593F322A
SHA1:	8E39E67FCB90868254FFD9282EBAE73A5FB34D26
SHA-256:	7DEE4B80114BAF622DD83E62E0DBA1A4A2F3C7A6961AA33D25BB5A4CB3097C38
SHA-512:	89FBE34C6A8A0DB730BF255882872332A4F2EB277BDC6C63427712EC3CE93AD1DD26FD3436B2045A5CE2E55E4D773700D932B068B3A806EC3E1AF9112E77423F
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":"13287916972879370","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\8d454001-03cc-42a8-ba1a-a4134cd05d7b.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\587ad5c5-835b-4e10-8cd7-57d6afe643ce.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\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):	5.173527429687989
Encrypted:	false
SSDEEP:	12:McxVva5KkkGHArBFUtucxL/0cxJ5f5KkkGHAryJ:MS5a5KkkGgPguSQSbf5KkkGga
MD5:	2AF66CD6BC1E4AD22A2543B641161C32
SHA1:	12239C07D8706857B56122F71D08F077F5D7DD1F
SHA-256:	F85C2126E2CAD6F60677B37D14E5834235830BD64A643656749AC4A192FA9B38
SHA-512:	AB15198C8A987125820D74FCA558134F5E077031150800A938B752FB4FC3A262D77A91CE401E4955D86BF99901E09120A4196B2282C962AC12B5CEAB806E44AD
Malicious:	false
Reputation:	low
Preview:	2022/01/29-00:03:42.177 1a84 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2022/01/29-00:03:42.198 1a84 Recovering log #3.2022/01/29-00:03:42.200 1a84 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\Local Storage\leveldb\LOG.old (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.173527429687989
Encrypted:	false
SSDEEP:	12:McxVva5KkkGHArBFUtucxL/0cxJ5f5KkkGHAryJ:MS5a5KkkGgPguSQSbf5KkkGga
MD5:	2AF66CD6BC1E4AD22A2543B641161C32
SHA1:	12239C07D8706857B56122F71D08F077F5D7DD1F
SHA-256:	F85C2126E2CAD6F60677B37D14E5834235830BD64A643656749AC4A192FA9B38
SHA-512:	AB15198C8A987125820D74FCA558134F5E077031150800A938B752FB4FC3A262D77A91CE401E4955D86BF99901E09120A4196B2282C962AC12B5CEAB806E44AD
Malicious:	false
Reputation:	low
Preview:	2022/01/29-00:03:42.177 1a84 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2022/01/29-00:03:42.198 1a84 Recovering log #3.2022/01/29-00:03:42.200 1a84 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\Network Persistent Statece (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):	4.954960881489904
Encrypted:	false

SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BI
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"adve rtised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5} ,"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.172360919480405
Encrypted:	false
SSDEEP:	12:Mcx8+va5KkkGHArqiuFUtucxCX/0cxC3V5f5KkkGHArq2J:MSta5KkkGgCguSC8SCXf5KkkGg7
MD5:	82180698775DADDED6A8692C12E024C8
SHA1:	099067DEBD39AA3B18FD9B9FC302014582FFB4F5
SHA-256:	8B77BF4B65BD6F6F971B977ADD92521D40070CDE3415CAFB43EB9EE0152C2626
SHA-512:	AE395F51A03A231AF47BF2E79C422CC75A25786BFD4BD975CB1ABB8901F7CBAA3F1822176223AA4CD4029D4FF6EB153DB964B18C4F1DCAC5D0C2AF6D5DD66 F0A
Malicious:	false
Reputation:	low
Preview:	2022/01/29-00:03:42.245 227c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2022/01/29-00:03:42.247 227c Recovering log #3.2022/01/29-00:03:42.247 227c 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\Platform Notifications\LOG.old (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.172360919480405
Encrypted:	false
SSDEEP:	12:Mcx8+va5KkkGHArqiuFUtucxCX/0cxC3V5f5KkkGHArq2J:MSta5KkkGgCguSC8SCXf5KkkGg7
MD5:	82180698775DADDED6A8692C12E024C8
SHA1:	099067DEBD39AA3B18FD9B9FC302014582FFB4F5
SHA-256:	8B77BF4B65BD6F6F971B977ADD92521D40070CDE3415CAFB43EB9EE0152C2626
SHA-512:	AE395F51A03A231AF47BF2E79C422CC75A25786BFD4BD975CB1ABB8901F7CBAA3F1822176223AA4CD4029D4FF6EB153DB964B18C4F1DCAC5D0C2AF6D5DD66 F0A
Malicious:	false
Reputation:	low
Preview:	2022/01/29-00:03:42.245 227c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Platform Notifications/MANIFEST-000001.2022/01/29-00:03:42.247 227c Recovering log #3.2022/01/29-00:03:42.247 227c 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:S8ltHIS+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):	5.2161895343398665
Encrypted:	false
SSDEEP:	12:McrTva5KkkGHArAFUtucrx/0cr4P5f5KkkGHArfJ:Miza5KkkGgkgui6i4Bf5KkkGgV
MD5:	B0FCD722D3653CB1431395807B9BC694
SHA1:	E1F689E4B381C6FF87B5C8709CAB17028EC653DC
SHA-256:	F41346B5AE6DBEC51ACCCD54B7B6E963B04CCAC0E4C39D4F27BC02B0BEBC950B
SHA-512:	C128A6E01FF49E98338B10D85D2537E3BE52A1C7A27E5D50E2C4711F1216C9023DA60CCCA19B8F3886FBC3017AFC38F2114320111D3BDE62B6520371F1B7E49
Malicious:	false
Reputation:	low
Preview:	2022/01/29-00:03:57.984 2268 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2022/01/29-00:03:57.985 2268 Recovering log #3.2022/01/29-00:03:57.988 2268 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.2161895343398665
Encrypted:	false
SSDEEP:	12:McrTva5KkkGHArAFUtucrx/0cr4P5f5KkkGHArfJ:Miza5KkkGgkgui6i4Bf5KkkGgV
MD5:	B0FCD722D3653CB1431395807B9BC694
SHA1:	E1F689E4B381C6FF87B5C8709CAB17028EC653DC
SHA-256:	F41346B5AE6DBEC51ACCCD54B7B6E963B04CCAC0E4C39D4F27BC02B0BEBC950B
SHA-512:	C128A6E01FF49E98338B10D85D2537E3BE52A1C7A27E5D50E2C4711F1216C9023DA60CCCA19B8F3886FBC3017AFC38F2114320111D3BDE62B6520371F1B7E49
Malicious:	false
Reputation:	low
Preview:	2022/01/29-00:03:57.984 2268 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2022/01/29-00:03:57.985 2268 Recovering log #3.2022/01/29-00:03:57.988 2268 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	modified
Size (bytes):	402
Entropy (8bit):	5.292940400878136
Encrypted:	false
SSDEEP:	6:MFypyq2PWXp+N23iKKdKks8Y5JKKhdIFUtqVTFa1ZmwYVTFgF8lRkwOWXp+N23iC:MZva5KkkOrsFUtu01/05z5f5KkkOrzJ
MD5:	532C017B3309DB181779C3AC9346B288
SHA1:	AA89FF9B45FD66406FCA4E572B82B9D25487F3CF
SHA-256:	D28773F6559A07150490E2F4BA25FC167E18BF0196EF3036047EE1954E7FBF4E
SHA-512:	E0B76FD9B0785522DA1905AEBD5F85B1EA25D1068945B5C954107CFCE42CE18F73BC40877A4BCD83570D4277129820DDBA031655D279ECB4B1822B2D87178EF
Malicious:	false

Reputation:	low
Preview:	2022/01/29-00:04:32.731 19e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2022/01/29-00:04:32.733 19e4 Recovering log #3.2022/01/29-00:04:32.734 19e4 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\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.oldMP (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.292940400878136
Encrypted:	false
SSDEEP:	6:MFypyq2PWXp+N23iKKdKks8Y5JKKhdIFUtqVTFa1ZmwYVTFgF8lRkwOWXp+N23iC:MZva5KkkOrsFUtu01/05z5f5KkkOrzJ
MD5:	532C017B3309DB181779C3AC9346B288
SHA1:	AA89FF9B45FD66406FCA4E572B82B9D25487F3CF
SHA-256:	D28773F6559A07150490E2F4BA25FC167E18BF0196EF3036047EE1954E7FBF4E
SHA-512:	E0B76FD9B0785522DA1905AEBD5F85B1EA25D1068945B5C954107CFCE42CE18F73BC40877A4BCD83570D4277129820DDBA031655D279ECB4B1822B2D87178E6 F
Malicious:	false
Reputation:	low
Preview:	2022/01/29-00:04:32.731 19e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2022/01/29-00:04:32.733 19e4 Recovering log #3.2022/01/29-00:04:32.734 19e4 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\a7a4422b-15f5-42f9-be21-ba60cbad20ba.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):	5179
Entropy (8bit):	4.986603094492097
Encrypted:	false
SSDEEP:	96:nWCAge9pcKIr/ok0JCKL8/XWUSkDU1xLbOTQVuwn:nWCM9pc84KQhSkDULf
MD5:	9F6CEC822E1EE722D9469811B27BCDFB
SHA1:	E838234972FF90C354466CC8434CC547AC57694A
SHA-256:	A2915D751DBCC452059E134EC88E04ABC315CE4A92D5E565D301CC0CE4FB0170
SHA-512:	CF7CD93DD1C492D456996946800A2EC88FB8FEBFE521B83B5523B3029E0746E58C0594698D435C7DC2A78DB5CBA6DA464FF73C206F5DA8CC01476F8DAED343 B4
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287916973390501","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\a971a55d-d534-4666-802d-7c47102ecebc.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):	5179
Entropy (8bit):	4.9864997753703
Encrypted:	false
SSDEEP:	96:nWCAge9pcKIr1ok0JCKL8/XWUSkDU1xLbOTQVuwn:nWCM9pci4KQhSkDULf
MD5:	E8B10EDA5C76C9501FC287E38AF73C04
SHA1:	C9D31654D3ACA03F9AC489EA209964C4B6291770
SHA-256:	4E269E9CEAAC53BD8C2BCD896407427AA2D78DAEAAE020242339F5B43D8DCACD
SHA-512:	9F795011F189D6AF100F8945F22160292146D2C2855E1C9AF5A802C97684DA52E00B041789046B48D508E67EC6F71CB73DD2BC331E8C69C2D059A98710A4BAE3
Malicious:	false
Reputation:	low

