ID: 513883
Cookbook: browseurl.jbs
Time: 16:40:13
Date: 02/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

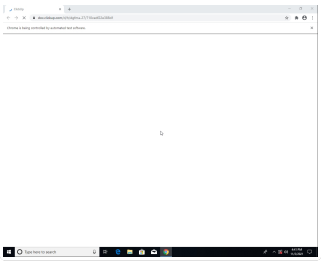
Windows Analysis Report https://doc.clickup.com/d/h/d…

Overview

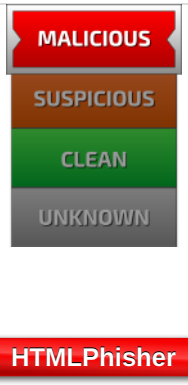
General Information

Sample URL:	http://https://doc.clickup.com/d/h/dgfma-27/710cedf22e388d1
Analysis ID:	513883
Infos:	

Most interesting Screenshot:



Detection



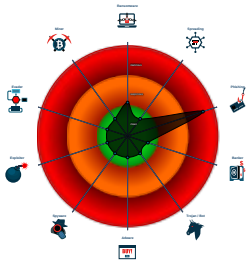
HTMLPhisher

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Phishing site detected (based on fav…
- Yara detected HtmlPhish10
- Phishing site detected (based on log…
- Phishing site detected (based on im…
- HTML body contains low number of …
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6600 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "https://doc.clickup.com/d/h/dgfma-27/710cedf22e388d1 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6812 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1564,4810638549202391110,5699968190218675685,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1928 /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

Click to jump to signature section

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

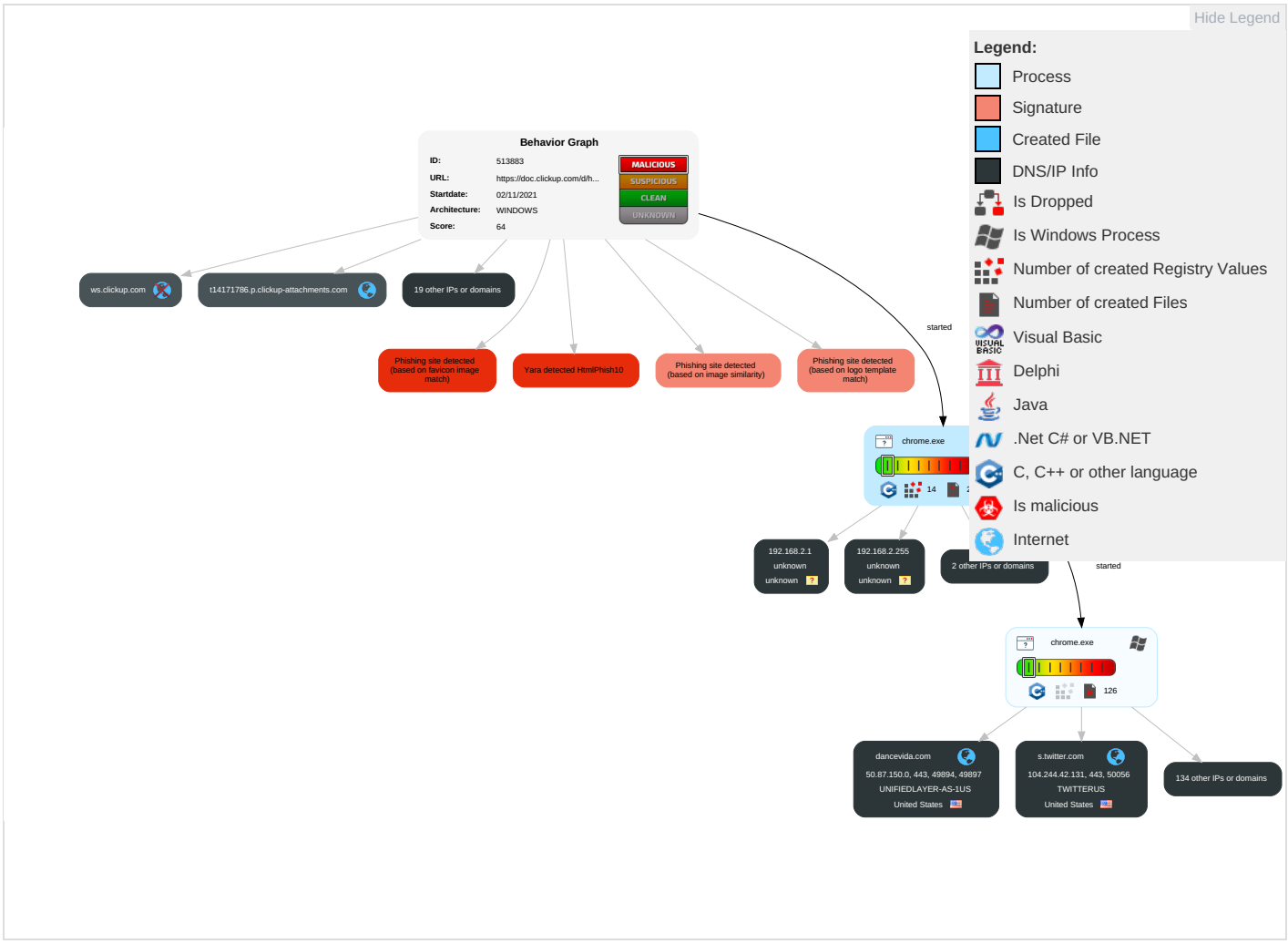
Phishing site detected (based on logo template match)

Phishing site detected (based on image similarity)

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	Process Injection 1	Masquerading 3	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitior
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

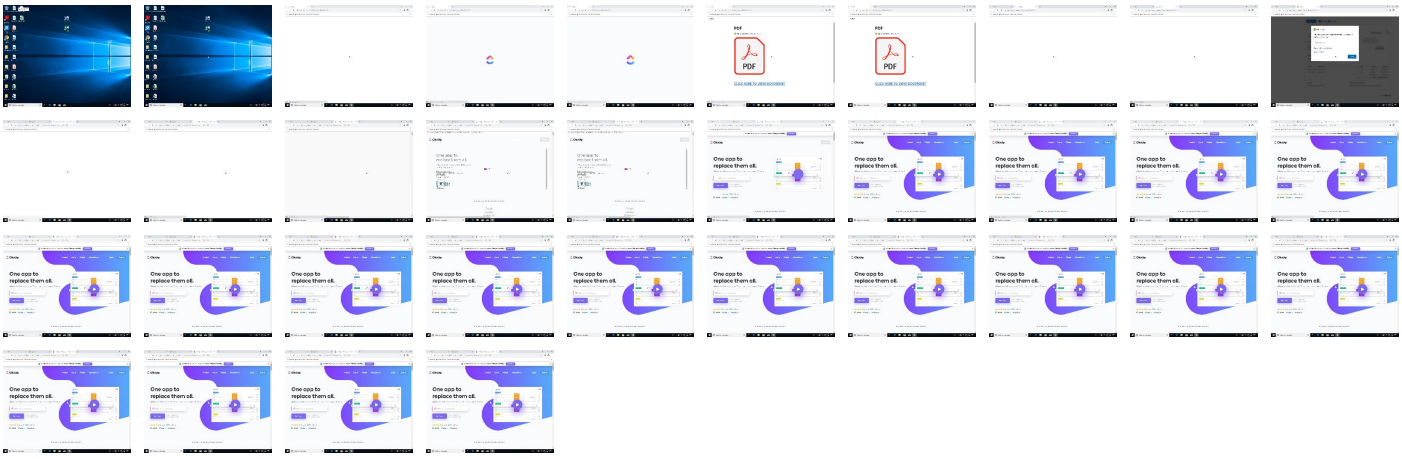
Behavior Graph

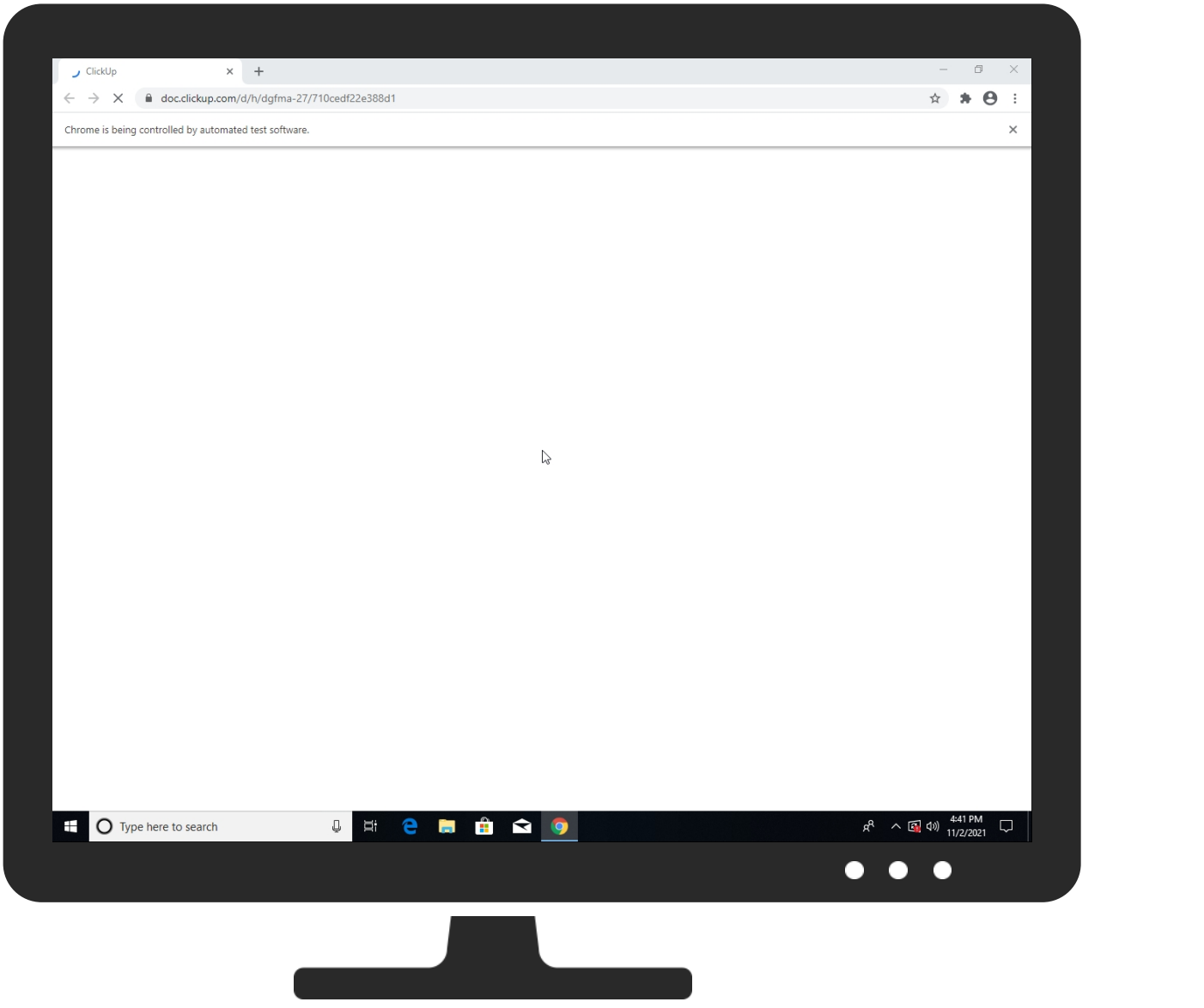


Screenshots

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://doc.clickup.com/d/h/dgfma-27/710cedf22e388d1	3%	Virustotal		Browse
http://https://doc.clickup.com/d/h/dgfma-27/710cedf22e388d1	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.googleoptimize.com	0%	URL Reputation	safe	
http://https://us-central1-adaptive-growth.cloudfunctions.net	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://www.google.co.uk	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	172.217.168.3	true	false		high
forms.hubspot.com	104.19.154.83	true	false		high
clickup.com	18.66.112.90	true	false		high
cu-prod-de-ws.eu-central-1.elasticbeanstalk.com	52.58.90.176	true	false		high
ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com	18.204.101.20	true	false		high
d10w4ikcrdu13z.cloudfront.net	18.66.97.12	true	false		high
platform.twitter.map.fastly.net	151.101.12.157	true	false		unknown
core.thepointyspritesclub.com	34.199.234.25	true	false		unknown
client.mutinycdn.com	13.32.99.34	true	false		unknown
t.co	104.244.42.197	true	false		high
track.hubspot.com	104.19.155.83	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
js.hs-scripts.com	104.17.210.204	true	false		high
dx.steelhousemedia.com	54.69.84.146	true	false		high
d3dib22dsdvm11.cloudfront.net	18.66.97.111	true	false		high
www.google.com	172.217.168.68	true	false		high
cs1227.wpc.alphacdn.net	192.229.221.185	true	false		unknown
tracking.g2crowd.com	104.18.27.190	true	false		high
q.quora.com	3.225.133.12	true	false		high
usage.trackjs.com	138.197.155.84	true	false		high
static-cdn.hotjar.com	52.222.236.39	true	false		high
quora.map.fastly.net	151.101.1.2	true	false		unknown
d2ycxbs0cq3yaz.cloudfront.net	13.32.121.73	true	false		high
px.steelhousemedia.com	54.245.46.233	true	false		high
match.adsrvr.org	52.223.40.198	true	false		high
js.intercomcdn.com	18.66.139.43	true	false		high
star-mini.c10r.facebook.com	157.240.27.35	true	false		high
js.hs-banner.com	104.18.21.191	true	false		unknown
fluffy-alpaca-j1w7zdv61tmqz86b33z4c6tl.herokudns.com	3.234.77.173	true	false		unknown
stats.l.doubleclick.net	142.250.145.154	true	false		high
s.twitter.com	104.244.42.131	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dysvscllmejh2.cloudfront.net	52.222.236.50	true	false		high
ww.steelhousemedia.com	44.238.216.23	true	false		high
monetization-framework.bsa.netdna-cdn.com	108.161.189.78	true	false		high
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
api-iam.intercom.io	99.83.219.81	true	false		high
www.googleoptimize.com	142.250.203.110	true	false		unknown
dualstack.reddit.map.fastly.net	151.101.1.140	true	false		unknown
in-live.live.eks.hotjar.com	54.76.144.107	true	false		high
googleads.g.doubleclick.net	172.217.168.66	true	false		high
reddit.map.fastly.net	151.101.1.140	true	false		unknown
www.google.co.uk	216.58.215.227	true	false		unknown
prod.appnexus.map.fastly.net	151.101.1.108	true	false		unknown
clients.l.google.com	142.250.203.110	true	false		high
calendly.com	172.66.41.40	true	false		high
googlehosted.l.googleusercontent.com	142.250.203.97	true	false		high
d5txjkmyderx.cloudfront.net	18.66.97.12	true	false		high
alb-event-1454785217.us-east-1.elb.amazonaws.com	34.234.150.139	true	false		high
dancevida.com	50.87.150.0	true	false		unknown
afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com	54.147.21.139	true	false		high
global-v2.clearbit.com	18.168.94.208	true	false		high
hat.thepointyspritesclub.com	18.66.139.27	true	false		unknown
d3uwzcb5nysxzm.cloudfront.net	52.222.214.92	true	false		high
js.hs-analytics.net	104.17.68.176	true	false		unknown
x.clearbit.com	18.169.251.168	true	false		high
dl7g9llrghqi1.cloudfront.net	18.66.112.118	true	false		high
pop-edc2.mix.linkedin.com	108.174.11.85	true	false		high
us-central1-adaptive-growth.cloudfunctions.net	216.239.36.54	true	false		unknown
insight.adsrvr.org	52.223.40.198	true	false		high
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com	54.85.240.191	true	false		high
script.hotjar.com	18.66.112.122	true	false		high
cdn.pdst.fm	35.244.142.80	true	false		unknown
nexus-websocket-a.intercom.io	35.174.127.31	true	false		high
stackpath.bootstrapcdn.com	104.18.10.207	true	false		high
accounts.google.com	172.217.168.45	true	false		high
www-google-analytics.l.google.com	216.58.215.238	true	false		high
ws.zoominfo.com	104.16.101.12	true	false		high
pop-esv5.mix.linkedin.com	108.174.11.37	true	false		high
www-googletagmanager.l.google.com	172.217.168.8	true	false		high
widget.intercom.io	13.32.99.55	true	false		high
api.clickup.com	18.194.89.172	true	false		high
d279x8308vq8mj.cloudfront.net	18.66.112.76	true	false		high
doc-cdn.clickup.com	18.66.112.24	true	false		high
embeds.driftcdn.com	13.32.99.26	true	false		unknown
vars.hotjar.com	18.66.139.40	true	false		high
gentle-meadow-3800.shrouded-lake-4691.herokuspace.com	44.237.209.143	true	false		unknown
t14171786.p.clickup-attachments.com	18.66.112.18	true	false		unknown
api.getdrip.com	52.222.236.11	true	false		high
app.clickup.com	18.193.151.4	true	false		high
ib.anycast.adnxs.com	185.33.220.243	true	false		high
js.hscollectedforms.net	104.17.128.171	true	false		unknown
alb.reddit.com	unknown	unknown	false		high
static.ads-twitter.com	unknown	unknown	false		unknown
presence.api.drift.com	unknown	unknown	false		high
metrics.api.drift.com	unknown	unknown	false		high
5001341-41.chat.api.drift.com	unknown	unknown	false		high
app-cdn.clickup.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
sdk-services.minervaknows.com	unknown	unknown	false		unknown
use.fontawesome.com	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
js.driftt.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
static.hotjar.com	unknown	unknown	false		high
conversation.api.drift.com	unknown	unknown	false		high
www.redditstatic.com	unknown	unknown	false		high
acdn.adnxs.com	unknown	unknown	false		high
aadcdn.msauth.net	unknown	unknown	false		unknown
doc.clickup.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://js.driftt.com/core?embedId=dxfgnwx9niuc®ion=US&forceShow=false&skipCampaigns=false&sessionId=51f50fdc-cab6-4534-a616-c5d9535e693b&sessionStarted=1635896519.113&campaignRefreshToken=97217105-29d7-45cc-aa23-fa5f6ec739c4&hideController=false&pageLoadStartTime=1635896502841&mode=CHAT&driftEnableLog=false	false		high
http://https://js.driftt.com/core/chat?region=US&driftEnableLog=false&pageLoadStartTime=1635896502841	false		high
http://https://sdk-services.minervaknows.com/tunnel/index.html?xdm_e=https%3A%2F%2Fclickup.com&xdm_c=default5389&xdm_p=1	true		unknown
http://https://clickup.com/?utm_source=clickup&utm_medium=doc&utm_campaign=14171786	false		high
http://https://vars.hotjar.com/box-d09a446edefba0dcce5d5143e1840e9a.html	false		high
http://https://doc.clickup.com/d/h/dgfma-27/710cedf22e388d1	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.19.155.83	track.hubspot.com	United States		13335	CLOUDFLARENETUS	false
216.58.215.238	www-google-analytics.l.google.com	United States		15169	GOOGLEUS	false
35.174.127.31	nexus-websocket-a.intercom.io	United States		14618	AMAZON-AESUS	false
151.101.1.2	quora.map.fastly.net	United States		54113	FASTLYUS	false
104.18.21.191	js.hs-banner.com	United States		13335	CLOUDFLARENETUS	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
3.234.77.173	fluffy-alpaca-j1w7zdv61tmqz86b33z4c6tl.herokudns.com	United States		14618	AMAZON-AESUS	false
44.238.216.23	ww.steelhousemedia.com	United States		16509	AMAZON-02US	false
185.33.220.243	ib.anycast.adnxs.com	Netherlands		29990	ASN-APPNEXUS	false
3.225.133.12	q.quora.com	United States		14618	AMAZON-AESUS	false
54.76.144.107	in-live.live.eks.hotjar.com	United States		16509	AMAZON-02US	false
54.245.46.233	px.steelhousemedia.com	United States		16509	AMAZON-02US	false
216.58.215.227	www.google.co.uk	United States		15169	GOOGLEUS	false
52.222.214.92	d3uwzcb5nysxzm.cloudfront.net	United States		16509	AMAZON-02US	false
18.66.139.27	hat.thepointyspritesclub.com	United States		3	MIT-GATEWAYSUS	false
52.222.236.11	api.getdrip.com	United States		16509	AMAZON-02US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
192.229.221.185	cs1227.wpc.alphacdn.net	United States		15133	EDGECASTUS	false
52.28.94.139	unknown	United States		16509	AMAZON-02US	false
104.18.10.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
108.161.189.78	monetization-framework.bsa.netdna-cdn.com	United States		33438	HIGHWINDS2US	false
172.217.168.68	www.google.com	United States		15169	GOOGLEUS	false
104.17.210.204	js.hs-scripts.com	United States		13335	CLOUDFLARENETUS	false
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
44.237.209.143	gentle-meadow-3800.shrouded-lake-4691.herokuspace.com	United States		16509	AMAZON-02US	false
18.66.139.43	js.intercomcdn.com	United States		3	MIT-GATEWAYSUS	false
18.66.139.40	vars.hotjar.com	United States		3	MIT-GATEWAYSUS	false
172.217.168.66	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
34.199.234.25	core.thepointyspritesclub.com	United States		14618	AMAZON-AESUS	false
13.32.99.55	widget.intercom.io	United States		16509	AMAZON-02US	false
54.85.240.191	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com	United States		14618	AMAZON-AESUS	false
18.66.112.24	doc-cdn.clickup.com	United States		3	MIT-GATEWAYSUS	false
104.244.42.197	t.co	United States		13414	TWITTERUS	false
99.83.219.81	api-iam.intercom.io	United States		16509	AMAZON-02US	false
151.101.1.140	dualstack.reddit.map.fastly.net	United States		54113	FASTLYUS	false
18.168.94.208	global-v2.clearbit.com	United States		3	MIT-GATEWAYSUS	false
52.222.236.39	static-cdn.hotjar.com	United States		16509	AMAZON-02US	false
52.58.90.176	cu-prod-de-ws.eu-central-1.elasticbeanstalk.com	United States		16509	AMAZON-02US	false
104.17.68.176	js.hs-analytics.net	United States		13335	CLOUDFLARENETUS	false
18.66.112.18	t14171786.p.clickup-attachments.com	United States		3	MIT-GATEWAYSUS	false
172.66.41.40	calendly.com	United States		13335	CLOUDFLARENETUS	false
54.147.21.139	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com	United States		14618	AMAZON-AESUS	false
13.32.99.26	embeds.driftcdn.com	United States		16509	AMAZON-02US	false
34.234.150.139	alb-event-1454785217.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.203.97	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
108.174.11.85	pop-edc2.mix.linkedin.com	United States		14413	LINKEDINUS	false
104.16.101.12	ws.zoominfo.com	United States		13335	CLOUDFLARENETUS	false
104.17.128.171	js.hscollectedforms.net	United States		13335	CLOUDFLARENETUS	false
54.69.84.146	dx.steelhousemedia.com	United States		16509	AMAZON-02US	false
18.194.89.172	api.clickup.com	United States		16509	AMAZON-02US	false
157.240.27.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false
18.169.251.168	x.clearbit.com	United States		3	MIT-GATEWAYSUS	false
104.19.154.83	forms.hubspot.com	United States		13335	CLOUDFLARENETUS	false
104.244.42.131	s.twitter.com	United States		13414	TWITTERUS	false
13.32.99.34	client.mutinycdn.com	United States		16509	AMAZON-02US	false
18.204.101.20	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
18.66.112.90	clickup.com	United States		3	MIT-GATEWAYSUS	false
52.222.236.50	dysvscllmejh2.cloudfront.net	United States		16509	AMAZON-02US	false
216.239.36.54	us-central1-adaptive-growth.cloudfunctions.net	United States		15169	GOOGLEUS	false
52.223.40.198	match.adsrvr.org	United States		8987	AMAZONEXPANSIONGB	false
18.66.112.122	script.hotjar.com	United States		3	MIT-GATEWAYSUS	false
151.101.12.157	platform.twitter.map.fastly.net	United States		54113	FASTLYUS	false
18.66.97.111	d3dib22dsdvm11.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
18.66.97.12	d10w4ikcrdu13z.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
18.66.112.118	dl7g9llrghqi1.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
142.250.203.110	www.googleoptimize.com	United States		15169	GOOGLEUS	false
18.66.112.76	d279x8308vq8mj.cloudfront.net	United States		3	MIT-GATEWAYSUS	false
13.32.121.73	d2ycxbs0cq3yaz.cloudfront.net	United States		16509	AMAZON-02US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
18.66.97.110	unknown	United States		3	MIT-GATEWAYSUS	false
172.217.168.8	www-googletagmanager.l.google.com	United States		15169	GOOGLEUS	false
172.217.168.3	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
151.101.1.108	prod.appnexus.map.fastly.net	United States		54113	FASTLYUS	false
34.193.113.164	unknown	United States		14618	AMAZON-AESUS	false
142.250.145.154	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
18.193.151.4	app.clickup.com	United States		16509	AMAZON-02US	false
35.244.142.80	cdn.pdst.fm	United States		15169	GOOGLEUS	false
138.197.155.84	usage.trackjs.com	United States		14061	DIGITALOCEAN-ASNUS	false
50.87.150.0	dancevida.com	United States		46606	UNIFIEDLAYER-AS-1US	false
104.18.27.190	tracking.g2crowd.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.255
192.168.2.1
192.168.2.7
192.168.2.3
192.168.2.5
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	513883
Start date:	02.11.2021
Start time:	16:40:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://doc.clickup.com/d/h/dgfma-27/710cedf22e388d1
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:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.phis.win@25/180@105/86
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://storage.googleapis.com/eknknle.appspot.com/23971.html • Browse: https://clickup.com/?utm_source=clickup&utm_medium=doc&utm_campaign=14171786 • Browse: https://clickup.com/blog/series-c
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
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\08b3984d-2389-4f9a-bd23-e9b132d48017.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):	176145
Entropy (8bit):	6.046974781743798
Encrypted:	false
SSDEEP:	3072:SIxcSRcPWIiRuBYC0RgGKjG0sQRAUAZvtkhVPPLA7bV/nYorVcI8XIssElYTRU:LTclNI1B8RPyc3gbV/njhcI8II6RU
MD5:	ABDE20C5C1DC720920AA3B9F9A30BEC4
SHA1:	4943C0FB537D8C8D50CB13DD4221A5F120E75482
SHA-256:	03B2B4A7D6D266369EB2ACA682FBC002F8C19C5EC5D1E7FEED8AE976EE61D3BA
SHA-512:	1AF3F6F1CAA6BDBEB4B3974B29DDBB4866B84EC9D0BEE7D07EDF7CC3429F5647B2833BD3F8C37C4D57A6F941F32D25C8BF781C244FC2893ECF2CB92EE03F7E23
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":1.635896478109835e+12,"network":1.63586768e+12,"ticks":122113334.0,"uncertainty":3968425.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0l1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909086161"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\196cb929-19ca-416d-9aea-672f5031c0c6.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):	176145
Entropy (8bit):	6.046974781743798
Encrypted:	false
SSDEEP:	3072:SIxcSRcPWIiRuBYC0RgGKjG0sQRAUAZvtkhVPPLA7bV/nYorVcI8XIssElYTRU:LTclNI1B8RPyc3gbV/njhcI8II6RU
MD5:	ABDE20C5C1DC720920AA3B9F9A30BEC4
SHA1:	4943C0FB537D8C8D50CB13DD4221A5F120E75482
SHA-256:	03B2B4A7D6D266369EB2ACA682FBC002F8C19C5EC5D1E7FEED8AE976EE61D3BA
SHA-512:	1AF3F6F1CAA6BDBEB4B3974B29DDBB4866B84EC9D0BEE7D07EDF7CC3429F5647B2833BD3F8C37C4D57A6F941F32D25C8BF781C244FC2893ECF2CB92EE03F7E23
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":1.635896478109835e+12,"network":1.63586768e+12,"ticks":122113334.0,"uncertainty":3968425.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0l1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909086161"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\1e36a580-b618-4913-8590-efbf8ad35c5f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	184617
Entropy (8bit):	6.076258192596406
Encrypted:	false
SSDEEP:	3072:zkjIxcSRcPWIiRuBYC0RgGKjG0sQRAUAZvtkhVPPLA7bV/nYorVcI8XIssElYTRU:ouTclNI1B8RPyc3gbV/njhcI8II6RU
MD5:	2C4B69C68661CF99375BABEEE9381E12
SHA1:	EC88E1005C7691FF6A94FF9E802264CA68BF58F7
SHA-256:	44139441AECF2933ECA39322C72FB8285344ECE27D2B48A98707AE2925ED48EF
SHA-512:	148F9BCE41B6023B9230A66987DFF2F3CEED580D10F84135E9FEE28DFAA1880D09123173039C3866B45C2DC093B29CC59B8FEBD8C66FD6C4F55A4C664E8C7CE

