ID: 508766
Cookbook: browseurl.jbs
Time: 15:46:06
Date: 25/10/2021
Version: 33.0.0 White Diamond

Table of Contents

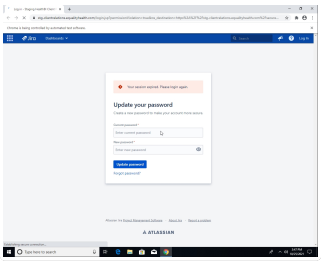
Windows Analysis Report https://stg-clientrelations.equ…

Overview

General Information

Sample URL:	http://https://stg-clientrelations.equalityhealth.com/secure/ChangeUserPassword!default.jspa?username=n.martinez@chcfl.org
Analysis ID:	508766
Infos:	

Most interesting Screenshot:



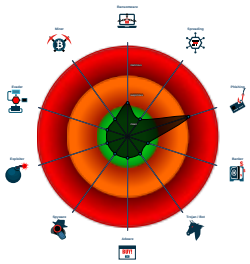
Detection

Score:	21
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Ask for current and new password
- URL contains potential PII (phishing…
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 3212 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://stg-clientrelations.equalityhealth.com/secure/ChangeUserPassword!default.jspa?username=n.martinez@chcfl.org' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 4072 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1572,18266022950293399891,13773735986418769558,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1936 /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

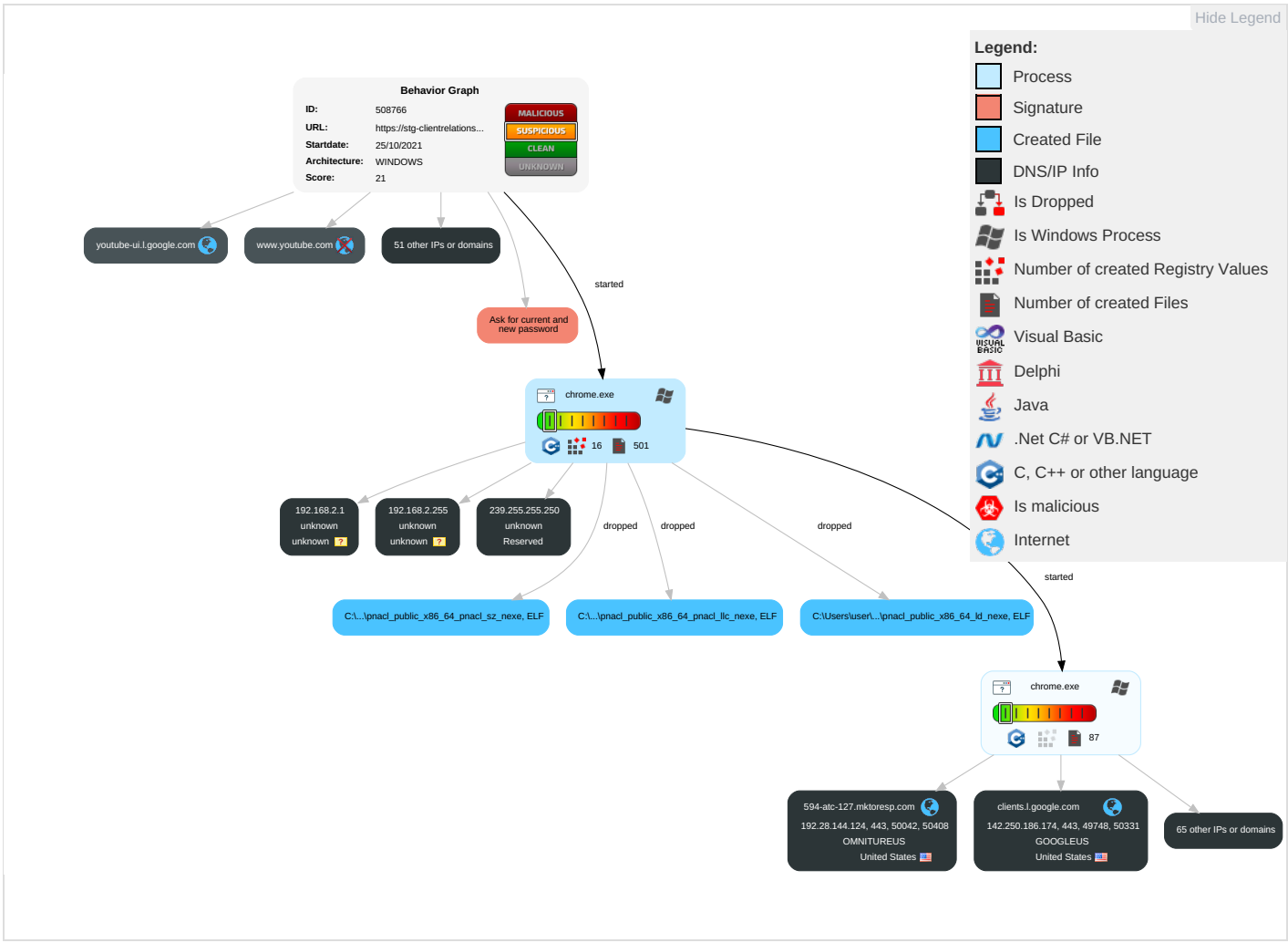
Phishing:

Ask for current and new password

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	In
Valid Accounts 1	Windows Management Instrumentation	Valid Accounts 1	Valid Accounts 1	Masquerading 3	GUI Input Capture 1	System Service Discovery	Remote Services	GUI Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S P
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1	Valid Accounts 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		C B F

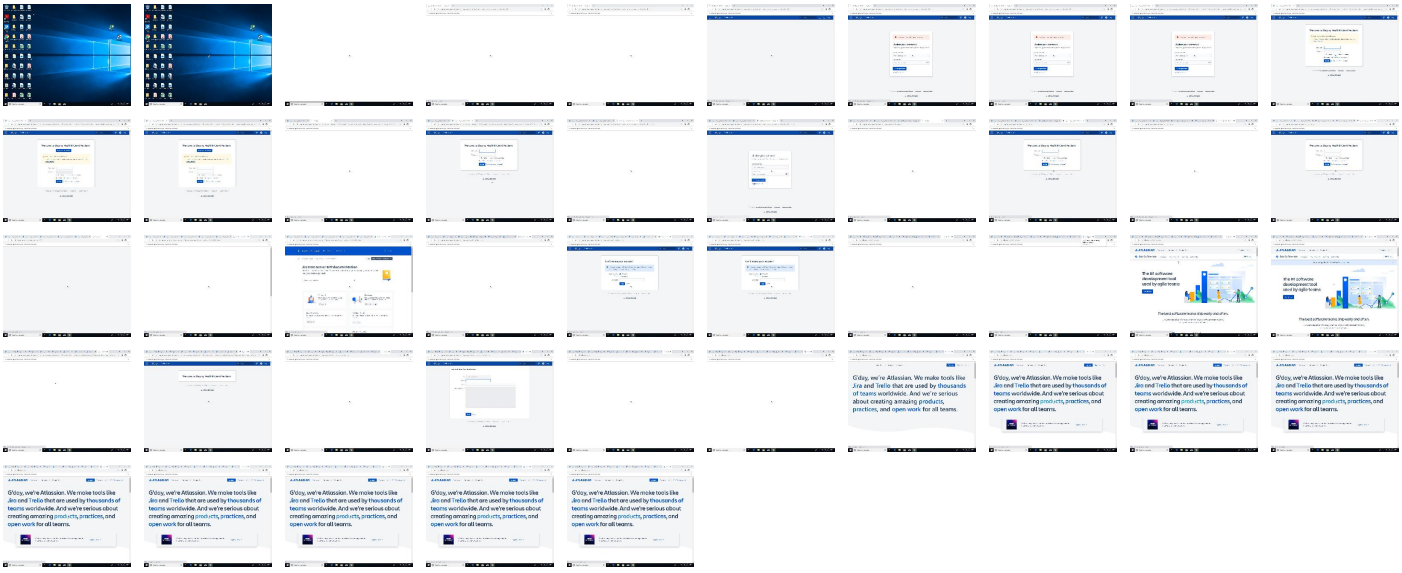
Behavior Graph

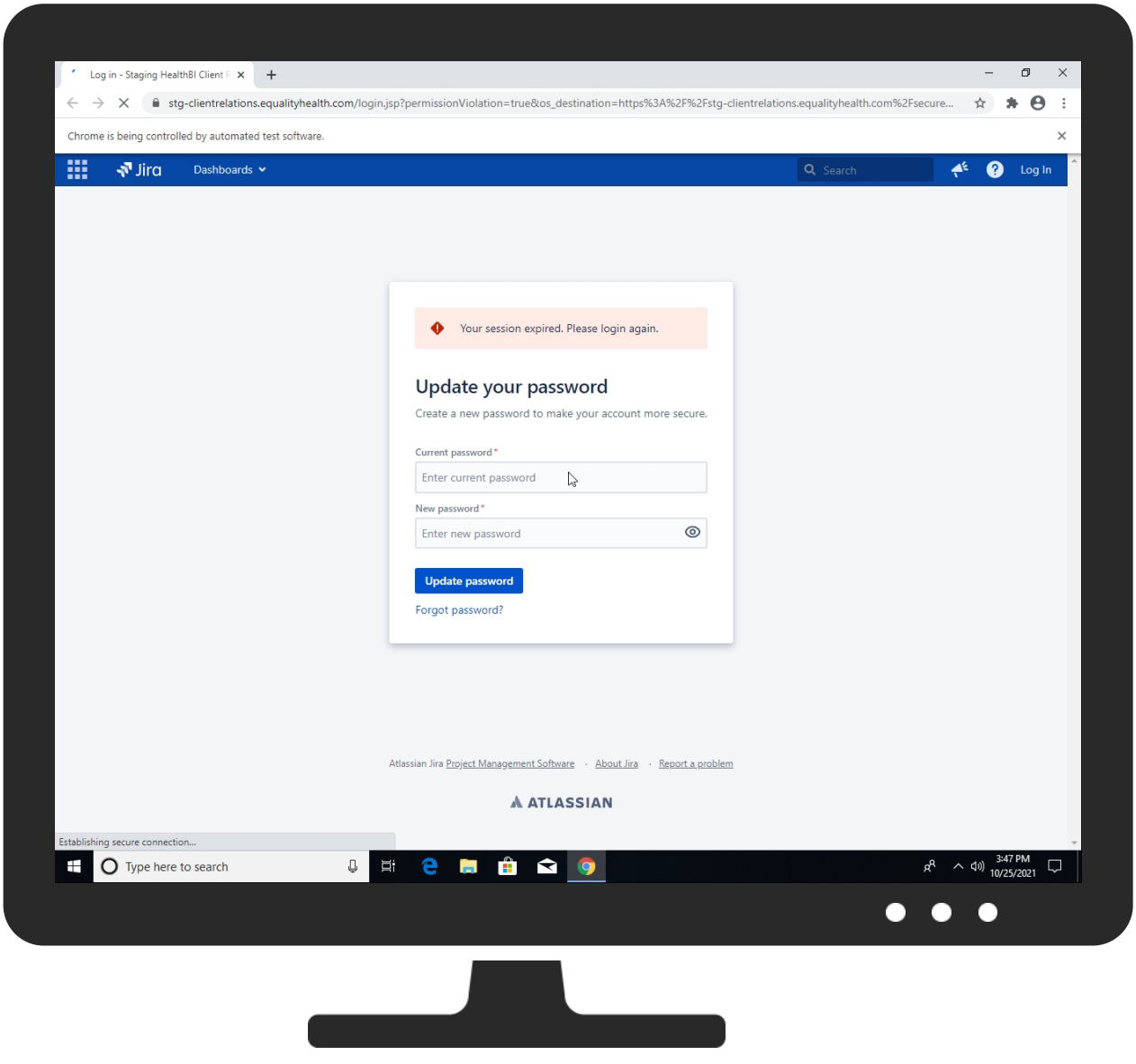


Screenshots

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://stg-clientrelations.equalityhealth.com/secure/ChangeUserPassword!default.jspa?username=n.martinez@chcfl.org	0%	Virustotal		Browse
http://https://stg-clientrelations.equalityhealth.com/secure/ChangeUserPassword!default.jspa?username=n.martinez@chcfl.org	0%	Avira URL Cloud	safe	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\3212_2067475749_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\3212_2067475749_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\3212_2067475749_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\3212_2067475749_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\3212_2067475749_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\3212_2067475749_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.atlassian.com_oeu1635202071179r0.6121722167079615$$1096093$$tracker_optimizely	0%	Avira URL Cloud	safe	
http://https://stg-clientrelations.equalityhealth.com/secure/ChangeUserPassword!default.jspa?username=n.martinez@chcfl.org	0%	Virustotal		Browse
http://https://confluence.atlassian.com_oeu1635202071179r0.6121722167079615$$10828395850$$layer_map	0%	Avira URL Cloud	safe	
http://https://confluence.atlassian.com_oeu1635202071179r0.6121722167079615$$10828395850$$layer_states	0%	Avira URL Cloud	safe	
http://https://confluence.atlassian.com_pending_events	0%	Avira URL Cloud	safe	
http://https://confluence.atlassian.com_oeu1635202071179r0.6121722167079615$$10828395850$$variation_map	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://stg-clientrelations.equalityhealth.com/login.jsp?permissionViolation=true&os_destination=htt	0%	Avira URL Cloud	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://www.atlassian.com_oeu1635202071179r0.6121722167079615$$1096093$$event_queue	0%	Avira URL Cloud	safe	
http://https://www.atlassian.com_oeu1635202071179r0.6121722167079615$$1096093$$variation_map.	0%	Avira URL Cloud	safe	
http://https://www.atlassian.com_oeu1635202071179r0.6121722167079615$$1096093$$layer_states	0%	Avira URL Cloud	safe	
http://https://confluence.atlassian.com_oeu1635202071179r0.6121722167079615$$10828395850$$visitor_profile	0%	Avira URL Cloud	safe	
http://https://www.atlassian.com_oeu1635202071179r0.6121722167079615$$1096093$$layer_map	0%	Avira URL Cloud	safe	
http://https://stg-clientrelations.equalityhealth.com	0%	Avira URL Cloud	safe	
http://https://confluence.atlassian.com_oeu1635202071179r0.6121722167079615$$10828395850$$tracker_optimizel	0%	Avira URL Cloud	safe	
http://https://www.atlassian.com_oeu1635202071179r0.6121722167079615$$1096093$$events	0%	Avira URL Cloud	safe	
http://https://stg-clientrelations.equalityhealth.com/secure/ChangeUserPassword	0%	Avira URL Cloud	safe	
http://https://www.atlassian.com_oeu1635202071179r0.6121722167079615$$1096093$$visitor_profile	0%	Avira URL Cloud	safe	
http://https://www.atlassian.com_pending_events	0%	Avira URL Cloud	safe	
http://https://confluence.atlassian.com_oeu1635202071179r0.6121722167079615$$10828395850$$session_stateZ	0%	Avira URL Cloud	safe	
http://https://www.atlassian.com_oeu1635202071179r0.6121722167079615$$1096093$$session_stateZ	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
collector-pxvryik386.px-cloud.net	35.186.220.184	true	false		unknown
segments.company-target.com	54.192.66.96	true	false		unknown
platform.twitter.map.fastly.net	199.232.136.157	true	false		unknown
t.co	104.244.42.5	true	false		high
dnyjdqemy55m3.cloudfront.net	216.137.37.113	true	false		high
api.demandbase.com	216.137.37.71	true	false		high
594-atc-127.mktoresp.com	192.28.144.124	true	false		unknown
www.google.com	142.250.203.100	true	false		high
api.segment.io	54.70.105.250	true	false		high
pixel.pointmediatracker.com	54.192.66.98	true	false		unknown
polyfill.io	151.101.1.26	true	false		high
id.rlcdn.com	35.244.174.68	true	false		high
global.stargate.cse.ss-inf.net	18.184.99.132	true	false		unknown
star-mini.c10r.facebook.com	157.240.9.35	true	false		high
match.prod.bidr.io	52.49.53.128	true	false		unknown
stats.l.doubleclick.net	173.194.79.155	true	false		high
s.twitter.com	104.244.42.131	true	false		high
dualstack.reddit.map.fastly.net	151.101.1.140	true	false		unknown
youtube-ui.l.google.com	142.250.186.174	true	false		high
googleads.g.doubleclick.net	142.250.203.98	true	false		high
reddit.map.fastly.net	151.101.1.140	true	false		unknown
s2-cloudinary-pin-sni.map.fastly.net	151.101.2.92	true	false		unknown
d1jsfcerjrfe3w.cloudfront.net	54.192.66.87	true	false		high
clients.l.google.com	142.250.186.174	true	false		high
googlehosted.l.googleusercontent.com	172.217.168.33	true	false		high
cdn.cookielaw.org	104.16.148.64	true	false		high
perimeterx2.map.fastly.net	151.101.1.40	true	false		unknown
dart.l.doubleclick.net	172.217.168.38	true	false		high
cdn.evgnet.com	151.101.64.114	true	false		unknown
docs.atlassian.com	185.166.143.0	true	false		high
pop-eda6.mix.linkedin.com	108.174.11.69	true	false		high
events.launchdarkly.com	54.209.55.173	true	false		high
prod-tracking-web-alb-482381516.us-east-1.elb.amazonaws.com	35.172.51.134	true	false		high
client-error-log-962704628.us-east-1.elb.amazonaws.com	3.224.118.21	true	false		high
d1jpmzxkzfzfaz.cloudfront.net	216.137.37.2	true	false		high
c-ct-eu.contentsquare.net	52.30.94.8	true	false		unknown
adservice.google.com	172.217.168.66	true	false		high
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
dn1f1hmdujj40.cloudfront.net	13.33.93.218	true	false		high
p.adsymptotic.com	104.18.102.194	true	false		high
www.google.fr	172.217.168.67	true	false		high
dc61fd7f-0769-521a-b271-bd73d5e7f644.prd.edge-inf.net	185.166.143.5	true	false		unknown
d3lzof3wnsn9tm.cloudfront.net	54.192.66.67	true	false		high
pagead46.l.doubleclick.net	142.250.203.98	true	false		high
accounts.google.com	142.250.203.109	true	false		high
www-google-analytics.l.google.com	142.250.203.110	true	false		high
p13nlog-1106815646.us-east-1.elb.amazonaws.com	34.197.14.190	true	false		high
www-googletagmanager.l.google.com	142.250.186.72	true	false		high
d3bdzitctqoj2j.cloudfront.net	54.192.66.54	true	false		high
cs41.wac.edgecastcdn.net	93.184.220.66	true	false		high
webrecorder-prod-1682395302.us-east-1.elb.amazonaws.com	23.23.73.109	true	false		high
api.company-target.com	54.192.66.24	true	false		unknown
fp2c5c.wac.kappacdn.net	152.195.15.58	true	false		unknown
global.event.prod.bidr.io	52.211.108.19	true	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
geolocation.onetrust.com	104.20.184.68	true	false		high
scripts.demandbase.com	54.192.66.106	true	false		high
stg-clientrelations.equalityhealth.com	76.9.179.216	true	false		unknown
metal.prod.atl-paas.net	unknown	unknown	false		high
alb.reddit.com	unknown	unknown	false		high
static.ads-twitter.com	unknown	unknown	false		unknown
www.atlassian.com	unknown	unknown	false		high
a1096093.cdn.optimizely.com	unknown	unknown	false		high
errors.client.optimizely.com	unknown	unknown	false		high
atl-global.atlassian.com	unknown	unknown	false		high
cdn-mr.contentful.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
www.youtube.com	unknown	unknown	false		high
platform.twitter.com	unknown	unknown	false		high
wac-cdn.atlassian.com	unknown	unknown	false		high
logx.optimizely.com	unknown	unknown	false		high
www.redditstatic.com	unknown	unknown	false		high
web-analytics.engagio.com	unknown	unknown	false		high
wac-cdn-2.atlassian.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
px.ads.linkedin.com	unknown	unknown	false		high
munchkin.marketo.net	unknown	unknown	false		unknown
cdn.optimizely.com	unknown	unknown	false		high
api.atlassian.com	unknown	unknown	false		high
5406241.fls.doubleclick.net	unknown	unknown	false		high
cnv.event.prod.bidr.io	unknown	unknown	false		unknown
c.clicktale.net	unknown	unknown	false		high
api-private.atlassian.com	unknown	unknown	false		high
cdn.bizibly.com	unknown	unknown	false		unknown
confluence.atlassian.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
tapi.optimizely.com	unknown	unknown	false		high
ing-district.clicktale.net	unknown	unknown	false		high
cdn.bizible.com	unknown	unknown	false		high
cdnssl.clicktale.net	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
app.launchdarkly.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
xxid.atl-paas.net	unknown	unknown	false		high
analytics.twitter.com	unknown	unknown	false		high
adservice.google.fr	unknown	unknown	false		high
client.px-cloud.net	unknown	unknown	false		unknown
snap.licdn.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://stg-clientrelations.equalityhealth.com/secure/ChangeUserPassword!default.jspa?username=n.martinez@chcfl.org	true	• 0%, Virustotal, Browse	unknown
http://https://stg-clientrelations.equalityhealth.com/secure/ForgotLoginDetails.jspa	true		unknown
http://https://stg-clientrelations.equalityhealth.com/login.jsp?os_destination=%2Fsecure%2FChangeUserPassword%21default.jspa%3Fusername%3Dn.martinez%40chcfl.org	true		unknown
http://https://www.atlassian.com/	false		high
http://https://adservice.google.com/ddm/fls/i/dc_pre=CLL9wuvZ5fMCFQ6IUQodFzAGxA;src=5406241;type=global;cat=wac-v0;ord=1;num=5568152833281;gtm=2wgak0;auiddc=1421621436.1635202105;u1=%2522990f44e-5736-4d68-93d7-11d32e9d67b2%2522;~oref=https%3A%2F%2Fwww.atlassian.com%2F	false		high
http://https://stg-clientrelations.equalityhealth.com/secure/ContactAdministrators!default.jspa	true		unknown
http://https://stg-clientrelations.equalityhealth.com/login.jsp?permissionViolation=true&os_destination=https%3A%2F%2Fstg-clientrelations.equalityhealth.com%2Fsecure%2FChangeUserPassword!default.jspa	true		unknown
http://https://www.atlassian.com/software/jira	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://5406241.fls.doubleclick.net/activityi;dc_pre=CLL9wuvZ5fMCFQ6IUQodFzAGxA;src=5406241;type=global;cat=wac-v0;ord=1;num=5568152833281;gtm=2wgak0;auiddc=1421621436.1635202105;u1=%2522990f44e-5736-4d68-93d7-11d32e9d67b2%2522;~oref=https%3A%2F%2Fwww.atlassian.com%2F?	false		high
http://https://stg-clientrelations.equalityhealth.com/secure/ChangeUserPassword!default.jspa?username=n.martinez@chcfl.org#main	true		unknown
http://www.atlassian.com/	false		high
http://https://confluence.atlassian.com/jiracoreserver0819/jira-core-server-8-19-documentation-1086414660.html	false		high
http://https://stg-clientrelations.equalityhealth.com/login.jsp?permissionViolation=true&os_destination=%2Fsecure%2FAboutPage.jspa%2Fsecure%2FAboutPage.jspa&page_caps=&user_role=	true		unknown
http://https://stg-clientrelations.equalityhealth.com/login.jsp	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.28.144.124	594-atc-127.mktoresp.com	United States		15224	OMNITUREUS	false
23.23.73.109	webrecorder-prod-1682395302.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
54.192.66.67	d3lzof3wnsn9tm.cloudfront.net	United States		14618	AMAZON-AESUS	false
104.16.148.64	cdn.cookielaw.org	United States		13335	CLOUDFLARENETUS	false
104.20.184.68	geolocation.onetrust.com	United States		13335	CLOUDFLARENETUS	false
142.250.186.72	www-googletagmanager.l.google.com	United States		15169	GOOGLEUS	false
35.186.220.184	collector-pxvryik386.px-cloud.net	United States		15169	GOOGLEUS	false
35.172.51.134	prod-tracking-web-alb-482381516.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
151.101.1.40	perimeterx2.map.fastly.net	United States		54113	FASTLYUS	false
151.101.2.92	s2-cloudinary-pin-sni.map.fastly.net	United States		54113	FASTLYUS	false
54.192.66.54	d3bdzitctqoj2j.cloudfront.net	United States		14618	AMAZON-AESUS	false
54.192.66.96	segments.company-target.com	United States		14618	AMAZON-AESUS	false
54.209.55.173	events.launchdarkly.com	United States		14618	AMAZON-AESUS	false
216.137.37.71	api.demandbase.com	United States		8014	BATELNETBS	false
216.137.37.113	dnyjdqemy55m3.cloudfront.net	United States		8014	BATELNETBS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
54.70.105.250	api.segment.io	United States		16509	AMAZON-02US	false
13.33.93.218	dn1f1hmdujj40.cloudfront.net	United States		16509	AMAZON-02US	false
151.101.64.114	cdn.evgnet.com	United States		54113	FASTLYUS	false
142.250.186.174	youtube-ui.l.google.com	United States		15169	GOOGLEUS	false
54.192.66.87	d1jsfcerjrfe3w.cloudfront.net	United States		14618	AMAZON-AESUS	false
76.9.179.216	stg-clientrelations.equalityhealth.com	United States		13649	ASN-VINSUS	false
34.197.14.190	p13nlog-1106815646.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
172.217.168.67	www.google.fr	United States		15169	GOOGLEUS	false
185.166.143.5	dc61fd7f-0769-521a-b271-bd73d5e7f644.prd.edge-inf.net	Germany		16509	AMAZON-02US	false
185.166.143.0	docs.atlassian.com	Germany		16509	AMAZON-02US	false
142.250.203.109	accounts.google.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
18.184.99.132	global.stargate.cse.ss-inf.net	United States		16509	AMAZON-02US	false
18.184.99.133	unknown	United States		16509	AMAZON-02US	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
151.101.1.26	polyfill.io	United States		54113	FASTLYUS	false
216.137.37.2	d1jpmzxkzfzfaz.cloudfront.net	United States		8014	BATELNETBS	false
172.217.168.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
173.194.79.155	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1
192.168.2.255