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287916973390501","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\b395bfc2-58f0-4f12-97ce-b809f2be6e39.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):	5.536096174408642
Encrypted:	false
SSDEEP:	384:kKKtoLlLPX91kXqKf/pUZNCgVLH2HfDprUNHGCnT3kpzD45G:9LlD91kXqKf/pUZNCgVLH2HflrUxGCn0
MD5:	B80BEC32217EEFA840B7F38A34DE34A7
SHA1:	051F3F15E273D3D9155D0DAF9455A902A78C5B1C
SHA-256:	25BAC288636D03D5EBB0E137C29DDB69CA4821D9607724A3F0E442581C5F403F
SHA-512:	31C8E2A0911FAB905505761C833333D2009FADDFA3E8F23E78E190BAC71C4DF1D71B26C1899F3BFA72F6BA3025BCE30699E627F26F481460E98E56B44460C02(
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":"13287916972879370","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\c6c8b5e2-7c82-4146-b005-e00f37ceb06c.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):	5220
Entropy (8bit):	4.992497574376744
Encrypted:	false
SSDEEP:	96:nWCrVe9pcKIrJok0JCKL8/XWUSkDU1x9bOTQVuwn:nWC89pcS4KQhSkDULl
MD5:	A36A40C2F5621A2166F2B4C16466C9C4
SHA1:	CF749CA52E644A6FC72E36504DDC933CB4786B7A
SHA-256:	FFB25BFF2CF926B3BD317CBB4CC5E564A167718073C97A547B06CC57D0986CF7
SHA-512:	D90E951B9BCD8F20DBD3CA7CF7B1BF252A198688D1C90995AC8AAD6EAF42AA26FB2BCE10A22770DFC928A362E0EB54BF3B57FBC491E0120048F52F6DFF83A3C3
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287916973390501","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\c95f0593-85cd-4064-aefe-83e05df14dc4.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):	5460
Entropy (8bit):	4.924610733289941
Encrypted:	false
SSDEEP:	96:JTOCXGDHzlMyrmYBbOB1EuGWzG2YGaFExGCsG/GIGpYAGWXGabBGHpGOBGtG5RG1:JTOCXGDHzlMySYBbOBKuftYox/s8/IYc
MD5:	82BDE46B911E1A478A032DF9AA579275
SHA1:	444FAFA190C4A67B2D855E0678173025F9A51F84
SHA-256:	89884E85417F0BDEC83323A946A8035294BB0FA083C7EFFF82FB62A0B81036F5
SHA-512:	37523E301F08AE63A4C1543D5F6BA402CF06CFE2EA0A003D6008C1DA95EBD79C57E49F08AB623F358BA4BA1F92B9D360644A9048DBA620CF1C9C349B88AF1DD3

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://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13290508974844485","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13290508974868506","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13290508975

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\d389d252-a51e-410a-befb-c0892fd8eb6f.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\d8384415-6176-443a-a8c0-77ba29e02f00.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):	5816
Entropy (8bit):	5.19439050602884
Encrypted:	false
SSDEEP:	96:nWCrse9/9cKIreok0JCKL8/XWUSkDU1x9bOTQVuwn:nWCf91cP4KQhSkDULl
MD5:	464120AAA1DA9D3008C6F0F76B261D3E
SHA1:	1B76CE6B5D1C89B6CA83BDFA306D0CB96981FA7D
SHA-256:	B64284A7F4F82A6605EA11F65EB776FE0AAF32B84E38703D2C76D94FC0C5302C
SHA-512:	C467B6B6B00534F1BF8E5962529A9BFBD49D5BC365D356CA3041B56DB2147632035708492F0462AD3DAC4B3759C19DCF245A0D6E81A4F9F5EF9E92F618284B2
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13287916973390501","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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\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:tblolIrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691 724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Version