C:\Users\user\AppData\Local\Google\Chrome\User Data\1e36a580-b618-4913-8590-efbf8ad35c5f.tmp	
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":1.635896478109835e+12,"network":1.63586768e+12,"ticks":122113334.0,"uncertainty":3968425.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0l1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909086161"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\20e2d359-defc-45ae-b19b-ff08f5cacaaa.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):	184616
Entropy (8bit):	6.076258717829855
Encrypted:	false
SSDEEP:	3072:HkJIxcSRcPWIiRuBYC0RgGKjG0sQRAUAZvtkhVPPLA7bV/nYorVcI8XIssElYTRU:EMTclNI1B8RPyc3gbV/njhcI8II6RU
MD5:	7E1C233ACD9E24C4CCD4EA8FAB3D5031
SHA1:	F88E5AB0F1EC56995BEF76B7F6FF77D08F9C9D79
SHA-256:	FEA1A13B496DE765CED89F7F6EBC5DA5F2960D437B18DBCE75CFB368AFCC2338
SHA-512:	C4A7FEF9B5B05319FEEDBE58C0B6AA186C6A55EE23C2FB2D71E5C4F5D2AA936453A47B222361220BF95BA4BD613E0C249831179F825269111082F27A7B36BF4
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":1.635896478109835e+12,"network":1.63586768e+12,"ticks":122113334.0,"uncertainty":3968425.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0l1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909820208"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\4957f72f-c20e-4139-abe5-be3aa277a0bb.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):	184616
Entropy (8bit):	6.076259663517651
Encrypted:	false
SSDEEP:	3072:HkjIxcSRcPWIiRuBYC0RgGKjG0sQRAUAZvtkhVPPLA7bV/nYorVcI8XIssElYTRU:EuTclNI1B8RPyc3gbV/njhcI8II6RU
MD5:	D0D6A3E2EDCA0E944B127C60A4CA9EC4
SHA1:	2AADEE72F24D8A2182783C8974AD503D8315FA12
SHA-256:	E859C60974DD2B580EA2967FD87292C5BD7DB46315D214EE5DBE210FE4ACE2C2
SHA-512:	3E0FA411B9F7375ADA0523DFBCCAA5940A2462C6EA1CA539BCAFF22CB161B4B00F97037BF61DA5D337F86CC294AE8DA637353FB16C45457A7BDDAFC522F10A4C
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":1.635896478109835e+12,"network":1.63586768e+12,"ticks":122113334.0,"uncertainty":3968425.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0l1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909820208"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\8cfc8cec-ad05-4085-bf48-f704c60445c8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	96680
Entropy (8bit):	3.7508949323950866
Encrypted:	false
SSDEEP:	384:GrzQkmlnJdhOYV9/EbNYrxvUw3bouTHOrG/CrtyECRxbS6uNrJQmtaBiowkLOmS2:f2Cl5me7TIeDXo8GAfbaYKiI01x
MD5:	32E5E2265A9ED17D3233AA88424033B4
SHA1:	D24B3A6423A08CEE91BDA5481BFBDF39D1CAD7A2
SHA-256:	693DC1911E6E464FD7C1BA036943949F732DEE796879DA830A7C16B07E47B448
SHA-512:	72B6FEB184DD21724A24306C34B357C841B573C50C0AF02C86E38ADE559ECAC2A31E50E36D5FC18D2A3A78100174CD67FAA02E5DA065CAF796D1A8C5D03CB8A

C:\Users\user\AppData\Local\Google\Chrome\User Data\8cfc8cec-ad05-4085-bf48-f704c60445c8.tmp	
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....J8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.......m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.......1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXJFIsz6I:+rJJ
MD5:	CE74DBAFA9F4B2CE737AF2E3003A3465
SHA1:	2F58FDA138667FA4941DE1AA201DD70EFF4AAC75
SHA-256:	896C9BD2EDA0D6EEA85229BA58AB7E423D179FD5567CBF0DC9B7EBC1D0539E1D
SHA-512:	8A377209C5DB20248067D2B8283610B58370F6EB8A8AAB1741674414AC07B124678A89A5D85AFA563D09CD526114DA0EE534BDF36A35E43D4DA7FC2D63977D5
Malicious:	false
Reputation:	low
Preview:	sdPC......................@.*.L..nM._bM

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\17641d58-96f6-461d-a767-9da121ba3f84.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):	5190
Entropy (8bit):	4.984491983343196
Encrypted:	false
SSDEEP:	96:n73h55q9pYKIkik0JCKL8lkb1YbOTQVuwn:nzhK9pYOk4KokbI
MD5:	82C8378C9E72F7C630A3552A6FD5C0BB
SHA1:	CB28882E30381419BB0797827C30AAE6B84D7CB8
SHA-256:	0606ED08E36A77C8A9DBA68ABB2B122535CC97B522293C667A99F27AC49A1CC8
SHA-512:	F75A5266E845F70EFF3F7276A8DCD5454DD62D24DF3135BF6B992D19685F1F259B6330798736CC8124DA79097037F4B134E2A290DA94E2D8A83C06D78A7C0D58
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280370076667147","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser _infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_pl acement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"co untryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0" ,"0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\24afbe05-2cc6-4a3d-b74b-e8bc731f8626.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):	5154
Entropy (8bit):	4.985671179879935
Encrypted:	false
SSDEEP:	96:n73hRq/9pYKIUik0JCKL8lkb1YbOTQVuwn:nzha9pY2k4KokbI
MD5:	7DBFC9C41E35385D3625C6221CE26CD7
SHA1:	5F63764A7C4D1145E2CE7C4A0961FCB918E34125
SHA-256:	FF1AFCE9D3B4B34E357275E2092190D747972F31B172B1CB71224A8B0BB118D6
SHA-512:	D7055C3B16CEFCB9A2194E8D80F60A9D6BC5A6548639BF35A3036236289F331976A8BC81EC75C401A7DB02E9371DA3DAA62414B7F63F1D1185C8D9EE6BA77D 2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\24afbe05-2cc6-4a3d-b74b-e8bc731f8626.tmp

Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280370076667147","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\534f35dd-e55a-4395-b594-37d864d190d7.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):	4289
Entropy (8bit):	4.91716859947933
Encrypted:	false
SSDEEP:	96:JDHXTOazIayY6Vn6M5TFI3q6xKh0T1E2gVGhLJhj:JDHXTOazIayY6Vn6ITFI3q6xa0TK2gVW
MD5:	76F980874429309740BBCB2E6637EA65
SHA1:	634528E3E936E63FB0F547133CF3B0D47E311924
SHA-256:	04684565FD790C82A14A61BFDA346262D570B13B4E14D0C99646B97A30EFE859
SHA-512:	DCFB1EB74A2238904B61332D509CFBFCA6FB03CEC87D783D3411E94054476FDA94DE5A1DCEB0B2EF7A9EAB73348AE55D0FC5D4BF742C6585F7E9DAE63816D9A
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.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":"13282962078379339","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13282962078402805","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13282962078532627","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"e

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\569baa0d-a828-4763-9a02-8bb6e60b6685.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):	5462
Entropy (8bit):	5.005428714195453
Encrypted:	false
SSDEEP:	96:n73h7Vq9pYKIkik0JCKL8LkXhvkb1PbOTQVuwn:nzhc9pYOk4KSkXVkbx
MD5:	219A0F6BB5A9D93CB5D0371D156D51F3
SHA1:	6892606188D63058C7DB350287907A4A07F34232
SHA-256:	6A19557F9D43BF0D0C965264CB7CF864ABC98A59876494FF173753B94CB921E5
SHA-512:	463A1083F458071D405E922EE93524DAC1D5CF9E037AD8A0C5A890C04ED0D67A610B551D7FFB02801DC7D9A31BB84D886640BC4F6F67B5B1DCEA9A3E5EC868C
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280370076667147","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5cab01e5-00a0-4267-9f2f-25048009478e.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	537
Entropy (8bit):	5.546122727860212
Encrypted:	false
SSDEEP:	12:YY9RAJ9+UAnI8gcUQLmDMpL/fN+UAnIbAcUNlx+UAnI4Q:YY9RAeUX8rfwU56NlcUSQ
MD5:	A334D8CD071856B6B50A8ABCEE0E3346
SHA1:	B5DF7DA287460CB255A7E220496A05A951A78B26
SHA-256:	9D4ABE816CEA3FBEE46F9819C9A26A284E18E56360074BD87C4DD446F0043FA4
SHA-512:	AD7E51DF87B251504800E565E29FCA3BB9635C4053CE0FDBF0292B1FF1BC1623654BF6FA026799162B6F86D7BBEFD608F80A7F0050F6F4D7EB5EB7C66906D6BC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5cab01e5-00a0-4267-9f2f-25048009478e.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1667432512.290796,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1635896512.290802},{"expiry":1667432505.165795,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1635896505.165802},{"expiry":1667432502.855094,"host":"opXOuPncEqRjkYSjAgcGEU30CFS/DB8Obxt4KuKod80=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1635896502.855103}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\85854394-f043-4d22-a26c-9e6b64c96a87.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):	5.570178417277114
Encrypted:	false
SSDEEP:	384:c1ttaLlNGXT1kXqKf/pUZNCgVLH2HfD0rUzHGym/gJj4P:VLlKT1kXqKf/pUZNCgVLH2HfIrUTGPg6
MD5:	0A1D098B1BD20D9F4C0017D1C7A9D8A0
SHA1:	AA308794830C093CBA3F3758A1CD968E943A631E
SHA-256:	6D235C57B9A2C58D79C81AE41A01EA61345E8FB0FA0AD659EB59944405F254D3
SHA-512:	DF27FF5DCE044B924447C0467C1745976C84B138D9685531E5EC02225E5CB75EDB47BD74C65DD6228682229944AC8207A0B5EDD791B812A5B1769C7A2A3ABA0
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":"13280370076074715","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\85b1897b-40dd-4a36-88c9-a43ca7ae2e23.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):	5155
Entropy (8bit):	4.9862379633123615
Encrypted:	false
SSDEEP:	96:n73h55q9pYKIUik0JCKL8lkb1YbOTQVuwn:nzhK9pY2k4KokbI
MD5:	39DAAEE3ADC21EB71348BF255D7446F6
SHA1:	768BDD6565038F4D53F25D0F2B53DCBDC86E5794
SHA-256:	D9A7D16098CA03CFECFBBF1FA05791526A61A598D5A239975F3FE7CC12323835
SHA-512:	9A28FC741080FED6D9C965247D0971637C74F69D0AF4C78FE69AFC67F690AA73D4BE52AD974E35027862CB5D92FC6D8DFA8BA0D7A6D815579C930223EC47F4D A
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280370076667147","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9a06a518-2a00-4dc8-a9df-b8eefa68fa7e.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):	5.583176778442783
Encrypted:	false
SSDEEP:	384:c1ttaLlNGXT1kXqKf/pUZNCgVLH2HfD0rUumwgJj4ld:VLlKT1kXqKf/pUZNCgVLH2HfIrUkgJjl
MD5:	43ED02B188EC102C154EBB3F66686AE7
SHA1:	A49642575C73FAB7E7B26277F62B1CDDDDF9D3EA
SHA-256:	E48180559EE06E38FC3F42B19D483954209E3B7C92BB0ACB28F0B27E46BE3E6E
SHA-512:	0502F18F50AF04DE046B48BC604163B8828BE5984BE9B66E89AE626A01BB7652BEF608051D8B319DEFD339EB61D2EB3F2D54997565BAF0B7DA56AC8DD68AE33 3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9a06a518-2a00-4dc8-a9df-b8eefa68fa7e.tmp	
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":"13280370076074715","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/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

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+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSklhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhIktCK62v2P3OZQAWupWsYzCnvk=","L

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
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):	380
Entropy (8bit):	5.2270204239339915
Encrypted:	false
SSDEEP:	6:mLdE53+q2PcNwi23iKKdK25+Xqx8chI+IFUt8djXmZmwqdIFlVkwOcNwi23iKKdP:B53+vLZ5KkTXfchI3FUtKXm/9mV54Z5G
MD5:	407E6CF4A138E3E2C50B66497C10194E
SHA1:	C4B3D6BBA14F76C43E022422FD838DDCDD605379
SHA-256:	5D96ED312FB8E08383D57B07C2D2F18177D93A2AA7BFA5ED42CDB42AC8A2D068
SHA-512:	F969A0E836F3EF2BF4970EF62684DB6DFA39932CC1C86ACA71D21B4DA6ABF5BAEBE3B1AB84C5925C619345E1D48AE1A8A7901A067B6415C92689F77EA0C9BA51
Malicious:	false
Reputation:	low
Preview:	2021/11/02-16:41:35.801 1a2c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/11/02-16:41:35.803 1a2c Recovering log #3.2021/11/02-16:41:35.804 1a2c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	380
Entropy (8bit):	5.2270204239339915
Encrypted:	false
SSDEEP:	6:mLdE53+q2PcNwi23iKKdK25+Xqx8chI+IFUt8djXmZmwqdIFlVkwOcNwi23iKKdP:B53+vLZ5KkTXfchI3FUtKXm/9mV54Z5G
MD5:	407E6CF4A138E3E2C50B66497C10194E
SHA1:	C4B3D6BBA14F76C43E022422FD838DDCDD605379
SHA-256:	5D96ED312FB8E08383D57B07C2D2F18177D93A2AA7BFA5ED42CDB42AC8A2D068
SHA-512:	F969A0E836F3EF2BF4970EF62684DB6DFA39932CC1C86ACA71D21B4DA6ABF5BAEBE3B1AB84C5925C619345E1D48AE1A8A7901A067B6415C92689F77EA0C9BA51
Malicious:	false
Reputation:	low
Preview:	2021/11/02-16:41:35.801 1a2c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/11/02-16:41:35.803 1a2c Recovering log #3.2021/11/02-16:41:35.804 1a2c 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):	640
Entropy (8bit):	5.141784272793393
Encrypted:	false
SSDEEP:	12:gP/xtf2NRRXtTUBKi+SpJBUTAGSuETTSJim1IA7saCFgPBk778B/xgskZBa9sdmI:k3f2zRXtCuGv6NSugTeim1IQLY78BJgH
MD5:	8C20A867CE58054A86A7F17E152DEF63
SHA1:	7D70D52400EED7345DA45B80E19EEC3C56AA401E
SHA-256:	38BEAB26513A24F3F1E613C1CA5E83D2893D3E8EC770342306EF6E1DE219CB06
SHA-512:	D39E9FF4DFFDB13212A31F697746022F291D35584175B248048A8547107500ACC76A27849FC0374AABA3AFCF48C3F22EFF3AA3F270D60A129C547127C4113F64
Malicious:	false
Reputation:	low
Preview:	....."C....27..710cedf22e388d1..clickup..com..d..dgfma..doc..h..https..pdf*k.....27.....710cedf22e388d1.....clickup.....com.....d.....dgfma.....doc.....h.....https.....pdf..2.....0.....1.....2.....3.....7.....8.....a.....c.....d.....e.....f.....g.....h.....i.....k.....l.....m.....o.....p.....s.....t.....u...:\.....Bp...l..... .....*4https://doc.clickup.com/d/h/dgfma-27/710cedf22e388d12.PDF:.....:.....J....."%...