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	508766
Start date:	25.10.2021
Start time:	15:46:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://stg-clientrelations.equalityhealth.com/secure/ChangeUserPassword!default.jspa?username=n.martinez@chcfl.org
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:	20
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:	SUS
Classification:	sus21.phis.win@46/206@71/38
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://stg-clientrelations.equalityhealth.com/login.jsp?os_destination=%2Fsecure%2FChangeUserPassword%21default.jspa%3Fusername%3Dn.martinez%40chcfl.org • Browse: https://stg-clientrelations.equalityhealth.com/secure/ChangeUserPassword!default.jspa?username=n.martinez@chcfl.org#main • Browse: https://stg-clientrelations.equalityhealth.com/secure/MyJiraHome.jspa • Browse: https://stg-clientrelations.equalityhealth.com/secure/Dashboard.jspa • Browse: https://docs.atlassian.com/jira/jcore-docs-0819/ • Browse: https://stg-clientrelations.equalityhealth.com/secure/ForgotLoginDetails.jspa • Browse: https://www.atlassian.com/software/jira • Browse: https://stg-clientrelations.equalityhealth.com/secure/AboutPage.jspa/secure/AboutPage.jspa • Browse: https://stg-clientrelations.equalityhealth.com/secure/ContactAdministrators!default.jspa • Browse: http://www.atlassian.com/
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
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\1f0d5f95-d96e-47fb-9eee-751e45ba4b85.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\1f0d5f95-d96e-47fb-9eee-751e45ba4b85.tmp	
Category:	dropped
Size (bytes):	97400
Entropy (8bit):	3.74926407895533
Encrypted:	false
SSDEEP:	384:k7bgoC1X5NxasVNvUXNorhvkA3r4eHHyXGPSrdCw2hxLmuexr9gmp1vRSYEUXOqn:dGqlZSOwDceHHIM2kHXu0K6kEpR
MD5:	1B1731240BF360091EAF9AB308E82A42
SHA1:	300178DF4360892050A3F55A1771EEC400C1A680
SHA-256:	B8D7436D8E2B3376FE3B7FEA5784846005C6F814A02431A344D09AE9B3AE1807
SHA-512:	5E0474E78AB0054697CB9F0EB29213BDDA5B7457737E15AFAED00DD9BA029AF599BD344991D1EB357661B08D135A96A87BE2FE0D4CC9083A5220FC6260FA892 6
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...^!8.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\22e19acd-3170-4572-a8a1-0721bdded551.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):	380482
Entropy (8bit):	6.027415555523889
Encrypted:	false
SSDEEP:	6144:Urd0hqhdMNnOvBS8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBE:60hqhdMY/xzurRDn9nfNxF4ijZVtilBE
MD5:	6F321834DB2F80CC5C54D1D62A9A6974
SHA1:	4A8A132B166CA1467BEA91BDDA2D0640A945ADA1
SHA-256:	78019DCAB170E9D00E6F0C70C41DEC2DC56F1E67A2797E95911A6D1A69324169
SHA-512:	79F1FA694C610BDB425B6D761E3474644C0C9072378FFD5F3038B80D8CF1EB1282E281C03B3CBDE21ED0D0030BE69060B2802FFC458099C0B546A92DC3833A9
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":1.635202029838458e+12,"network":1.635169631e+12,"ticks":118833701.0,"uncertainty":3807020.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075705080"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\35ab2c62-b0bf-4872-a8ab-9c2107d68d58.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):	380284
Entropy (8bit):	6.027049117863129
Encrypted:	false
SSDEEP:	6144:1rd0hqhdMNnOvBS8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBE:z0hqhdMY/xzurRDn9nfNxF4ijZVtilBE
MD5:	52274F13E65FE3B682AFD04843C0E2F2
SHA1:	4E2D8C7318907DFE5D459A8DB0F42E100213AA1E
SHA-256:	84BA6BE90F9BF9148AE9BFBFD533514B15EFFDC9BD3F5C30EB6D6CCE17494F95
SHA-512:	C2B5B94178FE10DC39F1D060EDBD9F9EC17C22EA9E413C7D3872D874C5EFD426ACE99FFE96D9F500BEE13DD5F1623660D0BCBF73C66BA656B8434193436D8(0
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.635202029838458e+12,"network":1.635169631e+12,"ticks":118833701.0,"uncertainty":3807020.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075705080"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\56796f95-7c33-4ec2-8de6-ea1e127a6d7a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\56796f95-7c33-4ec2-8de6-ea1e127a6d7a.tmp

Size (bytes):	92724
Entropy (8bit):	3.7495178765833344
Encrypted:	false
SSDEEP:	384:X7bgoC1X6aVUXNorhvkA3r4eHHyXGPSrdCwixLmuexr9gmpeRSYEUXOqukNF1YRV:5qlZSObDceHmM2kHXu0K6kEpg
MD5:	FD6368515121836A1466855024F734BF
SHA1:	87859E25CD7A29B59DC79D35AE1D236F3DD9BEC2
SHA-256:	5A55242CE8CD2259F9E429815D92EEB10D755D3751B48480878543BDABCF0810
SHA-512:	BC3F91573428853EB1CA6EDC7925EBD6952A9B788FD0901A212B4A7631F60D7A7766F84CE6536C53DA25E2E9061BB1B7FD4B9CA9F703F0BAC6662EF1D825AD(B
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...^!8.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\69e2b7c9-4d8c-4177-a4d7-378d16809b23.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):	380568
Entropy (8bit):	6.027531033959462
Encrypted:	false
SSDEEP:	6144:/rd0hqhdMNnOvBS8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBE:J0hqhdMY/xzurRDn9nfNxF4ijZVtilBE
MD5:	989899C8B40E74B1CB634C3A58D91995
SHA1:	890B374EEB1987507DEBB0E3937DDF3830C7D604
SHA-256:	02C540807220BC15D8CD6D06B9B7B34C986C70A90C4928D0A602C0EB6776E87F
SHA-512:	D61B7825988488B3B31FFB68D20377DCE0E93A1C6AD16CBF0782E641817C94F5E14799AE1ECC871FE918954EE2480C7067CF64E7C3CDAE9833EF0995631A1A7
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":1.635202029838458e+12,"network":1.635169631e+12,"ticks":118833701.0,"uncertainty":3807020.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075705080"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\6c9175e5-db26-4ba6-ab5d-b53eba0bc189.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):	376701
Entropy (8bit):	6.014813935546984
Encrypted:	false
SSDEEP:	6144:8rd0hqhdMNnOvBS8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBE:C0hqhdMY/xzurRDn9nfNxF4ijZVtilBE
MD5:	33F55B13BC81C9A8E9BBFD3741EBCDD1
SHA1:	9301B453E9EB750F931DA0B93A17E0D029C3BABE
SHA-256:	DBC11CBD6DE3E10DE53C3BB00D02EA59C432248D5767C32000066104476F6325
SHA-512:	883DDB55D97B59434D72CD55207A996B045EBB788B8B6E243987EF3FB2083F58AD660379E797C4A361B02EADCD620BF2C162D025DA829E45668B16B713093FF3
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":1.635202029838458e+12,"network":1.635169631e+12,"ticks":118833701.0,"uncertainty":3807020.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075705080"},"policy":{"last_statistics_update":"13279675627239

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Size (bytes):	40
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXYDu6cR9n:+Y66cR9
MD5:	7A9D405E9218ED86C7ED3BB729DAA896
SHA1:	E5BB69E833231B755B20E5A0C9B2392D8B923C66
SHA-256:	D83D002DFE4F96C43A6FBF24FC7AA739945731ABDEC2AFB53EDDCE2D2D87D6AF
SHA-512:	F34290BF6A4B1AA63F47436C0788FC1DAC7B970A1861EF1D1891826FD3DFD0FD484A900E23A3024C19CA93DE842BF8B5BC7A5E159362A4C3A36AE8D47C8551A 7
Malicious:	false
Reputation:	low
Preview:	sdPC....................8...?E."..N_.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3e51e616-c64c-4935-8c9a-b0823bfa91e2.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):	5.536099168095207
Encrypted:	false
SSDEEP:	384:OA/tZLl2WXJ1kXqKf/pUZNCgVLH2HfDZrUVHGBnT1eOrp3z4I:VLlXJ1kXqKf/pUZNCgVLH2HftrUpGBn7
MD5:	84457DFF9994ACC6DFD4334638B774B2
SHA1:	50DF4D3E9B62D0DB1B6D0057B4B67B92D650BEDE
SHA-256:	34DF9EDD3C6F205695E92430F8F91F4111A4B05DFEDBC294A5AADCFA4D0036FE
SHA-512:	E84F1BA2C05DC432665C3C0CCA9FA34D92435A4DCE816EBFECCD8191B43882EC506486B7EA1A54DD0191A9B7F751F4A9D7F2E1E57BE2F0E552C7EEB5E73F3 B8
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":"13279675627684411","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\46826242-4d9b-43f8-b18f-d9c733bd18b0.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):	5851
Entropy (8bit):	5.190925197979137
Encrypted:	false
SSDEEP:	96:nQrd3BN94swSKIznSIk0JCKL8cptKkS11BgbOTQVuwn:nQrh94swS8C4KppskSxy
MD5:	5AD7A24773ED65C47442222A6B550D91
SHA1:	5FCAD9FC39B0E8A656D4AEEECD401D51D013FCBD
SHA-256:	AA3B56A5059DEB972FEA3F388D705587601627B09254B1B129A05AB3BC7EDE1C
SHA-512:	A186A1314AB1605C1EE72D57D32162574256049148FECC624F969C6BC74F1E5B655A13E6DF0F9AB6324B04A11F3181B2C43D5B81E12E1F4C6E7F14D66767FFF8
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13279675628379593","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","1538886"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\80c274e5-85f8-42c9-bc4a-d44b968f47fc.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\80c274e5-85f8-42c9-bc4a-d44b968f47fc.tmp	
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8fe405e3-9334-46a1-8a07-5ef2c7198ff4.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):	2952
Entropy (8bit):	4.9168118102370535
Encrypted:	false
SSDEEP:	48:Y26qtwTCXDHzM3zs9GsvRLsOZrq9s4yKs5yQs5H5sAMHls5R6VLs5Acs5GSs56Kd:JxOTCXDHzMMdPrUdFDGc6VXAOKfVD
MD5:	37809121BB3F49925844034D597C9E08
SHA1:	BEC9361AD14B57CF7947B398CD96B159C441B20F
SHA-256:	98ED46E9F9E2E240BD1FE6BDDB6FD072FB5C370B0902981F4D99953D93896653
SHA-512:	8A953B9DDABBD1D85AC0B2C1763FE2ADD1E7E6C344E73FBBFF2566E682392C28D3286EF86F8A9B1004C790B98C34F76B574A7BDA24708889CCC3EC089DAB5AC7
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13282267629933726","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13282267629956501","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":tr

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\990108db-418d-40b3-9ab7-126b2bc91a85.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):	2693
Entropy (8bit):	4.871875630348377
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhE:+GDGTHGmGHDW1/nOIbmOGlGGhVG
MD5:	592337A19B0490E714DD7C93B0752E5C
SHA1:	6B82A52F479E5D78D8AC311454F7C43F65345D0B
SHA-256:	941A456CAA476B0A1BC22C290F8F71D3FD52F5C6C1B5E9606A0847CA0BC177FD
SHA-512:	6D0AEE47C9D2C33E8E246AE508A9C4A8E91881697CA1F64E66A8288197D83E8EBEF89CD6C12B965C4CE460A952912E8637587885AE0FE4F722350D916EBCAB02
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","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:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+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=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/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
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):	374
Entropy (8bit):	5.210958159920271
Encrypted:	false
SSDEEP:	6:maHyq2P923iKKdK25+Xqx8chI+IFUtnKFh1ZmwBuwjRkwO923iKKdK25+Xqx8chn:pHyv45KkTXfchI3FUtnq/BtjR5L5KkTM
MD5:	BCDF97399A7312D8218B2A1AC77D3E9A
SHA1:	E09CFF9C4BA4CAF4D6A3023FF72F41A3524E3317
SHA-256:	FE705682235D4FE4556F4803B0615DDDC828E17F10D0CB55156F15774DC3033C
SHA-512:	5954891AE9E490D5F74E7E6A40F28C5E2A7289B42A4078CAB52E29A79E0EB6C9FD56ED7D182FB6D70D2CD0A81ECCDBB932252F89C893266F3C456EFB0AC7E4C3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Preview:	2021/10/25-15:47:30.303 18e0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/10/25-15:47:30.304 18e0 Recovering log #3.2021/10/25-15:47:30.305 18e0 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):	374
Entropy (8bit):	5.210958159920271
Encrypted:	false
SSDEEP:	6:maHyq2P923iKKdK25+Xqx8chI+IFUtnKFh1ZmwBuwjRkwO923iKKdK25+Xqx8chn:pHyv45KkTXfchI3FUtnq/BtjR5L5KkTM
MD5:	BCDF97399A7312D8218B2A1AC77D3E9A
SHA1:	E09CFF9C4BA4CAF4D6A3023FF72F41A3524E3317
SHA-256:	FE705682235D4FE4556F4803B0615DDDC828E17F10D0CB55156F15774DC3033C
SHA-512:	5954891AE9E490D5F74E7E6A40F28C5E2A7289B42A4078CAB52E29A79E0EB6C9FD56ED7D182FB6D70D2CD0A81ECCDBB932252F89C893266F3C456EFB0AC7E4C3
Malicious:	false
Reputation:	low
Preview:	2021/10/25-15:47:30.303 18e0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/10/25-15:47:30.304 18e0 Recovering log #3.2021/10/25-15:47:30.305 18e0 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):	1851
Entropy (8bit):	5.672829082273069
Encrypted:	false
SSDEEP:	48:AM1yG09VYvGSTEy+8db98poFq+Rpdk+Mjcm:A8yGGiGS40sp4NRpdPscm
MD5:	6C675E412EF3905C9EA34C5231139EB0
SHA1:	EFFE38C2AB2730A8A3B61A613402D7DD580AF783
SHA-256:	1EC09020CA084FA24D968229EF11F340A422FEA9532973752A787858FD01A00B
SHA-512:	024B709D90D7DDA5489035DA5AB4B33CE79A1440FAF0E812E6D8C9A1DDD5A9352B0DEE87BF908F3A5F563FD169197A364391FEDA1C5E1959DD0839B0AB1E653
Malicious:	false
Reputation:	low
Preview:	....."......changeuserpassword..client..clientrelations..com..default..destination..equalityhealth..healthbi..https..in..jsp..jspa..log..login..os..permissionviolation..relations..secure..staging..stg..true..chcfl..martinez..n..org..password..update..username..your*.....changeuserpassword.....chcfl.....client.....clientrelations.....com.....default.....destination.....equalityhealth.....healthbi.....https.....in.....jsp.....jspa.....log.....login.....martinez.....n.....org.....os.....password.....permissionviolation.....relations.....secure.....staging.....stg.....true.....update.....username.....your..2.....a.....b.....c.....d.....e.....f.....g.....h.....i.....j.....l.....m.....n.....o.....p.....q.....r.....s.....t.....u.....v.....w.....y..

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_www.atlassian.com_0.indexeddb.leveldb\CURRENT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_www.atlassian.com_0.indexeddb.leveldb\CURRENT (copy)	
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Uv:1qIFUv
MD5:	46295CAC801E5D4857D09837238A6394
SHA1:	44E0FA1B517DBF802B18FAF0785EEEA6AC51594B
SHA-256:	0F1BAD70C7BD1E0A69562853EC529355462FCD0423263A3D39D6D0D70B780443
SHA-512:	8969402593F927350E2CEB4B5BC2A277F3754697C1961E3D6237DA322257FBAB42909E1A742E22223447F3A4805F8D8EF525432A7C3515A549E984D3EFF72B23
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000001.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\https_www.atlassian.com_0.indexeddb.leveldb\MANIFEST-000001	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	23
Entropy (8bit):	4.142914673354254
Encrypted:	false
SSDEEP:	3:Fdb+4Ll:Zl
MD5:	3FD11FF447C1EE23538DC4D9724427A3
SHA1:	1335E6F71CC4E3CF7025233523B4760F8893E9C9
SHA-256:	720A78803B84CBCC8EB204D5CF8EA6EE2F693BE0AB2124DDF2B81455DE02A3ED
SHA-512:	10A3BD3813014EB6F8C2993182E1FA382D745372F8921519E1D25F70D76F08640E84CB8D0B554CCD329A6B4E6DE6872328650FEFA91F98C3C0CFC204899EE824
Malicious:	false
Reputation:	low
Preview:	.....idb_cmp1.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	69070
Entropy (8bit):	5.5061444748148665
Encrypted:	false
SSDEEP:	1536:w9ewYgWp1GGYrgyjUgmp1Khl41TtV/hl41TtV4L7cJAB4jQMlxrzhl41TtVbyR:6OL74c4jQ4xp
MD5:	AE9A935DB60951A1BC710C5F0220692B
SHA1:	DCF0EEB685E539E9B4883EF7C613FB2C9F76CF89
SHA-256:	9AFB3AB99522EFC9988A553D966217DDDE1BB17D2FC552CF71A3CD2B8C992ACD
SHA-512:	9D964F358BB7CE94F46AD8A2810866BBEF1B052A23F383A92BEC45FFAA9B59C441E285A798FBEDC5589ACF6248E794B33A3BD156B6E777CF59E8D7CC9B00EF4E
Malicious:	false
Reputation:	low
Preview:	.d.....VERSION.1.8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Q_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.persistent.CloudProvider7.{"cloudEnabled":false,"notifiedHangoutsPrivacy":false}.S_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.persistent.IdentityService6.{"signedIn":false,"userEmail":null,"kioskAuth":false}.Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..215468000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2020-09-30 07:43:16.96][INFO][mr.Init] MR instance ID: 6870862c-e226-4872-ad79-5f23fe89a0ec\n","[2020-09-30 07:43:16.96][INFO][mr.Init] Native Cast MRP is disabled.\n","[2020-09-30 07:43:16.96][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2020-09-30 07:43:16.96][INFO

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000004.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3334
Entropy (8bit):	5.498810727749736
Encrypted:	false
SSDEEP:	96:Ia7wMQdbOYh0bQ5fgGDrS0ZKMp9pSopx1pS+pE:IywDd6Yh0E5fgaZTp9pfpnp7pE
MD5:	20E5B42DF81E4A279CDFBA2115163EFF
SHA1:	4BCB376E428BF5EAEC38F5537400552E2E242FCF
SHA-256:	FDBF37D90FEAD7D5852829F826F5A153554CDA60DA603F63C931F85DE743229D
SHA-512:	6151CDCA9CBFAF56B0A799EDE8C7DB0F74099790EA30106B2EB7E26AD1D698945623A8367E4F24628CE65AF1AF355E1D0933949A1D389EE09D26F4F506EDF83
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000004.log	
Reputation:	low
Preview:	vX-e.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService;.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..747539000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-10-25 15:48:48.07][INFO][mr.Init] MR instance ID: d6b31e19-74f6-423a-90f9-b0f4d84a300a\n","[2021-10-25 15:48:48.07][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-10-25 15:48:48.07][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-10-25 15:48:48.08][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-10-25 15:48:48.08][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-10-25 15:48:48.08][INFO][mr.CastProvider] Query enabled: true\n","[2021-10-25 15:48:48.08][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2693
Entropy (8bit):	4.871875630348377
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhE:+GDGTHGmGHDW1/nOIbmOGlGGhVG
MD5:	592337A19B0490E714DD7C93B0752E5C
SHA1:	6B82A52F479E5D78D8AC311454F7C43F65345D0B
SHA-256:	941A456CAA476B0A1BC22C290F8F71D3FD52F5C6C1B5E9606A0847CA0BC177FD
SHA-512:	6D0AEE47C9D2C33E8E246AE508A9C4A8E91881697CA1F64E66A8288197D83E8EBEF89CD6C12B965C4CE460A952912E8637587885AE0FE4F722350D916EBCAB02
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State75 (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):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DBCAA
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\PreferencesL (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):	5149
Entropy (8bit):	4.97448316853818
Encrypted:	false
SSDEEP:	96:nQrr3GN9pSKIznylk0JCKL8cptKkS11pbOTQVuwn:nQrG9pS8C4KppskSZ
MD5:	89DABF5968FEFC84CA6EEF812164B371
SHA1:	67D673CD846AD20E3B497621BDC2593FE3C9C795
SHA-256:	6B35EEC0EA4AB144165C3E74E711A23C6B5BCAB39FB303304DCFB827514F37CC
SHA-512:	A1CC14F0CCC7393907CD1302BFD161DD12576B21B9F4DD9E0C8F9046DAE06480165449A762927308EE258811E4F9ECA61B770906C26B8AA1571E642F91781D50
Malicious:	false
Reputation:	low