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

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

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

Size (bytes):	190504
Entropy (8bit):	6.045211002044502
Encrypted:	false
SSDEEP:	3072:+/S1Cm78VKMvHOz5zXnZIFYLp964jYLftLt8aZpNkFcbXaflB0u1GOJmA3iuR6:AHm78s6OtziYLpDjqd8aqfllUOoSiuR6
MD5:	B28C1CB0569424CDCD06896FAF7C0690
SHA1:	7CAC6C13805E58B58995964769B6B1A1C87BF2A5
SHA-256:	8F591E350C7D0DE332363F8CE9C4542D7C5FCAE2C31665BAF8AB37F2562FC8C2
SHA-512:	CFCD2A278E28A0F2C872D166CDB7BE880FC9998987252D619F5EBE9F07829110F62FA58254DEABCA445A62E156B5011A68DC25DB7DA4A0E749184FF267C03D 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":1.643443374882769e+12,"network":1.643410977e+12,"ticks":131913429.0,"uncertainty":3949173.0}},"os_crypt":{"encrypte d_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrY iwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYq Qj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"pa ssword_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799825646"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State. (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	198892
Entropy (8bit):	6.074047217748358
Encrypted:	false
SSDEEP:	6144:q2Hm78s6OtziYLpDjqd8aqfllUOoSiuR6:q2HFz4hLZS7o1
MD5:	FF3D96DF2CF95776F3727B04A578075F
SHA1:	5BEABDDFEF56CED74A94E8F74CFBA5204A542FD7
SHA-256:	A2589991AB95A11AB70F344164A0A2FB4B84834AD85E8CA04FEE133E4C0D7C15
SHA-512:	2FEA03BB6D4934FC5017B54E85A9CC3975597E12A3E02FE1B0A0E8577D34674E8FAE74B73C312990714EC3BEEF829B5D098F8DBD39A07CC931F0798C2FD9F98 1
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":1.643443374882769e+12,"network":1.643410977e+12,"ticks":131913429.0,"uncertainty":3949173.0}},"os_crypt":{"encrypte d_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrY iwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYq Qj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"pa ssword_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799825646"},"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):	198892
Entropy (8bit):	6.074045909795173
Encrypted:	false
SSDEEP:	6144:0RHm78s6OtziYLpDjqd8aqfllUOoSiuR6:0RHFz4hLZS7o1
MD5:	D76A2C39CBD1FC15E9A1F56A4DF26106
SHA1:	8D16A2305B55F933428CB0C401DFACA924A09744
SHA-256:	E411230D1FCE3DEF4157BB42E881995CF0681CBBAFDE23AF4B94DE905B613ED2
SHA-512:	19748990491271541A848C455A555CE1C909DCF007B3FA117F1E6131411B29837FE5EC9D1C1EE2FE83B5E717B859AC203A43C69012FA6FED4F9903A5B585B636
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":1.643443374882769e+12,"network":1.643410977e+12,"ticks":131913429.0,"uncertainty":3949173.0}},"os_crypt":{"encrypte d_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrY iwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYq Qj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"pa ssword_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):	94696
Entropy (8bit):	3.7451973054831993
Encrypted:	false
SSDEEP:	384:tjO5lbcuk8bUFgNNr+vRb36dbKHLGGuRr8/pfqxivnfWrEJmUX87VxFOO7LxNA1c:MK1NqKqWEevorDLs/r+DKBfVRO
MD5:	1868FB55738F30D4270A05C5B0A10AEA
SHA1:	9972208D165C0433381AA0D6E4C629327DF28286
SHA-256:	91C879AF137FC3C1D2F6C422D1B6CFB4806DBE9BA9D2914246361856C263B9A4
SHA-512:	E167BB9ABE260A512D4B83668CE3836FBFB208DEA18DC762617696E731918A7213CA9E1A582EB23A70AF2AC58184B5DB67EDD169E5FD468776DD021F0F33E4(8
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...PR8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info CacheMP (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97400
Entropy (8bit):	3.745238339289495
Encrypted:	false
SSDEEP:	384:8jO5lbcukoEbjVYeFgNNr+vRb36dbKHLGGuRr8/pfqxivnfWrEJmUAi87VxFOO7h:W6K1NqKkWEevorDLs/r+DKBfVRe
MD5:	6DA0394760B5BA505907FE85AF0E3BD9
SHA1:	5D18E60E4C5782602C9EA9DB04DD4B65B4E5B54A
SHA-256:	AF9DB2FCC54A221E4F81C3622B1423A10560DF86C4AA283672748AEF031AC9AE
SHA-512:	C5C1E2455841B31162BE1C4A3683749E432AF7E6EEDD7850BDB9DB3CB01866507A36E2279AFBD5DA4481984E0D39608D6E24FD91E8E078DA61EB4198E0A1FF 0
Malicious:	false
Reputation:	low
Preview:	t|.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...PR8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\a8fd2781-74a2-4e7b-b891-0b2347b44d85.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):	190504
Entropy (8bit):	6.045211002044502
Encrypted:	false
SSDEEP:	3072:+/S1Cm78VKMvHOz5zXnZIFYLp964jYLftLt8aZpNkFcbXaflB0u1GOJmA3iuR6:AHm78s6OtziYLpDjqd8aqfllUOoSiuR6
MD5:	B28C1CB0569424CDCD06896FAF7C0690
SHA1:	7CAC6C13805E58B58995964769B6B1A1C87BF2A5
SHA-256:	8F591E350C7D0DE332363F8CE9C4542D7C5FCAE2C31665BAF8AB37F2562FC8C2
SHA-512:	CFCD2A278E28A0F2C872D166CDB7BE880FC9998987252D619F5EBE9F07829110F62FA58254DEABCA445A62E156B5011A68DC25DB7DA4A0E749184FF267C03D 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":1.643443374882769e+12,"network":1.643410977e+12,"ticks":131913429.0,"uncertainty":3949173.0}},"os_crypt":{"encrypte d_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrY iwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYq Qj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"pa ssword_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799825646"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\c008613e-7421-4823-b346-283cad985b47.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	198892
Entropy (8bit):	6.074047217748358
Encrypted:	false
SSDEEP:	6144:q2Hm78s6OtziYLpDjqd8aqfIlUOoSiuR6:q2HFz4hLZS7o1
MD5:	FF3D96DF2CF95776F3727B04A578075F
SHA1:	5BEABDDFEF56CED74A94E8F74CFBA5204A542FD7
SHA-256:	A2589991AB95A11AB70F344164A0A2FB4B84834AD85E8CA04FEE133E4C0D7C15
SHA-512:	2FEA03BB6D4934FC5017B54E85A9CC3975597E12A3E02FE1B0A0E8577D34674E8FAE74B73C312990714EC3BEEF829B5D098F8DBD39A07CC931F0798C2FD9F98 1
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":1.643443374882769e+12,"network":1.643410977e+12,"ticks":131913429.0,"uncertainty":3949173.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799825646"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\da49494b-f6b6-4bbe-acea-e1c09787c2ab.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	198892
Entropy (8bit):	6.074045909795173
Encrypted:	false
SSDEEP:	6144:0RHm78s6OtziYLpDjqd8aqfIlUOoSiuR6:0RHFz4hLZS7o1
MD5:	D76A2C39CBD1FC15E9A1F56A4DF26106
SHA1:	8D16A2305B55F933428CB0C401DFACA924A09744
SHA-256:	E411230D1FCE3DEF4157BB42E881995CF0681CBBAFDE23AF4B94DE905B613ED2
SHA-512:	19748990491271541A848C455A555CE1C909DCF007B3FA117F1E6131411B29837FE5EC9D1C1EE2FE83B5E717B859AC203A43C69012FA6FED4F9903A5B585B636
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":1.643443374882769e+12,"network":1.643410977e+12,"ticks":131913429.0,"uncertainty":3949173.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABAL2tyan+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\f325a433-621f-4cfd-82a0-468f0a5cd00c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	198892
Entropy (8bit):	6.07404790616915
Encrypted:	false
SSDEEP:	6144:VMHm78s6OtziYLpDjqd8aqfIlUOoSiuR6:VMHFz4hLZS7o1
MD5:	57DEE9F827ECA29B1158D1BC122DE4F4
SHA1:	A0D1B4F5FAEBB2222368330D7C2E70CC643783B7
SHA-256:	9457DCD594DEE9545DFFA970C44DFDC1E88C7792553EA8901A06AB23593CE9C1
SHA-512:	628A0286695D6636BB5875F0EF48BB003AB8E2F000F66A758DC8FB87D33EE892F9589AE138A1822A41ECB6004AE10A43F492F1001D5FA7344768BDD31DBB7B67
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":1.643443374882769e+12,"network":1.643410977e+12,"ticks":131913429.0,"uncertainty":3949173.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/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\fc3dc7cd-d016-42ad-ae97-114c7505f0af.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94696
Entropy (8bit):	3.7451973054831993
Encrypted:	false
SSDEEP:	384:tjO5lbcuk8bUFgNNr+vRb36dbKHLGGuRr8/pfqxivnfWrEJmUX87VxFOO7LxNA1c:MK1NqKqWEevorDLs/r+DKBfVRO
MD5:	1868FB55738F30D4270A05C5B0A10AEA
SHA1:	9972208D165C0433381AA0D6E4C629327DF28286
SHA-256:	91C879AF137FC3C1D2F6C422D1B6CFB4806DBE9BA9D2914246361856C263B9A4
SHA-512:	E167BB9ABE260A512D4B83668CE3836FBFB208DEA18DC762617696E731918A7213CA9E1A582EB23A70AF2AC58184B5DB67EDD169E5FD468776DD021F0F33E40 8
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...PR8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Temp\219b646a-cd29-44dc-bd11-dbb6057c3b33.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F2 5F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\5330c1eb-1ebf-48d1-8634-2d3cc72d12b0.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:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C 88
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..$.J....+M!.Hz.n`U.I)N.\|b.I....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z ....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5SI..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\6516_374337630\LICENSE

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1558
Entropy (8bit):	5.11458514637545
Encrypted:	false
SSDEEP:	48:OBOCrYJ4rYJVwUCLHDy43HV713XEyMmZ3teTHn:LCrYJ4rYJVwUCHZ3Z13XtdUTH
MD5:	EE002CB9E51BB8DFA89640A406A1090A
SHA1:	49EE3AD535947D8821FFDEB67FFC9BC37D1EBBB2
SHA-256:	3DBD2C90050B652D63656481C3E5871C52261575292DB77D4EA63419F187A55B
SHA-512:	D1FDCC436B8CA8C68D4DC7077F84F803A535BF2CE31D9EB5D0C466B62D6567B2C59974995060403ED757E92245DB07E70C6BDDBF1C3519FED300CC5B9BF917C
Malicious:	false
Reputation:	low
Preview:	// Copyright 2015 The Chromium Authors. All rights reserved..//.// Redistribution and use in source and binary forms, with or without.// modification, are permitted provided that the following conditions are.// met:.//.// * Redistributions of source code must retain the above copyright.// notice, this list of conditions and the following disclaimer..// * Redistributions in binary form must reproduce the above.// copyright notice, this list of conditions and the following disclaimer.// in the documentation and/or other materials provided with the.// distribution..// * Neither the name of Google Inc. nor the names of its.// contributors may be used to endorse or promote products derived from.// this software without specific prior written permission..//.// THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS.// "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT.// LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR.// A PARTICULAR

C:\Users\user\AppData\Local\Temp\6516_374337630_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):	1511
Entropy (8bit):	5.989302167311014
Encrypted:	false
SSDEEP:	24:pZRj/flTU3YfKFjoYs7aoXET3J74L/V9OVadG6oX+1SEt5zWNJX5n:p/hUIfKE7akEzF4mIpkYINN5
MD5:	1B1A744394D197EC915E379FB7942527
SHA1:	1C4E23D596EF6B76FEB464AC4C287B363BCA2C8E
SHA-256:	0C3F6C4D72C3E22ABC1FB56F4CD99F1F269EB05885882172980864A85EC91BD4
SHA-512:	8E09F4370535C77AA113A221E65765AF6E75F353FC329CF2059232B5A657A12357B99A539306185A0F13B1AD606491509C82840D2DAEFB489C8AA506D9ABFE6E
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJMSUNFTlNFIiwicm9vdF9oYXNoIjoiUGIwc2tBVUxaUzFqWldTQnctV0hIRkltRlhVcExiZDlUcVkwR2ZHSHBWcyJ9LHsicGF0aCI6ImNybC1zZXQiLCJyb290X2hhc2giOiJmSDdsdkhlSERENU9UWkNFMnNqaUQ5ZmZYdVhENTBfTEFxSmY3NWpnUnZ3In0seyJwYXRoIjoibWFuaWZlc3QuanNvbiIsInJvb3RfaGFzaCI6IkwtSlNRZlk1c29KMlVRc0U0akRyZ3pzc3FNX3R0NnVvbnpBSzgzTHpPN2cifV0sImZvcm1hdCI6InRyZWVoYXNoIiwiaGFzaF9ibG9ja19zaXplIjo0MDk2fV0sIml0ZW1faWQiOiJoZm5rcGltbGhoZ2lIYWRkZ2ZlbWpob2ZtZmJsbW5pYyIsIml0ZW1fdmVyc2lvbiI6IjcxMjYiLCJwcm90b2NvbF92ZXJzaW9uIjoxfQ","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"jbiQ1HY71EZgvAGkp-cFOU4Gs2Qh66A6EIBI5mOJA8PvoE5XO_GO0RMM6We3kRsIXKNog3NUzR1a-sAuiCiNP7iU13Kz1KHRCKLBvzKYcqx0HEaRc3HsQh4XkOzN03QGeKaSWZG8ymd3hLWfYg_sn-gnJ4QVlmFKJX1SLNe-Wc5aebsrB9QO0cwZ_Uth3qOyEDBxK5-7nS0wYl3gmtRIORBrN_8OaysdZT9z2jci_oNVQV4Rsv9EIcClCMw3KNhC7Q5