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy)	
Size (bytes):	2724
Entropy (8bit):	4.858441642519087
Encrypted:	false
SSDEEP:	48:YXsPMHi5s7MHgKsSMH/zs8MHIs51tFsL6zsbWsdCshDysuMHCLsKMH9swIMHlYhj:XGiQGBGFGJ12LLHDwGyGkGihj
MD5:	9E0C31BCE1C83C78981EB86A29E2879B
SHA1:	3973E5D4DA1BC0BB99B78D1DFA7BEA045C85E173
SHA-256:	3D1BDA968D1CFF79DBD0C4B9D2A22367E9D9B8374622CD4263BD39137D8FE584
SHA-512:	D196B2993F4A46AFFD38DBA59866B048221D5CF6EAB1574846D1799B748BD71B09BE28D8154B16D97AEA300C7EE13719DC2E5034EC9D8913C6A6B399BDEBC2E
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544495618845","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31528},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345624305","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":26637},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345531701","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":53820},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345601356","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":36228},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

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):	5154
Entropy (8bit):	4.985671179879935
Encrypted:	false
SSDEEP:	96:n73hRq/9pYKIUik0JCKL8lkb1YbOTQVuwn:nzha9pY2k4KokbI
MD5:	7DBFC9C41E35385D3625C6221CE26CD7
SHA1:	5F63764A7C4D1145E2CE7C4A0961FCB918E34125
SHA-256:	FF1AFCE9D3B4B34E357275E2092190D747972F31B172B1CB71224A8B0BB118D6
SHA-512:	D7055C3B16CEFCB9A2194E8D80F60A9D6BC5A6548639BF35A3036236289F331976A8BC81EC75C401A7DB02E9371DA3DAA62414B7F63F1D1185C8D9EE6BA77D2
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280370076667147","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences\ (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5190
Entropy (8bit):	4.984491983343196
Encrypted:	false
SSDEEP:	96:n73h55q9pYKIkik0JCKL8lkb1YbOTQVuwn:nzhK9pYOk4KokbI
MD5:	82C8378C9E72F7C630A3552A6FD5C0BB
SHA1:	CB28882E30381419BB0797827C30AAE6B84D7CB8
SHA-256:	0606ED08E36A77C8A9DBA68ABB2B122535CC97B522293C667A99F27AC49A1CC8
SHA-512:	F75A5266E845F70EFF3F7276A8DCD5454DD62D24DF3135BF6B992D19685F1F259B6330798736CC8124DA79097037F4B134E2A290DA94E2D8A83C06D78A7C0D58
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280370076667147","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\PreferencesrO (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):	5155
Entropy (8bit):	4.9862379633123615

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\PreferencesrO (copy)	
Encrypted:	false
SSDEEP:	96:n73h55q9pYKIUik0JCKL8lkb1YbOTQVuwn:nzhK9pY2k4KokbI
MD5:	39DAAEE3ADC21EB71348BF255D7446F6
SHA1:	768BDD6565038F4D53F25D0F2B53DCBDC86E5794
SHA-256:	D9A7D16098CA03CFECFBBF1FA05791526A61A598D5A239975F3FE7CC12323835
SHA-512:	9A28FC741080FED6D9C965247D0971637C74F69D0AF4C78FE69AFC67F690AA73D4BE52AD974E35027862CB5D92FC6D8DFA8BA0D7A6D815579C930223EC47F4D A
Malicious:	false
Reputation:	low
Preview:	

{"account_id_migration_state":2,"account_tracker_service_last_update":"13280370076667147","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

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):	17092
Entropy (8bit):	5.583176778442783
Encrypted:	false
SSDEEP:	384:c1ttaLlNGXT1kXqKf/pUZNCgVLH2HfD0rUumwgJj4ld:VLlKT1kXqKf/pUZNCgVLH2HfIrUkgJjI
MD5:	43ED02B188EC102C154EBB3F66686AE7
SHA1:	A49642575C73FAB7E7B26277F62B1CDDDDF9D3EA
SHA-256:	E48180559EE06E38FC3F42B19D483954209E3B7C92BB0ACB28F0B27E46BE3E6E
SHA-512:	0502F18F50AF04DE046B48BC604163B8828BE5984BE9B66E89AE626A01BB7652BEF608051D8B319DEFD339EB61D2EB3F2D54997565BAF0B7DA56AC8DD68AE33 3
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":"13280370076074715","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 Preferencesr@ (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):	5.577541734713801
Encrypted:	false
SSDEEP:	384:c1ttvLlNGXT1kXqKf/pUZNCgVLH2HfD0rUwdmpgJj4dl:KLlKT1kXqKf/pUZNCgVLH2HfIrUlgJj8
MD5:	EA69FD7AEE02AEA8249C0C8FA4DBF273
SHA1:	3E63CDFCD9C4E4AC1C3D89230E8D880B9DAB1FF9
SHA-256:	4827B36EC278740E73769AED840CE5816BC72AB5554908539B017D2589B2A7DC
SHA-512:	28E88A6738D10FCD21A13DB788B2A064925634C40852CE194F2AEC844C53202BFD4AE228EB6F35372566FC6DBDBE155C4785E5040C6569DC883C9BEE69C0757
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":"13280370076074715","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\44a78d28-a3fb-4026-812d-04b4d1f5cc10.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):	325
Entropy (8bit):	4.957371343316884

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\44a78d28-a3fb-4026-812d-04b4d1f5cc10.tmp	
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5hsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sd7sBdLJlyH7E4f3K33y
MD5:	363D9EBEDB5030036B53B6B28E8A8EA5
SHA1:	1C7C9012156AC8295EB465BC774430A866096832
SHA-256:	466FE09323B709A587648157D77298132B29F7CD916CD68EF6B28A0FC5EE355B
SHA-512:	9C9A230BAF627B8A9856C0AC66E4EA262C304BBC2272662F4213EB617297DFE222E0CCC4FC0F22B04FAFB3125D55D774174700B381EA3FF90B8C3D11926E023
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544335120983","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:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898I58
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):	325
Entropy (8bit):	4.957371343316884
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5hsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sd7sBdLJlyH7E4f3K33y
MD5:	363D9EBEDB5030036B53B6B28E8A8EA5
SHA1:	1C7C9012156AC8295EB465BC774430A866096832
SHA-256:	466FE09323B709A587648157D77298132B29F7CD916CD68EF6B28A0FC5EE355B
SHA-512:	9C9A230BAF627B8A9856C0AC66E4EA262C304BBC2272662F4213EB617297DFE222E0CCC4FC0F22B04FAFB3125D55D774174700B381EA3FF90B8C3D11926E023
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544335120983","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:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898I58
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
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):	438
Entropy (8bit):	5.175194230049838
Encrypted:	false
SSDEEP:	12:u+SvLZ5KkkGHArBFUts+tZ/W+1D54Z5KkkGHAryJ:utl5KkkGgPgsEg6Vo5KkkGga
MD5:	263A307592356852BC38F81065140065
SHA1:	507C3849FF34936DFD53CBB487C779CEE3CBBDB8
SHA-256:	AEEA455F274A0674EA2B5753C9C199F8658E15417B17D1581F14A4565E1117B4
SHA-512:	B4B898E9390E5712B6170804B79C4B8F86EE39507AEBB05DCB29F56CD9C677B9C8CD7AC6440A0DE77038139718AECCBE7C8F5E8583CAA9C934DC917DDB72D90
Malicious:	false
Reputation:	low
Preview:	2021/11/02-16:42:24.915 1a28 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/11/02-16:42:24.919 1a28 Recovering log #3.2021/11/02-16:42:24.920 1a28 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	440
Entropy (8bit):	5.20395703956083
Encrypted:	false
SSDEEP:	12:u+j+vLZ5KkkGHArqiuFUts+mFXXHSZ/W+diV54Z5KkkGHArq2J:ull5KkkGgCgsnFn4Eo5KkkGg7
MD5:	37B36B70BB35FC7E4BBD1304208352A6
SHA1:	DA1D384970902960E5FE90682983DC79DE7C046D
SHA-256:	E37142E3FE3644E2D4FD9FA403774130AB9FAB82EBDC0B61A0D1888705FF7BAA
SHA-512:	4B90CBA8C531DF343C71293F175F0A6404870BBA240214095B0A00FC872F97F77EDC7CB1ACD67727F724F83055602E7844B58CEA657FE91495A45E3C86B17E65
Malicious:	false
Reputation:	low
Preview:	2021/11/02-16:42:24.967 22bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/11/02-16:42:24.970 22bc Recovering log #3.2021/11/02-16:42:24.971 22bc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	80
Entropy (8bit):	3.4921535629071894
Encrypted:	false
SSDEEP:	3:S8ltHlS+QUl1ASEGhTFljl:S85aEFljl
MD5:	69449520FD9C139C534E2970342C6BD8
SHA1:	230FE369A09DEF748F8CC23AD70FD19ED8D1B885
SHA-256:	3F2E9648DFDB2DDB8E9D607E8802FEF05AFA447E17733DD3FD6D933E7CA49277
SHA-512:	EA34C39AEA13B281A6067DE20AD0CDA84135E70C97DB3CDD59E25E6536B19F7781E5FC0CA4A11C3618D43FC3BD3FBC120DD5C1C47821A248B8AD351F9F4E667
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):	426

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Entropy (8bit):	5.169589650139176
Encrypted:	false
SSDEEP:	12:u5+vLZ5KkkGHArAFUts0KW/WXV54Z5KkkGHArfJ:u+l5KkkGgkgsr3o5KkkGgV
MD5:	2E7E3CD5C33D6D8C860D2DE799E9BF39
SHA1:	AD71592273FAD7DFDFCFAEF2B1E578B55E6F5BBA
SHA-256:	E31D24AEF6C27831B8CCEF8610181BCD3283370791D8409D334EC140649BB05E
SHA-512:	4FBD0DDA8431210E89FEA1E3A2D199D89E0FDF0C31754B8E4880EF56BB8812A4D95CA528A902B0845419F3324414523E9F0E840526A88238165F58799FBD54DF
Malicious:	false
Reputation:	low
Preview:	2021/11/02-16:42:46.284 223c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Session Storage/MANIFEST-000001.2021/11/02-16:42:46.285 223c Recovering log #3.2021/11/02-16:42:46.286 223c 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\f0e63c3a-5353-4d2b-a6f4-e22457659e11.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):	325
Entropy (8bit):	4.96345415074364
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5Z0WlyhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sd/0WCsBdLJlyH7E4f3K33y
MD5:	1FE877DDE8B96DED122AC08BB07A83C5
SHA1:	5BEA5FFAF686474CE8ACA1D95500C29D65007745
SHA-256:	3AD373EB6FF8EA394964EDA2A9E53ADD8DBA11DC9716ED3CA672F10DF369BA4D
SHA-512:	1854F005CD691674FCF27376150ABD6F036A79C42BB4FFECDCCA14A74CB21D8ADF2552CACE631E6E9C92C58E7EF27279CA30CE5648C8EB90B06F2247A462003
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544342473569","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	410
Entropy (8bit):	5.297558419098248
Encrypted:	false
SSDEEP:	12:pi+vLZ5KkkOrsFUt5KW/BV54Z5KkkOrzJ:pTl5Kk+gFo5Kkn
MD5:	FC92D65B5B24070CFA4C7BDE62366712
SHA1:	BBFB4D36D9A16FFAB8AE8EEE1D2E1812D60DAE41
SHA-256:	45C4757C1D4E84B3074E4005DC72A1FE89D0C524DF7094442BE319B0E2522B5E
SHA-512:	EA547725632531D37EE6CBF4246F3A8FCC57CB121E5D5DC824D106C6B1D060D3ABE9F479804A3A21E65BAB850D2E86AE78B3CE7FBE9ECB8454D5AA2147316A5C
Malicious:	false
Reputation:	low
Preview:	2021/11/02-16:43:46.825 223c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/11/02-16:43:46.826 223c Recovering log #3.2021/11/02-16:43:46.826 223c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	537
Entropy (8bit):	5.546122727860212
Encrypted:	false
SSDEEP:	12:YY9RAJ9+UAnI8gcUQLmDMpL/fN+UAnIbAcUNlx+UAnI4Q:YY9RAeUX8rfwU56NlcUSQ
MD5:	A334D8CD071856B6B50A8ABCEE0E3346
SHA1:	B5DF7DA287460CB255A7E220496A05A951A78B26
SHA-256:	9D4ABE816CEA3FBEE46F9819C9A26A284E18E56360074BD87C4DD446F0043FA4
SHA-512:	AD7E51DF87B251504800E565E29FCA3BB9635C4053CE0FDBF0292B1FF1BC1623654BF6FA026799162B6F86D7BBEFD608F80A7F0050F6F4D7EB5EB7C66906D6BC
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity (copy)	
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1667432512.290796,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1635896512.290802},{"expiry":1667432505.165795,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1635896505.165802},{"expiry":1667432502.855094,"host":"opXOuPncEqRjkYSjAgcGEU30CFS/DB8Obxt4KuKod80=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1635896502.855103}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a1ab4027-fee8-4615-a381-623252bb0600.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):	6059
Entropy (8bit):	5.196588504747379
Encrypted:	false
SSDEEP:	96:n73h73q9rDZMYKIkik0JCKL8QkJIUkb13bOTQVuwn:nzhG9rSYOk4KdkJVkb5
MD5:	B092DF3D39344B4CE420E6C691E99392
SHA1:	ED5E117649D14250188781BD210DA10F05806D52
SHA-256:	6010F0094104F82F8A1DD575D40B1E0FD2C8E53B82E9CEA2B5638CD87F8DBD67
SHA-512:	5DF3BC6D5CB3F741CD4C263CCA6BA52AAD6617F47ACEC9679B0B964F97DCE3A71273D8CFE2A1CA4A2A8E7DC87F2C767AF8E1E46A45970D43B2F9905037A66 46
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280370076667147","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","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","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\aec44e02-d87c-43b1-b127-f08ba9140069.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c50ea795-e894-4750-9cde-20a142015f97.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):	5.536177252123554
Encrypted:	false
SSDEEP:	384:c1ttaLlNGXT1kXqKf/pUZNCgVLH2HfD0rUzHGInTWmhgJj4I:VLlKT1kXqKf/pUZNCgVLH2HfIrUTGIng
MD5:	A036AF74A21C5BB09FB28BC3E75ED185
SHA1:	3FC318CAC43988D47CD467169D40B366B2DA9668
SHA-256:	9B27A0F62003BA342E113EC24E3212D583654FC9AF37715196514E8885105A60
SHA-512:	E26210A1524FF896DD508C582811FF1B3502866FB9676CDB58E9BD6BAD1070788C681448DBA5C6CDE2FB03BCD09F7D58DE32E7D6AC8B783D06535105E47525D
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":"13280370076074715","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\c65b2555-4813-406f-919a-c255279dc9a9.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):	4568
Entropy (8bit):	4.914275300164391
Encrypted:	false
SSDEEP:	96:JDHXTOazIayY6Vn6M5TmGhLxGr3GIGPxGMhGyGnGIE/GRG6j:JDHXTOazIayY6Vn6ITmQLxu3D+xVfa8G
MD5:	DA6E928EB4C605633366604993B9B7CC
SHA1:	C1D2A63FC0600FA7AB421F1E5E0018E843096708
SHA-256:	1BA787204C90D0A851F26E9C873B65722D63DC3710FBA87084C6363CDBE517B7
SHA-512:	D9669A083F5AC1C82A40FF53FCB93EBFC2070217A5CB28E5562CEAB10ADDC758278F488F60D52DBE28ADBEDAB75B41A4CB49D2E5E1E3F1DF05974CE77877EDB1
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.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":"13282962078379339","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13282962078402805","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13282962078532627","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"e

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c7b49cf5-8eef-443e-93bf-6ff2ad0d6605.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):	5.570127136317139
Encrypted:	false
SSDEEP:	384:c1ttaLlNGXT1kXqKf/pUZNCgVLH2HfD0rUzHG5mngJj4h:VLlKT1kXqKf/pUZNCgVLH2HfIrUTG0gg
MD5:	FD8F203FABD375A3DAFA1467FCF007EC
SHA1:	B5E6D94530F7FC389B7E64D91B529EDFA756F9AB
SHA-256:	8ED678BF95D9D85B9A03E7CA10EB720E69AA28FB71D6F1BC4B9C08F40FFFA137
SHA-512:	E76FD0CA850524C9B0ADC7923AADD7121D2994154FA7F7244EB3771C7D4A4CA8D717187C29D41D8B091938888F07F5BBC12F2F485BCD54BCDACE9EF56F60499
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":"13280370076074715","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/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c93ab753-fb64-44cf-b0d9-d3a1c87f616b.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):	2724
Entropy (8bit):	4.858441642519087
Encrypted:	false
SSDEEP:	48:YXsPMHi5s7MHgKsSMH/zs8MHIs51tFsL6zsbWsdCshDysuMHCLsKMH9swIMHlYhj:XGiQGBGFGJ12LLHDwGyGkGihj
MD5:	9E0C31BCE1C83C78981EB86A29E2879B
SHA1:	3973E5D4DA1BC0BB99B78D1DFA7BEA045C85E173
SHA-256:	3D1BDA968D1CFF79DBD0C4B9D2A22367E9D9B8374622CD4263BD39137D8FE584
SHA-512:	D196B2993F4A46AFFD38DBA59866B048221D5CF6EAB1574846D1799B748BD71B09BE28D8154B16D97AEA300C7EE13719DC2E5034EC9D8913C6A6B399BDEBC2E
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544495618845","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31528},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345624305","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":26637},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345531701","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":53820},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345601356","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":36228},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp

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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENTMP (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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\fcafcbf8-344b-448a-ba7b-b4deb242271e.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):	5.577541734713801
Encrypted:	false
SSDEEP:	384:c1ttvLlNGXT1kXqKf/pUZNCgVLH2HfD0rUwdmpgJj4dl:KLlKT1kXqKf/pUZNCgVLH2HflrUlgJj8
MD5:	EA69FD7AEE02AEA8249C0C8FA4DBF273
SHA1:	3E63CDFCD9C4E4AC1C3D89230E8D880B9DAB1FF9
SHA-256:	4827B36EC278740E73769AED840CE5816BC72AB5554908539B017D2589B2A7DC
SHA-512:	28E88A6738D10FCD21A13DB788B2A064925634C40852CE194F2AEC844C53202BFD4AE228EB6F35372566FC6DBDBE155C4785E5040C6569DC883C9BEE69C0757
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13280370076074715","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	184616
Entropy (8bit):	6.076258717829855
Encrypted:	false
SSDEEP:	3072:HkJIxcSRcPWIiRuBYC0RgGKjG0sQRAUAZvtkhVPPLA7bV/nYorVcI8XIssElYTRU:EMTclNI1B8RPyc3gbV/njhcI8II6RU
MD5:	7E1C233ACD9E24C4CCD4EA8FAB3D5031
SHA1:	F88E5AB0F1EC56995BEF76B7F6FF77D08F9C9D79
SHA-256:	FEA1A13B496DE765CED89F7F6EBC5DA5F2960D437B18DBCE75CFB368AFCC2338
SHA-512:	C4A7FEF9B5B05319FEEDBE58C0B6AA186C6A55EE23C2FB2D71E5C4F5D2AA936453A47B222361220BF95BA4BD613E0C249831179F825269111082F27A7B36BF4I
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":1.635896478109835e+12,"network":1.63586768e+12,"ticks":122113334.0,"uncertainty":3968425.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909820208"},"plugins":{"metadata":{"adobe-flash-player":{"displ