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

{"account_id_migration_state":2,"account_tracker_service_last_update":"13279675628379593","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","1538886"],"daily_received_length":["0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\PreferencesMP (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5241
Entropy (8bit):	4.981162953331023
Encrypted:	false
SSDEEP:	96:nQrW3iN9pSKIznSIk0JCKL8cptKkS11BgbOTQVuwn:nQrD9pS8C4KppskSxy
MD5:	8DF5EC6547E46CF454AB575EC72D03C8
SHA1:	FECC85465AE097E19DC5BC94C90D7AB6A80DFA96
SHA-256:	EF4727ACD36E119A5AC39386107815C90AD42AD416D094D16FEA8981480F6815
SHA-512:	592ACC3607180C3FFE13EA49D44132316E927DB1C26BB0F041CBB7AB62E6312B8B107A06E49F99536D7BF7D42CC252B97EFE50833F859D13449269371CDCCEA
Malicious:	false
Reputation:	low
Preview:	

{"account_id_migration_state":2,"account_tracker_service_last_update":"13279675628379593","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","1538886"],"daily_received_length":["0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferencesm (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):	5148
Entropy (8bit):	4.9727470667848
Encrypted:	false
SSDEEP:	96:nQrYqG9pSKIznpIk0JCKL8cptKkS11pbOTQVuwn:nQrc9pSvC4KppskSZ
MD5:	4318C5C00E9D26B79C19BE231690DFFF
SHA1:	5CF48EFC05EF64040DC0B027636E21066C2A2F68
SHA-256:	B68EBAF8AB4DCB65B27ED13F8C18D1B954B6F09BFFE06D34DB324D0ACCA14E79
SHA-512:	E839314EACDFAC753C439F03F5811EB88FF2264D46959064207231D456E95B66BEC076D2C092B8306D441499C826F8517CA253A415FDEFA7660D3F12C06D0BD
Malicious:	false
Reputation:	low
Preview:	

{"account_id_migration_state":2,"account_tracker_service_last_update":"13279675628379593","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","1538886"],"daily_received_length":["0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19182
Entropy (8bit):	5.570360145487577
Encrypted:	false
SSDEEP:	384:OA/tZLl2WXJ1kXqKf/pUZNCgVLH2HfDZrUVHGQeOrAz4l:VLlXJ1kXqKf/pUZNCgVLH2HftrUpGQeQ
MD5:	94B1A5F221B99B8A9DAFF6B5B331BBED
SHA1:	35BD3E12A2DF2C9D2BD86F1A73AC6662533EDE6E
SHA-256:	1FFCC413346919E0822FBCE055FBA4EDDCF0F0559FC4E13D6A5FB80CA9E28CEB
SHA-512:	884EF40B07136A0A1C1CFDF326E5FEA8C0B177403FF70FD6A3C2C1EE95EDAF480A03C55A5CFA80DE0C7D8B333704803BC4240CB9BF0671B4FAE96534518DFF B2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	
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":"13279675627684411","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\Secure Preferences7 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19181
Entropy (8bit):	5.570062438982786
Encrypted:	false
SSDEEP:	384:OA/tZLl2WXJ1kXqKf/pUZNCgVLH2HfDZrUVHGxeOrAz4H:VLlXJ1kXqKf/pUZNCgVLH2HftrUpGxe2
MD5:	06048E50B7D6A4704C953B9E573F4E2F
SHA1:	ED3FB97AA45BBA0FF0D9B5321E3DFB6900722190
SHA-256:	68D7E784313BE207BA8963267C9FF57792255E2ACABE84416631D9774454DE3D
SHA-512:	26383A7A31F32FC3AC0ABF58B0DD9962A5488217DFFE65D7A85481B8F9F54178DD5EE1DC4C77B7D14D761E60B54A891A46FE93878E0E9C108A32EB838751E38
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":"13279675627684411","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\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\40b66be9-35cd-4ad6-9ab6-669a4e085c7f.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):	4.960516863228614
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRKXk1Yn:YHO8sdVAsBdLJlyH7E4f3K3X
MD5:	5B45E0CEDCB5409B4858999793DF47DE
SHA1:	7DA7AF96784FB4D533BDCE72106C34BDF8915B57
SHA-256:	6735F5007FE7FB81AE2C83512AAE6DC3F93B372ED7FB630BAAC5CB03344F53BF
SHA-512:	CD6664D21C47739715606FE4D6DA37C101E8D83C7B1464B93B0CE85DE039B63C8113A568377561CDE2E5AEF486F6840C56A39AE38F2C92C8F07D16FF4B679F0
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"3G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\5c5831dc-c898-45de-bd8a-33464a231574.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):	325
Entropy (8bit):	4.956993026220225
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdVAsBdLJlyH7E4f3K33y
MD5:	0C03D530AC97788D62D27B2802C34D83
SHA1:	20F78B6B32D98FA52846C70DF78E4E5CEF663E2D
SHA-256:	7941FADA9867DAAE08EBC196BAFC6952DD506842C3E7D8FB14DF9D4E402D894B
SHA-512:	D5905C124060997A14322D12DECE5C00C63F7174743C740C974D00E88B03F203909CC2AC972B2759E8087B0B10F6306C6E66BF853319B5AC96907F34C8456C80
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","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:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898I 58
Malicious:	false
Reputation:	low
Preview:	.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State7f (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):	4.960516863228614
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRKXk1Yn:YHO8sdVAsBdLJlyH7E4f3K3X
MD5:	5B45E0CEDCB5409B4858999793DF47DE
SHA1:	7DA7AF96784FB4D533BDCE72106C34BDF8915B57
SHA-256:	6735F5007FE7FB81AE2C83512AAE6DC3F93B372ED7FB630BAAC5CB03344F53BF
SHA-512:	CD6664D21C47739715606FE4D6DA37C101E8D83C7B1464B93B0CE85DE039B63C8113A568377561CDE2E5AEF486F6840C56A39AE38F2C92C8F07D16FF4B679F0
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","port":443,"protocol_str":"quic"}],"isol ation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"3G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent StateMP (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.956993026220225
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5rAcJksDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdVAsBdLJlyH7E4f3K33y
MD5:	0C03D530AC97788D62D27B2802C34D83
SHA1:	20F78B6B32D98FA52846C70DF78E4E5CEF663E2D
SHA-256:	7941FADA9867DAAE08EBC196BAFC6952DD506842C3E7D8FB14DF9D4E402D894B
SHA-512:	D5905C124060997A14322D12DECE5C00C63F7174743C740C974D00E88B03F203909CC2AC972B2759E8087B0B10F6306C6E66BF853319B5AC96907F34C8456C80
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542588505091","port":443,"protocol_str":"quic"}],"isol ation":[],"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\3e1adf5a-10fa-4898-aa9d-04ff5234da99.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):	4.976576189225149
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5OV/sDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdysBdLJlyH7E4f3K33y
MD5:	5886A009EB58EE06A16EFD6D1BA9A046
SHA1:	A867B5052F3FBB811693DF8CE3FDAA794F2F2E40

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\3e1adf5a-10fa-4898-aa9d-04ff5234da99.tmp	
SHA-256:	9E3392126DE2D81D019E0AB3E17F20BADD0EC9FBD944BCB7C4DAF449D937D496
SHA-512:	D24F30A2E35F903AC10AACC4425C58BECB1C6BE2BA30A3C2B9D9D46CE04914AA71F55B3B16ED89081AD65A7090C77F5DC4A258B7B98D71E6A994D176536FBI27
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248542597817103","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:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E889858
Malicious:	false
Reputation:	low
Preview:	....

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):	404
Entropy (8bit):	5.3136159079036
Encrypted:	false
SSDEEP:	12:ple8v45KkkOrsFUtnI9/BIP5L5KkkOrzJ:GeG45Kk+gIABL5Kkn
MD5:	AE4FBD8E48CEDE4C50AB0D2F2E5B8786
SHA1:	5A8EC314D01BFFE341E5328F308D8C0099DE1B41
SHA-256:	6E326C2A8B94F2CD0A6974CBC37C352354E189AC1C88E8CDD88F57921551F8A0
SHA-512:	9F607F16C7B0ABD5D13B4030BA75FEB01B0670872DA0160A0DF68A5397022815B1B9E966311068B7E09B056B3AEA4DDDE1A333ED05FAB9B0525FF1E6D049746
Malicious:	false
Reputation:	low
Preview:	2021/10/25-15:48:48.108 16b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/10/25-15:48:48.109 16b0 Recovering log #3.2021/10/25-15:48:48.109 16b0 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\b50a4ad7-42ba-4833-b5c6-51aa20007283.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):	371
Entropy (8bit):	5.513555169132608
Encrypted:	false
SSDEEP:	6:YAQNCHQY4m9RfSHJR8wXwlmUUAnIMp5bt/tcGJYc/+8hZy8B8wXwlmUUAnIMObtU:Y3G9RAJ9+UAnI8lLWctfN+UAnIfAmQ
MD5:	DE088AEB0778E9E780DF638C3C8A4456
SHA1:	2A2D5C9B8C1EBCFBE6369A4968DB3D20364A8A64
SHA-256:	8379898EED8CF2032220A0FAAC8E590AE98C827881ACC4A2AB82AC1B21803421
SHA-512:	971694DB1FBAE81101BB6FC76F106D326BCD0B8BDAABC72763F70A9D5CC838A14C32714F3105FDD3CFBEBAA8681624AC1905D993EF095DFC87C149D66976730
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1666738104.830005,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1635202104.830011},{"expiry":1635223705.421486,"host":"OIRr0rxJ9rYO6SV/uhAVw9MZKZeFdckXz9Hgl3/HWMo=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1635202105.421492}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\c57b9a72-31a4-4e57-ab9c-654ae96cc744.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):	5148
Entropy (8bit):	4.9727470667848
Encrypted:	false
SSDEEP:	96:nQrYqG9pSKIznpIk0JCKL8cptKkS11pbOTQVuwn:nQrc9pSvC4KppskSZ
MD5:	4318C5C00E9D26B79C19BE231690DFFF
SHA1:	5CF48EFC05EF64040DC0B027636E21066C2A2F68
SHA-256:	B68EBAF8AB4DCB65B27ED13F8C18D1B954B6F09BFFE06D34DB324D0ACCA14E79
SHA-512:	E839314EACDFAC753C439F03F5811EB88FF2264D46959064207231D456E95B66BEC076D2C092B8306D441499C826F8517CA253A415FDEFA7660D3F12C06D0BD(
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13279675628379593","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","1538886"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	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\databases\Databases.db	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	0.3408437618760242
Encrypted:	false
SSDEEP:	12:TLiqixnGb0EiDFIlTSFbyrKZb9YwFOqAyl+FxOUwa5qgufTJpbZ75fOSG:TLi2NiD+lZk/Fj+6UwccNp15fBG
MD5:	089C02B21909DD4D739ADC2F093231BF
SHA1:	B33D36CAF38B5B342ACD0EFA9DC0F6F6C37D5F85

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\databases\Databases.db	
SHA-256:	184814D16B8115D3929672ABCFBAD21D2440E3F41257AAC26429764340FA19EA
SHA-512:	55C049C05F9E2A2AFE7BEB4096191D603CBCA209F21F0842F5D13FD4382A0AA103FF183EFE407A76F13EEE4763A1158C7951106E3BE1EDE272DD81FABEB98B0F
Malicious:	false
Reputation:	low
Preview:	SQLite format 3......@ ....C..........g.....P..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\e8358643-669b-4874-b8b7-3a7b04a1727f.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):	5.570062438982786
Encrypted:	false
SSDEEP:	384:OA/tZLl2WXJ1kXqKf/pUZNCgVLH2HfDZrUVHGxeOrAz4H:VLlXJ1kXqKf/pUZNCgVLH2HftrUpGxe2
MD5:	06048E50B7D6A4704C953B9E573F4E2F
SHA1:	ED3FB97AA45BBA0FF0D9B5321E3DFB6900722190
SHA-256:	68D7E784313BE207BA8963267C9FF57792255E2ACABE84416631D9774454DE3D
SHA-512:	26383A7A31F32FC3AC0ABF58B0DD9962A5488217DFFE65D7A85481B8F9F54178DD5EE1DC4C77B7D14D761E60B54A891A46FE93878E0E9C108A32EB838751E38
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":"13279675627684411","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\ea032bef-9c29-484b-bd9f-f0c1d4a4fb98.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):	5241
Entropy (8bit):	4.981162953331023
Encrypted:	false
SSDEEP:	96:nQrW3iN9pSKIznSIk0JCKL8cptKkS11BgbOTQVuwn:nQrD9pS8C4KppskSxy
MD5:	8DF5EC6547E46CF454AB575EC72D03C8
SHA1:	FECC85465AE097E19DC5BC94C90D7AB6A80DFA96
SHA-256:	EF4727ACD36E119A5AC39386107815C90AD42AD416D094D16FEA8981480F6815
SHA-512:	592ACC3607180C3FFE13EA49D44132316E927DB1C26BB0F041CBB7AB62E6312B8B107A06E49F99536D7BF7D42CC252B97EFE50833F859D13449269371CDCCEA
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13279675628379593","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","1538886"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f1a30738-4ffc-4b3c-bac2-5d34e716647e.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):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DBCAA
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f1a30738-4ffc-4b3c-bac2-5d34e716647e.tmp	
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f46683bd-8ed6-49be-ad55-df1507e63c57.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):	5149
Entropy (8bit):	4.974515538033643
Encrypted:	false
SSDEEP:	96:nQrr3GN9pSKIznEIk0JCKL8cptKkS11pbOTQVuwn:nQrG9pSaC4KppskSZ
MD5:	1487170818E5F8622F87A458830689B3
SHA1:	B145C6D46ECAB28C61E7D57FEB7AE63CDFE334E8
SHA-256:	A3878C6F22CD2D6D27474666451047F445CD112780249DA8C342377A78F3E4F4
SHA-512:	397537635AC247622C552D91BDC900CB57CF530736E16935C44E6EF45A60F6ADD806084CDB606EBDE04C417A4AD79544452C6F4D3227FCDC8314861525ADFCE
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13279675628379593","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","1538886"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f8db037d-2993-4f15-b0bf-435d8ae2ebb5.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):	5.570360145487577
Encrypted:	false
SSDEEP:	384:OA/tZLl2WXJ1kXqKf/pUZNCgVLH2HfDZrUVHGQeOrAz4l:VLlXJ1kXqKf/pUZNCgVLH2HftrUpGQeQ
MD5:	94B1A5F221B99B8A9DAFF6B5B331BBED
SHA1:	35BD3E12A2DF2C9D2BD86F1A73AC6662533EDE6E
SHA-256:	1FFCC413346919E0822FBCE055FBA4EDDCF0F0559FC4E13D6A5FB80CA9E28CEB
SHA-512:	884EF40B07136A0A1C1CFDF326E5FEA8C0B177403FF70FD6A3C2C1EE95EDAF480A03C55A5CFA80DE0C7D8B333704803BC4240CB9BF0671B4FAE96534518DFFB2
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":"13279675627684411","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\fb9546d5-ba83-402c-b749-4bf63875488d.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):	5149
Entropy (8bit):	4.97448316853818
Encrypted:	false
SSDEEP:	96:nQrr3GN9pSKIznyIk0JCKL8cptKkS11pbOTQVuwn:nQrG9pS8C4KppskSZ
MD5:	89DABF5968FEFC84CA6EEF812164B371
SHA1:	67D673CD846AD20E3B497621BDC2593FE3C9C795
SHA-256:	6B35EEC0EA4AB144165C3E74E711A23C6B5BCAB39FB303304DCFB827514F37CC
SHA-512:	A1CC14F0CCC7393907CD1302BFD161DD12576B21B9F4DD9E0C8F9046DAE06480165449A762927308EE258811E4F9ECA61B770906C26B8AA1571E642F91781D50
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\fb9546d5-ba83-402c-b749-4bf63875488d.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13279675628379593","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245950640095768","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","1538886"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tbloIlrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	380284
Entropy (8bit):	6.027049117863129
Encrypted:	false
SSDEEP:	6144:1rd0hqhdMNnOvBS8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBE:z0hqhdMY/xzurRDn9nfNxF4ijZVtilBE
MD5:	52274F13E65FE3B682AFD04843C0E2F2
SHA1:	4E2D8C7318907DFE5D459A8DB0F42E100213AA1E
SHA-256:	84BA6BE90F9BF9148AE9BFBFD533514B15EFFDC9BD3F5C30EB6D6CCE17494F95
SHA-512:	C2B5B94178FE10DC39F1D060EDBD9F9EC17C22EA9E413C7D3872D874C5EFD426ACE99FFE96D9F500BEE13DD5F1623660D0BCBF73C66BA656B8434193436D80
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":1.635202029838458e+12,"network":1.635169631e+12,"ticks":118833701.0,"uncertainty":3807020.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075705080"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local StateI (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local Statel (copy)	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	380284
Entropy (8bit):	6.027049220022618
Encrypted:	false
SSDEEP:	6144:Wrd0hqhdMNnOvBS8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBE:g0hqhdMY/xzurRDn9nfNxF4ijZVtilBE
MD5:	4C940F78D3218C6FF8A6CAA1C6DE8AAA
SHA1:	DC17622ADF6AE9CCDFE9D180018758FF2D4468DC
SHA-256:	36AE17688519A5EFD14D66BAD078694F76BD2C571A681BEEBE2B76F69BDD8C89
SHA-512:	73C9C40AB940F7471FC7DC55672EA3A7877C59E7F0968EFE32FDCCD8EAB49F02BB69C5F67F77222C21C71598BC468172CD9082A76179FC236C8BAFFB97E16A(A
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":1.635202029838458e+12,"network":1.635169631e+12,"ticks":118833701.0,"uncertainty":3807020.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075705080"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache.7 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97400
Entropy (8bit):	3.74926407895533
Encrypted:	false
SSDEEP:	384:k7bgoC1X5NxasVNvUXNorhvkA3r4eHHyXGPSrdCw2hxLmuexr9gmp1vRSYEUXOqn:dGqlZSOwDceHHIM2kHXu0K6kEpR
MD5:	1B1731240BF360091EAF9AB308E82A42
SHA1:	300178DF4360892050A3F55A1771EEC400C1A680
SHA-256:	B8D7436D8E2B3376FE3B7FEA5784846005C6F814A02431A344D09AE9B3AE1807
SHA-512:	5E0474E78AB0054697CB9F0EB29213BDDA5B7457737E15AFAED00DD9BA029AF599BD344991D1EB357661B08D135A96A87BE2FE0D4CC9083A5220FC6260FA892 6
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...^!8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\..... .m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o .g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cachero (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.7495178765833344
Encrypted:	false
SSDEEP:	384:X7bgoC1X6aVUXNorhvkA3r4eHHyXGPSrdCwixLmuexr9gmpeRSYEUXOqukNF1YRV:5qlZSObDceHmM2kHXu0K6kEpg
MD5:	FD6368515121836A1466855024F734BF
SHA1:	87859E25CD7A29B59DC79D35AE1D236F3DD9BEC2
SHA-256:	5A55242CE8CD2259F9E429815D92EEB10D755D3751B484808785 43BDABCF0810
SHA-512:	BC3F91573428853EB1CA6EDC7925EBD6952A9B788FD0901A212B4A7631F60D7A7766F84CE6536C53DA25E2E9061BB1B7FD4B9CA9F703F0BAC6662EF1D825AD(B
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...^!8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir3212_2020003175\Ruleset Data	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Subresource Filter\Indexed Rules\27\scoped_dir3212_2020003175\Ruleset Data

Category:	dropped
Size (bytes):	142248
Entropy (8bit):	4.846958959177541
Encrypted:	false
SSDEEP:	3072:o4epnfQf5uBcSbURPN450zSpInSzpnDfSixPcylmrRX3jOht:o4gfu5uBnb7VxPgrRH2
MD5:	CF3E632B2AF9CF2DF74E474897575FF3
SHA1:	57A1F95D817477FE2C7A5D04A476788D322C85C3
SHA-256:	41D2FF5C77B413F73FD74964606980CB85B53D0A18C58A5596B0FDFBE7D149DE
SHA-512:	E6E262100577E4FDB6521B58E8407AAE401DAAAFCC2891C0F9D849AA9F5AAF18C2AB1B96B0719B1D8870ECA4832E75BEB5EE81C847699C8497CB2D8F5D98AEDF
Malicious:	false
Reputation:	low
Preview:	.....S.....<..... ...X...l...h...d...0.....X...T...P...L...H.....@...<.....4...0...,.....|...`...D..... .....P/.....ozama.....h/.....g.bat..... ./.....onwod.....0.../.....ennab...../.....nozam...../.....geips...../.....rekoj...../.....lgoog.....0.....uotpo.....(0.....lreko..... 0.....$R..... ...Q...Q...Q...Q...Q...R..hQ...Q...Q...Q...Q..<Q...Q...Q...Q...Q...Q...Q...Q...P...Q...P...Q...Q...Q...Q...P...Q...Q...Q...Q...Q...Q..hP...Q..HP...Q..\|Q..xQ.. P..pQ..lQ..hQ..dQ ..`Q..\Q..XQ..TQ..PQ..LQ..HQ..DQ..@Q...O...O..4Q..0Q..,Q..(Q..$Q.. Q...Q...Q...Q..tO...Q..TO..8O...Q...P...P...O...P...P...P...P...P...P...P...P...P...P...P...P...P...P...P...P...P...P...P...P...N...P...N...P...P...P...P...P...P...P..XN..<N.. N..xP..tP..pP..lP..hP..dP...M..\P..XP..TP..PP...M..HP...M..@P..<P..8P..4P..0P..,P..(P..$P.. P...P...P...P...P...P...P..HM...P..