C:\Users\user\AppData\Local\Temp\6516_374337630\crl-set

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	22671
Entropy (8bit):	7.824553974830855
Encrypted:	false
SSDEEP:	384:j26XPKhMeWUUkWVPpDddm84WDzyloBLY0Lq5LV8QzIF0trtaYG9V3t/8tPJBr:jf10CVBDXOWnyloW0L8V8S80rsYGROP
MD5:	2FCF403D5E5F7A47D30A174BA03972D6
SHA1:	B39B31422107AF9C5FE97085831E9BBC9E7E1B76
SHA-256:	DECDCEAD357DAB40EB5CBBA8BDFD46FDD4B217E790EF00950C8ABE7D5DB2478B
SHA-512:	EF70B94FDAFF1372B30290AE2ACBB80CEE6BD10C0CDADBD7FCED1E4ACB644AD3BBC8D9054E5103FB90527B843038079ABB565AF00DEE716CB3E6FF75EA1606ED

Malicious:	false
Reputation:	low
Preview:	".{"Version":0,"ContentType":"CRLSet","Sequence":7126,"DeltaFrom":0,"NumParents":194,"BlockedSPKIs":["Jdoa1Yu/z7In2HI7GFfUwY57qnQXtPnv+TZrXoafizk=","Ii5LVLuYp+5dX+uWM/mR08MwDpUU2t57DU+CjHlPjoc=","yP3cdcsb27WMB7TqhHKH9iZIndZrwQomrdm1dbOgo40=","BN3pqpp59hSYaCMl+ghwJ2cH+5ypU4QSC0aJMmhJT8k=","tbqN1/iVZMKInT1kU8hJmMd4JJGbZOoINapimGWRvlA=","wO0gU0a7veButWD1zuAqNjTiR0p+ds+PvvVjuxF90OM=","eBpM8ukkUvPuAdDDgaQhTzkEFlw5CtvWH80RJE4Jstw=","/NdsyiNH5c1bOTR/Uc9DZUtpor/JBzZwpr5H2HAebg4=","lo26afv/Fb83YgiUMa3lp+rUt+rxvnACaBC8V9HGT24=","fNKVt1VEgIq9lAIGbwg3xarcAuM7YVDGZE3goJZZ8jw=","9Sk9R+041MMbLULe47WzrOl8omyirANl42Iu6AlTH7s=","nFmjzK6kaZhCsGjPxSz5RdtRmGlXyDLNsYynOEn7ue4=","OUz/WJ5okxLPwHHuC8Gf5MYGIWzlQ0Kd5tti5C27O8E=","NuqWEoyJg5+2IfitDh7gucIgb2Kre02ixnZYk8m3ztI=","pqyh7JgJzFtIIf+dKcXr5lGWC5Gx8ZzIm1Xvh4GKlQk=","MO/kE4JHbDOA8C9+I+ZrovhnsFnuHqaHlrRBuFtdElY=","r1kVGOLmxg67/AkHr6pJvEBR1F5/IUq/7nUS7gD2Ye0=","6EnHF2yT32X2S2FpgjZuVmMReBK2+ivAyPqK6u5Bgcw=","0x7DkoW3pTGdAVfbQg7YfHQ+Mzu8d/h3H3BGT0NqYEk=","h7/Yr

C:\Users\user\AppData\Local\Temp\6516_374337630\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):	3.9441006138261616
Encrypted:	false
SSDEEP:	3:SUbGObDlXxEOg9iURVgGWlEB:SUSOlhq9iLGkm
MD5:	DD945DFA99472C4805B5CE9A20028B60
SHA1:	AC56F4EEB8D671E07826179D5027880712CC21C9
SHA-256:	05D453FA569F4E87EC8AAECF5E561B62B60F66FBB7430AFB1C20F76132AF619D
SHA-512:	6E06EA4CEA06614352D51AEFD6D0CB765AD4741C6C9E05F771C90618CDC53AE0A3D0E99AD5208A09A68EEE298F8A849D86AB57B93641739E9285460D4176E4E0
Malicious:	false
Reputation:	low
Preview:	1.18db281f705eaafdf4f24ce2c5e956718346234ee5d9b4ad140bec3f3a8d4af8

C:\Users\user\AppData\Local\Temp\6516_374337630\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	191
Entropy (8bit):	4.784974198700875
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFJNchRmwnhFgS1bTFHJEeSWU4pv/8F/FxLj2RF2fcTZTotL:F6VlM8mxS1bQWfB0NpK4aotL
MD5:	D7EBEEA548C1B7C2326EE6F382179377
SHA1:	EF43ABAF9FBAF2E6B2EBF42DB86FD323AE89F78F
SHA-256:	2FE25241F639B28276510B04E230EB833B2CA8CFEDB7ABA89F300AF372F33BB8
SHA-512:	985BE0492627F5BD237252FC962B7E7CDD19C0FC32BF4910624B5BD63857330DBC7F7E32644AB078C143835E11E7F2C95A5C7385A0836D01169381E7B2499D76
Malicious:	false
Reputation:	low
Preview:	{. "manifest_version": 2,. "name": "crl-set-8330309774708728989.data",. "version": "7126",. "imageName": "image.squash",. "squash": true,. "fsType": "squashfs",. "isRemovable": false.}

C:\Users\user\AppData\Local\Temp\6516_862130722_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):	1765
Entropy (8bit):	6.016932513650603
Encrypted:	false
SSDEEP:	48:p/hKAGj0FnAp7XgNGIaku9E5tPJXaWqkbszesM:R5Gj0FAlsaBmfPsRD3M
MD5:	6D1D175F88B64546105E3E7C31D1129A
SHA1:	75A1B56F55BB62B05365A0FDBFC7941DE77CBFAF
SHA-256:	A0BC246E8E160A9BB32FA60F4E7A04D148A17125F426509466031E07731FDF81
SHA-512:	5C80908331E30C7EAD67F7F6C5AB064B07626FD9C58925A0D2124D66B25C5AE2F218BDACFB68AFCB332E88EB297CFB7E0A7A9E5E1E54C9B7A510FEF095F9B54F
Malicious:	false
Reputation:	low

Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJtYW5pZmVzdC5qc29uIiwicm9vdF9oYXNoIjoiSUxrUllPSmhIVEZaclLRmN5UC12SkJrVjNWbWVLdHo4d1hEb2VPWjBZMCJ9LHsicGF0aCI6InNzbF9lcnJvcl9hc3Npc3RhbnQucGIiLCJyb290X2hhc2giOiJyRFZLUnlPcXBQQnI3RGhkM2VTazBKZzYxUlJXOVNzeHFBYU95WDFiWHFjIn1dLCJmb3JtYXQiOiJ0cmVlaGFzaCIsImhhc2hfYmxvY2tfc2l6ZSI6NDA5Nn1dLCJpdGVtX2lkIjoiZ2lla2NtbWxua2xlbmxhb21wcGtwaGtuam1ubnBuZWgiLCJpdGVtX3ZlcnNpb24iOiI3IiwicHJvdG9jb2xfdmVyc2lvbiI6MX0","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"nBdNk-7bgnEftAs4hWaHwF1Lk9pt7Eh6pcqe2gyNsE7VnVRp-H27tm1RFAF4htCUlXNJxX6YY-MUiK2DqJpQ3c73KDaFV8DcnadQfcXO3Lbrw7jLYSUaSdzujPkTyhuFcq_BhK0KWiIJ0aJgh7nVOBfAa5AbE6oFlLKMB2Ls0gmzS1-a5hUIu4rw2h9r9jkr6gLYbein5Jk2hdwW3u-1GNjyki4dftG2iZNAI8VhUf5gnCiF4AHCnYSGJsM0RGkmO_HJlzgwpQpP3RDsG2ioeKgxL-kcHhjXWOj3uVGyxpp1FkyHGkeGuqpFZMAxx3CEBiOtFj7i3iQxkgEW-E3uMKI3yA