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):	184616
Entropy (8bit):	6.076259663517651
Encrypted:	false
SSDEEP:	3072:HkjIxcSRcPWIiRuBYC0RgGKjG0sQRAUAZvtkhVPPLA7bV/nYorVcI8XIssElYTRU:EuTclNI1B8RPyc3gbV/njhcI8II6RU
MD5:	D0D6A3E2EDCA0E944B127C60A4CA9EC4
SHA1:	2AADEE72F24D8A2182783C8974AD503D8315FA12
SHA-256:	E859C60974DD2B580EA2967FD87292C5BD7DB46315D214EE5DBE210FE4ACE2C2
SHA-512:	3E0FA411B9F7375ADA0523DFBCCAA5940A2462C6EA1CA539BCAFF22CB161B4B00F97037BF61DA5D337F86CC294AE8DA637353FB16C45457A7BDDAFC522F10A4C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State. (copy)	
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":1.635896478109835e+12,"network":1.63586768e+12,"ticks":122113334.0,"uncertainty":3968425.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909820208"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local StateiC (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):	184617
Entropy (8bit):	6.076258192596406
Encrypted:	false
SSDEEP:	3072:zkjIxcSRcPWIiRuBYC0RgGKjG0sQRAUAZvtkhVPPLA7bV/nYorVcI8XIssElYTRU:ouTclNI1B8RPyc3gbV/njhcI8II6RU
MD5:	2C4B69C68661CF99375BABEEE9381E12
SHA1:	EC88E1005C7691FF6A94FF9E802264CA68BF58F7
SHA-256:	44139441AECF2933ECA39322C72FB8285344ECE27D2B48A98707AE2925ED48EF
SHA-512:	148F9BCE41B6023B9230A66987DFF2F3CEED580D10F84135E9FEE28DFAA1880D09123173039C3866B45C2DC093B29CC59B8FEBD8C66FD6C4F55A4C664E8C7CE
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":1.635896478109835e+12,"network":1.63586768e+12,"ticks":122113334.0,"uncertainty":3968425.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909086161"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\a31a9a66-ea59-45c9-a7e4-8b752862b527.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97400
Entropy (8bit):	3.751024414071255
Encrypted:	false
SSDEEP:	384:krzQkmlnJdhOYV9/EbNYrxvUw3bouTHOrG/CrtyECRxbS6uNrJQmtBfBiowkLOmx:B2Cl5me0TIeDXo8GAfbaYKiI01b
MD5:	D7B0EFA8C7C9A45613A19D5DBDFEA930
SHA1:	456FF99342D4C2D4065493F8C6E6C06E0E922612
SHA-256:	D5F7F412F1166F9A2398C80052528CDB821D25F62F97290EC2EE730EA929EF08
SHA-512:	1E517C8FF8F303B6E0924CB6F55F3FC40F7439F61189CB0758F9143E32CC32FC7EE63282E816925870A86016A21716F024234D04DEB8C38A6EF30EF26C015AEA
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....J8.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\c9883b85-0a05-4a3d-9eeb-32d7df1b873a.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):	184617
Entropy (8bit):	6.076257970833012
Encrypted:	false
SSDEEP:	3072:zk+IxcSRcPWIiRuBYC0RgGKjG0sQRAUAZvtkhVPPLA7bV/nYorVcI8XIssElYTRU:o/TclNI1B8RPyc3gbV/njhcI8II6RU
MD5:	2BA3504B758F3966E84CE4D843B49A7F
SHA1:	0A0167D71766084D51510066161E8A2410BF17BD
SHA-256:	6524B3C859C547ADC07416EE30B70D36BA0D636D99D1900A12794B14A7BC9CB5
SHA-512:	28984BB424580D62DC37E78F23E014D2AA64E22EFE07DE871466B796F51FB22F1FD03BC057EDF1A585F846E5D942AE76D9D1DEBD1584C3E6EBF831FD55DB9FA
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\c9883b85-0a05-4a3d-9eeb-32d7df1b873a.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.635896478109835e+12,"network":1.63586768e+12,"ticks":122113334.0,"uncertainty":3968425.0}},"os_crypt":{"encrypted_key":"RFB BUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZM f3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+ g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909086161"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Google\Chrome\User Data\d633b3ed-eae4-4586-9c92-2030e25bb835.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):	176145
Entropy (8bit):	6.046974781743798
Encrypted:	false
SSDEEP:	3072:SIxcSRcPWIiRuBYC0RgGKjG0sQRAUAZvtkhVPPLA7bV/nYorVcI8XIssElYTRU:LTclNI1B8RPyc3gbV/njhcI8II6RU
MD5:	ABDE20C5C1DC720920AA3B9F9A30BEC4
SHA1:	4943C0FB537D8C8D50CB13DD4221A5F120E75482
SHA-256:	03B2B4A7D6D266369EB2ACA682FBC002F8C19C5EC5D1E7FEED8AE976EE61D3BA
SHA-512:	1AF3F6F1CAA6BDBEB4B3974B29DDBB4866B84EC9D0BEE7D07EDF7CC3429F5647B2833BD3F8C37C4D57A6F941F32D25C8BF781C244FC2893ECF2CB92EE03F7 E23
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":1.635896478109835e+12,"network":1.63586768e+12,"ticks":122113334.0,"uncertainty":3968425.0}},"os_crypt":{"encrypted_key":"RFB BUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZM f3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+ g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909086161"},"plugins":{"metadata":{"adobe-flash-player":{"displ

C:\Users\user\AppData\Local\Temp\42a5e963-1e63-42d4-a5be-5152e63bf5f4.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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\920805d9-f1e3-4f74-a020-618d5b3595eb.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:	086C124DE3A01BE467647F3BCB4EA05105F690AB45417A0E3D38935ABA9E2381DF59AF98D0FFF7823CEFD5390B48807352E135AC70977AED7B413A8CC48FB59
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\920805d9-f1e3-4f74-a020-618d5b3595eb.tmp	
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.:.Ipr..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\b71ac7ab-7b08-4c52-b455-202b7471d2b7.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\bb5c1034-db5b-44fd-9dde-3d4a27929949.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:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
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..$.J....+M!.Hz.n`U.I)N.|b.l....{.K@]6.LlP/....](.A.....l...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...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_dir6600_443859871\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:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770C
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_dir6600_443859871\CRX_INSTALL_locales\ca\messages.json

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\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:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CE B4
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": "C onnecteu-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_dir6600_443859871\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:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D84885 B
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_dir6600_443859871\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:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C5 E0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_u navailable": {.. "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 comp leted.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\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

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\de\messages.json	
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB805 52
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_una vailable": {.. "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 trans action could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\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:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavail able": {.. "message": ". ...."..".. },.. "craw_connect_to_network": {.. "message": "..... .. .."..".. },.. "iap_unavailable": {.. "message": ".. ...."..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\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:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65 FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "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_dir6600_443859871\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:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65 FFD9
Malicious:	false

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\en_GB\messages.json	
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_dir6600_443859871\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:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE018
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_dir6600_443859871\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:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA3
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_dir6600_443859871\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_dir6600_443859871\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:	3B92B6C86D30FD36AA3CEFF8773BA60C3FC5CC19C693540137044C5838A5503895C770C0336A4D0A3DB5E42F3FB36274D8D3F85B9DCA2F3EC0E974FDDB0BEA D8
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Storen maksut".. },.. "app_name": {.. "message": "Chrome Web Storen maksut".. },.. "craw_app_unavail able": {.. "message": "Sovellus ei ole t.ll. hetkell. k.ytett.viss..".. },.. "craw_connect_to_network": {.. "message": "Muodosta verkkoyhteys.".. },.. "iap_unavai lable": {.. "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_dir6600_443859871\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_dir6600_443859871\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:	D7EF7F5AD7EF1A1595825D79B69E2B1E988AD3CF1F3881496FCCD30F241E4E9C6E457F9F5D0F855DE3536DB7A40C3E1C55946B50D3F556F4A35285066A0CD6F
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_dir6600_443859871\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

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\hi\messages.json	
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_dir6600_443859871\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:	D7629978FC031EA5F716F9C1065FB2FEAB48C15F10CD68830DC966FA1002C03DDC7ACDE314C7D075F9F3A0A68552A6ACBCCDEE24CF20B6C3DD1BCE6562D03 6E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "app_name": {.. "message": "Pla.anja u web-trgovini Chrome".. },.. "craw _app_unavailable": {.. "message": "Aplikacija trenuta.no nije dostupna.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se s mre.om.".. },.. "iap_unavailable": {.. "message": "Pla.anje u aplikaciji trenuta.no nije dostupno.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be comple ted.".. },.. "please_sign_in": {.. "message": "Prijavite se na Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\hu\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	683
Entropy (8bit):	4.675370843321512
Encrypted:	false
SSDEEP:	12:1HEJVJiGGVJi+WYpU34Hpo9O+dgMmfgijO8ZpU34Huo9O03OyZnLAOfTYBIAYm:1HEVrk5WYpQzTUg/8ZpwoXOGAOfYIAd
MD5:	85609CF8623582A8376C206556ED2131
SHA1:	1E16EB70DB5E59BB684866FF3E3925C2DEF25A12
SHA-256:	32A249749F12ADB6A220BF9ADC272C7E5D9AD5497A38B0086D961E3ABA17FBC6
SHA-512:	27883430865D3CFA6EDFE8C6CE1442BD96150B5CE520CCF7D556A330CAA6392C712B47BD86F7350E174876BC681F6DEC94D1312402655B0AF90883A2899EC78
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Internetes .ruh.z Fizet.si rendszere".. },.. "app_name": {.. "message": "Chrome Internetes .ruh.z Fizet.si r endszere".. },.. "craw_app_unavailable": {.. "message": "Az alkalmaz.s jelenleg nem .rhet. el.".. },.. "craw_connect_to_network": {.. "message": "K.rj.k, csatlako zzon egy h.l.zathoz.".. },.. "iap_unavailable": {.. "message": "Az alkalmaz.son bel.li fizet.s jelenleg nem .rhet. el.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Jelentkezzen be a Chrome-ba.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\id\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	604
Entropy (8bit):	4.465685261172395
Encrypted:	false
SSDEEP:	12:1HEJs25bGGs25b+WYpU34ORBHAeSJ+dgkmO8ZpU34s22C/SzFAs03OyZnLAOfTYR:1HEBaA6WYpaHFH8ZptOYOGAOf2D
MD5:	EAB2B946D1232AB98137E760954003AA
SHA1:	60BDC2937905B311D2C9844DF2D639D7AC9F7F67
SHA-256:	C6E8800450602DE0F39FE9F6854472383813FB454B08ABAE7E25A9167CE004C3
SHA-512:	970FEC9A9EF0BAF7F693C4C5977F3B47914579C5B5414FCE9DBB5E4574659A5BB9AD2DE0CC886B368F49C019785AF7D2D7FE82F71341F039EADC399ED776CA 2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\id\messages.json	
Preview:	{.. "app_description": {.. "message": "Pembayaran Chrome Webstore".. },.. "app_name": {.. "message": "Pembayaran Chrome Webstore".. },.. "craw_app_unavailable": {.. "message": "Aplikasi tidak tersedia saat ini.".. },.. "craw_connect_to_network": {.. "message": "Sambungkan ke jaringan.".. },.. "iap_unavailable": {.. "message": "Pembayaran Dalam Aplikasi saat ini tidak tersedia.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Harap masuk ke Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\it\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	603
Entropy (8bit):	4.479418964635223
Encrypted:	false
SSDEEP:	12:1HEJsqd/bGGsqd/b+WYpU34OcX4+dgUvIO8ZpU34vq703OyZnLAOfTYsD:1HEXd/aKd/6WYpZrv58ZpskOGAOfzD
MD5:	A328EEF5E841E0C72D3CD7366899C5C8
SHA1:	2851ED658385804E87911643F5A4200B1FB26E13
SHA-256:	CD891C45F7586FB4A2514205A11F260E4A6D4482FA03D901909DD9F57BE0536D
SHA-512:	E47297896E981774EC3B59D41B89D6BA9333F6B4435EB9727D8645A46B10C7D408ADE06844871FA757382FBE7E645276449DB7B1B23BC59C9A71A5CB5A5ECC5
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamenti Chrome Web Store".. },.. "app_name": {.. "message": "Pagamenti Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "App al momento non disponibile.".. },.. "craw_connect_to_network": {.. "message": "Collegati a una rete.".. },.. "iap_unavailable": {.. "message": "La funzione Pagamenti In-App non . al momento disponibile.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accedi a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\ja\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	697
Entropy (8bit):	5.20469020877498
Encrypted:	false
SSDEEP:	12:1HEJ07uGG07u+WYpU34DB+dgnsVztO8ZpU34MwiB03OyZnLAOfTYmSH:1HEcnDNWYp1kxU8Zp2wiqOGAOfpSH
MD5:	9B3A5D473C3F2BBFAEECE94A07A940B8
SHA1:	61BACA342CF766BBA15C7B4D892A0E7DAC9405AA
SHA-256:	706312A4A2AEF3317223F141EB2B82685345B7EED444F16BB4DF3A272716DA1F
SHA-512:	94F6FEE9A11BD890AB8211C98D1CC142348961EBCF756F66477A3E3A76519804B70BE0AE4E551739F8AFE32D7ADE6EDE04EF6B9B9EED03E3A857E6058EEDD4C6
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome ....".. },.. "app_name": {.. "message": "Chrome ....".. },.. "craw_app_unavailable": {.. "message": ".....".. },.. "craw_connect_to_network": {.. "message": "..".. },.. "iap_unavailable": {.. "message": "..".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Chrome .....".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\ko\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):	631
Entropy (8bit):	5.160315577642469
Encrypted:	false
SSDEEP:	12:1HEJ1GG1+WYpU34K3aT+dgh8d0HTO8ZpU34KaNkaT03OyZnLAOfTY/YeHx:1HEajWYpc3aSl0Hq8Zpc6kasOGAOfyYA
MD5:	9F6B4D82A70C74CA751E2EAE70FAB5CF
SHA1:	0534F125FFCE8222277CF2BE3401C59DAF9217F8
SHA-256:	D1467B8D037114403E8F4EFC52E88C4A7FEB96126BE4CFF883FEFF1084EF7E68
SHA-512:	ED9319830314385D09C06F62EE34186E8CA576C857981205E4468A28B3ACD2AB03384E77B866032C324ABDD97A56EFD08E2D6E0C79D563578B3EC52517819BD8
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_dir6600_443859871\CRX_INSTALL_locales\lt\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\lt\messages.json	
Size (bytes):	665
Entropy (8bit):	4.66839186029557
Encrypted:	false
SSDEEP:	12:1HEJpqHnkGGpqHnk+WYpU346M+dgV6O8ZpU34WzSWz03OyZnLAOfTYx:1HELqHtKqHPWYpM3A8ZpwGzOGAOfg
MD5:	4CA644F875606986A9898D04BDAE3EA5
SHA1:	722A10569E93975129D67FBDB75B537D9D622AD1
SHA-256:	7C311AB751D840D750C11553C083785813E079C1D464FE568A98C9E3EF3DB96C
SHA-512:	E575E3D0622F5BD4B6C0EE79128A1B1F1882195670139D1983F4377D847141B8FB8EBB8BCED82AF3A220ED07D3577AFBE085BADC0E9C7678292B80E3EC5D344
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. },.. "app_name": {.. "message": ".Chrome. internetin.s parduotuv.s mok.jimo sistema".. },.. "craw_app_unavailable": {.. "message": "Programa .iuo metu negalima.".. },.. "craw_connect_to_network": {.. "message": "Prisijunkite prie tinklo.".. },.. "iap_unavailable": {.. "message": "Mok.jimai programoje .iuo metu negalimi.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prisijunkite prie .Chrome..".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\lv\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):	671
Entropy (8bit):	4.631774066483956
Encrypted:	false
SSDEEP:	12:1HEJFhVbGGFhVb+WYpU34wDoz+dgGedBO8ZpU34wF03OyZnLAOfTYGYID:1HENQKkWYp2Doy/em8Zp2WOGAOfRYID
MD5:	C5CE2C51391EAFD3DA9E4C71549A3C28
SHA1:	1F67FF6EF6E90C0CE3AAF56ED543A3EFD381574D
SHA-256:	1FA1DF2CA8516DEF490FB8484E9AA498ACFF80EEF5C9258FFE42D3678E6C7DED
SHA-512:	C85F6281E682F52BC2147DEA7E2F3BB4DC48D98BADA8687B05C6C7271C78EA7F5431CD51671A4184C9AE004FC53C016E3C594697F483195CCBA08A93821EEF
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome interneta veikala maks.jumu sist.ma".. },.. "app_name": {.. "message": "Chrome interneta veikala maks.jumu s ist.ma".. },.. "craw_app_unavailable": {.. "message": "Lietotne pagaid.m nav pieejama.".. },.. "craw_connect_to_network": {.. "message": "L.dzu, izveidojiet savienojumu ar t.klu.".. },.. "iap_unavailable": {.. "message": "Maks.jumi lietotn.s pa.laik nav pieejami.".. },.. "jwt_retrieve_failed": {.. "message": "The transacti on could not be completed.".. },.. "please_sign_in": {.. "message": "L.dzu, pierakstieties p.rl.k. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\nb\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):	4.555032032637389
Encrypted:	false
SSDEEP:	12:1HEJhiOGGhiO+WYpU34OHSN+dgFjdGFZO8ZpU34JgdN03OyZnLAOfTYiD:1HEDiHIitWYpCYJ8ZpD1OGAOfRD
MD5:	93C459A23BC6953FF744C35920CD2AF9
SHA1:	162F884972103A08ADB616A7EB3598431A2924C5
SHA-256:	2CD700AEB57D89C2E73333D0702556EE3FF3863516170F85669BC680FCBDC4E0
SHA-512:	F76E6E8D8499306883C3EC1E774F7E8BB6B601096DA5A14D17D3E7D5732829542041E42B7350466589291ADCC83FB065FD591B4E20CFCF8EDC586E128ECBFCE
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Nettmarked-betalinger".. },.. "app_name": {.. "message": "Chrome Nettmarked-betalinger".. },.. "craw_app _unavailable": {.. "message": "Appen er utilgjengelig for .yeblikket.".. },.. "craw_connect_to_network": {.. "message": "Du m. koble til et nettverk.".. },.. "iap _unavailable": {.. "message": "Betaling i app er ikke tilgjengelig for .yeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Du m. logge p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\nl\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	615
Entropy (8bit):	4.4715318546237315
Encrypted:	false
SSDEEP:	12:1HEJJQGkbGGJQGkb+WYpU34OQKJT+dgiXUmvFZO8ZpU34g7JT03OyZnLAOfTYMD:1HErxkaqxk6WYptndXI8ZpTOGAOfbD
MD5:	7A8F9D0249C680F64DEC7650A432BD57
SHA1:	53477198AEE389F6580921B4876719B400A23CA1
SHA-256:	92BE7C2DC9CFBE5A65E9CE6488D364C8D7EC19E7B67A31E4D43C1CB2B169671C