C:\Users\user\AppData\Local\Google\Chrome\User Data\c4d67247-41ae-452c-90cc-45c2b39ce342.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):	380284
Entropy (8bit):	6.027049220022618
Encrypted:	false
SSDEEP:	6144:Wrd0hqhdMNnOvBS8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBE:g0hqhdMY/xzurRDn9nfNxF4ijZVtilBE
MD5:	4C940F78D3218C6FF8A6CAA1C6DE8AAA
SHA1:	DC17622ADF6AE9CCDFE9D180018758FF2D4468DC
SHA-256:	36AE17688519A5EFD14D66BAD078694F76BD2C571A681BEEBE2B76F69BDD8C89
SHA-512:	73C9C40AB940F7471FC7DC55672EA3A7877C59E7F0968EFE32FDCCD8EAB49F02BB69C5F67F77222C21C71598BC468172CD9082A76179FC236C8BAFFB97E16AA
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":1.635202029838458e+12,"network":1.635169631e+12,"ticks":118833701.0,"uncertainty":3807020.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075705080"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\d80684d9-0e2f-4c1c-999a-fd01222f413e.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):	380284
Entropy (8bit):	6.027049020768082
Encrypted:	false
SSDEEP:	6144:Srd0hqhdMNnOvBS8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBE:00hqhdMY/xzurRDn9nfNxF4ijZVtilBE
MD5:	B564C28966E2A49A18CFD7A4459B4CAE
SHA1:	83D9CFE031E7695FCD139E6AC51515B0FB26B55E
SHA-256:	76E95BDBA16191F3D1AB434CED9C68F7BBBE0B143A86163A10369BCB573B0393
SHA-512:	9B3A9F4F11C33F90CCA7F446735BB77C2653C8AB6BECF0B89018D9F06308CE54CB4776F401B3B5DB709B749186172E994F9FABF5F7C9BFB9D5D532A582C8D3D7
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":1.635202029838458e+12,"network":1.635169631e+12,"ticks":118833701.0,"uncertainty":3807020.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075705080"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\3212_122078107_metadata\verified_contents.json

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

C:\Users\user\AppData\Local\Temp\3212_122078107_metadata\verified_contents.json

Category:	dropped
Size (bytes):	1309
Entropy (8bit):	5.997538210898862
Encrypted:	false
SSDEEP:	24:pZRj/flTd0PVmddLCszkaoXMU7MeQA4elll1qWBRcoXhlARvyILHpX:p/hd8AdlAkakMUweVnIlgcRck+ARyQ
MD5:	3FFCEDA47FF272479111605EB1CF2E13
SHA1:	94BAD756A9E11F2CE7E0829970C6B5130FCCC97B
SHA-256:	7C5598280B9AA42FC25F0B69785A140682013D9D3CE7E0EBFAB36733AC29E46A
SHA-512:	57D3808ACFFC1247F7F6630400BDE03330FDCDAB7DA7680011DB01A01F1E2C6E390101D884C3DF2E6D7EEFCC2FC5AFBE1A019664CC5E2E18E5E468162390FC 1
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiO lt7InBhdGgiOiJtYW5pZmVzdC5qc29uIiwicm9vdF9oYXNoIjoiMVNxb1lWcFJNWmpjY2hVUk8takxjbWE5dUR5bGlaMnlGeGVfNVdLMjRiQSJ9XSwiZm9ybWF0IjoidHJ lZWhhc2giLCJoYXNoX2Jsb2NrX3NpemUiOjQwOTZ9XSwiaXRlbV9pZCI6Imxsa2dqZmZjZHBmZm1oaWFrbWZjZGNibG9oY2NwZm1vIiwiaXRlbV92ZXJzaW9uIjoiMS4wL jAuOSIsInByb3RvY29sX3ZlcnNpb24iOjF9","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"Bh1re0dYOdwSjaDJUKd5n VHYjKj8c_NDyv8GggspjC0bAQpzKZYwhXl876OFZqK6Ami3gsdoAJdOj_Xt9i1wrkXTa-rjRAV4GQ_uHqUso2xgdaOxIK4FReeesQ1qdZtKJIlbVWTGQBaheNba_Z3AjJL Dpd-xdniKfP0Sza0JGcRnn4kQa_9GZ5MJ-kl5-5vjrmP1lE1CrXQnaOiNBZkVpsWjb8wWxKtBMT8Vu79443eabBrx0KENcKtdhS7u30vH8cX1KyotQHFAcTr0f3LnMSWKq VSgJ81wU60a-pprHLb4dgC-3H-OWcyFElbklFeRWbsQC2p8Htnty1Kx4A85Hg"},{"header":{"kid":"webstore"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature": "KO8y7bHAHsNn1ITlwX6f3hVgeyifRsSivvWUQ_M

C:\Users\user\AppData\Local\Temp\3212_122078107\manifest.fingerprint

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.8537208244903915
Encrypted:	false
SSDEEP:	3:SXtQsmWXqdA9GuScVhh:SSsmWXqmZvVhh
MD5:	749030B21BE048D27B4B19164D29675B
SHA1:	A12124894725A2015C077675C37580C32C8F8600
SHA-256:	BA66E68B4543D06BDD4A67E5E5307844F9833FED3A2083567C27774638A4E325
SHA-512:	ED01E53FCB258BC9CC9459D4DD877AB0B1C676DEC0767214FA219516EB456BB01F7AEB397E70276F4491A1E12B6B317C66C060C6C5AAF5A45B2267471CFBB2 3
Malicious:	false
Reputation:	low
Preview:	1.2881b30d5044c9959cea23288d290b7e765565850a38228136df79022a98498e

C:\Users\user\AppData\Local\Temp\3212_122078107\manifest.json

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	299
Entropy (8bit):	4.704226969201291
Encrypted:	false
SSDEEP:	6:zeXC6WQpVyTJCAEIfd26VO9bIA6VCM/C6wrhKXk7Vm01LwyAGI/zqSkhl:0eTJCAEQLO9hQCMDgK0711LqGikH
MD5:	888C93212CF7DB002AB870A463A43D2B
SHA1:	739755489EB84106C3C565E6BF563EA0CB49FDBE
SHA-256:	D52AA8615A513198DC7215113BE8CB7266BDB83CA5899DB21717BFE562B6E1B0
SHA-512:	C3F54BBC1CB73DB932576EA4030F61C3FFD300716A9777EDB4CF819A5F7951F78F3EBC8396AC94B2A6A0BBB3DD2A821B4C2CE0FEC091DF5C3DB4BDBA77B7E 0D0
Malicious:	false
Reputation:	low
Preview:	{. "description" : "Origin Trials public key updates and disabled features list",. "manifest_version" : 2,. "minimum_chrome_version" : "50",. "name" : "Origin Trials Updates",. "origin-trials" : null,. "update_url" : "https://clients2.google.com/service/update2/crx",. "version" : "1.0.0.9".}

C:\Users\user\AppData\Local\Temp\3212_1614450587\Filtering Rules

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	91662
Entropy (8bit):	5.445218573812661
Encrypted:	false
SSDEEP:	1536:dP10tSrXGbnSboNUeJvnp6591jYFmwN6DokKwA38:P0tRbnHKmh6pjYowgD1+8

C:\Users\user\AppData\Local\Temp\3212_1614450587\Filtering Rules	
MD5:	1B20DD5F6D92AC4EA703F7DD8654B2D2
SHA1:	C4F9C3301C59AFD213DDE0D6B450ACEA4BE1E282
SHA-256:	041E9E35F6BDA335B925AC90CEC7C565F823E8B6B362584B2EB56DA955F17FDE
SHA-512:	ECE136D4D9AADB3E9683CCD6144D8AEBDC1A5A686C3DD92C53BBCCCDF0588B8C519F24618CF0249A9405DB9F35E06CE45B5FD23202CB9C8D8F8C2097716826B
Malicious:	false
Reputation:	low
Preview:	.....o0.8.@.R.-728x90.....o0.8.@.R.adtdp.com^.....o*...epaper.timesgroup.com*...nbcsports.com*...windalert.com*...kowb1290.com*...k2radio.com*...vimeo.com*.. .koel.com*...uefa.com0.8.@.R#googletagservices.com/tag/js/gpt.js.....o0.8.@.R./ad-inserter/.+.....0.8.@.R.g.ezoic.net/ezosuigenerisc.js.9.....o*...adcore.com.au..*.. .adcore.ch..0.8.@.R./adcore_.....o0.8.@.R.uwoaptee.com^.....o0.8.@.R.ayads.co^.....o0.8.@.R._468_60..8.....o0.8.@.R)bancodevenezuela.com/imagenes/publicidad/.....o0.8.@.R..adbutler-.....o0.8.@.R.adrecover.com^.>.....o*...google.com0.8.@.R!developers.google.com/google-ads/.....o0.8.@.R.aso1.net^.-.....o*...vk .com0.8.@.R.vk.me/css/al/ads.css.+.....o0.8.@.R.mysmth.net/nForum/*/ADAgent_.%.....0.8.@.R.discordapp.com/banners/.D.....o*...daum.net0.8.@.R)daumcdn.net/adfit/static/ad-native.min.js.'.....o0.8.@.R.looker.com/api/internal/."......o0.8.@.R.broadstreetads.com^.....o0.8.@.R./banner.cgi?.....o*...thefreedictionary.com*..

C:\Users\user\AppData\Local\Temp\3212_1614450587\LICENSE.txt	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	24623
Entropy (8bit):	4.588307081140814
Encrypted:	false
SSDEEP:	384:mva5sf5dXrCN7tnBxpxkepTqzazijFgZk231Py9zD6WApYbm0:mvagXreRnTqzazWgj0v6XqD
MD5:	D33AAA5246E1CE0A94FA15BA0C407AE2
SHA1:	11D197ACB61361657D638154A9416DC3249EC9FB
SHA-256:	1D4FF95CE9C6E21FE4A4FF3B41E7A0DF88638DD449D909A7B46974D3DFAB7311
SHA-512:	98B1B12FF0991FD7A5612141F83F69B86BC5A89DD62FC472EE5971817B7BBB612A034C746C2D81AE58FDF6873129256A89AA8BB7456022246DC4515BAAE2454B
Malicious:	false
Reputation:	low
Preview:	EasyList Repository Licences.... Unless otherwise noted, the contents of the EasyList repository.. (https://github.com/easylist) is dual licensed under the GNU General.. Public License version 3 of the License, or (at your option) any later.. version, and Creative Commons Attribution-ShareAlike 3.0 Unported, or.. (at your option) any later version. You may use and/or modify the files.. as permitted by either licence; if required, "The EasyList authors.. (https://easylist.to/)" should be attributed as the source of the.. material. All relevant licence files are included in the repository..... Please be aware that files hosted externally and referenced in the.. repository, including but not limited to subscriptions other than.. EasyList, EasyPrivacy, EasyList Germany and EasyList Italy, may be.. available under other conditions; permission must be granted by the.. respective copyright holders to authorise the use of their material.....Creative Commons Attribut

C:\Users\user\AppData\Local\Temp\3212_1614450587_metadata\verified_contents.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1529
Entropy (8bit):	5.982586926845733
Encrypted:	false
SSDEEP:	24:pZRj/flTHYYG6CkYbKWvgjeT3SzkaoXs3secwzXITLm7oXN68gdu8v22LWmZ:p/h4d5bKETCkaknTwrD7kw8AuL2LWg
MD5:	6ABC3D5978FB1923B01B724C9BF650FE
SHA1:	4B7885693DF9971A4C8908FF36AEB8C8AEFA35BF
SHA-256:	61997A1114C0BFC1AE793D5BBE59BFA35C32AF28072E6B2F46E360490CD7402B
SHA-512:	20C38E7DB25C9FCB9122092632C714B3A52A4CB4AC6D8B88F6F162302C28090D7278FFA4A20697B247FC1329D69648F41C78D3E7353A63190EC109792265C2F1
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJGaWx0ZXJpbmcgUnVsZXMiLCJyb290X2hhc2giOiJvVmpUZ0dCOXh1NUZvdy1YOHBMSUd3N3c3bzRtWHBRU2lSMVB5U2ZFUG1zIn0seyJwYXRoIjoiTElDRU5TRS50eHQiLCJyb290X2hhc2giOiIyaWswNmk0TFlCdVNHNWphRGFIS253NE9pdnVSRzZsQ0JKMVk0TGtzRFJJIn0seyJwYXRoIjoibWFuaWZlc3QuanNvbiIsInJvb3RfaGFzaCI6IlpPazM1MWhHSnhHdFdwNXI1SUVyc2RLRTF4WVE2QmlrcDUydnI1ZDhaZ2cifV0sImZvcm1hdCI6InRyZWVoYXNoIiwiaGFzaF9ibG9ja19zaXplIjo0MDk2fV0sIml0ZW1faWQiOiJnY21qa21nZGxnbmtrY29jbW9laW1pbmFpam1tam5paSIsIml0ZW1fdmVyc2lvbiI6IjkuMzAuMCIsInByb3RvY29sX3ZlcnNpb24iOjF9","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"Y3LhZVwztDSZ5AuBNgXe7VKETu2kD6_AcJaojgZVhFD8942owYRMUcn7zbIdpWAI63bX0GC1iT6hMNiDgSxPunZep3sHvuizqznjZYwkXT16Ej2z5iRb_CwkZO73VXN1GELnCYS8Aj0Wz5jsAdqxfh0zy_36dH6Kekv6cJs-uAmWvimsX__rmkef76WxK22qGG0vA5vjlrlvez8tQ4ZUKJCVSdvE7yxupPcnTKrSRHemFyCLQ

C:\Users\user\AppData\Local\Temp\3212_1614450587\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.8311952575506543
Encrypted:	false
SSDEEP:	3:ScZDE31DJyhD5sBdEWMrADXcOkla:Scm3JJyhD4MrAjcOk4
MD5:	0CF8794448514BC0C92C3B1335B9979C

C:\Users\user\AppData\Local\Temp\3212_1614450587\manifest.fingerprint	
SHA1:	D3BA9AB39D5C0C9FAC9A77F29177862E88041D10
SHA-256:	A17B2ABBBDF9CFEE923CF399C0E48E528D927B06829BA3AA378514AD70989542
SHA-512:	297821DA4DC84A7DEC178FBDB3E197DA7E513C40102A513646F543CDA1017765F335858F4F1D6328DA8A6291367CF665F4CE3AD85117EC0537F180C8CE1272F
Malicious:	false
Reputation:	low
Preview:	1.960fae5df394ff065f95f2d0a5ab95a9bf88a270103c8ed2080959eedf3836fc

C:\Users\user\AppData\Local\Temp\3212_1614450587\manifest.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	115
Entropy (8bit):	4.545910352797257
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFHXG7LGMdv5HcDKhtUJKS1Gv:F6VlMZWuMt5SKPS1Gv
MD5:	9826ADA46C629E7D0233C6079456A4DA
SHA1:	CCAFC047ABB6DF35A1EB262CDF274DE747DFB598
SHA-256:	64E937E758462711AD5A9E6BE4812BB1D284D71610E818A4A79DAFAF977C6608
SHA-512:	8BA91A6DB13D7D8C5EA66E2403AE9722CEBDD6B15E8F8522374E980CE9C3DEBB1C508BB33FAC94D87CA58A5E4C7201DB0FBCA034E840E33A23A2D48F091BC AC9
Malicious:	false
Reputation:	low
Preview:	{. "manifest_version": 2,. "name": "Subresource Filtering Rules",. "ruleset_format": 1,. "version": "9.30.0".}.

C:\Users\user\AppData\Local\Temp\3212_1826751422\LICENSE	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1558
Entropy (8bit):	5.11458514637545
Encrypted:	false
SSDEEP:	48:OBOCrYJ4rYJVwUCLHDy43HV713XEyMmZ3teTHn:LCrYJ4rYJVwUCHZ3Z13XtdUTH
MD5:	EE002CB9E51BB8DFA89640A406A1090A
SHA1:	49EE3AD535947D8821FFDEB67FFC9BC37D1EBBB2
SHA-256:	3DBD2C90050B652D63656481C3E5871C52261575292DB77D4EA63419F187A55B
SHA-512:	D1FDCC436B8CA8C68D4DC7077F84F803A535BF2CE31D9EB5D0C466B62D6567B2C59974995060403ED757E92245DB07E70C6BDDBF1C3519FED300CC5B9BF91 C
Malicious:	false
Reputation:	low
Preview:	// Copyright 2015 The Chromium Authors. All rights reserved..//.// Redistribution and use in source and binary forms, with or without.// modification, are permitted provided that the following conditions are.// met:.//.// * Redistributions of source code must retain the above copyright.// notice, this list of conditions and the following disclaimer..// * Redistributions in binary form must reproduce the above.// copyright notice, this list of conditions and the following disclaimer.// in the documentation and/or other materials provided with the.// distribution..// * Neither the name of Google Inc. nor the names of its.// contributors may be used to endorse or promote products derived from.// this software without specific prior written permission..//.// THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS.// "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT.// LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR.// A PARTICULAR

C:\Users\user\AppData\Local\Temp\3212_1826751422_metadata\verified_contents.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1511
Entropy (8bit):	5.988901218146699
Encrypted:	false
SSDEEP:	24:pZRj/flTU3YiaRIBjoYkWV7aoXn5Z2RCzlI+oXh6oMJ59aulMT7FmI7:p/hUId47aknn4CzlHkhyrlMT7FmI7
MD5:	BDBD826DE13C31EDE35B5E642649F5DF
SHA1:	41C0DB1031DF47F13E9BA89C5B8D215D345CFC13
SHA-256:	5918740B174A827FE1AA04C98D8ED06A95B4CE6DE9D02F3491675FDD44BB3416
SHA-512:	0F8A5EA3060C4A3D128341FE041AD36B9CCA934B112A42ABD0361D549A61D3E3649D850F3F66C17166C46F360D5B46B7E85469B6BE652864CB88BCDD7CD1EB 7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\3212_1826751422_metadata\verified_contents.json	
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJMSUNFTlNFIiwicm9vdF9oYXNoIjoiUGIwc2tBVUxaUzFqWldTQnctV0hIRkltRlhVcExxiZDlUcVkwR2ZHSHBWcyJ9LHsicGF0aCI6ImNybC1zZXQiLCJyb290X2hhc2giOiJSbzF5Nm9aOG5xckctOGxNa0FrMEVnSC1GTGM3MF9PX3N4aHVZMEFxeWNJIn0seyJwYXRoIjoibWFuaWZlc3QuanNvbiIsInJvb3RfaGFzaCI6IlVxZnhMOG43RkJoNC1Ja296NlVzQ2VLUnpJclRHZzlSMFRlNjMwSzBwR28ifV0sImZvcm1hdCI6InRyZWVoYXNoIiwiaGFzaF9ibG9ja19zaXplIjo0MDk2fV0sImI0ZW1faWQiOiJoZm5rcGltbGhoZ2llYWRkZ2ZlbWpob2ZtZmJsbW5pYiIsIml0ZW1fdmVyc2lvbiI6IjY5MzUiLCJwcm90b2NvbF92ZXJzaW9uIjoxfQ","signatures":[{"header":{"kid":"publisher"},"protected":"eyJhbGciOiJSUzI1NiJ9","signature":"Dq5JYMauq6lg4o1zNhLzKMGA_4d2Lj8ldqElNOEM94z26jBOQbvpdscu1Gy4SiT0qnZ2Ih2xcUan7_Z4Ea05VZrz2JcIKOXKMFDzg3DB4opMkXR3UHW-KrpcoQ8vLNPc4Secsh5WGHT9o-5BadErELxUjUM0m_fjaDzPgLNkyJvNcnHcqDnUC20WkhvrkbuRASD8siADEW2dTQZMjQ8_oJ4HUrgoaYVAAu76IPyUmwQ3SdqWCMvCEQp3xRpNbp1o8j1

C:\Users\user\AppData\Local\Temp\3212_1826751422\crl-set	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	22443
Entropy (8bit):	7.821161818050178
Encrypted:	false
SSDEEP:	384:i20XPK2MeWUUIrH+pDzbm80WDzyloH83GQo450S8yzFP0tKDaWG9S3c/LaPJBr:iVO0RHIDv2WnyloKGQo3S8It0KuWGRuP
MD5:	865FF4C87232F18F09DBDEFBDEECF1D5
SHA1:	D42FE7C96AE63C9D400D719DBC8180A9728BC40D
SHA-256:	7E1EC6A83F3ABC2026A0FCD9A2265645CBF7E0ABEF4CBC63A518B160FBC9F0BA
SHA-512:	528E461688EEBE287A001F0F837A7B97CAAE62E10E9AE950BA1B71A1D8AB6D71A231F041468AB541645685B1EC6BE29DFDE5338932154EAF7970CB626DD21B7C
Malicious:	false
Reputation:	low
Preview:	".{"Version":0,"ContentType":"CRLSet","Sequence":6935,"DeltaFrom":0,"NumParents":194,"BlockedSPKIs":["Jdoa1Yu/z7In2HI7GFfUwY57qnQXtPnv+TZrXoafizk=","Ii5LVLuYp+5dX+uWM/mR08MwDpUU2t57DU+CjHlPjoc=","yP3cdcsb27WMB7TqhHKH9iZIndZrwQomrdm1dbOgo40=","BN3pqpp59hSYaCMl+ghwJ2cH+5ypU4QSC0aJMmhJT8k=","tbqN1/iVZMKInT1kU8hJmMd4JJGbZOoINapimGWRvlA=","wO0gU0a7veButWD1zuAqNjTiR0p+ds+PvvVjuxF90OM=","eBpM8ukkUvPuAdDDgaQhTzkEFlw5CtvWH80RJE4Jstw=","/NdsyiNH5c1bOTR/Uc9DZUtpor/JBzZwpr5H2HAebg4=","lo26afv/Fb83YgiUMa3lp+rUt+rxvnACaBC8V9HGT24=","fNKVt1VEgIq9lAlGbwg3xarcAuM7YVDGZE3goJZZ8jw=","9Sk9R+041MMbLULe47WzrOl8omyirANl42Iu6AlTH7s=","nFmjzK6kaZhCsGjPxSz5RdtRmGlXyDLNsYynOEn7ue4=","OUz/WJ5okxLPwHHuC8Gf5MYGIWzlQ0Kd5tti5C27O8E=","NuqWEoyJg5+2IfitDh7gucIgb2Kre02ixnZYk8m3ztI=","xpENC6nt31kzNBSf7f6HOF83tiU1S7Q5XAriyN9I4Xw=","MO/kE4JHbDOA8C9+I+ZrovhnsFnuHqaHlrRBuFtdElY=","r1kVGOLmxg67/AkHr6pJvEBR1F5/IUq/7nUS7gD2Ye0=","6EnHF2yT32X2S2FpgjZuVmMReBK2+ivAyPqK6u5Bgcw=","0x7DkoW3pTGdAVfbQg7YfHQ+Mzu8d/h3H3BGT0NqYEk=","h7/Yr

C:\Users\user\AppData\Local\Temp\3212_1826751422\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.8973244693173252
Encrypted:	false
SSDEEP:	3:SR9Gl0Uo0zeYSQWDpDUAARQnV3TW:SW035/QWDmlOV3TW
MD5:	ABBBE95C30F735EB49726373DE01832E
SHA1:	2E1C61A1384A8C2B883004DF70D88E246BBE3B50
SHA-256:	D9174220E9EA95D3F36F0AA9F83CE211AE555CCFCBD630C4A0925D73FC6601AF
SHA-512:	F14C0E53069DFA0256C320760AC7664A83CFCB7BD5809E1DFC19571F311FFC0DC8D7C9CBE9B3A660CAAC3ACAEC1371E4734C759DEC954D5DE1E592824D7D635
Malicious:	false
Reputation:	low
Preview:	1.402cd1c7bd02eabb0243d8400ebe5f601d7534fc814f1ee45b60935ea2633134