C:\Users\user\AppData\Local\Temp\6516_862130722\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):	3.9570514164363635
Encrypted:	false
SSDEEP:	3:SVCBGERJd9WaHpYx4eiXoA:SVCwERJdVMiXd
MD5:	C6ABF42CB5AF869629971C2E42A87FD5
SHA1:	6EB0FAE28D9466E76FA12E31FE6CDADD3ACCE4D1
SHA-256:	D281AFDA759075F4CB7D7CEEC4A3CB2AF135213B4D691F27090E13F238486AD1
SHA-512:	EDDF7E4883E82718743C589E8F2E48BEAD948428E730231FEFADAD380853343332BC56C9DC61C963B3F537CD4865B06FF330CEF012B152CEA35F8A0AA2C7B5D
Malicious:	false
Reputation:	low
Preview:	1.fd515ec0dc30d25a09641b8b83729234bc50f4511e35ce17d24fd996252eaace

C:\Users\user\AppData\Local\Temp\6516_862130722\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	76
Entropy (8bit):	4.169145448714876
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFY8Wypv/KS1f:F6VlMQyBSS1f
MD5:	4AAA0ED8099ECC1DA778A9BC39393808
SHA1:	0E4A733A5AF337F101CFA6BEA5EBC153380F7B05
SHA-256:	20B91160E2611D3159AD82857323FEBC906457756678AB73F305C3A1E399D18D
SHA-512:	DFA942C35E1E5F62DD8840C97693CDBFD6D71A1FD2F42E26CB75B98BB6A1818395ECDF552D46F07DFF1E9C74F1493A39E05B14E3409963EFF1ADA8889715289
Malicious:	false
Reputation:	low
Preview:	{. "manifest_version": 2,. "name": "sslErrorAssistant",. "version": "7".}

C:\Users\user\AppData\Local\Temp\6516_862130722\ssl_error_assistant.pb

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2816
Entropy (8bit):	6.108955364911366
Encrypted:	false
SSDEEP:	48:jkbh6AW2Bfc3osI6Hc3+XgU+EVeY55J4gXM/QDH4yq2dxckdfmkM:jkbhM2a3pntgQVb8Ylq2di
MD5:	E2F792C9E2DD86F39E8286B2EAD2FC70
SHA1:	8A32867614D2A23E473ED642056DED8E566687F9
SHA-256:	AC354A4723AAA4F06BEC385DDDE4A4D0983AD51456F52B31A8068EC97D5B5EA7
SHA-512:	6A7AF0CA1EFA65A89A9CA3B8DF0D2E24F21D91673C60CDFEEB02D33647442B01D535497249542F40E66E0D2DD3E9F8ED1F4A201FD97138D07A2B71366737E580
Malicious:	false
Reputation:	low

Preview:	...5.3sha256/fjZPHewEHTrMDX3l1ecEIeoy3WFxHyGplOLv28klbtI=.5.3sha256/m/nBiLhStttu1YmOz7Y3D2u1iB1dV2CbIfFa3R2YW5M=.5.3sha256/8Iuf4xR bVCmCMQTJn3rxlgIlO1IOKoyuSUgmXyfaIKs=.5.3sha256/8IHdrS+r6IWzSMcRcD/GA6mBxk1ECX8tGRW0rtGWILE=.5.3sha256/k/2eeJTznE32mblA/du19wpVDSI ReFX44M8wXa2JY30=.5.3sha256/urWd7jMwR6DJgvWhp6xfRHF5b/cba3iG0ggXtTR6AfM=.5.3sha256/IJPCDSE5tM9H3nuD5m6RU2i9KDdPXVn4qmC/ULlcZzc=.5.3sha256/0Gy8RMdbxHNWR2GQJ62QKDXORYf5JmMmnr1FJFPYpzM=.5.3sha256/8tTICtyaxIQrdbYYDdgZhTN0OpM9kYndvoImtw1Ys5E=.5.3sha256/F7HIlsaG0bpJ W8CzYekRbtFqLVTTGqwvuwPDqnlLct0=.5.3sha256/zaV2Aw1A742R1+WpXWvL5atsJbGmeSS6dzZOfe6f1Yw=.5.3sha256/UwOkRGMlP0K/mKNJdpQ0sTg2ean9Tje8 UTOvFYzt1GE=.5.3sha256/w7KUXE4/BAo1YVZdO3mBsrMpu4IQuN0mhUXUI//agVU=.5.3sha256/JnPvGqEn36FjHQlBXtG1uWwNtdMj1o2ojR/asqyypNk=.5.3sha256/AUSXlKDCf1X30WhWeAWbjToABfBkJrKWPL6KwEi5VH0=.5.3sha256/zSyVjjFJMIeXK0ktVTIjewwr6U5OePRqyY/nEXTI4P8=.5.3sha256/9dcHlrXN2WV/ehbEd MxMZ8lV4qvGejCtNC5r6nfTviM=.5.3sha256/E+0WZLGSIe5nddlVKZ5fYzaNHHCE3hNqi/OWZD3iKgA=.5.3sha2

C:\Users\user\AppData\Local\Temp\8b8b36ce-c0e7-4082-91e5-d7e7b7d239d5.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\c46ac0da-1f09-4b27-bcd4-8ed5c1889b19.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\scoped_dir6516_1879999964\5330c1eb-1ebf-48d1-8634-2d3cc72d12b0.tmp

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

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

C:\Users\user\AppData\Local\Temp\scoped_dir6516_1879999964\CRX_INSTALL_locales\bg\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir6516_1879999964\CRX_INSTALL_locales\ca\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir6516_1879999964\CRX_INSTALL_locales\cs\messages.json

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

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

C:\Users\user\AppData\Local\Temp\scoped_dir6516_1879999964\CRX_INSTALL_locales\da\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir6516_1879999964\CRX_INSTALL_locales\de\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir6516_1879999964\CRX_INSTALL_locales\el\messages.json

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

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

C:\Users\user\AppData\Local\Temp\scoped_dir6516_1879999964\CRX_INSTALL_locales\en\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir6516_1879999964\CRX_INSTALL_locales\en_GB\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir6516_1879999964\CRX_INSTALL_locales\es\messages.json

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

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

C:\Users\user\AppData\Local\Temp\scoped_dir6516_1879999964\CRX_INSTALL_locales\es_419\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir6516_1879999964\CRX_INSTALL_locales\et\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir6516_1879999964\CRX_INSTALL_locales\fi\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir6516_1879999964\CRX_INSTALL_locales\fil\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir6516_1879999964\CRX_INSTALL_locales\fr\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir6516_1879999964\CRX_INSTALL_locales\hi\messages.json

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

C:\Users\user\AppData\Local\Temp\scoped_dir6516_1879999964\CRX_INSTALL_locales\hr\messages.json

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

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

Static File Info

No static file info

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 29, 2022 00:02:55.647094011 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:55.647149086 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:55.647231102 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:55.647593021 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:55.647619963 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:55.653712034 CET	49746	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:55.653742075 CET	443	49746	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:55.653837919 CET	49746	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:55.654738903 CET	49746	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:55.654752970 CET	443	49746	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:55.656780005 CET	49747	443	192.168.2.3	142.250.203.109
Jan 29, 2022 00:02:55.656821966 CET	443	49747	142.250.203.109	192.168.2.3
Jan 29, 2022 00:02:55.656908035 CET	49747	443	192.168.2.3	142.250.203.109
Jan 29, 2022 00:02:55.657118082 CET	49747	443	192.168.2.3	142.250.203.109
Jan 29, 2022 00:02:55.657134056 CET	443	49747	142.250.203.109	192.168.2.3
Jan 29, 2022 00:02:55.702502966 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:55.702941895 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:55.703001976 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:55.704183102 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:55.704286098 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:55.709820032 CET	443	49746	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:55.710475922 CET	49746	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:55.710501909 CET	443	49746	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:55.711636066 CET	443	49746	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:55.711711884 CET	49746	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:55.716365099 CET	443	49747	142.250.203.109	192.168.2.3
Jan 29, 2022 00:02:55.716711044 CET	49747	443	192.168.2.3	142.250.203.109
Jan 29, 2022 00:02:55.716733932 CET	443	49747	142.250.203.109	192.168.2.3
Jan 29, 2022 00:02:55.720391035 CET	443	49747	142.250.203.109	192.168.2.3
Jan 29, 2022 00:02:55.720482111 CET	49747	443	192.168.2.3	142.250.203.109