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\nl\messages.json	
SHA-512:	969AB979546A741C0F3EDBEEB21BABA375FA8870D4FB9248CDD4C305736E332E10CAB7B64C5C078E60EC0CD73848101B390BE8F44B89C310058AF4C1CA3C8A A7
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalingen via Chrome Web Store".. },.. "app_name": {.. "message": "Betalingen via Chrome Web Store".. },.. "cr aw_app_unavailable": {.. "message": "App momenteel niet beschikbaar.".. },.. "craw_connect_to_network": {.. "message": "Maak verbinding met een netwerk.".. },.. "iap_unavailable": {.. "message": "In-app-betalingen is momenteel niet beschikbaar.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log in bij Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\pl\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):	636
Entropy (8bit):	4.646901997539488
Encrypted:	false
SSDEEP:	12:1HEJbiVbGGbiVb+WYpU34OBHlBi9+dgQUg6O8ZpU34bdbfilu03OyZnLAOfTYR5k:1HE5iVauiV6WYpIAYr8ZpxFiaOGAOfIC
MD5:	0E6194126AFCCD1E3098D276A7400175
SHA1:	E8127B905A640B1C46362FA6E1127BE172F4A40F
SHA-256:	E2699F98C511B18A2AFB82EAE9A4804B646C4FF1077D80E77C17A3943A6373C2
SHA-512:	A71F7C7BFBBF1E37E699601AF2E095C56CBA91F90CB7556477DF31D01B83ADFB1271E1775C9BA299FF6875BBFC2B6AB47488CC88E33DEF2F6F2E0E5AC687B7 77
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "app_name": {.. "message": "P.atno.ci w sklepie Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Aplikacja jest obecnie niedost.pna.".. },.. "craw_connect_to_network": {.. "message": "Po..cz si. z sieci..".. },.. "iap_unavailable": {.. "message": "P.atno.ci w ramach aplikacji s. teraz niedost.pne.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be com pleted.".. },.. "please_sign_in": {.. "message": "Zaloguj si. w Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\pt_BR\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):	636
Entropy (8bit):	4.515158874306633
Encrypted:	false
SSDEEP:	12:1HEJsc/bGGsc/b+WYpU34OLw+dgn/KzO8ZpU34FjIBMwGRO03OyZnLAOfTYN+KcY:1HEb/a8/6WYp4mZ8Zp7cKlOGAOf2tD
MD5:	86A2B91FA18B867209024C522ED665D5
SHA1:	63DEC245637818C76655E01FCB6D59784BC7184E
SHA-256:	6374880FDD1F8AF1EE8AEA6A06B73BE0AB265AFCEB4FE6F08BDE3B3989264B21
SHA-512:	DA6DBDE5028756421C2904F605632EE98831A25A1247E6238A931629B94CE8A00FD76F4235F118D2167304BD60F2C06B2AD78E54FF6CE53F8C38DF8C7B5AFCE
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pagamentos da Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos da Chrome Web Store".. },.. "craw _app_unavailable": {.. "message": "Aplicativo indispon.vel no momento.".. },.. "craw_connect_to_network": {.. "message": "Conecte-se a uma rede.".. },.. "iap_unavailable": {.. "message": "No momento, os Pagamentos no aplicativo n.o est.o dispon.veis.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Fa.a login no Google Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\pt_PT\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):	622
Entropy (8bit):	4.526171498622949
Encrypted:	false
SSDEEP:	12:1HEJsZUkbGGsZUkb+WYpU34OAE+dgqxKzO8ZpU34rEpBfvPO03OyZnLAOfTYLD:1HEmUka5Uk6WYpFvdxZ8ZpSTnPlOGAOS
MD5:	750A4800EDB93FBE56495963F9FB3B94
SHA1:	8BFB915488A4EB3CB33D68E2E59F1F8447DB7D61
SHA-256:	C1C94F65FABAF17DEF98A8587711A56D61B1E5607500E9B01F2824DB109F9E83
SHA-512:	2AEDEF5793406221BE76AF22031CE8C30AB5FAEAED09BB394C153E2EBE990C89C1A2A73B40D8A92842641AFCA8C77FFD808A2058602D3646FD8DAE2844406F 4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\pt_PT\messages.json	
Preview:	{.. "app_description": {.. "message": "Pagamentos via Chrome Web Store".. },.. "app_name": {.. "message": "Pagamentos via Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Aplica..o atualmente indispon.vel.".. },.. "craw_connect_to_network": {.. "message": "Ligue-se a uma rede.".. },.. "iap_unavailable": {.. "message": "Os Pagamentos na app est.o atualmente indispon.veis.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicie sess.o no Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\ro\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):	4.61125938671415
Encrypted:	false
SSDEEP:	12:1HEJqJrJZGGqJrJZ+WYpU344Hlx2Z+dgrVPlZO8ZpU34qT7hl3O03OyZnLAOfTYU:1HEC4D8WYpKow8WV68ZpKhoOGAOfoVGD
MD5:	98D43E4B1054A65DF3FA3CC40AB6FB6D
SHA1:	46E0A21C4DA2BB5D4D8F837AE211C1B6FA26E7E2
SHA-256:	113A13900CBA62FE8AED06751971C23A80A99B47F9BE219CF884D57DB19611D9
SHA-512:	A76DC53912A4F46714926B9EA2B22E909540E447F61F6DD72607AB7B3BB5D4A9B39E525B04C33AEC53BA813D14AC1FB5827275B2524E52B693E83171E1CD1466
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "app_name": {.. "message": "Pl..i prin Magazinul web Chrome".. },.. "craw_app_unavailable": {.. "message": ".n prezent, aplica.ia nu este disponibil..".. },.. "craw_connect_to_network": {.. "message": "Conecteaz.-te la o re.ea.".. },.. "iap_unavailable": {.. "message": "Pl..ile .n aplica.ie nu sunt disponibile momentan.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Conecteaz.-te la Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\ru\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):	744
Entropy (8bit):	4.918620852166656
Encrypted:	false
SSDEEP:	12:1HEJ7OJHZMSl3ZGG7OJHZMSl3Z+WYpU34zWJ2F+dgVtLSv/TO8ZpU347NWjT03On:1HElOJHZMq4uOJHZMq8WYpdWJ/YGHq8m
MD5:	DB2EDF1465946C06BD95C71A1E13AE64
SHA1:	FB4F3ECE9ECECEBBC6CA2A592A15FB9C1FDFB811
SHA-256:	FBAF22CE6E16DE174CED8CB5EA3098CCA1C3426A2111FF33BD3E64DA64ED67AB
SHA-512:	4E0CF00BAEF1757548DEB17BBE1AF55770A0A0F7351779EF55C7DEFA6D112D0227B8865C2C22E0EC62E6E2F1C8E1632A2D0CE6828D25C5ABBF143C990116F62
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_dir6600_443859871\CRX_INSTALL_locales\sk\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):	4.640777810668463
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34ORO+dgmmCO8ZpU34yH7u2Z03OyZnLAOfTYCUAi0D:1HEl4G8WYpetPmD8ZpcH7aOGAOfzUeD
MD5:	8DF215D1EFBDABB175CCDD68ED8DCB0A
SHA1:	2B374462137A38589A73FDD00A84CBDC7E50F9F4
SHA-256:	7FA16AF97E6CFC52EC6008EB679D3F30E7E0C24F9EF2D18A9228EAF4DED9D63B
SHA-512:	C0E623343BDAEB4731800D183B59F2FCFE285F0C7153EC99641FD84F2F2DCFE47D21E73F3D28B1240340453C5668EB0AFFBE087AAB62F1C88CD2A40CC44E595D
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": "Aplik.cia moment.lne nie je dostupn..".. },.. "craw_connect_to_network": {.. "message": "Pripojte sa k sieti.".. },.. "iap_unavailable": {.. "message": "Platby v aplik.cii moment.lne nie s. k dispoz.cii.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prihl.ste sa do prehliada.a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\sl\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\sl\messages.json	
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	617
Entropy (8bit):	4.5101656584816885
Encrypted:	false
SSDEEP:	12:1HEJGcyvmbZGGGcyvmbZ+WYpU34OBOEtf+dgca1ZO8ZpU34GcQArERff03OyZnLh:1HE4cyY4TcyY8WYpNoWa1w8ZpQcQ6AfK
MD5:	3943FA2A647AECEDFD685408B27139EE
SHA1:	0129DD19D28373359530B3B477FE8A9279DABB7D
SHA-256:	18AFF072EE0DF7C3495045435C752A805606E6D5D462EF2321C443F1773F4B3A
SHA-512:	42E62B3855611FF2E1D39C11404CB1A09825EE4CA6A8ACB3FF538B4574388F549E3BD79137DD4DC128A8DC44DD270D7D878E4AAD20DA8250A5C25297B0DEC0D
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Pla.ila v spletni trgovini Chrome".. },.. "app_name": {.. "message": "Pla.ila v spletni trgovini Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikacija trenutno ni na voljo.".. },.. "craw_connect_to_network": {.. "message": "Pove.ite se z omre.jem.".. },.. "iap_unavailable": {.. "message": "Pla.ila v aplikacijah trenutno niso na voljo.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Prijavite se v Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\sr\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):	743
Entropy (8bit):	4.913927107235852
Encrypted:	false
SSDEEP:	12:1HEJssbdOGGssbdO+WYpU347xBP+dgcucO8ZpU34s1muP03OyZnLAOfTYzDYD:1HEKsb59sbTWYplx4Xud8Zpy1mNOGAOv
MD5:	D485DF17F085B6A37125694F85646FD0
SHA1:	24D51D8642CDC6EFD5D8D7A4430232D8CDE25108
SHA-256:	7FFDE34C58E7C376C042DE64DEF6481DAE32BE8B70F0B18EDF536290CBE0C818
SHA-512:	0DDECFD860E99290B6C3AAA04F510272AE081CF2D93ED5832D9D6378EC9D36177FFBE213471247FB94721EA34A83E7665669200047091D0FDE134E3D763217E7
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_dir6600_443859871\CRX_INSTALL_locales\sv\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):	630
Entropy (8bit):	4.52964089437422
Encrypted:	false
SSDEEP:	12:1HEJJMkbGGJMkb+WYpU34OACwz+dgNPGFZO8ZpU34JgpXLSb03OyZnLAOfTYLdID:1HErMkaqMk6WYpTOcb8ZpDgdZOGAOf8Y
MD5:	D372B8204EB743E16F45C7CBD3CAAF37
SHA1:	C96C57219D292B01016B37DCF82E7C79AD0DD1E8
SHA-256:	B8BA77E0089B0676545EC16D32468B727812B444F90B33A7A5B748E6C36C4388
SHA-512:	33640529E0D5DCC5CA4BDB0615A2818E8D26C6FCB7B3474C08AC3EB67B9DB40E1F0A79954ED20728CD47A686D2533DCBC76ABCBDB917F8530C8DE8BBA6873E2E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalning via Chrome Web Store".. },.. "app_name": {.. "message": "Betalning via Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Appen .r inte tillg.nglig f.r tillf.llet.".. },.. "craw_connect_to_network": {.. "message": "Anslut till ett n.tverk.".. },.. "iap_unavailable": {.. "message": "Betalning i appen .r inte tillg.ngligt f.r n.rvarande.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Logga in i Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\th\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):	945
Entropy (8bit):	4.801079428724355
Encrypted:	false
SSDEEP:	24:1HEKa1dDa1/WYp6UFi72SmlG8ZpyactrW2SAOGAOfvSLD:WK2DNYp6U4y3bpyLxwGFW
MD5:	83E2D1E97791A4B2C5C69926EFB629C9

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\th\messages.json	
SHA1:	429600425CB0F196DDD717F940E94DBD8BFF2837
SHA-256:	2FECA577F43D97BAEEA464741D585892103585208FD0A935B810A03BDCE83C88
SHA-512:	60A5928DAA8CB4341487F477C56B5A98B83EDE50E5F4F55A802E01FDDAB86F3E795D391953D3D9214552D14D3F58C5A183693C613720FC12FC387D7B8F9B9AB
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_dir6600_443859871\CRX_INSTALL_locales\tr\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):	631
Entropy (8bit):	4.710869622361971
Encrypted:	false
SSDEEP:	12:1HEJ9Y8GG9Y8+WYpU34wWT+dgGb0GO8ZpU34wryd7T03OyZnLAOfTYGbPKG:1HE0jWYpyRnG8Zpyr/OGAOfFPn
MD5:	2CEAE0567B6BB1D240BBAD690A98CA3B
SHA1:	5944346FBD4A0797B13223895995CAB58E9ECD23
SHA-256:	A7CB86F30C9C31FE5540282C308BA96ADB4EC16EF98C87129EB88105E5BEF5FC
SHA-512:	108A07C6D03D7178E8D0FFEF5349E0249A898D864964FED8757BD8A08BC1C6D9613F2A6C01AA34A6606127D1C6CE14C229FA02586677DBB060B85E3E845950E
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Ma.azas. .demeleri".. },.. "app_name": {.. "message": "Chrome Web Ma.azas. .demeleri".. },.. "craw_app_unavailable": {.. "message": "Uygulama .u anda kullan.lam.yor.".. },.. "craw_connect_to_network": {.. "message": "L.tfen bir a.a ba.lan.n.".. },.. "iap_unavailable": {.. "message": "Uygulama ..i .demeler .u anda kullan.lamaz.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "L.tfen Chrome'da oturum a..n.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\uk\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):	720
Entropy (8bit):	4.977397623063544
Encrypted:	false
SSDEEP:	12:1HEJ7wILkSlXZGG7wILkSlXZ+WYpU34zb1Oy2P+dgSV1EjiTO8ZpU347qtfP2CTW:1HElwEkK4uwEkK8WYpd/dTV1e8Zptq5S
MD5:	AB0B56120E6B38C42CC3612BE948EF50
SHA1:	8B3F520E5713D9F116D68E71DAEED1F6E8D74629
SHA-256:	68ABA284751EB9C856032062EF9B1651E2A1E5CE5FDA0977FFC97D63BA7BED9E
SHA-512:	CD852A58217F739C1CD58567FF432D31A7AD3F68C884ABBA1DA95799BCD1545C6A5D3B06F319681C12B78AD0A709828DE4B22736316F148D21F5DB76A5BCCB F
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_dir6600_443859871\CRX_INSTALL_locales\vi\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):	695
Entropy (8bit):	4.855375139026009
Encrypted:	false
SSDEEP:	12:1HEJMAZrSFZGGMAZrSFZ+WYpU34WFHoz+dgdklzoO8ZpU34NFHoz03OyZnLAOfTU:1HEI4B8WYpAKytFZ8ZpXKMOGAOfd6D
MD5:	7EBB677FEAD8557D3676505225A7249A
SHA1:	F161B4B6001AEAEAB246FF8987F4D992B48D47BE
SHA-256:	051F96ED874C11C4A13589B5F68964E4F5B03B52DDA223D56524F2CA23760C04
SHA-512:	74FD267CF7E299FB8E7054605C3F651F057F676FF865082FA24F4916755456768DB0DA62DBC515D829B48AB1F9CFC8AD3E841DCBF1F194D5CB14C5335A192A0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\vi\messages.json	
Preview:	{.. "app_description": {.. "message": "Thanh to.n tr.n c.a h.ng Chrome tr.c tuy.n".. },.. "app_name": {.. "message": "Thanh to.n tr.n c.a h.ng Chrome tr.c tuy.n".. },.. "craw_app_unavailable": {.. "message": ".ng d.ng hi.n kh.ng kh. d.ng.".. },.. "craw_connect_to_network": {.. "message": "Vui l.ng k.t n.i v.i m.ng.".. },.. "iap_unavailable": {.. "message": "Thanh to.n trong .ng d.ng hi.n kh.ng kh. d.ng.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be compl eted.".. },.. "please_sign_in": {.. "message": "Vui l.ng ..ng nh.p v.o Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir6600_443859871\CRX_INSTALL_locales\zh_CN\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):	5.210259193489374
Encrypted:	false
SSDEEP:	12:1HEJ01GG01+WYpU34zeHz+dgfO8ZpU34YKiO03OyZnLAOfTYB6U:1HEplWYplSv8Zp+JOGAOfa6U
MD5:	BB73BF561BB79F89D9BF7C67C5AE5C65
SHA1:	2FADD3A1959B29C44830033A35C637D0311A8C9C
SHA-256:	D804F2A040D21D7511EFD5213D8E1721D64964A1A0DBB48E21622CEEDC9D967E
SHA-512:	627D44CEF1FE5C5ABD598BD47FF5E22B9EFC1CF98DDE3868FA9E5896C134A0C9C055AC34EDDADAE56B6690E51AEA89965D38F770552A85C732CC796795DC6D2
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_dir6600_443859871\CRX_INSTALL_locales\zh_TW\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):	634
Entropy (8bit):	5.386215984611281
Encrypted:	false
SSDEEP:	12:1HEJ2j62GG2j62+WYpU34m7T+dgc8nOO8ZpU34mvIO03OyZnLAOfTYAuH:1HEuSZCWYpsStwP8ZpROGAOfCH
MD5:	5FF50C673CC0C661D615F0CFD0E6DCA0
SHA1:	60DFF98DEAB9C4746B288BDD9C94B3BCAE5EAA85
SHA-256:	C6F8C640F3353A7B9B1432A0C139C1AEEC40133800E6C9B467B63991AD660308
SHA-512:	361D62D91F4931C5F34092C9F2C6A5323D5EEB82A24E7ABE11F7817D8D66341C0ECAD4DCB4B10873920C8D6A3CC9F5704889E178EB2549001A9F62BEDF6C801
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome .....".. },.. "app_name": {.. "message": "Chrome .....".. },.. "craw_app_unavailable": {.. "message": ".. .....".. },.. "craw_connect_to_network": {.. "message": "......".. },.. "iap_unavailable": {.. "message": ".....".. },.. "jwt_retrieve_failed": {.. "message ": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "... Chrome.".. }..}..