C:\Users\user\AppData\Local\Temp\3212_1826751422\manifest.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	192
Entropy (8bit):	4.825852116718429
Encrypted:	false
SSDEEP:	3:rR6TAulhFphifFJQwQQGY3BPFgS1GLEeSWU4pv/8F/FxLj2RF2fcTZTotL:F6VlMowLRKS1BWfB0NpK4aotL
MD5:	E406DAE605FA3C800909586BEDF4D406
SHA1:	906C97920EB17A0C4E6C4827DAA1DB2E517FF7DF
SHA-256:	52A7F12FC9FB141878F88928CFA52C09E291CC8AD31A0F51D137BADF42B4A46A
SHA-512:	2C6AAF55B4110095F4231A894B51860B3B6CF77B37EFD465C4B081D5545915932E60CFC8B5627F348511BCD9F2C801560BA1CBD8726F7C62D9DA55D9AB5C2E2
Malicious:	false
Reputation:	low
Preview:	{. "manifest_version": 2,. "name": "crl-set-11048381235692390475.data",. "version": "6935",. "imageName": "image.squash",. "squash": true,. "fsType": "squashfs",. "isRemovable": false.}

C:\Users\user\AppData\Local\Temp\3212_2067475749_metadata\verified_contents.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3034
Entropy (8bit):	5.876664552417901
Encrypted:	false
SSDEEP:	48:p/hEc9q0S+UTKYM43z8nqMsfWRUWEADM/W9n7lqFkakzcVTGkcYTPi6zM:RGcg5z/jjjHgUnV278+aWLy4
MD5:	8B6C3E16DFBF5FD1C9AC2267801DB38E
SHA1:	F5CADC5914DF858C96C189B092BC89C29407BBAA
SHA-256:	FD986A547D9585E98F451B87CA85DEB4B61EE540C6FAC678D7BEDABF04653095
SHA-512:	37048EF8FADF62A26CAEC6EE90AC192429AB1E99424E5C68FACA90C0DAD68642C761FDCAC03FC38FA930841F91FA145A6943EC7F168D4F2FA426F1F092C2F52
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiOlt7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY19wbmFjbF9qc29uliwicm9vdF9oYXNoIjoiVkNUSHNJVHNUSXVncWNhV2ctWHVpTU1sdWloV1FSTE1sQnpTTGprdGhETSJ9LHsicGF0aCI6Il9wbGF0Zm9ybV9veGVjaWZpYy94ODZfNjQvcG5hY2xfcHVibGljX3g4Nl82NF9jcnRiZWdpbl9mb3JfZWhfbyIsInJvb3RfaGFzaCI6ImxINWt2a1BvSVZZczZKVHhyOHc5Q2MxXzloVEJCX3lVSlF6VDZseVVNd0kifSx7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY194ODZfNjRfY3J0YmVnaW5fbyIsInJvb3RfaGFzaCI6IkVuLVFQTW1HUm1xbG9Ud1gzOTAzckpsMkw0R25sQmdET1FhZlNKaHJ4Nk0ifSx7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY194ODZfNjRfY3J0ZW5kX28iLCJyb290X2hhc2giOiJkT2lJVzRmdEdGNW9FY0k1UXYyYjBmdXNrUlYyaUVtdmxhbmV6MlpFc3VvIn0seyJwYXRoIjoiX3BsYXRmb3JtX3NwZWNpZmljL3g4Nl82NC9wbmFjbF9wdWJsaWNfeDg2XzY0X2xkX25leGUiLCJyb290X2hhc2giOiIzNEU5QU9EMmpqLWNoMzZQZ0NVV0YtMUpYWVhVdlNGY1I4bks1aWppcWNjIn0seyJwYXRoIjoiX3B

C:\Users\user\AppData\Local\Temp\3212_2067475749_platform_specific\x86_64\pnacl_public_pnacl_json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	507
Entropy (8bit):	4.68252584617246
Encrypted:	false
SSDEEP:	12:TjLJ7qaVgPPd8bdzQBXefosmc5T9+n6e1Cetm1JXcAwA:TJ7jViPOd8wfHmZ6RP15
MD5:	35D5F285F255682477F4C50E93299146
SHA1:	FB58813C4D785412F05962CD379434669DE79C2B
SHA-256:	5424C7B084EC4C8BA0A9C69683E5EE88C325BA28564112CC941CD22E392D8433
SHA-512:	59DF2D5F2684FACC80C72F9C4B7E280F705776076C9D843534F772D5A3D578BEE04289AEE81320F23FB4D743F3969EDF5BA53FEBBAC8A4D27F3BC53BCF271C3E
Malicious:	false
Reputation:	low
Preview:	{. "COMMENT": [. "This file serves as a template for the resource info description used by ", . "the NaCl Chrome plugin. It is kept in the NaCl repository to prevent ", . "hard-coding of NaCl-specific information inside the Chrome repository.".], . "abi-version": 1, . "pnacl-arch": "x86-64", . "pnacl-ld-name": "ld.nexe", . "pnacl-llc-name": "pnacl-llc.nexe", . "pnacl-sz-name": "pnacl-sz.nexe", . "pnacl-version": "5dfe030a71ca66e72c5719ef5034c2ed24706c43".}

C:\Users\user\AppData\Local\Temp\3212_2067475749_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_for_eh_o	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	2712
Entropy (8bit):	3.4025803725190906
Encrypted:	false
SSDEEP:	48:b/5D5V5PK82aTS6aTTw0Do1DttoyDNsEA:b/hbVic1ZtLDNsE
MD5:	604FF8F351A88E7A1DBD7C836378AE86
SHA1:	9D8D89AE9F13D6306E619A4EAAD51EDE91A5F9F3
SHA-256:	947E64BE43E821562CE894F1AFCC3D09CD7FF614C107FC94250CD3EA5C943302
SHA-512:	85B1EDA4C473E00034EE627B7ABB894A77E521BC6A91A91A4A3744CA7511CB0AF10B9723D9ECC2CE3378DD70B659DF842D8C11875958CB77070CF01EC0A1580
Malicious:	false
Reputation:	low
Preview:	.ELF.....>.....@.....@.....PH.....,$J.l=....J.$<A[..@.A...M..A..fffff.....PH.....,$J.l=....J.$<A[..D..A...M..A..fffff..... ....PH..1..,$J.l=....J.$<A[.....A...M..A..fffff.....PH..SP..h.....fff.....h.....fff.....J.$<[.,$J.l=....J.$<.....f..... .....NaCl....x86-64.....zR..x.....@....C....C.....8.....@....C....C.....T.....@....C....C.....p .....`....C....C..B..... .....<.....@.....X.....t.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pna

C:\Users\user\AppData\Local\Temp\3212_2067475749_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_o	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped

C:\Users\user\AppData\Local\Temp\3212_2067475749_platform_specific\x86_64\pnacl_public_x86_64_crtbegin_o	
Size (bytes):	2776
Entropy (8bit):	3.5335802354066246
Encrypted:	false
SSDEEP:	48:b/5D5V5ej5ej5PjDdaTS6aTTw6DV1DtFouoyDOsTy:b/hbEEVJB1ZFhLDOsT
MD5:	88C08CD63DE9EA244F70BFC53BBCADF6
SHA1:	8F38A113A66B18BAA02E2C995099CF1145A29DAA
SHA-256:	127F903CC986466AA5A13C17DFDD37AC99762F81A794180339069F48986BC7A3
SHA-512:	78D2500493A65A23D101EC2420DC5F0CE8C75EFAC425C28547121643E4FB568E9D827EF2C0F7068159E043C86B986F29BF92C6BADC675F160B63C7B3512EB95F
Malicious:	false
Reputation:	low
Preview:	.ELF.....>.....X.....@.....@.....PH.....,$J.l=....J.$<A[..@.A...M..A..fffff.....PH.....,$J.l=....J.$<A[..D..A...M..A..fffff..... ....PH..1..,$J.l=....J.$<A[.....A...M..A..fffff.....PH..,$J.l=....J.$<A[f.....A...M..A..fffff.....PH..,$J.l=....J.$<A[f.....A...M..A..fffff.....PH..SP..h.....fff..... .....J.$<[.,$J.l=....J.$<....f.K.....`.....P.....z.....NaCl....x86-64...clang version 3.7.0 (https://chromium.googlesource.com/a/native_ client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c9 4a3a7da70f0081724448f).....zR..x.....@....C....C.....8.....@....C....C.....T.....@....C....C.....p.....@....C....C.....@....C....C.....@...

C:\Users\user\AppData\Local\Temp\3212_2067475749_platform_specific\x86_64\pnacl_public_x86_64_crtend_o	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB relocatable, x86-64, version 1 (SYSV), not stripped
Category:	dropped
Size (bytes):	1520
Entropy (8bit):	2.799960074375893
Encrypted:	false
SSDEEP:	12:Bvx/ekjlM/NQQmTfR9yp9396QQmTfR9C6wRqD8MTDDw7lEOkSbfuEAXwX6BX2U8b:bDjO/NbmT3296bmT3Twk8qDwh7b7CD8
MD5:	75E79F5DB777862140B04CC6861C84A7
SHA1:	4DB7BDC80206765461AC68CEC03CE28689BBEE0C
SHA-256:	74E8885B87ED185E6811C23942FD9BD1FBAC9115768849AF95A9DECF6644B2EA
SHA-512:	FE3F86E926759E71494F2060C4ED3C883EBCAF20CB129A5AD7F142766C33FAB10B5FABC3C7C938E0E895E27EA0AC03CBFE8D0EEABF5300A4AD07F67FD96CC 253
Malicious:	false
Reputation:	low
Preview:	.ELF.....>.....@.....@.....NaCl....x86-64.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f)...text..comment..bss..group..note.GNU-stack..eh_frame..shstrtab..strtab..symtab..data..note.NaCl.ABI.x86-64.....!..... ..../../../pnacl/support/crtend.c.__EH_FRAME_END__..... .....@.....H.....P.....H.....

C:\Users\user\AppData\Local\Temp\3212_2067475749_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=7511538a3a6a0b862c772eace49075ed1bbe2377, stripped
Category:	dropped
Size (bytes):	2163864
Entropy (8bit):	6.07050487397106
Encrypted:	false
SSDEEP:	24576:HPHonIwYZJ0ykwVO7Owf31yJKzCtxO8RSV4lY+PbeHVxCtjFV4lBNeSAmfGqa+A7:HvSMRwf3SKmlY+PyPvnM2Gq+
MD5:	0BB967D2E99BE65C05A646BC67734833
SHA1:	220A41A326F85081A74C4BB7C5F4E115D1B4B960
SHA-256:	C6C2D0C2FC3E38A9BFA19C78066439C2F745393F1FD1C49C3C6777F697222C76
SHA-512:	8EF8689E00E4B210A30444D18ED6247F364995ABEB2FD272064C3AF671EEDB4D9B8B67CA56F72FEBF8F56896D4EA7EC4B10CB445FFA1C710C1F312E9DA0E48 6
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	.ELF.....>.... .....@.....!.....@.8...@.....{.....W..... .....@.....@.....P.td.....h.....h.....h.....4b.....4b.....Q.td.....NaCl....x86-64.....GNU.u.S.:j..,w...u...#w..... ?.....Y@.....@.....1@.....B@.....P@.....@X@.....``@.....h@.....pp@.....H.@.....@.....@.....@.....@.....@....`..@.....@.....A.....A.....p.....@..... .....?.....A.....5.....?5.5...?.5.....?.....P9.....PC.....?.....0@.....aCoc...?..`.(..?.y.P.D.?<.s..O.u.....$@.....@.....@..... .. ..@...`...`...`...`.....`...`...`...`...`...`...`.....`...

C:\Users\user\AppData\Local\Temp\3212_2067475749_platform_specific\x86_64\pnacl_public_x86_64_libcrt_platform_a	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	40552
Entropy (8bit):	4.127255967843258

C:\Users\user\AppData\Local\Temp\3212_2067475749_platform_specific\x86_64\pnacl_public_x86_64_libcrt_platform_a	
Encrypted:	false
SSDEEP:	768:xlP+1fzyUNVU5LmKxeOnjpD5eA/eUnUUxvT:xlP+1ryYMTekpD5eAWjuvT
MD5:	0CE951B216FCF76F754C9A845700F042
SHA1:	6F99A259C0C8DAD5AD29EE983D35B6A0835D8555
SHA-256:	7A1852EA4BB14A2A623521FA53F41F02F8BA3052046CF1AA0903CFAD0D1E1A7B
SHA-512:	7C2F9BF90EB1F43C17B4E14A077759FA9DC62A7239890975B2D6FD543B31289DC3B49AE456CA73B98DE9AC372034F340C708D23D9D3AAB05CCBDABDC56A631E
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 624 `.....,...8...Z(..e...e...t...t...y`..y`..y`..y`..y`..y`..y`..y`..y`..y`..y`..y`.....fmod.fmodf.memcmp.memcpy.memmove.memset.__nacl_read_tp.__pnacl_init_irt.longjmp.setjmp.__Sz_fptosi_f32_i64.__Sz_fptosi_f64_i64.__Sz_fptoui_f32_i32.__Sz_fptoui_f32_i64._Sz_fptoui_f64_i32.__Sz_fptoui_f64_i64.__Sz_sitofp_i64_f32.__Sz_sitofp_i64_f64.__Sz_uitofp_i32_f32.__Sz_uitofp_i32_f64.__Sz_uitofp_i64_f32.__Sz_uitofp_i64_f64.nacl_tp_tdb_offset.nacl_tp_tls_offset.__Sz_bitcast_16xi1_i16.__Sz_bitcast_8xi1_i8.__Sz_bitcast_i16_16xi1.__Sz_bitcast_i8_8xi1.__Sz_fptoui_4xi32_f32.__Sz_uitofp_4xi32_4xf32..e_fmod.o/ 0 0 0 644 2792 `..ELF.....>.....(.....@.....@.....PH..AVAUATSfI.~.M..I.. E....@.A.....D..D1.....8fI.~.M.....I.. E..A.....D..D..t.D....D..f....D..=....r...Y...^.[A\A]A^..@..,$J.I=....J.$<A[A...M..

C:\Users\user\AppData\Local\Temp\3212_2067475749_platform_specific\x86_64\pnacl_public_x86_64_libgcc_a	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	132784
Entropy (8bit):	3.6998481247844937
Encrypted:	false
SSDEEP:	384:Hf0mOXYmeKzQUIdedRFvT5p1Ee2HyAlL3O4:Hf7OXdmWRJT5p1R2HyAhO4
MD5:	C37CA2EB468E6F05A4E37DF6E6020D0F
SHA1:	EA787E5EADFB488632EC60D8B80B555796FA9FE9
SHA-256:	C1483ED423FEE15D86E8B5D698B2CDAB89186CE7FF9C4E3D5F3F961FD80D7C6E
SHA-512:	01281DE92B281FB29E1ACA96AA64B740B65CC3A9097307827F0D8DB9E1C164C56AFCDFA0BF138EA670A596D55CE2C8D722760744E9FC9343BB6514417BF333BA
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 942 `....;...|.....4...x..#...-...4l..E...M...U...]...n...u...~X...4.....L.....t...p.....`.....''...*...1...:...D...K...T...\...d...r|..|0.....x.....L.....\...8.....__clzti2.__compilerrt_fmax.__compilerrt_fmaxf.__compilerrt_logb.__compilerrt_logbf.__ctzti2.__divdc3.__divdi3.__divmoddi4.__divmodsi4.__divsc3.__divsi3.__divti3.__fixdfdi.__fixdfsi.__fixdfti.__fixsfdi.__fixsfsi.__fixsfti.__fixunsdfdi.__fixunsdfsi.__fixunsdfti.__fixunssfdi.__fixunssfsi.__fixunssfti.__floatdidf.__floatdisf.__floatsidf.__floatsisf.__floattidf.__floattisf.__floatundidf.__floatundisf.__floatunsidf.__floatunsisf.__floatuntidf.__floatuntisf.compilerrt_abort_impl.__moddi3.__modsi3.__modti3.__muldc3.__muloti4.__mulsc3.__multi3.__popcountdi2.__popcountsi2.__popcountti2.__powidf2.__powisf2.__udivdi3.__udivmoddi4.__udivmodsi4.__udivmodti4.__udivsi3.__udivti3.__umoddi3.__umodsi3.

C:\Users\user\AppData\Local\Temp\3212_2067475749_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_a	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	13514
Entropy (8bit):	3.8217211433441904
Encrypted:	false
SSDEEP:	192:uU9v4pXizdrEuxwk3vp20tprpdSGFwDqO:P9v4palvvc0tpFdSGFwmO
MD5:	4E8BEDA73EB7BD99528BF62B7835A3FA
SHA1:	DC0F263A7B2A649D11FF7B56FE9CFAC44F946036
SHA-256:	6B835FD48DF505EB336FF6518CE7B93BB0ED854DADAA5C1EEED48D420291F62C
SHA-512:	46116B8BABC719676D68FD40D2AC82F38A3D13D8A482ADFC6FC32A99170AC3420E52CC33242CCD0FA723ABF4FA5EDBB9CE16A09C729BF04AE4AFBB2F67A1E38B
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 94 `.....__pnacl_wrapper_start.__pnacl_real_irt_query_func.__pnacl_wrap_irt_query_func..shim_entry.o/ 0 0 0 644 7392 `..ELF.....>..... .....@.....@.....NaCl....x86-64.....A.L....A.L...D.....D....A.....t+.. u..t''..A.D.....A... .....A.D.....f..D..<.....Q.....V.....clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f).../../ppapi/native_client/src/untrusted/pnacl_irt_shim/shim_entry.c./mnt/data/b/build/slave/sdk/build/src/out_pnacl/x64.NACL_STARTUP_FINI.NACL_STARTUP_ENVC.NACL_STARTUP_ARGC.NACL_STARTUP_ARGV.NaClStartupInfoIndex.unsigned int.size_t.char.TYPE_na

C:\Users\user\AppData\Local\Temp\3212_2067475749_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_dummy_a	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	current ar archive
Category:	dropped
Size (bytes):	2078
Entropy (8bit):	3.21751839673526
Encrypted:	false

C:\Users\user\AppData\Local\Temp\3212_2067475749_platform_specific\x86_64\pnacl_public_x86_64_libpnacl_irt_shim_dummy_a	
SSDEEP:	24:MOcpdhWE5O/bZbmT3296bmT3TwQwDnvD/+R3:MHuECdaTS6aTTwXDvD/+l
MD5:	F950F89D06C45E63CE9862BE59E937C9
SHA1:	9CFAD34139CC428CE0C07A869C15B71A9632365D
SHA-256:	945B1C8A1666CBF05E8B8941B70D9D044BAAFB59B006F728F8995072DE7C4C40
SHA-512:	F9AFBB800A875EDCC63DEA4986179E73632B3182951A99C8B3D37DB454EFD7CC7192ECA5AC87514918A858BAD6DAEAB59548CA2E90EADA9900EF5B9F08E62C FC
Malicious:	false
Reputation:	low
Preview:	!<arch>./ 0 0 0 0 30 `.....\_pnacl_wrapper_start..// 20 `.dummy_shim_entry.o/.0 0 0 0 644 1840 `..ELF.....>.....@.....@.....PH..,$J.l=....J.$<.....f..D.....NaCl....x86-64...clang version 3.7.0 (https://chromium.googlesource.com/a/native_client/pnacl-clang.git ce163fdd0f16b4481e5cf77a16d45e9b4dc8300e) (https://chromium.googlesource.com/a/native_client/pnacl-llvm.git 7251d5b59fca15195c94a3a7da70f0081724448f).....zR..x..... ....C....C..... .....rela.text..comment..bss..group..note.GNU-stack..rela.eh_frame..shstrtab..strtab..symtab..data..note.NaCl.ABI.x86-64.....

C:\Users\user\AppData\Local\Temp\3212_2067475749_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=309d6d3d463e6b1b0690f39eb226b1e4c469b2ce, stripped
Category:	dropped
Size (bytes):	14091416
Entropy (8bit):	5.928868737447095
Encrypted:	false
SSDEEP:	196608:tKVqXp3Qev4dg6ilfHM8KLM2J3jqjnkZ:uqufB
MD5:	9B159191C29E766EBBF799FA951C581B
SHA1:	D1D4BBC63AB5FC1E4A54EB7B82095A6F2CE535EE
SHA-256:	2F4A3A0730142C5EE4FA2C05D27A5DEFC18886A382D45F5DB254B61B28ED642B
SHA-512:	0B4FF60B5428F81B8B1BCF3328CF80CBD88D8CE5E8BDBC236B06D5A54E7CF26168A3ABB348D87423DA613AB3F0B4D9B37CB5180804839F1CA158EC2B315DDE 00
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	.ELF.....>.... .....@.....@.8...@.....$.....!.....!.....'.....G..... .....@.....@.....P.td.....D.....Q.td.....NaCl....x86-64.....GNU.0.m=F>k....&...i..... ..0C.....0C..0C..0E.....0C.....0E.-DT.!.?.-DT.!.....?.....-DT.!...-DT.!.?.....?.....?.....?."..."..."..."....@.....`..... ...@...`..... ....@...`..... ...@...`..... ...@...`.....`...`.....@...@..... ....1..`3.. 4..`-..`-...:...:...F..@H..`H...H...F...F...G...H.. H. ..F..@G...I.. I..@I..@G...G...I...I...J...G..`I..

C:\Users\user\AppData\Local\Temp\3212_2067475749_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=4b15de4ab227d5e46213978b8518d53c53ce1db9, stripped
Category:	dropped
Size (bytes):	1901720
Entropy (8bit):	5.955741933854651
Encrypted:	false
SSDEEP:	12288:gXqUSpBjwQO2o8k+7zjidg4euCAauOILffvCpGy4Wh3BTFmHpq82K2/KsvPyla9d:gafZwcOdNe2auOepCBTFmJq3Kf8ksr
MD5:	9DC3172630E525854B232FF71499D77C
SHA1:	0082C58EDCE3769E90DB48E7C26090CE706AD434
SHA-256:	6AA1DA6C264E0AF4E32A004F4076C7557C6AC6D9C38B0C5DE97302D83FA248C3
SHA-512:	9E9584241A39EED1463D7D4C1B26AE570B839AA315778FF3400C61341EBA43B630307DE9F1532A265CA82EA69BDEA03EC9D963E59A18569C02DA8285449870FE
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	.ELF.....>.... .....@.....@.8...@.....0.....0.....Y..... .....@.....@.....P.td....t^.....t^.....t^.....W.....W.....Q.td.....NaCl....x86-64.....GNU.K..J.'..b.....<S...`...`.... ...@... @.....@.....Y@.....p.....@.....?.....?.....A.....5.....?5.5...?.5.....?.....P9.....PC.....?.....0@.....aCoc...?..`.(..? .y.P.D.?<.s..O.u.....$@.....@.....@`..`.....@..... ...`.. ... .`..... ... ...@...`.....@... Z...[...[...e..... ...@... ...@.. .`.....0...0...2..`4.. 6...7...9...~...~...z...{...{..