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 29, 2022 00:02:55.897552013 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:55.897957087 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:55.898298025 CET	49746	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:55.898622036 CET	443	49746	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:55.899420023 CET	49747	443	192.168.2.3	142.250.203.109
Jan 29, 2022 00:02:55.899714947 CET	443	49747	142.250.203.109	192.168.2.3
Jan 29, 2022 00:02:55.901040077 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:55.901077032 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:55.901359081 CET	49747	443	192.168.2.3	142.250.203.109
Jan 29, 2022 00:02:55.901402950 CET	443	49747	142.250.203.109	192.168.2.3
Jan 29, 2022 00:02:55.939935923 CET	49746	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:55.939954996 CET	443	49746	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:55.942712069 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:55.942981005 CET	49747	443	192.168.2.3	142.250.203.109
Jan 29, 2022 00:02:55.955770969 CET	443	49747	142.250.203.109	192.168.2.3
Jan 29, 2022 00:02:55.955938101 CET	443	49747	142.250.203.109	192.168.2.3
Jan 29, 2022 00:02:55.956023932 CET	49747	443	192.168.2.3	142.250.203.109
Jan 29, 2022 00:02:55.966243029 CET	49747	443	192.168.2.3	142.250.203.109
Jan 29, 2022 00:02:55.966300011 CET	443	49747	142.250.203.109	192.168.2.3
Jan 29, 2022 00:02:55.980940104 CET	49746	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:56.051341057 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.051477909 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.051532984 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:56.051548958 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.051582098 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.051626921 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:56.051644087 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.053236961 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.053317070 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:56.053333044 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.053982973 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.054056883 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:56.054070950 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.054383993 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.054452896 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:56.054465055 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.054990053 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.055068970 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:56.055079937 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.069467068 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.069569111 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:56.069602013 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.069788933 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.069860935 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:56.069876909 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.070940971 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.071016073 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.071033001 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:56.071053028 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.071113110 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:56.072035074 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.073203087 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.073273897 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.073297024 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:56.073318005 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.073374033 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:56.074307919 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.075448036 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.075516939 CET	443	49745	130.211.6.0	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 29, 2022 00:02:56.075525045 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:56.075539112 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.075587034 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:56.076626062 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.076733112 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.076792955 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:56.076806068 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.078939915 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.079010963 CET	49745	443	192.168.2.3	130.211.6.0
Jan 29, 2022 00:02:56.079025984 CET	443	49745	130.211.6.0	192.168.2.3
Jan 29, 2022 00:02:56.079169989 CET	443	49745	130.211.6.0	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 29, 2022 00:02:55.614727974 CET	192.168.2.3	8.8.8.8	0xc189	Standard query (0)	www.quiz-bliss.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:55.627072096 CET	192.168.2.3	8.8.8.8	0xed69	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:55.629982948 CET	192.168.2.3	8.8.8.8	0x737a	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:56.456367016 CET	192.168.2.3	8.8.8.8	0xf6d9	Standard query (0)	cdn-heroku.women.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:56.456648111 CET	192.168.2.3	8.8.8.8	0x3488	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:56.458707094 CET	192.168.2.3	8.8.8.8	0x59a2	Standard query (0)	img.women.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:56.500324011 CET	192.168.2.3	8.8.8.8	0x9936	Standard query (0)	s.pinimg.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:56.502662897 CET	192.168.2.3	8.8.8.8	0xf75	Standard query (0)	sb.scorecardresearch.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:56.538490057 CET	192.168.2.3	8.8.8.8	0x9e01	Standard query (0)	www.googletagservices.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:56.983953953 CET	192.168.2.3	8.8.8.8	0xb141	Standard query (0)	securepubads.g.doubleclick.net	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:57.267071009 CET	192.168.2.3	8.8.8.8	0x3432	Standard query (0)	ib.adnxs.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:57.270795107 CET	192.168.2.3	8.8.8.8	0x72a4	Standard query (0)	htlb.casalemedia.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:57.274928093 CET	192.168.2.3	8.8.8.8	0x8b27	Standard query (0)	fastlane.rubiconproject.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:57.606372118 CET	192.168.2.3	8.8.8.8	0x18d4	Standard query (0)	adservice.google.co.uk	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:57.608227015 CET	192.168.2.3	8.8.8.8	0xe49c	Standard query (0)	adservice.google.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:58.023237944 CET	192.168.2.3	8.8.8.8	0x7aeb	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:58.566647053 CET	192.168.2.3	8.8.8.8	0x49c6	Standard query (0)	img.women.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:04.911273003 CET	192.168.2.3	8.8.8.8	0x26ca	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:15.843106031 CET	192.168.2.3	8.8.8.8	0x7e2b	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:16.613723040 CET	192.168.2.3	8.8.8.8	0xc94b	Standard query (0)	dsum-sec.casalemedia.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:16.614518881 CET	192.168.2.3	8.8.8.8	0xb3f3	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:16.638485909 CET	192.168.2.3	8.8.8.8	0xce5e	Standard query (0)	s0.2mdn.net	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.022391081 CET	192.168.2.3	8.8.8.8	0xc585	Standard query (0)	googleads4.g.doubleclick.net	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.181843042 CET	192.168.2.3	8.8.8.8	0x63f8	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.182907104 CET	192.168.2.3	8.8.8.8	0x95f0	Standard query (0)	tr.blismedia.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 29, 2022 00:03:17.183476925 CET	192.168.2.3	8.8.8.8	0xbfc7	Standard query (0)	um.wbtrk.net	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.184542894 CET	192.168.2.3	8.8.8.8	0x8e8c	Standard query (0)	s.ad.smaato.net	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.185125113 CET	192.168.2.3	8.8.8.8	0x1e66	Standard query (0)	cs.media.net	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.186575890 CET	192.168.2.3	8.8.8.8	0xb095	Standard query (0)	rtb2-useast.e-volution.ai	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.256988049 CET	192.168.2.3	8.8.8.8	0xe864	Standard query (0)	cs.emxdgt.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.259310961 CET	192.168.2.3	8.8.8.8	0x14fb	Standard query (0)	a.tribalfusion.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.259547949 CET	192.168.2.3	8.8.8.8	0x8b72	Standard query (0)	um.simpli.fi	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.263844013 CET	192.168.2.3	8.8.8.8	0x1a92	Standard query (0)	match.360yield.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.266027927 CET	192.168.2.3	8.8.8.8	0x3a2d	Standard query (0)	um.wbtrk.net	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.267714977 CET	192.168.2.3	8.8.8.8	0x3ebb	Standard query (0)	tg.socdm.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.308453083 CET	192.168.2.3	8.8.8.8	0x1577	Standard query (0)	a.rfihub.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.597229958 CET	192.168.2.3	8.8.8.8	0x4e1f	Standard query (0)	s.tribalfusion.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:22.272322893 CET	192.168.2.3	8.8.8.8	0x47f7	Standard query (0)	s0.2mdn.net	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:24.143995047 CET	192.168.2.3	8.8.8.8	0x2647	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:24.157195091 CET	192.168.2.3	8.8.8.8	0xfc76	Standard query (0)	dsum-sec.casalemedia.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:24.182234049 CET	192.168.2.3	8.8.8.8	0x614f	Standard query (0)	ib.adnxs.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:46.307507038 CET	192.168.2.3	8.8.8.8	0x42e8	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:47.622658968 CET	192.168.2.3	8.8.8.8	0x760c	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:50.168093920 CET	192.168.2.3	8.8.8.8	0x394	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:57.041271925 CET	192.168.2.3	8.8.8.8	0xbf21	Standard query (0)	www.quiz-bliss.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:58.214770079 CET	192.168.2.3	8.8.8.8	0x7162	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:58.361192942 CET	192.168.2.3	8.8.8.8	0xdc35	Standard query (0)	img.women.com	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:58.983309031 CET	192.168.2.3	8.8.8.8	0x2008	Standard query (0)	sb.scorecardresearch.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 29, 2022 00:02:55.633460045 CET	8.8.8.8	192.168.2.3	0xc189	No error (0)	www.quiz-bliss.com		130.211.6.0	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:55.654922962 CET	8.8.8.8	192.168.2.3	0x737a	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:55.666261911 CET	8.8.8.8	192.168.2.3	0xed69	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:02:55.666261911 CET	8.8.8.8	192.168.2.3	0xed69	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:56.240607023 CET	8.8.8.8	192.168.2.3	0xfda0	No error (0)	www-google-analytics.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:56.475208044 CET	8.8.8.8	192.168.2.3	0x3488	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:02:56.475208044 CET	8.8.8.8	192.168.2.3	0x3488	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:56.483963966 CET	8.8.8.8	192.168.2.3	0x59a2	No error (0)	img.women.com		34.98.97.49	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 29, 2022 00:02:56.486432076 CET	8.8.8.8	192.168.2.3	0xf6d9	No error (0)	cdn-heroku.women.com	media-gcp.women.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:02:56.486432076 CET	8.8.8.8	192.168.2.3	0xf6d9	No error (0)	media-gcp.women.com		35.186.224.64	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:56.497474909 CET	8.8.8.8	192.168.2.3	0x861d	No error (0)	gstaticadssl.l.google.com		216.58.215.227	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:56.525590897 CET	8.8.8.8	192.168.2.3	0xf75	No error (0)	sb.scorecardresearch.com		143.204.215.108	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:56.525590897 CET	8.8.8.8	192.168.2.3	0xf75	No error (0)	sb.scorecardresearch.com		143.204.215.23	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:56.525590897 CET	8.8.8.8	192.168.2.3	0xf75	No error (0)	sb.scorecardresearch.com		143.204.215.7	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:56.525590897 CET	8.8.8.8	192.168.2.3	0xf75	No error (0)	sb.scorecardresearch.com		143.204.215.58	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:56.528831959 CET	8.8.8.8	192.168.2.3	0x9936	No error (0)	s.pinimg.com	s-pinimg-com.gslb.pinterest.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:02:56.528831959 CET	8.8.8.8	192.168.2.3	0x9936	No error (0)	s-pinimg-com.gslb.pinterest.com	2-01-37d2-0006.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:02:56.566591024 CET	8.8.8.8	192.168.2.3	0x9e01	No error (0)	www.googletagservices.com		172.217.168.2	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:57.024847031 CET	8.8.8.8	192.168.2.3	0xb141	No error (0)	securepubads.g.doubleclick.net	partnerad.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:02:57.024847031 CET	8.8.8.8	192.168.2.3	0xb141	No error (0)	partnerad.l.doubleclick.net		172.217.168.66	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:57.285326004 CET	8.8.8.8	192.168.2.3	0x3432	No error (0)	ib.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:02:57.285326004 CET	8.8.8.8	192.168.2.3	0x3432	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:02:57.285326004 CET	8.8.8.8	192.168.2.3	0x3432	No error (0)	ib.anycast.adnxs.com		185.33.221.13	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:57.285326004 CET	8.8.8.8	192.168.2.3	0x3432	No error (0)	ib.anycast.adnxs.com		185.33.220.242	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:57.285326004 CET	8.8.8.8	192.168.2.3	0x3432	No error (0)	ib.anycast.adnxs.com		185.33.220.240	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:57.285326004 CET	8.8.8.8	192.168.2.3	0x3432	No error (0)	ib.anycast.adnxs.com		185.33.221.14	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:57.285326004 CET	8.8.8.8	192.168.2.3	0x3432	No error (0)	ib.anycast.adnxs.com		185.33.223.38	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:57.285326004 CET	8.8.8.8	192.168.2.3	0x3432	No error (0)	ib.anycast.adnxs.com		185.33.221.52	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:57.285326004 CET	8.8.8.8	192.168.2.3	0x3432	No error (0)	ib.anycast.adnxs.com		185.33.221.90	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:57.285326004 CET	8.8.8.8	192.168.2.3	0x3432	No error (0)	ib.anycast.adnxs.com		185.33.220.145	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:57.285326004 CET	8.8.8.8	192.168.2.3	0x3432	No error (0)	ib.anycast.adnxs.com		185.33.221.89	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:57.285326004 CET	8.8.8.8	192.168.2.3	0x3432	No error (0)	ib.anycast.adnxs.com		185.33.221.15	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:57.285326004 CET	8.8.8.8	192.168.2.3	0x3432	No error (0)	ib.anycast.adnxs.com		185.33.221.91	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:57.285326004 CET	8.8.8.8	192.168.2.3	0x3432	No error (0)	ib.anycast.adnxs.com		185.33.220.216	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:57.288527966 CET	8.8.8.8	192.168.2.3	0x72a4	No error (0)	htlb.casalemedia.com	htlb.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:02:57.294650078 CET	8.8.8.8	192.168.2.3	0x8b27	No error (0)	fastlane.rubiconproject.com	tagged-by.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:02:57.631336927 CET	8.8.8.8	192.168.2.3	0x18d4	No error (0)	adservice.google.co.uk	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:02:57.631336927 CET	8.8.8.8	192.168.2.3	0x18d4	No error (0)	pagead46.l.doubleclick.net		142.250.203.98	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:57.633369923 CET	8.8.8.8	192.168.2.3	0xe49c	No error (0)	adservice.google.com		142.250.203.98	A (IP address)	IN (0x0001)