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 2, 2021 16:41:18.736198902 CET	192.168.2.7	8.8.8.8	0x35f2	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:18.744285107 CET	192.168.2.7	8.8.8.8	0xa43	Standard query (0)	doc.clickup.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:18.749103069 CET	192.168.2.7	8.8.8.8	0x51bd	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:19.766308069 CET	192.168.2.7	8.8.8.8	0x3f9a	Standard query (0)	doc-cdn.clickup.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:19.788389921 CET	192.168.2.7	8.8.8.8	0xb9a	Standard query (0)	scripts.attributionapp.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:20.377732992 CET	192.168.2.7	8.8.8.8	0x9a1a	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:20.532455921 CET	192.168.2.7	8.8.8.8	0xcbb7	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:20.533184052 CET	192.168.2.7	8.8.8.8	0x7471	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:23.023382902 CET	192.168.2.7	8.8.8.8	0x2088	Standard query (0)	app.clickup.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:23.146397114 CET	192.168.2.7	8.8.8.8	0xeeb5	Standard query (0)	app-cdn.clickup.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:23.314870119 CET	192.168.2.7	8.8.8.8	0x3496	Standard query (0)	ws.clickup.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:23.533267975 CET	192.168.2.7	8.8.8.8	0x991	Standard query (0)	t14171786.p.clickup-attachments.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:25.072038889 CET	192.168.2.7	8.8.8.8	0x92c2	Standard query (0)	usage.tracjs.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:25.073961973 CET	192.168.2.7	8.8.8.8	0xb06f	Standard query (0)	app-cdn.clickup.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:26.063818932 CET	192.168.2.7	8.8.8.8	0x853a	Standard query (0)	t14171786.p.clickup-attachments.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:26.092888117 CET	192.168.2.7	8.8.8.8	0x6357	Standard query (0)	doc-cdn.clickup.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:35.958420038 CET	192.168.2.7	8.8.8.8	0x96b	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:35.960793018 CET	192.168.2.7	8.8.8.8	0x7d06	Standard query (0)	use.fontawesome.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:35.962939024 CET	192.168.2.7	8.8.8.8	0xde94	Standard query (0)	dancevida.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:35.974908113 CET	192.168.2.7	8.8.8.8	0x6c8f	Standard query (0)	logincdn.msauth.net	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:36.008131027 CET	192.168.2.7	8.8.8.8	0xc7fc	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:36.013185024 CET	192.168.2.7	8.8.8.8	0x4c4d	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:36.021256924 CET	192.168.2.7	8.8.8.8	0xdf09	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:36.024295092 CET	192.168.2.7	8.8.8.8	0x2d2c	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:36.284329891 CET	192.168.2.7	8.8.8.8	0xc5e2	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:37.797674894 CET	192.168.2.7	8.8.8.8	0x4c9f	Standard query (0)	cdn.mcauto-images-production.sendgrid.net	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:39.442817926 CET	192.168.2.7	8.8.8.8	0x18fc	Standard query (0)	aadcdn.msauth.net	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:39.704468012 CET	192.168.2.7	8.8.8.8	0xf2d0	Standard query (0)	logincdn.msauth.net	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:40.862487078 CET	192.168.2.7	8.8.8.8	0x665c	Standard query (0)	clickup.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:41.698955059 CET	192.168.2.7	8.8.8.8	0x3e49	Standard query (0)	calendly.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:41.892390966 CET	192.168.2.7	8.8.8.8	0xe59f	Standard query (0)	www.googleoptimize.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:41.899087906 CET	192.168.2.7	8.8.8.8	0xbf04	Standard query (0)	client-registry.mutinycdn.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.049071074 CET	192.168.2.7	8.8.8.8	0xc88c	Standard query (0)	user-data.mutinycdn.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.055139065 CET	192.168.2.7	8.8.8.8	0x8151	Standard query (0)	static.hotjar.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 2, 2021 16:41:44.060923100 CET	192.168.2.7	8.8.8.8	0x5b7e	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.063527107 CET	192.168.2.7	8.8.8.8	0xb861	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.063930035 CET	192.168.2.7	8.8.8.8	0x174b	Standard query (0)	js.hs-scripts.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.280075073 CET	192.168.2.7	8.8.8.8	0x2d06	Standard query (0)	tag.getdrip.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.282198906 CET	192.168.2.7	8.8.8.8	0x585d	Standard query (0)	a.quora.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.292170048 CET	192.168.2.7	8.8.8.8	0xd83e	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.300211906 CET	192.168.2.7	8.8.8.8	0xbae5	Standard query (0)	cdn.firstpromoter.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.419747114 CET	192.168.2.7	8.8.8.8	0x86bf	Standard query (0)	tracking.g2crowd.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.484173059 CET	192.168.2.7	8.8.8.8	0x1fa	Standard query (0)	x.clearbitjs.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.550184011 CET	192.168.2.7	8.8.8.8	0x54a1	Standard query (0)	ws.zoominfo.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.600625992 CET	192.168.2.7	8.8.8.8	0xd1c2	Standard query (0)	script.hotjar.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.620012045 CET	192.168.2.7	8.8.8.8	0x6c2e	Standard query (0)	js.driftt.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.705912113 CET	192.168.2.7	8.8.8.8	0x51e9	Standard query (0)	q.quora.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.839440107 CET	192.168.2.7	8.8.8.8	0x4eb5	Standard query (0)	track.attributionapp.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.860248089 CET	192.168.2.7	8.8.8.8	0x88f3	Standard query (0)	www.redditstatic.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.871809006 CET	192.168.2.7	8.8.8.8	0x21b4	Standard query (0)	m.servedby-buysellads.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.876625061 CET	192.168.2.7	8.8.8.8	0xa5d0	Standard query (0)	cdn.pdst.fm	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.943329096 CET	192.168.2.7	8.8.8.8	0x3e6b	Standard query (0)	acdn.adnxs.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:45.621020079 CET	192.168.2.7	8.8.8.8	0x8ac6	Standard query (0)	api.clickup.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:45.928049088 CET	192.168.2.7	8.8.8.8	0x1ad	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:45.982819080 CET	192.168.2.7	8.8.8.8	0xcafd	Standard query (0)	static.ads-twitter.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:45.990231037 CET	192.168.2.7	8.8.8.8	0x4b34	Standard query (0)	sdk.minervaknows.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:45.990768909 CET	192.168.2.7	8.8.8.8	0xe2bc	Standard query (0)	dx.steelhousemedia.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.042157888 CET	192.168.2.7	8.8.8.8	0x467f	Standard query (0)	alb.reddit.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.106018066 CET	192.168.2.7	8.8.8.8	0xb428	Standard query (0)	api.getdrip.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.108473063 CET	192.168.2.7	8.8.8.8	0x9218	Standard query (0)	ib.adnxs.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.196413994 CET	192.168.2.7	8.8.8.8	0xb8ff	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.340146065 CET	192.168.2.7	8.8.8.8	0xb362	Standard query (0)	js.hscollectedforms.net	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.636280060 CET	192.168.2.7	8.8.8.8	0x3d9f	Standard query (0)	js.hs-analytics.net	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.639102936 CET	192.168.2.7	8.8.8.8	0x892d	Standard query (0)	js.hs-banner.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.832803965 CET	192.168.2.7	8.8.8.8	0x7fb5	Standard query (0)	hat.thepointysprites club.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.978045940 CET	192.168.2.7	8.8.8.8	0x2	Standard query (0)	vars.hotjar.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:47.014297962 CET	192.168.2.7	8.8.8.8	0xd016	Standard query (0)	us-central1-adaptive-growth.cloudfunctions.net	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:47.472970963 CET	192.168.2.7	8.8.8.8	0x6bf9	Standard query (0)	api-v2.mutinyhq.io	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:48.350956917 CET	192.168.2.7	8.8.8.8	0xe369	Standard query (0)	client.mutinycdn.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:49.034006119 CET	192.168.2.7	8.8.8.8	0xa761	Standard query (0)	x.clearbit.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 2, 2021 16:41:49.318309069 CET	192.168.2.7	8.8.8.8	0x2a5f	Standard query (0)	forms.hubspot.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:49.323941946 CET	192.168.2.7	8.8.8.8	0xb411	Standard query (0)	t.co	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:49.377322912 CET	192.168.2.7	8.8.8.8	0xe723	Standard query (0)	analytics.twitter.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:49.701217890 CET	192.168.2.7	8.8.8.8	0x7735	Standard query (0)	sdk-services.minervaknows.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:50.064011097 CET	192.168.2.7	8.8.8.8	0xb89d	Standard query (0)	core.thepointysprite sclub.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:52.929631948 CET	192.168.2.7	8.8.8.8	0x4aa	Standard query (0)	clickup.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:54.443466902 CET	192.168.2.7	8.8.8.8	0x46e6	Standard query (0)	in.hotjar.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:55.143771887 CET	192.168.2.7	8.8.8.8	0x9e05	Standard query (0)	px.steelhousemedia.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:56.279498100 CET	192.168.2.7	8.8.8.8	0xb3e7	Standard query (0)	ww.steelhousemedia.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:58.180936098 CET	192.168.2.7	8.8.8.8	0x1f49	Standard query (0)	insight.adsrvr.org	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:58.181777954 CET	192.168.2.7	8.8.8.8	0x7972	Standard query (0)	match.adsrvr.org	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:59.865612984 CET	192.168.2.7	8.8.8.8	0xc7cf	Standard query (0)	widget.intercom.io	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.205986023 CET	192.168.2.7	8.8.8.8	0xab6d	Standard query (0)	track.hubspot.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.281375885 CET	192.168.2.7	8.8.8.8	0xd38	Standard query (0)	js.intercomcdn.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.313299894 CET	192.168.2.7	8.8.8.8	0x26da	Standard query (0)	conversation.api.drift.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.313456059 CET	192.168.2.7	8.8.8.8	0x9717	Standard query (0)	metrics.api.drift.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.314244032 CET	192.168.2.7	8.8.8.8	0x21c8	Standard query (0)	customer.api.drift.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.716547966 CET	192.168.2.7	8.8.8.8	0x93c0	Standard query (0)	targeting.api.drift.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:02.508176088 CET	192.168.2.7	8.8.8.8	0x9e50	Standard query (0)	api-iam.intercom.io	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:02.774153948 CET	192.168.2.7	8.8.8.8	0xe98f	Standard query (0)	bootstrap.api.drift.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:08.489145041 CET	192.168.2.7	8.8.8.8	0x26a6	Standard query (0)	nexus-websocket-a.intercom.io	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:09.232018948 CET	192.168.2.7	8.8.8.8	0xea11	Standard query (0)	embeds.driftcdn.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:09.706062078 CET	192.168.2.7	8.8.8.8	0x755	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:14.202513933 CET	192.168.2.7	8.8.8.8	0x1cc3	Standard query (0)	5001341-41.chat.api.drift.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:14.205888033 CET	192.168.2.7	8.8.8.8	0xee3f	Standard query (0)	presence.api.drift.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:15.784424067 CET	192.168.2.7	8.8.8.8	0x37ff	Standard query (0)	event.api.drift.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:31.982297897 CET	192.168.2.7	8.8.8.8	0xa4c8	Standard query (0)	ws.clickup.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:37.852372885 CET	192.168.2.7	8.8.8.8	0xb5a1	Standard query (0)	match.adsrvr.org	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:37.856843948 CET	192.168.2.7	8.8.8.8	0xb604	Standard query (0)	insight.adsrvr.org	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:38.385122061 CET	192.168.2.7	8.8.8.8	0x51e2	Standard query (0)	px.steelhousemedia.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:51.865696907 CET	192.168.2.7	8.8.8.8	0xea33	Standard query (0)	core.thepointysprite sclub.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:43:16.741005898 CET	192.168.2.7	8.8.8.8	0xd7b3	Standard query (0)	5001341-41.chat.api.drift.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:43:17.413053989 CET	192.168.2.7	8.8.8.8	0xa8f7	Standard query (0)	presence.api.drift.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:43:36.434572935 CET	192.168.2.7	8.8.8.8	0xb72e	Standard query (0)	ws.clickup.com	A (IP address)	IN (0x0001)
Nov 2, 2021 16:43:41.010060072 CET	192.168.2.7	8.8.8.8	0x7dbc	Standard query (0)	nexus-websocket-a.intercom.io	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 16:41:18.755788088 CET	8.8.8.8	192.168.2.7	0x35f2	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:18.766567945 CET	8.8.8.8	192.168.2.7	0xa43	No error (0)	doc.clickup.com	app.clickup.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:18.766567945 CET	8.8.8.8	192.168.2.7	0xa43	No error (0)	app.clickup.com		18.193.151.4	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:18.766567945 CET	8.8.8.8	192.168.2.7	0xa43	No error (0)	app.clickup.com		52.28.94.139	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:18.766567945 CET	8.8.8.8	192.168.2.7	0xa43	No error (0)	app.clickup.com		35.159.5.202	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:18.776693106 CET	8.8.8.8	192.168.2.7	0x51bd	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:18.776693106 CET	8.8.8.8	192.168.2.7	0x51bd	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:19.783951998 CET	8.8.8.8	192.168.2.7	0x6bd5	No error (0)	www-googletagmanager.l.google.com		172.217.168.8	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:19.790469885 CET	8.8.8.8	192.168.2.7	0x3f9a	No error (0)	doc-cdn.clickup.com		18.66.112.24	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:19.790469885 CET	8.8.8.8	192.168.2.7	0x3f9a	No error (0)	doc-cdn.clickup.com		18.66.112.105	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:19.790469885 CET	8.8.8.8	192.168.2.7	0x3f9a	No error (0)	doc-cdn.clickup.com		18.66.112.61	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:19.790469885 CET	8.8.8.8	192.168.2.7	0x3f9a	No error (0)	doc-cdn.clickup.com		18.66.112.58	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:19.812081099 CET	8.8.8.8	192.168.2.7	0xb9a	No error (0)	scripts.attributionapp.com	d279x8308vq8mj.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:19.812081099 CET	8.8.8.8	192.168.2.7	0xb9a	No error (0)	d279x8308vq8mj.cloudfront.net		18.66.112.76	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:19.812081099 CET	8.8.8.8	192.168.2.7	0xb9a	No error (0)	d279x8308vq8mj.cloudfront.net		18.66.112.21	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:19.812081099 CET	8.8.8.8	192.168.2.7	0xb9a	No error (0)	d279x8308vq8mj.cloudfront.net		18.66.112.43	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:19.812081099 CET	8.8.8.8	192.168.2.7	0xb9a	No error (0)	d279x8308vq8mj.cloudfront.net		18.66.112.74	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:19.994158030 CET	8.8.8.8	192.168.2.7	0xfc13	No error (0)	www-google-analytics.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:20.395411015 CET	8.8.8.8	192.168.2.7	0x9a1a	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:20.395411015 CET	8.8.8.8	192.168.2.7	0x9a1a	No error (0)	stats.l.doubleclick.net		142.250.145.154	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:20.395411015 CET	8.8.8.8	192.168.2.7	0x9a1a	No error (0)	stats.l.doubleclick.net		142.250.145.155	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:20.395411015 CET	8.8.8.8	192.168.2.7	0x9a1a	No error (0)	stats.l.doubleclick.net		142.250.145.156	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:20.395411015 CET	8.8.8.8	192.168.2.7	0x9a1a	No error (0)	stats.l.doubleclick.net		142.250.145.157	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:20.550813913 CET	8.8.8.8	192.168.2.7	0x7471	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:20.551915884 CET	8.8.8.8	192.168.2.7	0xcbb7	No error (0)	www.google.co.uk		216.58.215.227	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 16:41:23.047187090 CET	8.8.8.8	192.168.2.7	0x2088	No error (0)	app.clickup.com		52.28.94.139	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:23.047187090 CET	8.8.8.8	192.168.2.7	0x2088	No error (0)	app.clickup.com		18.193.151.4	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:23.047187090 CET	8.8.8.8	192.168.2.7	0x2088	No error (0)	app.clickup.com		35.159.5.202	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:23.182835102 CET	8.8.8.8	192.168.2.7	0xeeb5	No error (0)	app-cdn.clickup.com	d5txjkmyderx.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:23.182835102 CET	8.8.8.8	192.168.2.7	0xeeb5	No error (0)	d5txjkmyderx.cloudfront.net		18.66.97.12	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:23.182835102 CET	8.8.8.8	192.168.2.7	0xeeb5	No error (0)	d5txjkmyderx.cloudfront.net		18.66.97.110	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:23.182835102 CET	8.8.8.8	192.168.2.7	0xeeb5	No error (0)	d5txjkmyderx.cloudfront.net		18.66.97.113	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:23.182835102 CET	8.8.8.8	192.168.2.7	0xeeb5	No error (0)	d5txjkmyderx.cloudfront.net		18.66.97.31	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:23.338646889 CET	8.8.8.8	192.168.2.7	0x3496	No error (0)	ws.clickup.com	cu-prod-de-ws.eu-central-1.elasticbeanstalk.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:23.338646889 CET	8.8.8.8	192.168.2.7	0x3496	No error (0)	cu-prod-de-ws.eu-central-1.elasticbeanstalk.com		52.58.90.176	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:23.338646889 CET	8.8.8.8	192.168.2.7	0x3496	No error (0)	cu-prod-de-ws.eu-central-1.elasticbeanstalk.com		3.125.213.119	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:23.338646889 CET	8.8.8.8	192.168.2.7	0x3496	No error (0)	cu-prod-de-ws.eu-central-1.elasticbeanstalk.com		52.29.55.84	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:23.556509972 CET	8.8.8.8	192.168.2.7	0x991	No error (0)	t14171786.p.clickup-attachments.com		18.66.112.18	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:23.556509972 CET	8.8.8.8	192.168.2.7	0x991	No error (0)	t14171786.p.clickup-attachments.com		18.66.112.62	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:23.556509972 CET	8.8.8.8	192.168.2.7	0x991	No error (0)	t14171786.p.clickup-attachments.com		18.66.112.20	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:23.556509972 CET	8.8.8.8	192.168.2.7	0x991	No error (0)	t14171786.p.clickup-attachments.com		18.66.112.69	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:25.090993881 CET	8.8.8.8	192.168.2.7	0x92c2	No error (0)	usage.trackjs.com		138.197.155.84	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:25.090993881 CET	8.8.8.8	192.168.2.7	0x92c2	No error (0)	usage.trackjs.com		51.89.217.92	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:25.090993881 CET	8.8.8.8	192.168.2.7	0x92c2	No error (0)	usage.trackjs.com		158.69.52.117	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:25.090993881 CET	8.8.8.8	192.168.2.7	0x92c2	No error (0)	usage.trackjs.com		167.114.119.127	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:25.116811037 CET	8.8.8.8	192.168.2.7	0xb06f	No error (0)	app-cdn.clickup.com	d5txjkmyderx.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:25.116811037 CET	8.8.8.8	192.168.2.7	0xb06f	No error (0)	d5txjkmyderx.cloudfront.net		18.66.97.110	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:25.116811037 CET	8.8.8.8	192.168.2.7	0xb06f	No error (0)	d5txjkmyderx.cloudfront.net		18.66.97.113	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:25.116811037 CET	8.8.8.8	192.168.2.7	0xb06f	No error (0)	d5txjkmyderx.cloudfront.net		18.66.97.31	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 16:41:25.116811037 CET	8.8.8.8	192.168.2.7	0xb06f	No error (0)	d5txjkmyderx.cloudfront.net		18.66.97.12	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:26.087368011 CET	8.8.8.8	192.168.2.7	0x853a	No error (0)	t14171786.p.clickup-attachments.com		18.66.112.69	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:26.087368011 CET	8.8.8.8	192.168.2.7	0x853a	No error (0)	t14171786.p.clickup-attachments.com		18.66.112.18	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:26.087368011 CET	8.8.8.8	192.168.2.7	0x853a	No error (0)	t14171786.p.clickup-attachments.com		18.66.112.20	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:26.087368011 CET	8.8.8.8	192.168.2.7	0x853a	No error (0)	t14171786.p.clickup-attachments.com		18.66.112.62	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:26.115247965 CET	8.8.8.8	192.168.2.7	0x6357	No error (0)	doc-cdn.clickup.com		18.66.112.61	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:26.115247965 CET	8.8.8.8	192.168.2.7	0x6357	No error (0)	doc-cdn.clickup.com		18.66.112.58	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:26.115247965 CET	8.8.8.8	192.168.2.7	0x6357	No error (0)	doc-cdn.clickup.com		18.66.112.105	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:26.115247965 CET	8.8.8.8	192.168.2.7	0x6357	No error (0)	doc-cdn.clickup.com		18.66.112.24	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:35.980813980 CET	8.8.8.8	192.168.2.7	0x96b	No error (0)	stackpath.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:35.980813980 CET	8.8.8.8	192.168.2.7	0x96b	No error (0)	stackpath.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:35.983901024 CET	8.8.8.8	192.168.2.7	0x7d06	No error (0)	use.fontawesome.com	use.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:36.007044077 CET	8.8.8.8	192.168.2.7	0x6c8f	No error (0)	logincdn.msauth.net	lgincdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:36.007044077 CET	8.8.8.8	192.168.2.7	0x6c8f	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:36.030330896 CET	8.8.8.8	192.168.2.7	0x4c4d	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:36.035738945 CET	8.8.8.8	192.168.2.7	0xc7fc	No error (0)	aadcdn.msauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:36.042066097 CET	8.8.8.8	192.168.2.7	0xdf09	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:36.042066097 CET	8.8.8.8	192.168.2.7	0xdf09	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:36.043731928 CET	8.8.8.8	192.168.2.7	0x2d2c	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:36.043731928 CET	8.8.8.8	192.168.2.7	0x2d2c	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:36.116519928 CET	8.8.8.8	192.168.2.7	0xde94	No error (0)	dancevida.com		50.87.150.0	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:36.324661970 CET	8.8.8.8	192.168.2.7	0xc5e2	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:36.324661970 CET	8.8.8.8	192.168.2.7	0xc5e2	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:37.895044088 CET	8.8.8.8	192.168.2.7	0x4c9f	No error (0)	cdn.mcauto-images-production.sendgrid.net	d3dib22dsdvm11.cloudfront.