C:\Users\user\AppData\Local\Temp\3212_2067475749\manifest.fingerprint	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	3.928261499316817
Encrypted:	false

C:\Users\user\AppData\Local\Temp\3212_2067475749\manifest.fingerprint	
SSDEEP:	3:STDLGswXEVBcVdBiTDt3zLsW:SPLGLErcVdBiDtf3
MD5:	C00BCE97F21B1AD61EB9B8CD001795EE
SHA1:	8E0392FF3DB267D847711C3F4E0D7468060E1535
SHA-256:	59F06F04230E32E8BC839F45B984D31D611930427B631C963D09E7064A602363
SHA-512:	9930E44A6ECC62505DBADCEED5E05645909FF09816FB12AAC0414E6D2830AC09758366C3B7D4EDD7839C87EB16DFA4C66D8981AE6237D408B37135C3506F4C2
Malicious:	false
Reputation:	low
Preview:	1.6f6bc93dcd62dc251850d2ff458fda96083ceb7fbe8eeb11248b8485ef2aea23

C:\Users\user\AppData\Local\Temp\3212_2067475749\manifest.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	573
Entropy (8bit):	4.859567579783832
Encrypted:	false
SSDEEP:	12:BLqG6yDJmL4mLDlG9hQ181G46XzrXc+EFfNqpaiOc+T5NqXIOclNqXL:BkylmL4mLDlJ18116XsRNqtZeNqXIZlE
MD5:	1863B86D0863199AFDA179482032945F
SHA1:	36F56692E12F2A1EFCA7736C236A8D776B627A86
SHA-256:	F14E451CE2314D29087B8AD0309A1C8B8E81D847175EF46271E0EB49B4F84DC5
SHA-512:	836556F3D978A89D3FC1F07FCED2732A17E314ED6A021737F087E32A69BFA46FD706EBBDFD3607FF42EDCB75DC463C29B9D9D2F122504F567BB95844F579831
Malicious:	false
Reputation:	low
Preview:	{."update_url": "https://clients2.google.com/service/update2/crx",.. "description": "Portable Native Client Translator Multi-CRX",.. "name": "PNaCl Translator Multi-CRX",.. "manifest_version": 2,.. "minimum_chrome_version": "30.0.0.0",.. "version": "0.57.44.2492",.. "platforms": [.. {.. "nacl_arch": "x86-32",.. "sub_package_path": "_platform_specific/x86_32/".. },.. {.. "nacl_arch": "x86-64",.. "sub_package_path": "_platform_specific/x86_64/".. },.. {.. "nacl_arch": "arm",.. "sub_package_path": "_platform_specific/arm/".. }..].}.

C:\Users\user\AppData\Local\Temp\7ea04feb-9187-4211-835c-bf698fef281c.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
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.$.....I-m.....m....ni...`..W.....R.p.b.+...+.\k.R$e~.J\.&c%.d...M..j..V.%...+1F....D....X\.1ct.<.....E.B.+.i@...8..^...&YR...I.o...,.....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-I..`.Q.{...F0D. D.'.N@.(..GK....m...A.0.."

C:\Users\user\AppData\Local\Temp\scoped_dir3212_1596502370\7ea04feb-9187-4211-835c-bf698fef281c.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\scoped_dir3212_1596502370\7ea04feb-9187-4211-835c-bf698fef281c.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\scoped_dir3212_1596502370\CRX_INSTALL_locales\am\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17307
Entropy (8bit):	5.461848619761356
Encrypted:	false
SSDEEP:	384:arfbEVrFvMP4rMhuDopC3vUuFBYZV6uml:aHEVrFvMP4KuFvr6D6uml
MD5:	26330929DF0ED4E86F06C00C03F07CE3
SHA1:	478F3B7E7A7E007BEE182B89C2EF6FFE6045E92C
SHA-256:	621B5139ED199022BB6529AF18ED4DC312AE9F3E90ECAF3B2C9E1D12114F5B22
SHA-512:	0BE6183A1BF12575C0F99960705D4249E79CDB8528C55FF132BE99A111F09494231AD6A36CD61B090A3B34C6971D68A29373BA346888E852C52E05DC14380682
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "....".. },.. "1213957982723875920": {.. "message": "..... ... .?".. },.. "1282768764603190 75": {.. "message": "..... ...".. },.. "1428448869078126731": {.. "message": ".... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "... ...".. },.. "1802762746589457177": {.. "message": "...".. },.. "1850397500312020388": {.. "message": ".$START_LINK$Google Home .....END_LINK ... . Chromecast ....? $START_SPAN$*END_SPAN",.. "placeholde

C:\Users\user\AppData\Local\Temp\scoped_dir3212_1596502370\CRX_INSTALL_locales\ar\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	16809
Entropy (8bit):	5.458147730761559
Encrypted:	false
SSDEEP:	192:0lprKC78JmUjk8RkeryFOYPATxLZ8fsbE3/IFV6c8TEKdl:Jrp8JjA8RkerK0lc3wFV6uml
MD5:	44325A88063573A4C77F6EF943B0FC3E
SHA1:	78908D766F3E7A0E4545E7BD823C8ED47C7164EB
SHA-256:	67A439A08804EF4BEF261BDBADD8F0FEFD51729167D01EDCA99DD4AF57D6108B
SHA-512:	889C02BC986794C58C76022E78F57F867DD1D5217687F12D679A33A2DB9E5A18F3A37CF94D8FE4585E747C78E4662EAB93361FF7D945990774C7CFCACCFB79D
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "....".. },.. "1213957982723875920": {.. "message": ".. .. ..".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": "....".. },.. "1636686747687494376": {.. "message": "......".. },.. "1802762746589457177": {.. "message": "..... .....".. },.. "1850397500312020388": {.. "message": "... .... Chromecast .. $START_LINK$..... Google HomeEND_LINK. $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {..

C:\Users\user\AppData\Local\Temp\scoped_dir3212_1596502370\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	18086
Entropy (8bit):	5.408731329060678
Encrypted:	false
SSDEEP:	192:4jjpr342SlwPIasR9VhMkACVmrv8evj+3eXivOMbb2vVzCkwRV6V6c8TEKdl:4ZrYo+rxT+qOV6V6uml
MD5:	6911CE87E8C47223F33BEF9488272E40
SHA1:	980398F076BB7D451B18D7FDE2DE09041B1F55AD
SHA-256:	273DEF0F67F0FA080802B85EF6F334DE50A19408F46BDF41F0F099B1F5501EEA
SHA-512:	CDB69405BB553E46DCF02F71B1A394307D0051E7FA662DFFEBA7888F30DD933F13C7FD6E32F1D7AEAEE8746316873B6E1D92029724ABDC75E49DCC092172EA2
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "......".. },.. "1213957982723875920": {.. "message": "... .. ..-..... ....?".. },.. "12827687 6460319075": {.. "message": "..... .. ..".. },.. "1428448869078126731": {.. "message": "..... .. ..".. },.. "1522140683318860351": {.. "message": "..... .. .., ...".. },.. "1550904064710828958": {.. "message": "......".. },.. "1636686747687494376": {.. "message": "......".. },.. "18027627 46589457177": {.. "message": ".... .. ..".. },.. "1850397500312020388": {.. "message": "..... .. .. Chromecast . $START_LINK$..... Google Hom eEND_LINK? $START_SPAN$*END_SPAN",.. "p

C:\Users\user\AppData\Local\Temp\scoped_dir3212_1596502370\CRX_INSTALL_locales\bn\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	19695
Entropy (8bit):	5.315564774032776
Encrypted:	false
SSDEEP:	384:PrUCrcTIOeswIW/Vre/sZn8TFfzheV6uml:lPswIWtoK8xfG6uml
MD5:	F9DDF525C07251282A3BFFCEE9A09ABB
SHA1:	A343A078E804AF400A8F3E1891E3390DA754A5CD
SHA-256:	C69C6C90F7EB8F10685CD815AF1F6F1B87CF30C4E8D95DF1D577DE1105AAD227
SHA-512:	EBD339C37162984672513019D470B92DF8B743DD69D4430361EF12D42FD1C208DBDE818A7BFE20BE8A7D63CD6E02B3F4344DEA1C4AEDB8719D789981A49DA4C
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "..... ...".. },.. "1213957982723875920": {.. "message": "..... ....?".. },.. "128276876460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... ....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": ".....".. },.. "1850397500312020388": {.. "message": "$START_LINK$ Google

C:\Users\user\AppData\Local\Temp\scoped_dir3212_1596502370\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15518
Entropy (8bit):	5.242542310885
Encrypted:	false
SSDEEP:	384:drGUBKxMF2ayv8FrIccUVFmwf+7d9VKS3V6uml:dCUBKxMFBy0FE3UzmQ+zkSl6uml
MD5:	A90CF7930E7C3BEC61EE252DEFAD574A
SHA1:	F630CA01114A7BDD39607CB84B8280CCE218A5C6
SHA-256:	A533740E17559E2ADF40B4555C60F21EEC84E92C09CDBC19EED033A0B4DD2474
SHA-512:	598F991B344FA6724617D6CE57BB0D6D64EF86B4F5317BF6AD5EDF43E6B0A385094E7885F7A8FA2B107405B31C3D9F76E92315BC1D9BB52ACD4ECAD342917DE1
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Es congela".. },.. "1213957982723875920": {.. "message": "Quina de les opcions.seg.ents descriu millor la vostra xarxa?".. },.. "128276876460319075": {.. "message": "Detecci. de dispositius".. },.. "1428448869078126731": {.. "message": "Flu.desa del v.deo".. },.. "1522140683318860351": {.. "message": "S'ha produ.t un error en la connexi.. Torneu-ho a provar.".. },.. "1550904064710828958": {.. "message": "Correcta".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volum".. },.. "1850397500312020388": {.. "message": "Pots veure el Chromecast a l'$START_LINK$aplicaci. Google.HomeEND_LINK?$START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "

C:\Users\user\AppData\Local\Temp\scoped_dir3212_1596502370\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15552
Entropy (8bit):	5.406413558584244
Encrypted:	false
SSDEEP:	192:eVdprJrG5efiTk93ebrxZR1fdc8VDCwT9fTV6c8TEKdl:2rMqiQerxQ88W7V6uml
MD5:	17E753EE877FDED25886D5F7925CA652
SHA1:	8E4EC969777CC0CEB7C12D0C1B9D87EBBB9C4678
SHA-256:	C562FCCFCE374D446BFAC30AC9B18FF17E7A3EF101C919FF857104917F300382
SHA-512:	33D61F6327FC81D7A45AA2CC97922DC527F5F43E54AA1A1638DA6EE407024A2F10CFD82CC5C3C581C2E7B216276987CB26C3FA95198572E139ACF29CC5B7ADB
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Video zamrz.".. },.. "1213957982723875920": {.. "message": "Kter. popis nejl.pe vystihuje va.i s..?".. },.. "128276876460319075": {.. "message": "Zji..ov.n. za..zen.".. },.. "1428448869078126731": {.. "message": "Plynulost videa".. },.. "1522140683318860351": {.. "message": "P.ipojen. se nezda.ilo. Zkuste to pros.m znovu.".. },.. "1550904064710828958": {.. "message": "Plynul.".. },.. "1636686747687494376": {.. "message": "Perfektn.".. },.. "1802762746589457177": {.. "message": "Hlasitost".. },.. "1850397500312020388": {.. "message": "Vid.te sv.j Chromecast v.$START_LINK$aplikaci Google Home END_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

C:\Users\user\AppData\Local\Temp\scoped_dir3212_1596502370\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Temp\scoped_dir3212_1596502370\CRX_INSTALL_locales\da\messages.json	
Size (bytes):	15340
Entropy (8bit):	5.2479291792849105
Encrypted:	false
SSDEEP:	192:+Upr8XnI1MY2kPuir8j7Rd3kbTWc4QtV6c8TEKdl:FrJ1H9br8h6eZCV6uml
MD5:	F08A313C78454109B629B37521959B33
SHA1:	3D585D52EC8B4399F66D4BE88CED10F4A034FCCC
SHA-256:	23BF7E5EDF70291CA6D8F4A64788C5B86379EECB628E3DFA7DD83344612F7564
SHA-512:	9F2868AEBBF7F6167A7EA120FE65E752F9A65D1DC51072AA2413B2FDE374DA2D169D455A4788E341717F694179E6F1FA80413C080D9CD8CB397C3E84668CBFE
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "Fryser".. },.. "1213957982723875920": {.. "message": "Hvilket af f.lgende udsagn beskriver bedst dit netv.rk?".. },.. "128276876460319075": {.. "message": "Enhedsregistrering".. },.. "1428448869078126731": {.. "message": "Videostabilitet".. },.. "152214068331 8860351": {.. "message": "Forbindelsen blev afbrudt. Pr.v igen.".. },.. "1550904064710828958": {.. "message": "Problemfri".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lydstyrke".. },.. "1850397500312020388": {.. "message": "Kan du se din Chromecast i $ START_LINK$ Google Home-appenEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "STAR

C:\Users\user\AppData\Local\Temp\scoped_dir3212_1596502370\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15555
Entropy (8bit):	5.258022363187752
Encrypted:	false
SSDEEP:	192:AJprM71A4qyJSwlk5KR5rtXsmvL0xhVw921YV6c8TEKdl:2re3jJS5A5rt8msA2KV6uml
MD5:	980FB419ED6ED94AD75686AFFB4E4C2E
SHA1:	871BFBCA6BCBA9197811883A93C50C0716562D57
SHA-256:	585C7814AFD2453232BC940252D4AE821D6E6CBCFD74A793F78E5DB8BA5342F1
SHA-512:	1681FA9C3BA882250A5005FB807D759EB8A634F1AA011725B1C865C0028BE7AB7BC16DC821A7F5BBFBA84C91E7D663ADE715284798E7E84E8FFF2D254488882
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "H.ngenbleiben".. },.. "1213957982723875920": {.. "message": "Welche dieser Aussagen beschreibt dein Netzwerk am besten?".. },.. "128276876460319075": {.. "message": "Ger.teerkennung".. },.. "1428448869078126731": {.. "message": "Videowiedergabequalit.t".. },.. "1522140683318860351": {.. "message": "Fehler beim Herstellen der Verbindung. Bitte versuche es noch einmal.".. },.. "1550904064710828958": {.. "message": "St.rungsfrei".. },.. "1636686747687494376": {.. "message": "Perfekt".. },.. "1802762746589457177": {.. "message": "Lautst.rke".. },.. "18503975003 12020388": {.. "message": "Siehst du deinen Chromecast in der $START_LINK$Google Home AppEND_LINK? $START_SPAN$*END_SPAN",.. "placeholde rs": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.

C:\Users\user\AppData\Local\Temp\scoped_dir3212_1596502370\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17941
Entropy (8bit):	5.465343004010711
Encrypted:	false
SSDEEP:	384:S0rDuhLh41cZrP3TzDBknbpgo6djlV6uml:S0fuBh46ZD3TzDinbpgoUK6uml
MD5:	40EB778339005A24FF9DA775D56E02B7
SHA1:	B00561CC7020F7FE717B5F692884253C689A7C61
SHA-256:	F56BF7C171AA20038EE30B754478B69A98F3014C89362779B0A8788C7B9BEEE1
SHA-512:	8BED281A33EC1E4E88A9F9D62BB13FE0266C0FAF8856D1DC2A843D26DD3CE5E7D1400FD3325ABD783B0364EC4FB1188AD941D56AEB9073BC365BE0D12DE6C 013
Malicious:	false
Reputation:	low
Preview:	{.. "1018984561488520517": {.. "message": "......".. },.. "1213957982723875920": {.. "message": ".... ... .;".. },.. "1282768 76460319075": {.. "message": "..... .....".. },.. "1428448869078126731": {.. "message": "..... .....".. },.. "1522140683318860351": {.. "message": "..... ....".. },.. "1550904064710828958": {.. "message": ".....".. },.. "1636686747687494376": {.. "message": ".....".. },.. "1802762746589457177": {.. "message": "..... ....".. },.. "1850397500312020388": {.. "message": "..... .. .. Chromecast .... $START_LINK$..... Google HomeEND_LINK; $START_SPAN $*$END_SPAN$",.. "placeholders": {.. "END_LINK": {.. "content

C:\Users\user\AppData\Local\Temp\scoped_dir3212_1596502370\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	14897
Entropy (8bit):	5.197356586852831
Encrypted:	false

C:\Users\user\AppData\Local\Temp\scoped_dir3212_1596502370\CRX_INSTALL_locales\en\messages.json	
SSDEEP:	96:2MKUOp5N7GTNMRuv6M0blt3FXGkW6/5NkkQ9NJKJhnH3t9F410sUA+ISN6cGDSyR:VKzprogudTGkWqrKcJhdIR+V6c8TEKdl
MD5:	8351AF4EA9BDD9C09019BC85D25B0016
SHA1:	F6EC1FFD291C8632758E01C9EE837B1AD18D4DCF
SHA-256:	F41C82D8A4F0E9B645656D630C882BE94A0FB7F8CEC0FE864B57298F0312B212
SHA-512:	75672B57F21F38F97341AD76A199AD764E9FBAB2384D701BF6EB06CEFDE6C4F20F047F9051A4E30D99621E5C1FBBDB9E38E8D2B47470806704B38DA130A146C
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205l7": {.. "message": "Freezes".. },.. "12139579827238759 20": {.. "message": "Which of the following best describes your network?".. },.. "128276876460319075": {.. "message": "Device Discovery".. },.. "1428448869078126731": {.. "message": "Video Smoothness".. },.. "1522140683318860 351": {.. "message": "Connection failed. Please try again.".. },.. "1550904064710828958": {.. "message": "Smooth".. },.. "1636686747687494376": {.. "message": "Perfect".. },.. "1802762746589457177": {.. "message": "Volume".. },.. "1850397500312020388": {.. "message": "Are you able to see your Chrom ecast in the $START_LINK$ Google Home appEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3".. },.. "START

C:\Users\user\AppData\Local\Temp\scoped_dir3212_1596502370\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15560
Entropy (8bit):	5.236752363299121
Encrypted:	false
SSDEEP:	192:NAgprfy1pTCukFr+1DIyDRoanvV6c8TEKdl:KMrq6FrmvV6uml
MD5:	8A70C18BB1090AA4D500DE9E8E4A00EF
SHA1:	8AFC097FA956C1317DB0835348B2DA19F0789669
SHA-256:	FF173D1CEF665B1234E02F11070ABD2B65230318150734579A03C7F31B4AE3F4
SHA-512:	140BAF40A4ABE9B8AF0855B0EBB7DFDF17869EDFC4EE1037C5EA7FDD8EDEBD4850E055B6A4D7B8782657618BCE1517813779BA01BA993CC838BB43E0BE71E EEE
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205l7": {.. "message": "Congelaci.n de im.genes".. },.. "1213957982723875920": {.. "message": ".Cu.l de las siguientes respuestas descr ibe mejor tu red?".. },.. "128276876460319075": {.. "message": "Detecci.n de dispositivo".. },.. "1428448869078126731": {.. "message": "Fluidez del v.deo".. },.. "1522140683318860351": {.. "message": "Error en la conexi.n. Vuelve a intentarlo.".. },.. "1550904064710828958": {.. "message": "V.deo fluido".. },.. "1636686747687494376": {.. "message": "Perfecta".. },.. "1802762746589457177": {.. "message": "Volumen".. },.. "1850397500312020388": {.. "message": ".Puedes ver tu Chromecast en la $START_LINK$aplicaci.n Google.HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "content": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {..

C:\Users\user\AppData\Local\Temp\scoped_dir3212_1596502370\CRX_INSTALL_locales\et\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	15139
Entropy (8bit):	5.228213017029721
Encrypted:	false
SSDEEP:	96:Z48bxhWYp5Ny5M63niwAKD4rrJSJ2RkPXh9P5NFP2+NBMU01jewUEVez3QOiSevy:ikxprot3lYkf/rHBc0KsUV6c8TEKdl
MD5:	A62F12BCBA6D2C579212CA2FF90F8266
SHA1:	F7E964A2D9BBDA364252BCE5CFBA3FD34FDD825E
SHA-256:	3EB3EB0B3B4A8E5A477D1B3C3A3891CCC7DC6B8879ECE243A7BD7C478068273D
SHA-512:	E300201245C00ADEC8F39D586875F8FA4607AB203572BF3CE353C1CA7CDCA05B8786810CA0CEE27E4EA54A5EFD53690F1EA7AA4148CFF472A66BB1120272356 6
Malicious:	false
Reputation:	low
Preview:	{.. "10189845614885205l7": {.. "message": "Hangub".. },.. "1213957982723875920": {.. "message": "Milline j.rgmistest v.idetest kirjeldab k.ige paremini teie v.rku?".. },.. "128276876460319075": {.. "message": "Seadme tuvastamine".. },.. "1428448869078126731": {.. "message": "Video sujuvus".. },.. "152 2140683318860351": {.. "message": ".hendamine eba.nnestus. Proovige uuesti.".. },.. "1550904064710828958": {.. "message": ".htlane".. },.. "163668674768 7494376": {.. "message": "T.iuslik".. },.. "1802762746589457177": {.. "message": "Helitugevus".. },.. "1850397500312020388": {.. "message": "Kas n.ete oma Chromecasti $START_LINK$rakenduses Google HomeEND_LINK? $START_SPAN$*END_SPAN",.. "placeholders": {.. "END_LINK": {.. "conte nt": "$1".. },.. "END_SPAN": {.. "content": "$2".. },.. "START_LINK": {.. "content": "$3"..