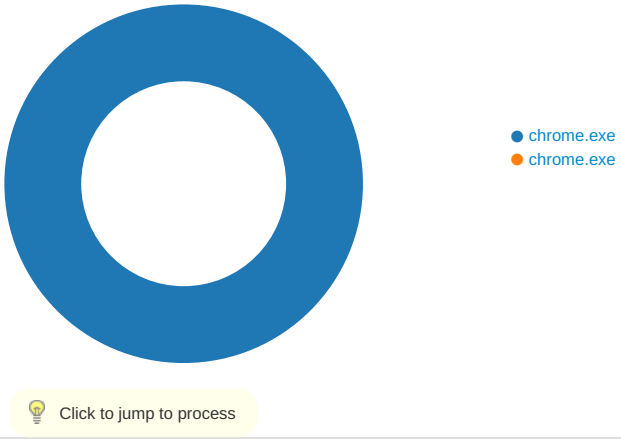
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 29, 2022 00:02:57.697981119 CET	8.8.8.8	192.168.2.3	0xf9d1	No error (0)	pagead-googlehosted.l.google.com		172.217.168.65	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:58.042224884 CET	8.8.8.8	192.168.2.3	0x7aeb	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)
Jan 29, 2022 00:02:58.594784975 CET	8.8.8.8	192.168.2.3	0x49c6	No error (0)	img.women.com		34.98.97.49	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:04.952872038 CET	8.8.8.8	192.168.2.3	0x26ca	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:03:04.952872038 CET	8.8.8.8	192.168.2.3	0x26ca	No error (0)	googlehosted.l.googleusercontent.com		172.217.168.33	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:15.861963034 CET	8.8.8.8	192.168.2.3	0x7e2b	No error (0)	googleads.g.doubleclick.net		172.217.168.2	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:15.886842966 CET	8.8.8.8	192.168.2.3	0x2298	No error (0)	pagead-googlehosted.l.google.com		172.217.168.65	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:16.634085894 CET	8.8.8.8	192.168.2.3	0xc94b	No error (0)	dsum-sec.casalemedia.com	dsum-sec.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:03:16.641491890 CET	8.8.8.8	192.168.2.3	0xb3f3	No error (0)	cm.g.doubleclick.net		172.217.168.34	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:16.665091038 CET	8.8.8.8	192.168.2.3	0xce5e	No error (0)	s0.2mdn.net	s0-2mdn-net.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:03:16.665091038 CET	8.8.8.8	192.168.2.3	0xce5e	No error (0)	s0-2mdn-net.l.google.com		172.217.168.6	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.048772097 CET	8.8.8.8	192.168.2.3	0xc585	No error (0)	googleads4.g.doubleclick.net		172.217.168.66	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.197993040 CET	8.8.8.8	192.168.2.3	0x63f8	No error (0)	px.ads.linkedin.com	www.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:03:17.197993040 CET	8.8.8.8	192.168.2.3	0x63f8	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:03:17.199424028 CET	8.8.8.8	192.168.2.3	0x95f0	No error (0)	tr.blismedia.com		34.96.105.8	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.201896906 CET	8.8.8.8	192.168.2.3	0xbfc7	No error (0)	um.wbtrk.net		127.0.0.2	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.202686071 CET	8.8.8.8	192.168.2.3	0x1e66	No error (0)	cs.media.net		184.87.212.24	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.205073118 CET	8.8.8.8	192.168.2.3	0xb095	No error (0)	rtb2-useast.e-volution.ai	e-volution.rtb-as-useast.ak-is2.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:03:17.205073118 CET	8.8.8.8	192.168.2.3	0xb095	No error (0)	e-volution.rtb-as-useast.ak-is2.net		174.137.133.49	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.206088066 CET	8.8.8.8	192.168.2.3	0x8e8c	No error (0)	s.ad.smaato.net		143.204.215.20	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.206088066 CET	8.8.8.8	192.168.2.3	0x8e8c	No error (0)	s.ad.smaato.net		143.204.215.106	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.206088066 CET	8.8.8.8	192.168.2.3	0x8e8c	No error (0)	s.ad.smaato.net		143.204.215.61	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.206088066 CET	8.8.8.8	192.168.2.3	0x8e8c	No error (0)	s.ad.smaato.net		143.204.215.85	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.275660992 CET	8.8.8.8	192.168.2.3	0xe864	No error (0)	cs.emxdgt.com		18.195.155.181	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.275758028 CET	8.8.8.8	192.168.2.3	0x8b72	No error (0)	um.simpli.fi	nl3ads5.simpli.fi		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:03:17.275758028 CET	8.8.8.8	192.168.2.3	0x8b72	No error (0)	nl3ads5.simpli.fi		169.50.137.182	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.281585932 CET	8.8.8.8	192.168.2.3	0x14fb	No error (0)	a.tribalfusion.com		104.18.12.5	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.281585932 CET	8.8.8.8	192.168.2.3	0x14fb	No error (0)	a.tribalfusion.com		104.18.13.5	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.282377958 CET	8.8.8.8	192.168.2.3	0x3a2d	No error (0)	um.wbtrk.net		127.0.0.2	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.285902023 CET	8.8.8.8	192.168.2.3	0x3ebb	No error (0)	tg.socdm.com	tg.dr.socdm.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 29, 2022 00:03:17.285902023 CET	8.8.8.8	192.168.2.3	0x3ebb	No error (0)	tg.dr.socdm.com		202.241.208.100	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.285902023 CET	8.8.8.8	192.168.2.3	0x3ebb	No error (0)	tg.dr.socdm.com		124.146.215.45	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.285902023 CET	8.8.8.8	192.168.2.3	0x3ebb	No error (0)	tg.dr.socdm.com		202.241.208.53	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.285902023 CET	8.8.8.8	192.168.2.3	0x3ebb	No error (0)	tg.dr.socdm.com		124.146.215.46	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.285902023 CET	8.8.8.8	192.168.2.3	0x3ebb	No error (0)	tg.dr.socdm.com		124.146.215.49	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.285902023 CET	8.8.8.8	192.168.2.3	0x3ebb	No error (0)	tg.dr.socdm.com		202.241.208.56	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.285902023 CET	8.8.8.8	192.168.2.3	0x3ebb	No error (0)	tg.dr.socdm.com		124.146.215.50	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.285902023 CET	8.8.8.8	192.168.2.3	0x3ebb	No error (0)	tg.dr.socdm.com		124.146.215.43	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.285902023 CET	8.8.8.8	192.168.2.3	0x3ebb	No error (0)	tg.dr.socdm.com		124.146.215.42	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.285902023 CET	8.8.8.8	192.168.2.3	0x3ebb	No error (0)	tg.dr.socdm.com		202.241.208.54	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.285902023 CET	8.8.8.8	192.168.2.3	0x3ebb	No error (0)	tg.dr.socdm.com		202.241.208.55	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.285902023 CET	8.8.8.8	192.168.2.3	0x3ebb	No error (0)	tg.dr.socdm.com		124.146.215.51	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.285902023 CET	8.8.8.8	192.168.2.3	0x3ebb	No error (0)	tg.dr.socdm.com		124.146.215.52	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.285902023 CET	8.8.8.8	192.168.2.3	0x3ebb	No error (0)	tg.dr.socdm.com		124.146.215.44	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.285902023 CET	8.8.8.8	192.168.2.3	0x3ebb	No error (0)	tg.dr.socdm.com		124.146.215.48	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.285902023 CET	8.8.8.8	192.168.2.3	0x3ebb	No error (0)	tg.dr.socdm.com		202.241.208.52	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.285902023 CET	8.8.8.8	192.168.2.3	0x3ebb	No error (0)	tg.dr.socdm.com		124.146.215.47	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.285902023 CET	8.8.8.8	192.168.2.3	0x3ebb	No error (0)	tg.dr.socdm.com		202.241.208.57	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.291023016 CET	8.8.8.8	192.168.2.3	0x1a92	No error (0)	match.360yield.com	ice.360yield.