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 16:41:37.895044088 CET	8.8.8.8	192.168.2.7	0x4c9f	No error (0)	d3dib22dsd vm11.cloud front.net		18.66.97.111	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:37.895044088 CET	8.8.8.8	192.168.2.7	0x4c9f	No error (0)	d3dib22dsd vm11.cloud front.net		18.66.97.58	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:37.895044088 CET	8.8.8.8	192.168.2.7	0x4c9f	No error (0)	d3dib22dsd vm11.cloud front.net		18.66.97.99	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:37.895044088 CET	8.8.8.8	192.168.2.7	0x4c9f	No error (0)	d3dib22dsd vm11.cloud front.net		18.66.97.109	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:39.472742081 CET	8.8.8.8	192.168.2.7	0x18fc	No error (0)	aadcdn.msa uth.net	aadcdnoriginwus2.azuree dge.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:39.733829021 CET	8.8.8.8	192.168.2.7	0xf2d0	No error (0)	logincdn.m sauth.net	lgincdn.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:39.733829021 CET	8.8.8.8	192.168.2.7	0xf2d0	No error (0)	cs1227.wpc .alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:40.923923969 CET	8.8.8.8	192.168.2.7	0x665c	No error (0)	clickup.com		18.66.112.90	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:40.923923969 CET	8.8.8.8	192.168.2.7	0x665c	No error (0)	clickup.com		18.66.112.125	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:40.923923969 CET	8.8.8.8	192.168.2.7	0x665c	No error (0)	clickup.com		18.66.112.92	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:40.923923969 CET	8.8.8.8	192.168.2.7	0x665c	No error (0)	clickup.com		18.66.112.66	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:41.721530914 CET	8.8.8.8	192.168.2.7	0x3e49	No error (0)	calendly.com		172.66.41.40	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:41.721530914 CET	8.8.8.8	192.168.2.7	0x3e49	No error (0)	calendly.com		172.66.42.216	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:41.911509037 CET	8.8.8.8	192.168.2.7	0xe59f	No error (0)	www.google optimize.com		142.250.203.110	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:41.918504953 CET	8.8.8.8	192.168.2.7	0xbf04	No error (0)	client-reg istry.muti nycdn.com	c3.shared.global.fastly.ne t		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:44.068151951 CET	8.8.8.8	192.168.2.7	0xc88c	No error (0)	user-data. mutinycdn.com	c3.shared.global.fastly.ne t		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:44.078155041 CET	8.8.8.8	192.168.2.7	0x8151	No error (0)	static.hotjar.com	static-cdn.hotjar.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:44.078155041 CET	8.8.8.8	192.168.2.7	0x8151	No error (0)	static-cdn .hotjar.com		52.222.236.39	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.078155041 CET	8.8.8.8	192.168.2.7	0x8151	No error (0)	static-cdn .hotjar.com		52.222.236.99	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.078155041 CET	8.8.8.8	192.168.2.7	0x8151	No error (0)	static-cdn .hotjar.com		52.222.236.73	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.078155041 CET	8.8.8.8	192.168.2.7	0x8151	No error (0)	static-cdn .hotjar.com		52.222.236.3	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.080431938 CET	8.8.8.8	192.168.2.7	0x5b7e	No error (0)	px.ads.lin kedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:44.080431938 CET	8.8.8.8	192.168.2.7	0x5b7e	No error (0)	mix.linkedin.com	glb-na.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:44.080431938 CET	8.8.8.8	192.168.2.7	0x5b7e	No error (0)	glb-na.mix .linkedin.com	pop-edc2.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:44.080431938 CET	8.8.8.8	192.168.2.7	0x5b7e	No error (0)	pop-edc2.m ix.linkedin.com		108.174.11.85	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.087472916 CET	8.8.8.8	192.168.2.7	0x174b	No error (0)	js.hs-scripts.com		104.17.210.204	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 16:41:44.087472916 CET	8.8.8.8	192.168.2.7	0x174b	No error (0)	js.hs-scripts.com		104.17.214.204	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.087472916 CET	8.8.8.8	192.168.2.7	0x174b	No error (0)	js.hs-scripts.com		104.17.212.204	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.087472916 CET	8.8.8.8	192.168.2.7	0x174b	No error (0)	js.hs-scripts.com		104.17.211.204	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.087472916 CET	8.8.8.8	192.168.2.7	0x174b	No error (0)	js.hs-scripts.com		104.17.213.204	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.094099045 CET	8.8.8.8	192.168.2.7	0xb861	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:44.094099045 CET	8.8.8.8	192.168.2.7	0xb861	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.302062988 CET	8.8.8.8	192.168.2.7	0x585d	No error (0)	a.quora.com	quora.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:44.302062988 CET	8.8.8.8	192.168.2.7	0x585d	No error (0)	quora.map.fastly.net		151.101.1.2	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.302062988 CET	8.8.8.8	192.168.2.7	0x585d	No error (0)	quora.map.fastly.net		151.101.65.2	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.302062988 CET	8.8.8.8	192.168.2.7	0x585d	No error (0)	quora.map.fastly.net		151.101.129.2	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.302062988 CET	8.8.8.8	192.168.2.7	0x585d	No error (0)	quora.map.fastly.net		151.101.193.2	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.313208103 CET	8.8.8.8	192.168.2.7	0x2d06	No error (0)	tag.getdrip.com	d10w4ikcrdu13z.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:44.313208103 CET	8.8.8.8	192.168.2.7	0x2d06	No error (0)	d10w4ikcrdu13z.cloudfront.net		18.66.97.12	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.313208103 CET	8.8.8.8	192.168.2.7	0x2d06	No error (0)	d10w4ikcrdu13z.cloudfront.net		18.66.97.73	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.313208103 CET	8.8.8.8	192.168.2.7	0x2d06	No error (0)	d10w4ikcrdu13z.cloudfront.net		18.66.97.69	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.313208103 CET	8.8.8.8	192.168.2.7	0x2d06	No error (0)	d10w4ikcrdu13z.cloudfront.net		18.66.97.111	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.313992023 CET	8.8.8.8	192.168.2.7	0xd83e	No error (0)	snap.licdn.com	od.linkedin.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:44.325391054 CET	8.8.8.8	192.168.2.7	0xbae5	No error (0)	cdn.firstpromoter.com	d2ycxbs0cq3yaz.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:44.325391054 CET	8.8.8.8	192.168.2.7	0xbae5	No error (0)	d2ycxbs0cq3yaz.cloudfront.net		13.32.121.73	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.325391054 CET	8.8.8.8	192.168.2.7	0xbae5	No error (0)	d2ycxbs0cq3yaz.cloudfront.net		13.32.121.12	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.325391054 CET	8.8.8.8	192.168.2.7	0xbae5	No error (0)	d2ycxbs0cq3yaz.cloudfront.net		13.32.121.40	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.325391054 CET	8.8.8.8	192.168.2.7	0xbae5	No error (0)	d2ycxbs0cq3yaz.cloudfront.net		13.32.121.74	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.442554951 CET	8.8.8.8	192.168.2.7	0x86bf	No error (0)	tracking.g2crowd.com		104.18.27.190	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.442554951 CET	8.8.8.8	192.168.2.7	0x86bf	No error (0)	tracking.g2crowd.com		104.18.26.190	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.507976055 CET	8.8.8.8	192.168.2.7	0x1fa	No error (0)	x.clearbitjs.com	global-v2.clearbit.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:44.507976055 CET	8.8.8.8	192.168.2.7	0x1fa	No error (0)	global-v2.clearbit.com		18.168.94.208	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 16:41:44.507976055 CET	8.8.8.8	192.168.2.7	0x1fa	No error (0)	global-v2.clearbit.com		18.169.251.168	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.572555065 CET	8.8.8.8	192.168.2.7	0x54a1	No error (0)	ws.zoominfo.com		104.16.101.12	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.572555065 CET	8.8.8.8	192.168.2.7	0x54a1	No error (0)	ws.zoominfo.com		104.16.168.82	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.640191078 CET	8.8.8.8	192.168.2.7	0xd1c2	No error (0)	script.hotjar.com		18.66.112.122	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.640191078 CET	8.8.8.8	192.168.2.7	0xd1c2	No error (0)	script.hotjar.com		18.66.112.126	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.640191078 CET	8.8.8.8	192.168.2.7	0xd1c2	No error (0)	script.hotjar.com		18.66.112.6	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.640191078 CET	8.8.8.8	192.168.2.7	0xd1c2	No error (0)	script.hotjar.com		18.66.112.111	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.643033028 CET	8.8.8.8	192.168.2.7	0x6c2e	No error (0)	js.driftt.com	dl7g9llrghqi1.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:44.643033028 CET	8.8.8.8	192.168.2.7	0x6c2e	No error (0)	dl7g9llrghqi1.cloudfront.net		18.66.112.118	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.643033028 CET	8.8.8.8	192.168.2.7	0x6c2e	No error (0)	dl7g9llrghqi1.cloudfront.net		18.66.112.39	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.643033028 CET	8.8.8.8	192.168.2.7	0x6c2e	No error (0)	dl7g9llrghqi1.cloudfront.net		18.66.112.41	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.643033028 CET	8.8.8.8	192.168.2.7	0x6c2e	No error (0)	dl7g9llrghqi1.cloudfront.net		18.66.112.55	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.725147963 CET	8.8.8.8	192.168.2.7	0x51e9	No error (0)	q.quora.com		3.225.133.12	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.725147963 CET	8.8.8.8	192.168.2.7	0x51e9	No error (0)	q.quora.com		3.230.50.184	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.725147963 CET	8.8.8.8	192.168.2.7	0x51e9	No error (0)	q.quora.com		18.215.205.165	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.725147963 CET	8.8.8.8	192.168.2.7	0x51e9	No error (0)	q.quora.com		3.225.115.141	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.725147963 CET	8.8.8.8	192.168.2.7	0x51e9	No error (0)	q.quora.com		18.205.51.212	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.725147963 CET	8.8.8.8	192.168.2.7	0x51e9	No error (0)	q.quora.com		3.224.194.150	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.725147963 CET	8.8.8.8	192.168.2.7	0x51e9	No error (0)	q.quora.com		34.230.123.66	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.860907078 CET	8.8.8.8	192.168.2.7	0x4eb5	No error (0)	track.attributionapp.com	fluffy-alpaca-j1w7zdv61tmqz86b33z4c6tl.herokudns.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:44.860907078 CET	8.8.8.8	192.168.2.7	0x4eb5	No error (0)	fluffy-alpaca-j1w7zdv61tmqz86b33z4c6tl.herokudns.com		3.234.77.173	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.860907078 CET	8.8.8.8	192.168.2.7	0x4eb5	No error (0)	fluffy-alpaca-j1w7zdv61tmqz86b33z4c6tl.herokudns.com		34.203.159.69	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.860907078 CET	8.8.8.8	192.168.2.7	0x4eb5	No error (0)	fluffy-alpaca-j1w7zdv61tmqz86b33z4c6tl.herokudns.com		52.207.65.73	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.860907078 CET	8.8.8.8	192.168.2.7	0x4eb5	No error (0)	fluffy-alpaca-j1w7zdv61tmqz86b33z4c6tl.herokudns.com		34.232.15.19	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 16:41:44.860907078 CET	8.8.8.8	192.168.2.7	0x4eb5	No error (0)	fluffy-alpaca-j1w7zd v61tmqz86b 33z4c6tl.h erokudns.com		34.203.165.114	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.860907078 CET	8.8.8.8	192.168.2.7	0x4eb5	No error (0)	fluffy-alpaca-j1w7zd v61tmqz86b 33z4c6tl.h erokudns.com		34.225.142.216	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.860907078 CET	8.8.8.8	192.168.2.7	0x4eb5	No error (0)	fluffy-alpaca-j1w7zd v61tmqz86b 33z4c6tl.h erokudns.com		34.226.109.249	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.860907078 CET	8.8.8.8	192.168.2.7	0x4eb5	No error (0)	fluffy-alpaca-j1w7zd v61tmqz86b 33z4c6tl.h erokudns.com		50.16.95.25	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.877262115 CET	8.8.8.8	192.168.2.7	0x88f3	No error (0)	www.reddit static.com	dualstack.reddit.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:44.877262115 CET	8.8.8.8	192.168.2.7	0x88f3	No error (0)	dualstack. reddit.map .fastly.net		151.101.1.140	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.877262115 CET	8.8.8.8	192.168.2.7	0x88f3	No error (0)	dualstack. reddit.map .fastly.net		151.101.65.140	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.877262115 CET	8.8.8.8	192.168.2.7	0x88f3	No error (0)	dualstack. reddit.map .fastly.net		151.101.129.140	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.877262115 CET	8.8.8.8	192.168.2.7	0x88f3	No error (0)	dualstack. reddit.map .fastly.net		151.101.193.140	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.891300917 CET	8.8.8.8	192.168.2.7	0x21b4	No error (0)	m.servedby-buysellads.com	monetization-framework.bsa.netdna-cdn.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:44.891300917 CET	8.8.8.8	192.168.2.7	0x21b4	No error (0)	monetization-framework.bsa.netdna-cdn.com		108.161.189.78	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.895293951 CET	8.8.8.8	192.168.2.7	0xa5d0	No error (0)	cdn.pdst.fm		35.244.142.80	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.960470915 CET	8.8.8.8	192.168.2.7	0x3e6b	No error (0)	acdn.adnxs.com	prod.appnexus.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:44.960470915 CET	8.8.8.8	192.168.2.7	0x3e6b	No error (0)	prod.appnexus.map.fastly.net		151.101.1.108	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.960470915 CET	8.8.8.8	192.168.2.7	0x3e6b	No error (0)	prod.appnexus.map.fastly.net		151.101.65.108	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.960470915 CET	8.8.8.8	192.168.2.7	0x3e6b	No error (0)	prod.appnexus.map.fastly.net		151.101.129.108	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:44.960470915 CET	8.8.8.8	192.168.2.7	0x3e6b	No error (0)	prod.appnexus.map.fastly.net		151.101.193.108	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:45.642903090 CET	8.8.8.8	192.168.2.7	0x8ac6	No error (0)	api.clickup.com		18.194.89.172	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:45.642903090 CET	8.8.8.8	192.168.2.7	0x8ac6	No error (0)	api.clickup.com		18.194.253.176	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:45.642903090 CET	8.8.8.8	192.168.2.7	0x8ac6	No error (0)	api.clickup.com		18.184.45.30	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:45.948784113 CET	8.8.8.8	192.168.2.7	0x1ad	No error (0)	googleads.g.doubleclick.net		172.217.168.66	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.002800941 CET	8.8.8.8	192.168.2.7	0xcafd	No error (0)	static.ads-twitter.com	platform.twitter.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:46.002800941 CET	8.8.8.8	192.168.2.7	0xcafd	No error (0)	platform.twitter.map.fastly.net		151.101.12.157	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 16:41:46.012343884 CET	8.8.8.8	192.168.2.7	0xe2bc	No error (0)	dx.steelhousemedia.com		54.69.84.146	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.012343884 CET	8.8.8.8	192.168.2.7	0xe2bc	No error (0)	dx.steelhousemedia.com		52.11.37.91	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.012343884 CET	8.8.8.8	192.168.2.7	0xe2bc	No error (0)	dx.steelhousemedia.com		44.236.162.197	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.012343884 CET	8.8.8.8	192.168.2.7	0xe2bc	No error (0)	dx.steelhousemedia.com		44.241.10.203	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.018115044 CET	8.8.8.8	192.168.2.7	0x4b34	No error (0)	sdk.minervaknows.com	d3uwzcb5nysxzm.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:46.018115044 CET	8.8.8.8	192.168.2.7	0x4b34	No error (0)	d3uwzcb5nysxzm.cloudfront.net		52.222.214.92	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.018115044 CET	8.8.8.8	192.168.2.7	0x4b34	No error (0)	d3uwzcb5nysxzm.cloudfront.net		52.222.214.21	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.018115044 CET	8.8.8.8	192.168.2.7	0x4b34	No error (0)	d3uwzcb5nysxzm.cloudfront.net		52.222.214.97	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.018115044 CET	8.8.8.8	192.168.2.7	0x4b34	No error (0)	d3uwzcb5nysxzm.cloudfront.net		52.222.214.107	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.062453032 CET	8.8.8.8	192.168.2.7	0x467f	No error (0)	alb.reddit.com	reddit.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:46.062453032 CET	8.8.8.8	192.168.2.7	0x467f	No error (0)	reddit.map.fastly.net		151.101.1.140	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.062453032 CET	8.8.8.8	192.168.2.7	0x467f	No error (0)	reddit.map.fastly.net		151.101.65.140	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.062453032 CET	8.8.8.8	192.168.2.7	0x467f	No error (0)	reddit.map.fastly.net		151.101.129.140	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.062453032 CET	8.8.8.8	192.168.2.7	0x467f	No error (0)	reddit.map.fastly.net		151.101.193.140	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.129059076 CET	8.8.8.8	192.168.2.7	0x9218	No error (0)	ib.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:46.129059076 CET	8.8.8.8	192.168.2.7	0x9218	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:46.129059076 CET	8.8.8.8	192.168.2.7	0x9218	No error (0)	ib.anycast.adnxs.com		185.33.220.243	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.129059076 CET	8.8.8.8	192.168.2.7	0x9218	No error (0)	ib.anycast.adnxs.com		185.33.220.244	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.129059076 CET	8.8.8.8	192.168.2.7	0x9218	No error (0)	ib.anycast.adnxs.com		185.33.221.53	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.129059076 CET	8.8.8.8	192.168.2.7	0x9218	No error (0)	ib.anycast.adnxs.com		185.33.221.90	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.129059076 CET	8.8.8.8	192.168.2.7	0x9218	No error (0)	ib.anycast.adnxs.com		185.33.221.50	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.129059076 CET	8.8.8.8	192.168.2.7	0x9218	No error (0)	ib.anycast.adnxs.com		185.33.220.145	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.129059076 CET	8.8.8.8	192.168.2.7	0x9218	No error (0)	ib.anycast.adnxs.com		185.33.220.216	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.129059076 CET	8.8.8.8	192.168.2.7	0x9218	No error (0)	ib.anycast.adnxs.com		185.33.223.38	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.149317980 CET	8.8.8.8	192.168.2.7	0xb428	No error (0)	api.getdrip.com		52.222.236.11	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.149317980 CET	8.8.8.8	192.168.2.7	0xb428	No error (0)	api.getdrip.com		52.222.236.47	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 16:41:46.149317980 CET	8.8.8.8	192.168.2.7	0xb428	No error (0)	api.getdrip.com		52.222.236.126	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.149317980 CET	8.8.8.8	192.168.2.7	0xb428	No error (0)	api.getdrip.com		52.222.236.106	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.213496923 CET	8.8.8.8	192.168.2.7	0xb8ff	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:46.213496923 CET	8.8.8.8	192.168.2.7	0xb8ff	No error (0)	star-mini.c10r.facebook.com		157.240.27.35	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.360199928 CET	8.8.8.8	192.168.2.7	0xb362	No error (0)	js.hscollectedforms.net		104.17.128.171	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.360199928 CET	8.8.8.8	192.168.2.7	0xb362	No error (0)	js.hscollectedforms.net		104.17.127.171	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.360199928 CET	8.8.8.8	192.168.2.7	0xb362	No error (0)	js.hscollectedforms.net		104.17.131.171	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.360199928 CET	8.8.8.8	192.168.2.7	0xb362	No error (0)	js.hscollectedforms.net		104.17.130.171	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.360199928 CET	8.8.8.8	192.168.2.7	0xb362	No error (0)	js.hscollectedforms.net		104.17.129.171	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.658401966 CET	8.8.8.8	192.168.2.7	0x3d9f	No error (0)	js.hs-analytics.net		104.17.68.176	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.658401966 CET	8.8.8.8	192.168.2.7	0x3d9f	No error (0)	js.hs-analytics.net		104.17.67.176	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.658401966 CET	8.8.8.8	192.168.2.7	0x3d9f	No error (0)	js.hs-analytics.net		104.17.71.176	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.658401966 CET	8.8.8.8	192.168.2.7	0x3d9f	No error (0)	js.hs-analytics.net		104.17.70.176	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.658401966 CET	8.8.8.8	192.168.2.7	0x3d9f	No error (0)	js.hs-analytics.net		104.17.69.176	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.661410093 CET	8.8.8.8	192.168.2.7	0x892d	No error (0)	js.hs-banner.com		104.18.21.191	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.661410093 CET	8.8.8.8	192.168.2.7	0x892d	No error (0)	js.hs-banner.com		104.18.20.191	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.880178928 CET	8.8.8.8	192.168.2.7	0x7fb5	No error (0)	hat.thepointysprites club.com		18.66.139.27	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.880178928 CET	8.8.8.8	192.168.2.7	0x7fb5	No error (0)	hat.thepointysprites club.com		18.66.139.72	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.880178928 CET	8.8.8.8	192.168.2.7	0x7fb5	No error (0)	hat.thepointysprites club.com		18.66.139.63	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:46.880178928 CET	8.8.8.8	192.168.2.7	0x7fb5	No error (0)	hat.thepointysprites club.com		18.66.139.78	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:47.002851009 CET	8.8.8.8	192.168.2.7	0x2	No error (0)	vars.hotjar.com		18.66.139.40	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:47.002851009 CET	8.8.8.8	192.168.2.7	0x2	No error (0)	vars.hotjar.com		18.66.139.28	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:47.002851009 CET	8.8.8.8	192.168.2.7	0x2	No error (0)	vars.hotjar.com		18.66.139.84	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:47.002851009 CET	8.8.8.8	192.168.2.7	0x2	No error (0)	vars.hotjar.com		18.66.139.117	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:47.042726994 CET	8.8.8.8	192.168.2.7	0xd016	No error (0)	us-central1-adaptive-growth.cloudfunctions.net		216.239.36.54	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:47.492517948 CET	8.8.8.8	192.168.2.7	0x6bf9	No error (0)	api-v2.mutinyhq.io	gentle-meadow-3800.shrouded-lake-4691.herokuspace.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 16:41:47.492517948 CET	8.8.8.8	192.168.2.7	0x6bf9	No error (0)	gentle-meadow-3800.shrouded-lake-4691.herokuspace.com		44.237.209.143	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:47.492517948 CET	8.8.8.8	192.168.2.7	0x6bf9	No error (0)	gentle-meadow-3800.shrouded-lake-4691.herokuspace.com		44.229.66.253	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:48.374799013 CET	8.8.8.8	192.168.2.7	0xe369	No error (0)	client.mutinycdn.com		13.32.99.34	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:48.374799013 CET	8.8.8.8	192.168.2.7	0xe369	No error (0)	client.mutinycdn.com		13.32.99.52	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:48.374799013 CET	8.8.8.8	192.168.2.7	0xe369	No error (0)	client.mutinycdn.com		13.32.99.93	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:48.374799013 CET	8.8.8.8	192.168.2.7	0xe369	No error (0)	client.mutinycdn.com		13.32.99.98	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:49.058522940 CET	8.8.8.8	192.168.2.7	0xa761	No error (0)	x.clearbit.com		18.169.251.168	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:49.058522940 CET	8.8.8.8	192.168.2.7	0xa761	No error (0)	x.clearbit.com		18.168.94.208	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:49.340492010 CET	8.8.8.8	192.168.2.7	0x2a5f	No error (0)	forms.hubspot.com		104.19.154.83	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:49.340492010 CET	8.8.8.8	192.168.2.7	0x2a5f	No error (0)	forms.hubspot.com		104.19.155.83	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:49.342690945 CET	8.8.8.8	192.168.2.7	0xb411	No error (0)	t.co		104.244.42.197	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:49.342690945 CET	8.8.8.8	192.168.2.7	0xb411	No error (0)	t.co		104.244.42.69	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:49.342690945 CET	8.8.8.8	192.168.2.7	0xb411	No error (0)	t.co		104.244.42.5	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:49.342690945 CET	8.8.8.8	192.168.2.7	0xb411	No error (0)	t.co		104.244.42.133	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:49.396055937 CET	8.8.8.8	192.168.2.7	0xe723	No error (0)	analytics.twitter.com	ads.twitter.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:49.396055937 CET	8.8.8.8	192.168.2.7	0xe723	No error (0)	ads.twitter.com	s.twitter.