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
Oct 25, 2021 15:47:09.729836941 CEST	192.168.2.5	8.8.8.8	0xac19	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:09.732521057 CEST	192.168.2.5	8.8.8.8	0x93ed	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:09.734330893 CEST	192.168.2.5	8.8.8.8	0x4640	Standard query (0)	stg-client relations.equalityhealth.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:24.005846977 CEST	192.168.2.5	8.8.8.8	0x605d	Standard query (0)	stg-client relations.equalityhealth.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:30.624794006 CEST	192.168.2.5	8.8.8.8	0x1c5d	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:47.856336117 CEST	192.168.2.5	8.8.8.8	0x18fc	Standard query (0)	docs.atlassian.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:48.420273066 CEST	192.168.2.5	8.8.8.8	0xa7c6	Standard query (0)	confluence.atlassian.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:49.787873030 CEST	192.168.2.5	8.8.8.8	0x66a4	Standard query (0)	cdn.cookielaw.org	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:49.791692019 CEST	192.168.2.5	8.8.8.8	0x54f1	Standard query (0)	polyfill.io	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:49.795130014 CEST	192.168.2.5	8.8.8.8	0x92f	Standard query (0)	cdn.evgnet.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:50.658108950 CEST	192.168.2.5	8.8.8.8	0x7004	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:51.017780066 CEST	192.168.2.5	8.8.8.8	0x2644	Standard query (0)	cdn.optimizely.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:51.150428057 CEST	192.168.2.5	8.8.8.8	0x95aa	Standard query (0)	geolocation.onetrust.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:51.390923023 CEST	192.168.2.5	8.8.8.8	0x3672	Standard query (0)	api.demandbase.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:51.492783070 CEST	192.168.2.5	8.8.8.8	0x909	Standard query (0)	a1096093.cdn.optimizely.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:51.525382996 CEST	192.168.2.5	8.8.8.8	0x2376	Standard query (0)	api-private.atlassian.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:52.134377956 CEST	192.168.2.5	8.8.8.8	0xd34b	Standard query (0)	atl-global.atlassian.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:52.440105915 CEST	192.168.2.5	8.8.8.8	0xf007	Standard query (0)	logx.optimizely.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:53.013835907 CEST	192.168.2.5	8.8.8.8	0x48bf	Standard query (0)	xxid.atl-paas.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:53.036331892 CEST	192.168.2.5	8.8.8.8	0xf204	Standard query (0)	app.launchdarkly.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:53.042807102 CEST	192.168.2.5	8.8.8.8	0x6d1a	Standard query (0)	events.launchdarkly.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:53.413634062 CEST	192.168.2.5	8.8.8.8	0xf4ba	Standard query (0)	confluence.atlassian.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:55.362999916 CEST	192.168.2.5	8.8.8.8	0x8ca5	Standard query (0)	web-analytics.engagio.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:57.406419992 CEST	192.168.2.5	8.8.8.8	0x438c	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:57.555008888 CEST	192.168.2.5	8.8.8.8	0x499	Standard query (0)	munchkin.marketo.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:57.663969994 CEST	192.168.2.5	8.8.8.8	0x911	Standard query (0)	dn1f1hmdujj40.cloudfront.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:57.800077915 CEST	192.168.2.5	8.8.8.8	0x7026	Standard query (0)	594-atc-127.mktoresp.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 25, 2021 15:47:57.840693951 CEST	192.168.2.5	8.8.8.8	0xbffb	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:58.012434959 CEST	192.168.2.5	8.8.8.8	0x3363	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:58.016608000 CEST	192.168.2.5	8.8.8.8	0x3b6b	Standard query (0)	www.google.fr	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:00.268840075 CEST	192.168.2.5	8.8.8.8	0x9525	Standard query (0)	www.atlassian.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:00.838838100 CEST	192.168.2.5	8.8.8.8	0xb2bb	Standard query (0)	wac-cdn.atlassian.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:00.841470957 CEST	192.168.2.5	8.8.8.8	0xfe45	Standard query (0)	wac-cdn-2.atlassian.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:00.903938055 CEST	192.168.2.5	8.8.8.8	0x5275	Standard query (0)	metal.prod.atl-paas.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:03.297733068 CEST	192.168.2.5	8.8.8.8	0x19d0	Standard query (0)	tapi.optimizely.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:04.148710012 CEST	192.168.2.5	8.8.8.8	0x4e0	Standard query (0)	client.px-cloud.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:04.204617977 CEST	192.168.2.5	8.8.8.8	0x6c7c	Standard query (0)	api.segment.io	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:04.939126015 CEST	192.168.2.5	8.8.8.8	0x5f3c	Standard query (0)	collector-pxvryik386.px-cloud.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:06.130630016 CEST	192.168.2.5	8.8.8.8	0x37d5	Standard query (0)	api.atlassian.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:06.659080029 CEST	192.168.2.5	8.8.8.8	0xb47a	Standard query (0)	cdn-mr.contentful.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:08.655776978 CEST	192.168.2.5	8.8.8.8	0x7778	Standard query (0)	wac-cdn-2.atlassian.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:10.465946913 CEST	192.168.2.5	8.8.8.8	0x1160	Standard query (0)	stg-client relations.equalityhealth.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:23.366857052 CEST	192.168.2.5	8.8.8.8	0x96f9	Standard query (0)	www.youtube.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.230340004 CEST	192.168.2.5	8.8.8.8	0xe1d0	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.294209957 CEST	192.168.2.5	8.8.8.8	0x794	Standard query (0)	5406241.fls.doubleclick.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.344858885 CEST	192.168.2.5	8.8.8.8	0x8924	Standard query (0)	scripts.demandbase.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.345779896 CEST	192.168.2.5	8.8.8.8	0xf9ec	Standard query (0)	platform.twitter.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.348462105 CEST	192.168.2.5	8.8.8.8	0x1b8b	Standard query (0)	cdnssl.clicktale.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.350169897 CEST	192.168.2.5	8.8.8.8	0xa4d0	Standard query (0)	cdn.bizible.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.384754896 CEST	192.168.2.5	8.8.8.8	0x8afc	Standard query (0)	www.redditstatic.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.445419073 CEST	192.168.2.5	8.8.8.8	0x3688	Standard query (0)	pixel.pointmediatracker.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.460398912 CEST	192.168.2.5	8.8.8.8	0x531b	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.787705898 CEST	192.168.2.5	8.8.8.8	0x612d	Standard query (0)	adservice.google.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.791232109 CEST	192.168.2.5	8.8.8.8	0xf58a	Standard query (0)	static.ads-twitter.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:26.290976048 CEST	192.168.2.5	8.8.8.8	0x4e33	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:26.501579046 CEST	192.168.2.5	8.8.8.8	0x228b	Standard query (0)	cnv.event.prod.bidr.io	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.007941008 CEST	192.168.2.5	8.8.8.8	0x708c	Standard query (0)	alb.reddit.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.056184053 CEST	192.168.2.5	8.8.8.8	0x92ae	Standard query (0)	match.prod.bidr.io	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.062262058 CEST	192.168.2.5	8.8.8.8	0x83cf	Standard query (0)	id.rlcdn.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.096086979 CEST	192.168.2.5	8.8.8.8	0xfb6d	Standard query (0)	analytics.twitter.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.189408064 CEST	192.168.2.5	8.8.8.8	0xc26	Standard query (0)	t.co	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.328164101 CEST	192.168.2.5	8.8.8.8	0x6758	Standard query (0)	api.company-target.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 25, 2021 15:48:27.337672949 CEST	192.168.2.5	8.8.8.8	0xb24f	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.479011059 CEST	192.168.2.5	8.8.8.8	0x760c	Standard query (0)	cdn.bizibly.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.570929050 CEST	192.168.2.5	8.8.8.8	0x52c	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.909363031 CEST	192.168.2.5	8.8.8.8	0x6c34	Standard query (0)	ing-district.clicktale.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.944413900 CEST	192.168.2.5	8.8.8.8	0x8b59	Standard query (0)	c.clicktale.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.959156990 CEST	192.168.2.5	8.8.8.8	0x1387	Standard query (0)	segments.company-target.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:28.596369028 CEST	192.168.2.5	8.8.8.8	0x4a50	Standard query (0)	p.adsymptotic.com	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:33.621453047 CEST	192.168.2.5	8.8.8.8	0x1771	Standard query (0)	adservice.google.fr	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:34.081753969 CEST	192.168.2.5	8.8.8.8	0xb252	Standard query (0)	errors.client.optimizely.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 15:47:09.747565985 CEST	8.8.8.8	192.168.2.5	0xac19	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:47:09.747565985 CEST	8.8.8.8	192.168.2.5	0xac19	No error (0)	clients.l.google.com		142.250.186.174	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:09.754123926 CEST	8.8.8.8	192.168.2.5	0x4640	No error (0)	stg-clientrelations.equalityhealth.com		76.9.179.216	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:09.758776903 CEST	8.8.8.8	192.168.2.5	0x93ed	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:24.022233963 CEST	8.8.8.8	192.168.2.5	0x605d	No error (0)	stg-clientrelations.equalityhealth.com		76.9.179.216	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:30.649651051 CEST	8.8.8.8	192.168.2.5	0x1c5d	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:47:30.649651051 CEST	8.8.8.8	192.168.2.5	0x1c5d	No error (0)	googlehosted.l.googleusercontent.com		172.217.168.33	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:47.876756907 CEST	8.8.8.8	192.168.2.5	0x18fc	No error (0)	docs.atlassian.com		185.166.143.0	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:47.876756907 CEST	8.8.8.8	192.168.2.5	0x18fc	No error (0)	docs.atlassian.com		185.166.143.2	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:47.876756907 CEST	8.8.8.8	192.168.2.5	0x18fc	No error (0)	docs.atlassian.com		185.166.143.1	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:48.444622040 CEST	8.8.8.8	192.168.2.5	0xa7c6	No error (0)	confluence.atlassian.com	confluence.prd.cst.atlassian.com		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:47:48.444622040 CEST	8.8.8.8	192.168.2.5	0xa7c6	No error (0)	confluence.prd.cst.atlassian.com	d3lzof3wnsn9tm.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:47:48.444622040 CEST	8.8.8.8	192.168.2.5	0xa7c6	No error (0)	d3lzof3wnsn9tm.cloudfront.net		54.192.66.67	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:48.444622040 CEST	8.8.8.8	192.168.2.5	0xa7c6	No error (0)	d3lzof3wnsn9tm.cloudfront.net		54.192.66.84	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:48.444622040 CEST	8.8.8.8	192.168.2.5	0xa7c6	No error (0)	d3lzof3wnsn9tm.cloudfront.net		54.192.66.98	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:48.444622040 CEST	8.8.8.8	192.168.2.5	0xa7c6	No error (0)	d3lzof3wnsn9tm.cloudfront.net		54.192.66.55	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:49.807889938 CEST	8.8.8.8	192.168.2.5	0x66a4	No error (0)	cdn.cookielaw.org		104.16.148.64	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 15:47:49.807889938 CEST	8.8.8.8	192.168.2.5	0x66a4	No error (0)	cdn.cookielaw.org		104.16.149.64	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:49.809500933 CEST	8.8.8.8	192.168.2.5	0x54f1	No error (0)	polyfill.io		151.101.1.26	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:49.809500933 CEST	8.8.8.8	192.168.2.5	0x54f1	No error (0)	polyfill.io		151.101.129.26	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:49.809500933 CEST	8.8.8.8	192.168.2.5	0x54f1	No error (0)	polyfill.io		151.101.65.26	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:49.809500933 CEST	8.8.8.8	192.168.2.5	0x54f1	No error (0)	polyfill.io		151.101.193.26	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:49.813139915 CEST	8.8.8.8	192.168.2.5	0x92f	No error (0)	cdn.evgnet.com		151.101.64.114	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:49.813139915 CEST	8.8.8.8	192.168.2.5	0x92f	No error (0)	cdn.evgnet.com		151.101.0.114	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:49.813139915 CEST	8.8.8.8	192.168.2.5	0x92f	No error (0)	cdn.evgnet.com		151.101.128.114	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:49.813139915 CEST	8.8.8.8	192.168.2.5	0x92f	No error (0)	cdn.evgnet.com		151.101.192.114	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:50.676579952 CEST	8.8.8.8	192.168.2.5	0x7004	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:47:51.039429903 CEST	8.8.8.8	192.168.2.5	0x2644	No error (0)	cdn.optimizely.com	cdn.o6.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:47:51.170244932 CEST	8.8.8.8	192.168.2.5	0x95aa	No error (0)	geolocation.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:51.170244932 CEST	8.8.8.8	192.168.2.5	0x95aa	No error (0)	geolocation.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:51.413198948 CEST	8.8.8.8	192.168.2.5	0x3672	No error (0)	api.demandbase.com		216.137.37.71	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:51.413198948 CEST	8.8.8.8	192.168.2.5	0x3672	No error (0)	api.demandbase.com		216.137.37.66	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:51.413198948 CEST	8.8.8.8	192.168.2.5	0x3672	No error (0)	api.demandbase.com		216.137.37.62	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:51.413198948 CEST	8.8.8.8	192.168.2.5	0x3672	No error (0)	api.demandbase.com		216.137.37.35	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:51.512819052 CEST	8.8.8.8	192.168.2.5	0x909	No error (0)	a1096093.cdn.optimizely.com	wildcard.cdn.optimizely.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:47:51.543951988 CEST	8.8.8.8	192.168.2.5	0x2376	No error (0)	api-private.atlassian.com	global.stargate.cse.ss-inf.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:47:51.543951988 CEST	8.8.8.8	192.168.2.5	0x2376	No error (0)	global.stargate.cse.ss-inf.net		18.184.99.132	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:51.543951988 CEST	8.8.8.8	192.168.2.5	0x2376	No error (0)	global.stargate.cse.ss-inf.net		18.184.99.131	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:51.543951988 CEST	8.8.8.8	192.168.2.5	0x2376	No error (0)	global.stargate.cse.ss-inf.net		18.184.99.133	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:52.175607920 CEST	8.8.8.8	192.168.2.5	0xd34b	No error (0)	atl-global.atlassian.com	atl-global-static.us-east-1.prod.public.atl-paas.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:47:52.175607920 CEST	8.8.8.8	192.168.2.5	0xd34b	No error (0)	atl-global-static.us-east-1.prod.public.atl-paas.net	dnyjdqemy55m3.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:47:52.175607920 CEST	8.8.8.8	192.168.2.5	0xd34b	No error (0)	dnyjdqemy55m3.cloudfront.net		216.137.37.113	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 15:47:52.175607920 CEST	8.8.8.8	192.168.2.5	0xd34b	No error (0)	dnyjdqemy55m3.cloudfront.net		216.137.37.59	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:52.175607920 CEST	8.8.8.8	192.168.2.5	0xd34b	No error (0)	dnyjdqemy55m3.cloudfront.net		216.137.37.64	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:52.175607920 CEST	8.8.8.8	192.168.2.5	0xd34b	No error (0)	dnyjdqemy55m3.cloudfront.net		216.137.37.55	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:52.460042953 CEST	8.8.8.8	192.168.2.5	0xf007	No error (0)	logx.optimizely.com	p13nlog-1106815646.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:47:52.460042953 CEST	8.8.8.8	192.168.2.5	0xf007	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		34.197.14.190	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:52.460042953 CEST	8.8.8.8	192.168.2.5	0xf007	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		35.174.227.42	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:52.460042953 CEST	8.8.8.8	192.168.2.5	0xf007	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		3.208.75.90	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:52.460042953 CEST	8.8.8.8	192.168.2.5	0xf007	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		54.147.196.25	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:52.460042953 CEST	8.8.8.8	192.168.2.5	0xf007	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		34.203.177.41	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:52.460042953 CEST	8.8.8.8	192.168.2.5	0xf007	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		52.55.122.255	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:52.460042953 CEST	8.8.8.8	192.168.2.5	0xf007	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		54.84.52.201	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:52.460042953 CEST	8.8.8.8	192.168.2.5	0xf007	No error (0)	p13nlog-1106815646.us-east-1.elb.amazonaws.com		52.55.216.247	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:53.035471916 CEST	8.8.8.8	192.168.2.5	0x48bf	No error (0)	xxid.atl-paas.net	d1jpmzxkzfzfaz.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:47:53.035471916 CEST	8.8.8.8	192.168.2.5	0x48bf	No error (0)	d1jpmzxkzfzfaz.cloudfront.net		216.137.37.2	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:53.035471916 CEST	8.8.8.8	192.168.2.5	0x48bf	No error (0)	d1jpmzxkzfzfaz.cloudfront.net		216.137.37.32	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:53.035471916 CEST	8.8.8.8	192.168.2.5	0x48bf	No error (0)	d1jpmzxkzfzfaz.cloudfront.net		216.137.37.16	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:53.035471916 CEST	8.8.8.8	192.168.2.5	0x48bf	No error (0)	d1jpmzxkzfzfaz.cloudfront.net		216.137.37.125	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:53.052575111 CEST	8.8.8.8	192.168.2.5	0xf204	No error (0)	app.launchdarkly.com	c3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:47:53.059020042 CEST	8.8.8.8	192.168.2.5	0x6d1a	No error (0)	events.launchdarkly.com		54.209.55.173	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:53.059020042 CEST	8.8.8.8	192.168.2.5	0x6d1a	No error (0)	events.launchdarkly.com		18.210.159.55	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:53.059020042 CEST	8.8.8.8	192.168.2.5	0x6d1a	No error (0)	events.launchdarkly.com		52.21.25.101	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 15:47:53.059020042 CEST	8.8.8.8	192.168.2.5	0x6d1a	No error (0)	events.launchdarkly.com		107.23.222.30	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:53.059020042 CEST	8.8.8.8	192.168.2.5	0x6d1a	No error (0)	events.launchdarkly.com		54.210.201.9	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:53.059020042 CEST	8.8.8.8	192.168.2.5	0x6d1a	No error (0)	events.launchdarkly.com		54.236.172.192	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:53.059020042 CEST	8.8.8.8	192.168.2.5	0x6d1a	No error (0)	events.launchdarkly.com		34.232.170.105	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:53.059020042 CEST	8.8.8.8	192.168.2.5	0x6d1a	No error (0)	events.launchdarkly.com		54.210.144.221	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:53.437107086 CEST	8.8.8.8	192.168.2.5	0xf4ba	No error (0)	confluence.atlassian.com	confluence.prd.cst.atlassian.com		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:47:53.437107086 CEST	8.8.8.8	192.168.2.5	0xf4ba	No error (0)	confluence.prd.cst.atlassian.com	d3lzof3wnsn9tm.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:47:53.437107086 CEST	8.8.8.8	192.168.2.5	0xf4ba	No error (0)	d3lzof3wnsn9tm.cloudfront.net		54.192.66.67	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:53.437107086 CEST	8.8.8.8	192.168.2.5	0xf4ba	No error (0)	d3lzof3wnsn9tm.cloudfront.net		54.192.66.84	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:53.437107086 CEST	8.8.8.8	192.168.2.5	0xf4ba	No error (0)	d3lzof3wnsn9tm.cloudfront.net		54.192.66.55	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:53.437107086 CEST	8.8.8.8	192.168.2.5	0xf4ba	No error (0)	d3lzof3wnsn9tm.cloudfront.net		54.192.66.98	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:53.964281082 CEST	8.8.8.8	192.168.2.5	0xbe91	No error (0)	www-googletagmanager.l.google.com		142.250.186.72	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:55.376211882 CEST	8.8.8.8	192.168.2.5	0xfa01	No error (0)	www-google-analytics.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:55.381584883 CEST	8.8.8.8	192.168.2.5	0x8ca5	No error (0)	web-analytics.engagio.com	prod-tracking-web-alb-482381516.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:47:55.381584883 CEST	8.8.8.8	192.168.2.5	0x8ca5	No error (0)	prod-tracking-web-alb-482381516.us-east-1.elb.amazonaws.com		35.172.51.134	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:55.381584883 CEST	8.8.8.8	192.168.2.5	0x8ca5	No error (0)	prod-tracking-web-alb-482381516.us-east-1.elb.amazonaws.com		34.195.40.113	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:57.427680016 CEST	8.8.8.8	192.168.2.5	0x438c	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:47:57.427680016 CEST	8.8.8.8	192.168.2.5	0x438c	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:57.574656963 CEST	8.8.8.8	192.168.2.5	0x499	No error (0)	munchkin.marketo.net	wildcard.marketo.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:47:57.686583996 CEST	8.8.8.8	192.168.2.5	0x911	No error (0)	dn1f1hmdujj40.cloudfront.net		13.33.93.218	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:57.686583996 CEST	8.8.8.8	192.168.2.5	0x911	No error (0)	dn1f1hmdujj40.cloudfront.net		13.33.93.55	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:57.686583996 CEST	8.8.8.8	192.168.2.5	0x911	No error (0)	dn1f1hmdujj40.cloudfront.net		13.33.93.213	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:57.686583996 CEST	8.8.8.8	192.168.2.5	0x911	No error (0)	dn1f1hmdujj40.cloudfront.net		13.33.93.10	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:57.819441080 CEST	8.8.8.8	192.168.2.5	0x7026	No error (0)	594-atc-127.mktoresp.com		192.28.144.124	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:57.879715919 CEST	8.8.8.8	192.168.2.5	0xbffb	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 15:47:57.879715919 CEST	8.8.8.8	192.168.2.5	0xbffb	No error (0)	stats.l.doubleclick.net		173.194.79.155	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:57.879715919 CEST	8.8.8.8	192.168.2.5	0xbffb	No error (0)	stats.l.doubleclick.net		173.194.79.156	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:57.879715919 CEST	8.8.8.8	192.168.2.5	0xbffb	No error (0)	stats.l.doubleclick.net		173.194.79.157	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:57.879715919 CEST	8.8.8.8	192.168.2.5	0xbffb	No error (0)	stats.l.doubleclick.net		173.194.79.154	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:58.041111946 CEST	8.8.8.8	192.168.2.5	0x3b6b	No error (0)	www.google.fr		172.217.168.67	A (IP address)	IN (0x0001)