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:03:17.291023016 CET	8.8.8.8	192.168.2.3	0x1a92	No error (0)	ice.360yield.com	eu2-ice.360yield.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:03:17.291023016 CET	8.8.8.8	192.168.2.3	0x1a92	No error (0)	eu2-ice.360yield.com		18.197.199.94	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.291023016 CET	8.8.8.8	192.168.2.3	0x1a92	No error (0)	eu2-ice.360yield.com		52.29.17.185	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.291023016 CET	8.8.8.8	192.168.2.3	0x1a92	No error (0)	eu2-ice.360yield.com		52.28.181.192	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.291023016 CET	8.8.8.8	192.168.2.3	0x1a92	No error (0)	eu2-ice.360yield.com		18.192.251.227	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.291023016 CET	8.8.8.8	192.168.2.3	0x1a92	No error (0)	eu2-ice.360yield.com		52.57.206.212	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.291023016 CET	8.8.8.8	192.168.2.3	0x1a92	No error (0)	eu2-ice.360yield.com		52.57.83.77	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.291023016 CET	8.8.8.8	192.168.2.3	0x1a92	No error (0)	eu2-ice.360yield.com		3.67.130.206	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.291023016 CET	8.8.8.8	192.168.2.3	0x1a92	No error (0)	eu2-ice.360yield.com		52.28.100.19	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.327258110 CET	8.8.8.8	192.168.2.3	0x1577	No error (0)	a.rfihub.com	a.rfihub.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:03:17.616915941 CET	8.8.8.8	192.168.2.3	0x4e1f	No error (0)	s.tribalfusion.com		104.18.13.5	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:17.616915941 CET	8.8.8.8	192.168.2.3	0x4e1f	No error (0)	s.tribalfusion.com		104.18.12.5	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:22.297844887 CET	8.8.8.8	192.168.2.3	0x47f7	No error (0)	s0.2mdn.net	s0-2mdn-net.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:03:22.297844887 CET	8.8.8.8	192.168.2.3	0x47f7	No error (0)	s0-2mdn-net.l.google.com		172.217.168.6	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:24.170547009 CET	8.8.8.8	192.168.2.3	0x2647	No error (0)	cm.g.doubleclick.net		172.217.168.34	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 29, 2022 00:03:24.175601959 CET	8.8.8.8	192.168.2.3	0xfc76	No error (0)	dsum-sec.casalemedia.com	dsum-sec.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:03:24.201172113 CET	8.8.8.8	192.168.2.3	0x614f	No error (0)	ib.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:03:24.201172113 CET	8.8.8.8	192.168.2.3	0x614f	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:03:24.201172113 CET	8.8.8.8	192.168.2.3	0x614f	No error (0)	ib.anycast.adnxs.com		185.33.220.243	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:24.201172113 CET	8.8.8.8	192.168.2.3	0x614f	No error (0)	ib.anycast.adnxs.com		185.33.221.14	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:24.201172113 CET	8.8.8.8	192.168.2.3	0x614f	No error (0)	ib.anycast.adnxs.com		185.33.220.145	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:24.201172113 CET	8.8.8.8	192.168.2.3	0x614f	No error (0)	ib.anycast.adnxs.com		185.33.221.15	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:24.201172113 CET	8.8.8.8	192.168.2.3	0x614f	No error (0)	ib.anycast.adnxs.com		185.33.220.242	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:24.201172113 CET	8.8.8.8	192.168.2.3	0x614f	No error (0)	ib.anycast.adnxs.com		185.33.220.216	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:24.201172113 CET	8.8.8.8	192.168.2.3	0x614f	No error (0)	ib.anycast.adnxs.com		185.33.220.240	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:24.201172113 CET	8.8.8.8	192.168.2.3	0x614f	No error (0)	ib.anycast.adnxs.com		185.33.221.87	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:24.201172113 CET	8.8.8.8	192.168.2.3	0x614f	No error (0)	ib.anycast.adnxs.com		185.33.223.38	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:24.201172113 CET	8.8.8.8	192.168.2.3	0x614f	No error (0)	ib.anycast.adnxs.com		185.33.220.244	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:24.201172113 CET	8.8.8.8	192.168.2.3	0x614f	No error (0)	ib.anycast.adnxs.com		185.33.221.13	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:24.201172113 CET	8.8.8.8	192.168.2.3	0x614f	No error (0)	ib.anycast.adnxs.com		185.33.220.241	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:46.328704119 CET	8.8.8.8	192.168.2.3	0x42e8	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:03:46.328704119 CET	8.8.8.8	192.168.2.3	0x42e8	No error (0)	star-mini.c10r.facebook.com		157.240.17.35	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:47.643532991 CET	8.8.8.8	192.168.2.3	0x760c	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:03:47.643532991 CET	8.8.8.8	192.168.2.3	0x760c	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:50.187237978 CET	8.8.8.8	192.168.2.3	0x394	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:03:50.187237978 CET	8.8.8.8	192.168.2.3	0x394	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:57.104393005 CET	8.8.8.8	192.168.2.3	0xbf21	No error (0)	www.quiz-bliss.com		130.211.6.0	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:58.261276960 CET	8.8.8.8	192.168.2.3	0x7162	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jan 29, 2022 00:03:58.261276960 CET	8.8.8.8	192.168.2.3	0x7162	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:58.379762888 CET	8.8.8.8	192.168.2.3	0xdc35	No error (0)	img.women.com		34.98.97.49	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:59.034403086 CET	8.8.8.8	192.168.2.3	0x2008	No error (0)	sb.scorecardresearch.com		143.204.215.7	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:59.034403086 CET	8.8.8.8	192.168.2.3	0x2008	No error (0)	sb.scorecardresearch.com		143.204.215.108	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:59.034403086 CET	8.8.8.8	192.168.2.3	0x2008	No error (0)	sb.scorecardresearch.com		143.204.215.58	A (IP address)	IN (0x0001)
Jan 29, 2022 00:03:59.034403086 CET	8.8.8.8	192.168.2.3	0x2008	No error (0)	sb.scorecardresearch.com		143.204.215.23	A (IP address)	IN (0x0001)

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: **6516**, Parent PID: **580**

General

Target ID:	0
Start time:	00:02:51
Start date:	29/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "https://www.quiz-bliss.com/kittycantrell/harry-potter-20-year-anniversary-trivia-quiz-112821
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: **6740**, Parent PID: **6516**

General

Target ID:	2
Start time:	00:02:52
Start date:	29/01/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1536,9302057933297055962,10316816090944240565,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1924 /prefetch:8
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Disassembly

No disassembly