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:49.396055937 CET	8.8.8.8	192.168.2.7	0xe723	No error (0)	s.twitter.com		104.244.42.131	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:49.396055937 CET	8.8.8.8	192.168.2.7	0xe723	No error (0)	s.twitter.com		104.244.42.67	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:49.396055937 CET	8.8.8.8	192.168.2.7	0xe723	No error (0)	s.twitter.com		104.244.42.3	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:49.396055937 CET	8.8.8.8	192.168.2.7	0xe723	No error (0)	s.twitter.com		104.244.42.195	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:49.725184917 CET	8.8.8.8	192.168.2.7	0x7735	No error (0)	sdk-services.minervaknows.com	dysvscllmejh2.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:49.725184917 CET	8.8.8.8	192.168.2.7	0x7735	No error (0)	dysvscllmejh2.cloudfront.net		52.222.236.50	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:49.725184917 CET	8.8.8.8	192.168.2.7	0x7735	No error (0)	dysvscllmejh2.cloudfront.net		52.222.236.7	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:49.725184917 CET	8.8.8.8	192.168.2.7	0x7735	No error (0)	dysvscllmejh2.cloudfront.net		52.222.236.129	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:49.725184917 CET	8.8.8.8	192.168.2.7	0x7735	No error (0)	dysvscllmejh2.cloudfront.net		52.222.236.75	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 16:41:50.085452080 CET	8.8.8.8	192.168.2.7	0xb89d	No error (0)	core.thepointysprite sclub.com		34.199.234.25	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:50.085452080 CET	8.8.8.8	192.168.2.7	0xb89d	No error (0)	core.thepointysprite sclub.com		35.172.245.152	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:50.085452080 CET	8.8.8.8	192.168.2.7	0xb89d	No error (0)	core.thepointysprite sclub.com		54.83.110.109	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:50.085452080 CET	8.8.8.8	192.168.2.7	0xb89d	No error (0)	core.thepointysprite sclub.com		3.227.190.204	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:50.085452080 CET	8.8.8.8	192.168.2.7	0xb89d	No error (0)	core.thepointysprite sclub.com		52.45.196.192	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:50.085452080 CET	8.8.8.8	192.168.2.7	0xb89d	No error (0)	core.thepointysprite sclub.com		50.16.211.97	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:52.953264952 CET	8.8.8.8	192.168.2.7	0x4aa	No error (0)	clickup.com		18.66.112.66	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:52.953264952 CET	8.8.8.8	192.168.2.7	0x4aa	No error (0)	clickup.com		18.66.112.125	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:52.953264952 CET	8.8.8.8	192.168.2.7	0x4aa	No error (0)	clickup.com		18.66.112.92	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:52.953264952 CET	8.8.8.8	192.168.2.7	0x4aa	No error (0)	clickup.com		18.66.112.90	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:54.462677002 CET	8.8.8.8	192.168.2.7	0x46e6	No error (0)	in.hotjar.com	in-live.live.eks.hotjar.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:41:54.462677002 CET	8.8.8.8	192.168.2.7	0x46e6	No error (0)	in-live.live.eks.hotjar.com		54.76.144.107	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:54.462677002 CET	8.8.8.8	192.168.2.7	0x46e6	No error (0)	in-live.live.eks.hotjar.com		52.51.140.204	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:54.462677002 CET	8.8.8.8	192.168.2.7	0x46e6	No error (0)	in-live.live.eks.hotjar.com		54.78.108.238	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:54.462677002 CET	8.8.8.8	192.168.2.7	0x46e6	No error (0)	in-live.live.eks.hotjar.com		99.80.125.216	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:54.462677002 CET	8.8.8.8	192.168.2.7	0x46e6	No error (0)	in-live.live.eks.hotjar.com		63.34.251.77	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:54.462677002 CET	8.8.8.8	192.168.2.7	0x46e6	No error (0)	in-live.live.eks.hotjar.com		54.75.159.38	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:54.462677002 CET	8.8.8.8	192.168.2.7	0x46e6	No error (0)	in-live.live.eks.hotjar.com		52.50.124.16	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:54.462677002 CET	8.8.8.8	192.168.2.7	0x46e6	No error (0)	in-live.live.eks.hotjar.com		99.81.27.250	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:55.165803909 CET	8.8.8.8	192.168.2.7	0x9e05	No error (0)	px.steelhousemedia.com		54.245.46.233	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:55.165803909 CET	8.8.8.8	192.168.2.7	0x9e05	No error (0)	px.steelhousemedia.com		54.244.159.189	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:55.165803909 CET	8.8.8.8	192.168.2.7	0x9e05	No error (0)	px.steelhousemedia.com		44.225.29.129	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:55.165803909 CET	8.8.8.8	192.168.2.7	0x9e05	No error (0)	px.steelhousemedia.com		44.237.157.168	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:55.165803909 CET	8.8.8.8	192.168.2.7	0x9e05	No error (0)	px.steelhousemedia.com		52.10.121.135	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:56.299439907 CET	8.8.8.8	192.168.2.7	0xb3e7	No error (0)	ww.steelhousemedia.com		44.238.216.23	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:56.299439907 CET	8.8.8.8	192.168.2.7	0xb3e7	No error (0)	ww.steelhousemedia.com		44.238.130.186	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 16:41:58.200130939 CET	8.8.8.8	192.168.2.7	0x1f49	No error (0)	insight.adsrvr.org		52.223.40.198	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:58.200130939 CET	8.8.8.8	192.168.2.7	0x1f49	No error (0)	insight.adsrvr.org		35.71.131.137	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:58.200130939 CET	8.8.8.8	192.168.2.7	0x1f49	No error (0)	insight.adsrvr.org		15.197.193.217	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:58.200130939 CET	8.8.8.8	192.168.2.7	0x1f49	No error (0)	insight.adsrvr.org		3.33.220.150	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:58.200473070 CET	8.8.8.8	192.168.2.7	0x7972	No error (0)	match.adsrvr.org		52.223.40.198	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:58.200473070 CET	8.8.8.8	192.168.2.7	0x7972	No error (0)	match.adsrvr.org		35.71.131.137	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:58.200473070 CET	8.8.8.8	192.168.2.7	0x7972	No error (0)	match.adsrvr.org		15.197.193.217	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:58.200473070 CET	8.8.8.8	192.168.2.7	0x7972	No error (0)	match.adsrvr.org		3.33.220.150	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:59.887550116 CET	8.8.8.8	192.168.2.7	0xc7cf	No error (0)	widget.intercom.io		13.32.99.55	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:59.887550116 CET	8.8.8.8	192.168.2.7	0xc7cf	No error (0)	widget.intercom.io		13.32.99.47	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:59.887550116 CET	8.8.8.8	192.168.2.7	0xc7cf	No error (0)	widget.intercom.io		13.32.99.71	A (IP address)	IN (0x0001)
Nov 2, 2021 16:41:59.887550116 CET	8.8.8.8	192.168.2.7	0xc7cf	No error (0)	widget.intercom.io		13.32.99.25	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.227334976 CET	8.8.8.8	192.168.2.7	0xab6d	No error (0)	track.hubspot.com		104.19.155.83	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.227334976 CET	8.8.8.8	192.168.2.7	0xab6d	No error (0)	track.hubspot.com		104.19.154.83	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.303262949 CET	8.8.8.8	192.168.2.7	0xd38	No error (0)	js.intercomcdn.com		18.66.139.43	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.303262949 CET	8.8.8.8	192.168.2.7	0xd38	No error (0)	js.intercomcdn.com		18.66.139.67	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.303262949 CET	8.8.8.8	192.168.2.7	0xd38	No error (0)	js.intercomcdn.com		18.66.139.61	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.303262949 CET	8.8.8.8	192.168.2.7	0xd38	No error (0)	js.intercomcdn.com		18.66.139.109	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.331769943 CET	8.8.8.8	192.168.2.7	0x21c8	No error (0)	customer.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:42:00.331769943 CET	8.8.8.8	192.168.2.7	0x21c8	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		54.147.21.139	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.331769943 CET	8.8.8.8	192.168.2.7	0x21c8	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 16:42:00.331769943 CET	8.8.8.8	192.168.2.7	0x21c8	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.331769943 CET	8.8.8.8	192.168.2.7	0x21c8	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		50.16.7.188	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.333023071 CET	8.8.8.8	192.168.2.7	0x26da	No error (0)	conversation.api.drift.com	istio.api.drift.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:42:00.333023071 CET	8.8.8.8	192.168.2.7	0x26da	No error (0)	istio.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:42:00.333023071 CET	8.8.8.8	192.168.2.7	0x26da	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.333023071 CET	8.8.8.8	192.168.2.7	0x26da	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.333023071 CET	8.8.8.8	192.168.2.7	0x26da	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		54.147.21.139	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.333023071 CET	8.8.8.8	192.168.2.7	0x26da	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		50.16.7.188	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.333087921 CET	8.8.8.8	192.168.2.7	0x9717	No error (0)	metrics.api.drift.com	istio.api.drift.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:42:00.333087921 CET	8.8.8.8	192.168.2.7	0x9717	No error (0)	istio.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:42:00.333087921 CET	8.8.8.8	192.168.2.7	0x9717	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		54.147.21.139	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.333087921 CET	8.8.8.8	192.168.2.7	0x9717	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 16:42:00.333087921 CET	8.8.8.8	192.168.2.7	0x9717	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.333087921 CET	8.8.8.8	192.168.2.7	0x9717	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		50.16.7.188	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.737246990 CET	8.8.8.8	192.168.2.7	0x93c0	No error (0)	targeting.api.drift.com	istio.api.drift.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:42:00.737246990 CET	8.8.8.8	192.168.2.7	0x93c0	No error (0)	istio.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:42:00.737246990 CET	8.8.8.8	192.168.2.7	0x93c0	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.737246990 CET	8.8.8.8	192.168.2.7	0x93c0	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		54.147.21.139	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.737246990 CET	8.8.8.8	192.168.2.7	0x93c0	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		50.16.7.188	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:00.737246990 CET	8.8.8.8	192.168.2.7	0x93c0	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:02.525171041 CET	8.8.8.8	192.168.2.7	0x9e50	No error (0)	api-iam.intercom.io		99.83.219.81	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:02.525171041 CET	8.8.8.8	192.168.2.7	0x9e50	No error (0)	api-iam.intercom.io		75.2.88.188	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:02.793165922 CET	8.8.8.8	192.168.2.7	0xe98f	No error (0)	bootstrap.api.drift.com	istio.api.drift.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:42:02.793165922 CET	8.8.8.8	192.168.2.7	0xe98f	No error (0)	istio.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:42:02.793165922 CET	8.8.8.8	192.168.2.7	0xe98f	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:02.793165922 CET	8.8.8.8	192.168.2.7	0xe98f	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		54.147.21.139	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 16:42:02.793165922 CET	8.8.8.8	192.168.2.7	0xe98f	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		50.16.7.188	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:02.793165922 CET	8.8.8.8	192.168.2.7	0xe98f	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:08.508220911 CET	8.8.8.8	192.168.2.7	0x26a6	No error (0)	nexus-websocket-a.intercom.io		35.174.127.31	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:08.508220911 CET	8.8.8.8	192.168.2.7	0x26a6	No error (0)	nexus-websocket-a.intercom.io		34.237.73.95	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:08.508220911 CET	8.8.8.8	192.168.2.7	0x26a6	No error (0)	nexus-websocket-a.intercom.io		35.170.0.145	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:09.255120039 CET	8.8.8.8	192.168.2.7	0xea11	No error (0)	embeds.driftcdn.com		13.32.99.26	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:09.255120039 CET	8.8.8.8	192.168.2.7	0xea11	No error (0)	embeds.driftcdn.com		13.32.99.60	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:09.255120039 CET	8.8.8.8	192.168.2.7	0xea11	No error (0)	embeds.driftcdn.com		13.32.99.65	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:09.255120039 CET	8.8.8.8	192.168.2.7	0xea11	No error (0)	embeds.driftcdn.com		13.32.99.3	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:09.729192972 CET	8.8.8.8	192.168.2.7	0x755	No error (0)	px.ads.linkedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:42:09.729192972 CET	8.8.8.8	192.168.2.7	0x755	No error (0)	mix.linkedin.com	glb-na.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:42:09.729192972 CET	8.8.8.8	192.168.2.7	0x755	No error (0)	glb-na.mix.linkedin.com	pop-esv5.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:42:09.729192972 CET	8.8.8.8	192.168.2.7	0x755	No error (0)	pop-esv5.mix.linkedin.com		108.174.11.37	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:14.224778891 CET	8.8.8.8	192.168.2.7	0x1cc3	No error (0)	5001341-41.chat.api.drift.com	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:42:14.224778891 CET	8.8.8.8	192.168.2.7	0x1cc3	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		18.204.101.20	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:14.224778891 CET	8.8.8.8	192.168.2.7	0x1cc3	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		54.221.22.199	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:14.224778891 CET	8.8.8.8	192.168.2.7	0x1cc3	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		52.7.174.240	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:14.224778891 CET	8.8.8.8	192.168.2.7	0x1cc3	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		52.54.84.154	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 16:42:14.224778891 CET	8.8.8.8	192.168.2.7	0x1cc3	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		3.218.184.213	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:14.224778891 CET	8.8.8.8	192.168.2.7	0x1cc3	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		52.54.195.121	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:14.224778891 CET	8.8.8.8	192.168.2.7	0x1cc3	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		34.233.207.138	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:14.224778891 CET	8.8.8.8	192.168.2.7	0x1cc3	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		52.4.98.235	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:14.226257086 CET	8.8.8.8	192.168.2.7	0xee3f	No error (0)	presence.api.drift.com	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:42:14.226257086 CET	8.8.8.8	192.168.2.7	0xee3f	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		54.85.240.191	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:14.226257086 CET	8.8.8.8	192.168.2.7	0xee3f	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		54.173.95.250	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:14.226257086 CET	8.8.8.8	192.168.2.7	0xee3f	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		35.174.210.7	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:14.226257086 CET	8.8.8.8	192.168.2.7	0xee3f	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		52.0.218.127	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:15.802766085 CET	8.8.8.8	192.168.2.7	0x37ff	No error (0)	event.api.drift.com	alb-event-1454785217.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:42:15.802766085 CET	8.8.8.8	192.168.2.7	0x37ff	No error (0)	alb-event-1454785217.us-east-1.elb.amazonaws.com		34.234.150.139	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:15.802766085 CET	8.8.8.8	192.168.2.7	0x37ff	No error (0)	alb-event-1454785217.us-east-1.elb.amazonaws.com		34.231.2.68	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:16.373172998 CET	8.8.8.8	192.168.2.7	0xba1c	No error (0)	gstaticadssl.l.google.com		172.217.168.3	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:32.001890898 CET	8.8.8.8	192.168.2.7	0xa4c8	No error (0)	ws.clickup.com	cu-prod-de-ws.eu-central-1.elasticbeanstalk.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:42:32.001890898 CET	8.8.8.8	192.168.2.7	0xa4c8	No error (0)	cu-prod-de-ws.eu-central-1.elasticbeanstalk.com		52.58.90.176	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 16:42:32.001890898 CET	8.8.8.8	192.168.2.7	0xa4c8	No error (0)	cu-prod-de-ws.eu-central-1.elasticbeanstalk.com		52.29.55.84	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:32.001890898 CET	8.8.8.8	192.168.2.7	0xa4c8	No error (0)	cu-prod-de-ws.eu-central-1.elasticbeanstalk.com		3.125.213.119	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:37.871114969 CET	8.8.8.8	192.168.2.7	0xb5a1	No error (0)	match.adsrvr.org		52.223.40.198	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:37.871114969 CET	8.8.8.8	192.168.2.7	0xb5a1	No error (0)	match.adsrvr.org		35.71.131.137	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:37.871114969 CET	8.8.8.8	192.168.2.7	0xb5a1	No error (0)	match.adsrvr.org		15.197.193.217	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:37.871114969 CET	8.8.8.8	192.168.2.7	0xb5a1	No error (0)	match.adsrvr.org		3.33.220.150	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:37.874011040 CET	8.8.8.8	192.168.2.7	0xb604	No error (0)	insight.adsrvr.org		52.223.40.198	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:37.874011040 CET	8.8.8.8	192.168.2.7	0xb604	No error (0)	insight.adsrvr.org		35.71.131.137	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:37.874011040 CET	8.8.8.8	192.168.2.7	0xb604	No error (0)	insight.adsrvr.org		15.197.193.217	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:37.874011040 CET	8.8.8.8	192.168.2.7	0xb604	No error (0)	insight.adsrvr.org		3.33.220.150	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:38.409529924 CET	8.8.8.8	192.168.2.7	0x51e2	No error (0)	px.steelhousemedia.com		44.237.157.168	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:38.409529924 CET	8.8.8.8	192.168.2.7	0x51e2	No error (0)	px.steelhousemedia.com		54.245.46.233	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:38.409529924 CET	8.8.8.8	192.168.2.7	0x51e2	No error (0)	px.steelhousemedia.com		52.10.121.135	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:38.409529924 CET	8.8.8.8	192.168.2.7	0x51e2	No error (0)	px.steelhousemedia.com		44.225.29.129	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:38.409529924 CET	8.8.8.8	192.168.2.7	0x51e2	No error (0)	px.steelhousemedia.com		54.244.159.189	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:51.886121035 CET	8.8.8.8	192.168.2.7	0xea33	No error (0)	core.thepointysprite sclub.com		54.83.110.109	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:51.886121035 CET	8.8.8.8	192.168.2.7	0xea33	No error (0)	core.thepointysprite sclub.com		3.227.190.204	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:51.886121035 CET	8.8.8.8	192.168.2.7	0xea33	No error (0)	core.thepointysprite sclub.com		35.172.245.152	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:51.886121035 CET	8.8.8.8	192.168.2.7	0xea33	No error (0)	core.thepointysprite sclub.com		50.16.211.97	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:51.886121035 CET	8.8.8.8	192.168.2.7	0xea33	No error (0)	core.thepointysprite sclub.com		34.199.234.25	A (IP address)	IN (0x0001)
Nov 2, 2021 16:42:51.886121035 CET	8.8.8.8	192.168.2.7	0xea33	No error (0)	core.thepointysprite sclub.com		52.45.196.192	A (IP address)	IN (0x0001)
Nov 2, 2021 16:43:16.763098001 CET	8.8.8.8	192.168.2.7	0xd7b3	No error (0)	5001341-41.chat.api.drift.com	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:43:16.763098001 CET	8.8.8.8	192.168.2.7	0xd7b3	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		18.204.101.20	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 16:43:16.763098001 CET	8.8.8.8	192.168.2.7	0xd7b3	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		34.231.165.96	A (IP address)	IN (0x0001)
Nov 2, 2021 16:43:16.763098001 CET	8.8.8.8	192.168.2.7	0xd7b3	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		3.218.184.213	A (IP address)	IN (0x0001)
Nov 2, 2021 16:43:16.763098001 CET	8.8.8.8	192.168.2.7	0xd7b3	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		34.203.97.57	A (IP address)	IN (0x0001)
Nov 2, 2021 16:43:16.763098001 CET	8.8.8.8	192.168.2.7	0xd7b3	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		52.207.78.168	A (IP address)	IN (0x0001)
Nov 2, 2021 16:43:16.763098001 CET	8.8.8.8	192.168.2.7	0xd7b3	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		44.196.232.100	A (IP address)	IN (0x0001)
Nov 2, 2021 16:43:16.763098001 CET	8.8.8.8	192.168.2.7	0xd7b3	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		34.233.207.138	A (IP address)	IN (0x0001)
Nov 2, 2021 16:43:16.763098001 CET	8.8.8.8	192.168.2.7	0xd7b3	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		54.237.186.175	A (IP address)	IN (0x0001)
Nov 2, 2021 16:43:17.433099985 CET	8.8.8.8	192.168.2.7	0xa8f7	No error (0)	presence.api.drift.com	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 16:43:17.433099985 CET	8.8.8.8	192.168.2.7	0xa8f7	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		54.85.240.191	A (IP address)	IN (0x0001)
Nov 2, 2021 16:43:17.433099985 CET	8.8.8.8	192.168.2.7	0xa8f7	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		52.0.218.127	A (IP address)	IN (0x0001)
Nov 2, 2021 16:43:17.433099985 CET	8.8.8.8	192.168.2.7	0xa8f7	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		54.173.95.250	A (IP address)	IN (0x0001)
Nov 2, 2021 16:43:17.433099985 CET	8.8.8.8	192.168.2.7	0xa8f7	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		35.174.210.7	A (IP address)	IN (0x0001)
Nov 2, 2021 16:43:36.459530115 CET	8.8.8.8	192.168.2.7	0xb72e	No error (0)	ws.clickup.com	cu-prod-de-ws.eu-central-1.elasticbeanstalk.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 16:43:36.459530115 CET	8.8.8.8	192.168.2.7	0xb72e	No error (0)	cu-prod-de-ws.eu-central-1.elasticbeanstalk.com		52.58.90.176	A (IP address)	IN (0x0001)
Nov 2, 2021 16:43:36.459530115 CET	8.8.8.8	192.168.2.7	0xb72e	No error (0)	cu-prod-de-ws.eu-central-1.elasticbeanstalk.com		52.29.55.84	A (IP address)	IN (0x0001)
Nov 2, 2021 16:43:36.459530115 CET	8.8.8.8	192.168.2.7	0xb72e	No error (0)	cu-prod-de-ws.eu-central-1.elasticbeanstalk.com		3.125.213.119	A (IP address)	IN (0x0001)
Nov 2, 2021 16:43:41.029635906 CET	8.8.8.8	192.168.2.7	0x7dbc	No error (0)	nexus-websocket-a.intercom.io		34.237.73.95	A (IP address)	IN (0x0001)
Nov 2, 2021 16:43:41.029635906 CET	8.8.8.8	192.168.2.7	0x7dbc	No error (0)	nexus-websocket-a.intercom.io		35.170.0.145	A (IP address)	IN (0x0001)
Nov 2, 2021 16:43:41.029635906 CET	8.8.8.8	192.168.2.7	0x7dbc	No error (0)	nexus-websocket-a.intercom.io		35.174.127.31	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6600 Parent PID: 5036

General

Start time:	16:41:14
Start date:	02/11/2021
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://doc.clickup.com/d/h/dgfma-27/710cedf22e388d1
Imagebase:	0x7ff76d1c0000
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

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 6812 Parent PID: 6600

General

Start time:	16:41:15
Start date:	02/11/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1564,4810638549202391110,5699968190218675685,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1928 /prefetch:8
Imagebase:	0x7ff76d1c0000
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

Show Windows behavior

Disassembly

Code Analysis