Oct 25, 2021 15:47:58.050898075 CEST	8.8.8.8	192.168.2.5	0x3363	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:00.287563086 CEST	8.8.8.8	192.168.2.5	0x9525	No error (0)	www.atlassian.com	dc61fd7f-0769-521a-b271-bd73d5e7f644.prd.edge-inf.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:00.287563086 CEST	8.8.8.8	192.168.2.5	0x9525	No error (0)	dc61fd7f-0769-521a-b271-bd73d5e7f644.prd.edge-inf.net		185.166.143.5	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:00.287563086 CEST	8.8.8.8	192.168.2.5	0x9525	No error (0)	dc61fd7f-0769-521a-b271-bd73d5e7f644.prd.edge-inf.net		185.166.143.3	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:00.287563086 CEST	8.8.8.8	192.168.2.5	0x9525	No error (0)	dc61fd7f-0769-521a-b271-bd73d5e7f644.prd.edge-inf.net		185.166.143.4	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:00.862427950 CEST	8.8.8.8	192.168.2.5	0xfe45	No error (0)	wac-cdn-2.atlassian.com	wac-platform.multicdn.cloudinary.com		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:00.862427950 CEST	8.8.8.8	192.168.2.5	0xfe45	No error (0)	wac-platform.multicdn.cloudinary.com	2-01-49b5-014e.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:00.862427950 CEST	8.8.8.8	192.168.2.5	0xfe45	No error (0)	s2-cloudinary-pin-sni.map.fastly.net		151.101.2.92	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:00.862427950 CEST	8.8.8.8	192.168.2.5	0xfe45	No error (0)	s2-cloudinary-pin-sni.map.fastly.net		151.101.66.92	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:00.862427950 CEST	8.8.8.8	192.168.2.5	0xfe45	No error (0)	s2-cloudinary-pin-sni.map.fastly.net		151.101.130.92	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:00.862427950 CEST	8.8.8.8	192.168.2.5	0xfe45	No error (0)	s2-cloudinary-pin-sni.map.fastly.net		151.101.194.92	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:00.876153946 CEST	8.8.8.8	192.168.2.5	0xb2bb	No error (0)	wac-cdn.atlassian.com	d3bdzitctqoj2j.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:00.876153946 CEST	8.8.8.8	192.168.2.5	0xb2bb	No error (0)	d3bdzitctqoj2j.cloudfront.net		54.192.66.54	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:00.876153946 CEST	8.8.8.8	192.168.2.5	0xb2bb	No error (0)	d3bdzitctqoj2j.cloudfront.net		54.192.66.121	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:00.876153946 CEST	8.8.8.8	192.168.2.5	0xb2bb	No error (0)	d3bdzitctqoj2j.cloudfront.net		54.192.66.4	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:00.876153946 CEST	8.8.8.8	192.168.2.5	0xb2bb	No error (0)	d3bdzitctqoj2j.cloudfront.net		54.192.66.63	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:00.926055908 CEST	8.8.8.8	192.168.2.5	0x5275	No error (0)	metal.prod.atl-paas.net	d1jsfcerjrfe3w.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:00.926055908 CEST	8.8.8.8	192.168.2.5	0x5275	No error (0)	d1jsfcerjrfe3w.cloudfront.net		54.192.66.87	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:00.926055908 CEST	8.8.8.8	192.168.2.5	0x5275	No error (0)	d1jsfcerjrfe3w.cloudfront.net		54.192.66.113	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 15:48:00.926055908 CEST	8.8.8.8	192.168.2.5	0x5275	No error (0)	d1jsfcerjr fe3w.cloud front.net		54.192.66.6	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:00.926055908 CEST	8.8.8.8	192.168.2.5	0x5275	No error (0)	d1jsfcerjr fe3w.cloud front.net		54.192.66.15	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:03.320445061 CEST	8.8.8.8	192.168.2.5	0x19d0	No error (0)	tapi.optim izely.com	t.o.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:04.166701078 CEST	8.8.8.8	192.168.2.5	0x4e0	No error (0)	client.px-cloud.net	perimeterx2.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:04.166701078 CEST	8.8.8.8	192.168.2.5	0x4e0	No error (0)	perimeterx 2.map.fastly.net		151.101.1.40	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:04.166701078 CEST	8.8.8.8	192.168.2.5	0x4e0	No error (0)	perimeterx 2.map.fastly.net		151.101.65.40	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:04.166701078 CEST	8.8.8.8	192.168.2.5	0x4e0	No error (0)	perimeterx 2.map.fastly.net		151.101.129.40	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:04.166701078 CEST	8.8.8.8	192.168.2.5	0x4e0	No error (0)	perimeterx 2.map.fastly.net		151.101.193.40	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:04.222512007 CEST	8.8.8.8	192.168.2.5	0x6c7c	No error (0)	api.segment.io		54.70.105.250	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:04.222512007 CEST	8.8.8.8	192.168.2.5	0x6c7c	No error (0)	api.segment.io		54.213.130.70	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:04.222512007 CEST	8.8.8.8	192.168.2.5	0x6c7c	No error (0)	api.segment.io		52.43.10.86	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:04.222512007 CEST	8.8.8.8	192.168.2.5	0x6c7c	No error (0)	api.segment.io		35.164.248.150	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:04.222512007 CEST	8.8.8.8	192.168.2.5	0x6c7c	No error (0)	api.segment.io		52.32.165.57	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:04.222512007 CEST	8.8.8.8	192.168.2.5	0x6c7c	No error (0)	api.segment.io		34.215.76.123	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:04.222512007 CEST	8.8.8.8	192.168.2.5	0x6c7c	No error (0)	api.segment.io		54.190.208.247	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:04.222512007 CEST	8.8.8.8	192.168.2.5	0x6c7c	No error (0)	api.segment.io		35.155.235.224	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:04.955085993 CEST	8.8.8.8	192.168.2.5	0x5f3c	No error (0)	collector-pxvryik386.px-cloud.net		35.186.220.184	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:06.157584906 CEST	8.8.8.8	192.168.2.5	0x37d5	No error (0)	api.atlass ian.com	global.stargate.cse.ss-inf.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:06.157584906 CEST	8.8.8.8	192.168.2.5	0x37d5	No error (0)	global.sta rgate.cse.ss-inf.net		18.184.99.133	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:06.157584906 CEST	8.8.8.8	192.168.2.5	0x37d5	No error (0)	global.sta rgate.cse.ss-inf.net		18.184.99.131	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:06.157584906 CEST	8.8.8.8	192.168.2.5	0x37d5	No error (0)	global.sta rgate.cse.ss-inf.net		18.184.99.132	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:06.679001093 CEST	8.8.8.8	192.168.2.5	0xb47a	No error (0)	cdn-mr.con tentful.com	b3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:08.717361927 CEST	8.8.8.8	192.168.2.5	0x7778	No error (0)	wac-cdn-2. atlassian.com	wac-platform.multicdn.cloudinary.com		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:08.717361927 CEST	8.8.8.8	192.168.2.5	0x7778	No error (0)	wac-platfo rm.multicd n.cloudinary.com	2-01-49b5-014e.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:08.717361927 CEST	8.8.8.8	192.168.2.5	0x7778	No error (0)	s2-cloudinary-pin-sni.map.fastly.net		151.101.2.92	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:08.717361927 CEST	8.8.8.8	192.168.2.5	0x7778	No error (0)	s2-cloudinary-pin-sni.map.fastly.net		151.101.66.92	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 15:48:08.717361927 CEST	8.8.8.8	192.168.2.5	0x7778	No error (0)	s2-cloudinary-pin-sni.map.fastly.net		151.101.130.92	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:08.717361927 CEST	8.8.8.8	192.168.2.5	0x7778	No error (0)	s2-cloudinary-pin-sni.map.fastly.net		151.101.194.92	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:10.486229897 CEST	8.8.8.8	192.168.2.5	0x1160	No error (0)	stg-client relations.equalityhealth.com		76.9.179.216	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:23.384970903 CEST	8.8.8.8	192.168.2.5	0x96f9	No error (0)	www.youtube.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:23.384970903 CEST	8.8.8.8	192.168.2.5	0x96f9	No error (0)	youtube-ui.l.google.com		142.250.186.174	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:23.384970903 CEST	8.8.8.8	192.168.2.5	0x96f9	No error (0)	youtube-ui.l.google.com		172.217.18.110	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:23.384970903 CEST	8.8.8.8	192.168.2.5	0x96f9	No error (0)	youtube-ui.l.google.com		142.250.184.238	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:23.384970903 CEST	8.8.8.8	192.168.2.5	0x96f9	No error (0)	youtube-ui.l.google.com		172.217.23.110	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:23.384970903 CEST	8.8.8.8	192.168.2.5	0x96f9	No error (0)	youtube-ui.l.google.com		142.250.184.206	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:23.384970903 CEST	8.8.8.8	192.168.2.5	0x96f9	No error (0)	youtube-ui.l.google.com		142.250.185.110	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:23.384970903 CEST	8.8.8.8	192.168.2.5	0x96f9	No error (0)	youtube-ui.l.google.com		142.250.185.142	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:23.384970903 CEST	8.8.8.8	192.168.2.5	0x96f9	No error (0)	youtube-ui.l.google.com		142.250.185.174	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:23.384970903 CEST	8.8.8.8	192.168.2.5	0x96f9	No error (0)	youtube-ui.l.google.com		142.250.185.206	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:23.384970903 CEST	8.8.8.8	192.168.2.5	0x96f9	No error (0)	youtube-ui.l.google.com		142.250.185.238	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:23.384970903 CEST	8.8.8.8	192.168.2.5	0x96f9	No error (0)	youtube-ui.l.google.com		142.250.185.78	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:23.384970903 CEST	8.8.8.8	192.168.2.5	0x96f9	No error (0)	youtube-ui.l.google.com		142.250.181.238	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:23.384970903 CEST	8.8.8.8	192.168.2.5	0x96f9	No error (0)	youtube-ui.l.google.com		172.217.16.142	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:23.384970903 CEST	8.8.8.8	192.168.2.5	0x96f9	No error (0)	youtube-ui.l.google.com		216.58.212.174	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:23.384970903 CEST	8.8.8.8	192.168.2.5	0x96f9	No error (0)	youtube-ui.l.google.com		142.250.74.206	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:23.384970903 CEST	8.8.8.8	192.168.2.5	0x96f9	No error (0)	youtube-ui.l.google.com		142.250.186.46	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.251759052 CEST	8.8.8.8	192.168.2.5	0xe1d0	No error (0)	snap.licdn.com	od.linkedin.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:25.320620060 CEST	8.8.8.8	192.168.2.5	0x794	No error (0)	5406241.fls.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:25.320620060 CEST	8.8.8.8	192.168.2.5	0x794	No error (0)	dart.l.doubleclick.net		172.217.168.38	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.367533922 CEST	8.8.8.8	192.168.2.5	0xf9ec	No error (0)	platform.twitter.com	cs472.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:25.367533922 CEST	8.8.8.8	192.168.2.5	0xf9ec	No error (0)	cs472.wac.edgecastcdn.net	cs1-apr-8315.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:25.367533922 CEST	8.8.8.8	192.168.2.5	0xf9ec	No error (0)	cs1-apr-8315.wac.edgecastcdn.net	wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 15:48:25.367533922 CEST	8.8.8.8	192.168.2.5	0xf9ec	No error (0)	cs1-lb-eu.8315.ecdns.net	cs41.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:25.367533922 CEST	8.8.8.8	192.168.2.5	0xf9ec	No error (0)	cs41.wac.edgecastcdn.net		93.184.220.66	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.371279001 CEST	8.8.8.8	192.168.2.5	0xa4d0	No error (0)	cdn.bizible.com	fp2c5c.wac.108ca.kappacdn.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:25.371279001 CEST	8.8.8.8	192.168.2.5	0xa4d0	No error (0)	fp2c5c.wac.108ca.kappacdn.net	fp2c5c.wac.kappacdn.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:25.371279001 CEST	8.8.8.8	192.168.2.5	0xa4d0	No error (0)	fp2c5c.wac.kappacdn.net		152.195.15.58	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.372313023 CEST	8.8.8.8	192.168.2.5	0x1b8b	No error (0)	cdnssl.clicktale.net	cdn-dsa.clicktale.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:25.381946087 CEST	8.8.8.8	192.168.2.5	0x8924	No error (0)	scripts.demandbase.com		54.192.66.106	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.381946087 CEST	8.8.8.8	192.168.2.5	0x8924	No error (0)	scripts.demandbase.com		54.192.66.43	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.381946087 CEST	8.8.8.8	192.168.2.5	0x8924	No error (0)	scripts.demandbase.com		54.192.66.75	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.381946087 CEST	8.8.8.8	192.168.2.5	0x8924	No error (0)	scripts.demandbase.com		54.192.66.107	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.403415918 CEST	8.8.8.8	192.168.2.5	0x8afc	No error (0)	www.redditstatic.com	dualstack.reddit.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:25.403415918 CEST	8.8.8.8	192.168.2.5	0x8afc	No error (0)	dualstack.reddit.map.fastly.net		151.101.1.140	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.403415918 CEST	8.8.8.8	192.168.2.5	0x8afc	No error (0)	dualstack.reddit.map.fastly.net		151.101.65.140	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.403415918 CEST	8.8.8.8	192.168.2.5	0x8afc	No error (0)	dualstack.reddit.map.fastly.net		151.101.129.140	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.403415918 CEST	8.8.8.8	192.168.2.5	0x8afc	No error (0)	dualstack.reddit.map.fastly.net		151.101.193.140	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.484750032 CEST	8.8.8.8	192.168.2.5	0x3688	No error (0)	pixel.pointmediatracker.com		54.192.66.98	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.484750032 CEST	8.8.8.8	192.168.2.5	0x3688	No error (0)	pixel.pointmediatracker.com		54.192.66.44	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.484750032 CEST	8.8.8.8	192.168.2.5	0x3688	No error (0)	pixel.pointmediatracker.com		54.192.66.80	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.484750032 CEST	8.8.8.8	192.168.2.5	0x3688	No error (0)	pixel.pointmediatracker.com		54.192.66.66	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.491529942 CEST	8.8.8.8	192.168.2.5	0x531b	No error (0)	px.ads.linkedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:25.491529942 CEST	8.8.8.8	192.168.2.5	0x531b	No error (0)	mix.linkedin.com	glb-na.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:25.491529942 CEST	8.8.8.8	192.168.2.5	0x531b	No error (0)	glb-na.mix.linkedin.com	pop-eda6.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:25.491529942 CEST	8.8.8.8	192.168.2.5	0x531b	No error (0)	pop-eda6.mix.linkedin.com		108.174.11.69	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.806966066 CEST	8.8.8.8	192.168.2.5	0xf58a	No error (0)	static.ads-twitter.com	platform.twitter.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:25.806966066 CEST	8.8.8.8	192.168.2.5	0xf58a	No error (0)	platform.twitter.map.fastly.net		199.232.136.157	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:25.814529896 CEST	8.8.8.8	192.168.2.5	0x612d	No error (0)	adservice.google.com		172.217.168.66	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 15:48:26.333478928 CEST	8.8.8.8	192.168.2.5	0x4e33	No error (0)	googleads.g.doubleclick.net		142.250.203.98	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:26.520090103 CEST	8.8.8.8	192.168.2.5	0x228b	No error (0)	cnv.event.prod.bidr.io	global.event.prod.bidr.io		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:26.520090103 CEST	8.8.8.8	192.168.2.5	0x228b	No error (0)	global.event.prod.bidr.io		52.211.108.19	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:26.520090103 CEST	8.8.8.8	192.168.2.5	0x228b	No error (0)	global.event.prod.bidr.io		52.214.117.3	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.024004936 CEST	8.8.8.8	192.168.2.5	0x708c	No error (0)	alb.reddit.com	reddit.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:27.024004936 CEST	8.8.8.8	192.168.2.5	0x708c	No error (0)	reddit.map.fastly.net		151.101.1.140	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.024004936 CEST	8.8.8.8	192.168.2.5	0x708c	No error (0)	reddit.map.fastly.net		151.101.65.140	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.024004936 CEST	8.8.8.8	192.168.2.5	0x708c	No error (0)	reddit.map.fastly.net		151.101.129.140	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.024004936 CEST	8.8.8.8	192.168.2.5	0x708c	No error (0)	reddit.map.fastly.net		151.101.193.140	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.081984997 CEST	8.8.8.8	192.168.2.5	0x92ae	No error (0)	match.prod.bidr.io		52.49.53.128	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.081984997 CEST	8.8.8.8	192.168.2.5	0x92ae	No error (0)	match.prod.bidr.io		52.215.68.151	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.081984997 CEST	8.8.8.8	192.168.2.5	0x92ae	No error (0)	match.prod.bidr.io		52.215.67.80	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.081984997 CEST	8.8.8.8	192.168.2.5	0x92ae	No error (0)	match.prod.bidr.io		52.30.222.33	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.081984997 CEST	8.8.8.8	192.168.2.5	0x92ae	No error (0)	match.prod.bidr.io		52.16.151.94	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.081984997 CEST	8.8.8.8	192.168.2.5	0x92ae	No error (0)	match.prod.bidr.io		52.49.238.187	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.081984997 CEST	8.8.8.8	192.168.2.5	0x92ae	No error (0)	match.prod.bidr.io		52.16.229.21	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.081984997 CEST	8.8.8.8	192.168.2.5	0x92ae	No error (0)	match.prod.bidr.io		54.77.6.213	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.082930088 CEST	8.8.8.8	192.168.2.5	0x83cf	No error (0)	id.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.114905119 CEST	8.8.8.8	192.168.2.5	0xfb6d	No error (0)	analytics.twitter.com	ads.twitter.com		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:27.114905119 CEST	8.8.8.8	192.168.2.5	0xfb6d	No error (0)	ads.twitter.com	s.twitter.com		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:27.114905119 CEST	8.8.8.8	192.168.2.5	0xfb6d	No error (0)	s.twitter.com		104.244.42.131	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.114905119 CEST	8.8.8.8	192.168.2.5	0xfb6d	No error (0)	s.twitter.com		104.244.42.67	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.114905119 CEST	8.8.8.8	192.168.2.5	0xfb6d	No error (0)	s.twitter.com		104.244.42.195	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.114905119 CEST	8.8.8.8	192.168.2.5	0xfb6d	No error (0)	s.twitter.com		104.244.42.3	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.207050085 CEST	8.8.8.8	192.168.2.5	0xc26	No error (0)	t.co		104.244.42.5	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.207050085 CEST	8.8.8.8	192.168.2.5	0xc26	No error (0)	t.co		104.244.42.133	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 15:48:27.207050085 CEST	8.8.8.8	192.168.2.5	0xc26	No error (0)	t.co		104.244.42.69	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.207050085 CEST	8.8.8.8	192.168.2.5	0xc26	No error (0)	t.co		104.244.42.197	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.350044012 CEST	8.8.8.8	192.168.2.5	0x6758	No error (0)	api.company-target.com		54.192.66.24	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.350044012 CEST	8.8.8.8	192.168.2.5	0x6758	No error (0)	api.company-target.com		54.192.66.2	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.350044012 CEST	8.8.8.8	192.168.2.5	0x6758	No error (0)	api.company-target.com		54.192.66.102	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.350044012 CEST	8.8.8.8	192.168.2.5	0x6758	No error (0)	api.company-target.com		54.192.66.68	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.355747938 CEST	8.8.8.8	192.168.2.5	0xb24f	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:27.499200106 CEST	8.8.8.8	192.168.2.5	0x760c	No error (0)	cdn.bizibly.com	fp2c5c.wac.108ca.kappacdn.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:27.499200106 CEST	8.8.8.8	192.168.2.5	0x760c	No error (0)	fp2c5c.wac.108ca.kappacdn.net	fp2c5c.wac.kappacdn.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:27.499200106 CEST	8.8.8.8	192.168.2.5	0x760c	No error (0)	fp2c5c.wac.kappacdn.net		152.195.15.58	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.586896896 CEST	8.8.8.8	192.168.2.5	0x52c	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:27.586896896 CEST	8.8.8.8	192.168.2.5	0x52c	No error (0)	star-mini.c10r.facebook.com		157.240.9.35	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.927934885 CEST	8.8.8.8	192.168.2.5	0x6c34	No error (0)	ing-district.clicktale.net	webrecorder-prod-1682395302.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:27.927934885 CEST	8.8.8.8	192.168.2.5	0x6c34	No error (0)	webrecorder-prod-1682395302.us-east-1.elb.amazonaws.com		23.23.73.109	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.927934885 CEST	8.8.8.8	192.168.2.5	0x6c34	No error (0)	webrecorder-prod-1682395302.us-east-1.elb.amazonaws.com		54.209.121.108	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.927934885 CEST	8.8.8.8	192.168.2.5	0x6c34	No error (0)	webrecorder-prod-1682395302.us-east-1.elb.amazonaws.com		52.1.57.199	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.927934885 CEST	8.8.8.8	192.168.2.5	0x6c34	No error (0)	webrecorder-prod-1682395302.us-east-1.elb.amazonaws.com		54.85.254.11	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.927934885 CEST	8.8.8.8	192.168.2.5	0x6c34	No error (0)	webrecorder-prod-1682395302.us-east-1.elb.amazonaws.com		3.208.156.83	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.927934885 CEST	8.8.8.8	192.168.2.5	0x6c34	No error (0)	webrecorder-prod-1682395302.us-east-1.elb.amazonaws.com		44.195.248.99	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.927934885 CEST	8.8.8.8	192.168.2.5	0x6c34	No error (0)	webrecorder-prod-1682395302.us-east-1.elb.amazonaws.com		34.205.224.37	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 15:48:27.927934885 CEST	8.8.8.8	192.168.2.5	0x6c34	No error (0)	webrecorder-prod-1682395302.us-east-1.elb.amazonaws.com		3.222.136.103	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.963423967 CEST	8.8.8.8	192.168.2.5	0x8b59	No error (0)	c.clicktale.net	c-ct-eu.contentsquare.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:27.963423967 CEST	8.8.8.8	192.168.2.5	0x8b59	No error (0)	c-ct-eu.contentsquare.net		52.30.94.8	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.963423967 CEST	8.8.8.8	192.168.2.5	0x8b59	No error (0)	c-ct-eu.contentsquare.net		34.251.174.164	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.963423967 CEST	8.8.8.8	192.168.2.5	0x8b59	No error (0)	c-ct-eu.contentsquare.net		34.243.8.13	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.963423967 CEST	8.8.8.8	192.168.2.5	0x8b59	No error (0)	c-ct-eu.contentsquare.net		46.51.203.243	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.963423967 CEST	8.8.8.8	192.168.2.5	0x8b59	No error (0)	c-ct-eu.contentsquare.net		52.208.183.15	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.963423967 CEST	8.8.8.8	192.168.2.5	0x8b59	No error (0)	c-ct-eu.contentsquare.net		52.213.24.133	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.963423967 CEST	8.8.8.8	192.168.2.5	0x8b59	No error (0)	c-ct-eu.contentsquare.net		54.77.197.90	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.963423967 CEST	8.8.8.8	192.168.2.5	0x8b59	No error (0)	c-ct-eu.contentsquare.net		54.228.44.63	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.989454985 CEST	8.8.8.8	192.168.2.5	0x1387	No error (0)	segments.company-target.com		54.192.66.96	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.989454985 CEST	8.8.8.8	192.168.2.5	0x1387	No error (0)	segments.company-target.com		54.192.66.128	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.989454985 CEST	8.8.8.8	192.168.2.5	0x1387	No error (0)	segments.company-target.com		54.192.66.74	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:27.989454985 CEST	8.8.8.8	192.168.2.5	0x1387	No error (0)	segments.company-target.com		54.192.66.63	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:28.616283894 CEST	8.8.8.8	192.168.2.5	0x4a50	No error (0)	p.adsymptotic.com		104.18.102.194	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:28.616283894 CEST	8.8.8.8	192.168.2.5	0x4a50	No error (0)	p.adsymptotic.com		104.18.99.194	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:28.616283894 CEST	8.8.8.8	192.168.2.5	0x4a50	No error (0)	p.adsymptotic.com		104.18.98.194	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:28.616283894 CEST	8.8.8.8	192.168.2.5	0x4a50	No error (0)	p.adsymptotic.com		104.18.100.194	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:28.616283894 CEST	8.8.8.8	192.168.2.5	0x4a50	No error (0)	p.adsymptotic.com		104.18.101.194	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:33.648514032 CEST	8.8.8.8	192.168.2.5	0x1771	No error (0)	adservice.google.fr	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:33.648514032 CEST	8.8.8.8	192.168.2.5	0x1771	No error (0)	pagead46.l.doubleclick.net		142.250.203.98	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:34.099884987 CEST	8.8.8.8	192.168.2.5	0xb252	No error (0)	errors.client.optimizely.com	client-error-log-962704628.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Oct 25, 2021 15:48:34.099884987 CEST	8.8.8.8	192.168.2.5	0xb252	No error (0)	client-error-log-962704628.us-east-1.elb.amazonaws.com		3.224.118.21	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:34.099884987 CEST	8.8.8.8	192.168.2.5	0xb252	No error (0)	client-error-log-962704628.us-east-1.elb.amazonaws.com		3.225.10.210	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 15:48:34.099884987 CEST	8.8.8.8	192.168.2.5	0xb252	No error (0)	client-error-log-962704628.us-east-1.elb.amazonaws.com		34.198.225.88	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:34.099884987 CEST	8.8.8.8	192.168.2.5	0xb252	No error (0)	client-error-log-962704628.us-east-1.elb.amazonaws.com		3.92.249.113	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:34.099884987 CEST	8.8.8.8	192.168.2.5	0xb252	No error (0)	client-error-log-962704628.us-east-1.elb.amazonaws.com		3.227.66.247	A (IP address)	IN (0x0001)
Oct 25, 2021 15:48:34.099884987 CEST	8.8.8.8	192.168.2.5	0xb252	No error (0)	client-error-log-962704628.us-east-1.elb.amazonaws.com		52.45.34.218	A (IP address)	IN (0x0001)

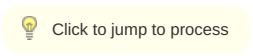
HTTP Request Dependency Graph

- www.atlassian.com

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 3212 Parent PID: 4676

General

Start time:	15:47:05
Start date:	25/10/2021
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://stg-clientrelations.equalityhealth.com/secure/ChangeUserPassword!default.jspa?username=n.martinez@chcfl.org'
Imagebase:	0x7ff677c70000
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: 4072 Parent PID: 3212

General

Start time:	15:47:07
Start date:	25/10/2021
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=1572,18266022950293399891,13773735986418769558,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1936 /prefetch:8
Imagebase:	0x7ff677c70000
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