ID: 514100
Cookbook: browseurl.jbs
Time: 20:39:48
Date: 02/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

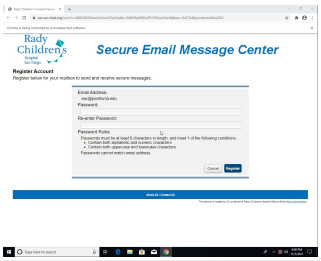
Windows Analysis Report https://secure-chsd.org/s/e?m…

Overview

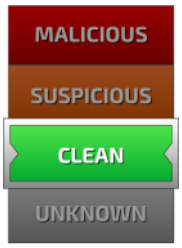
General Information

Sample URL:	http://https://secure-chsd.org/s/e?m=ABBOdSX2hand3rhcsO3vIAYp&c=ABBYByWB0o0PvF3l0uo5dmRj&em=EAC%40pointloma.EDU
Analysis ID:	514100
Infos:	

Most interesting Screenshot:



Detection

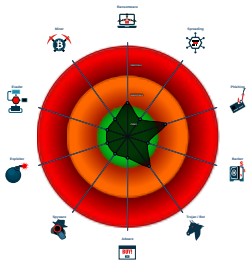


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- HTML body contains low number of …
- Connects to several IPs in different …
- No HTML title found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 2436 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "https://secure-chsd.org/s/e?m=ABBOdSX2hand3rhcsO3vIAYp&c=ABBYByWB0o0PvF3l0uo5dmRj&em=EAC%40pointloma%2eEDU MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 1592 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1536,1080383137737942703,10415530265892783596,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1920 /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

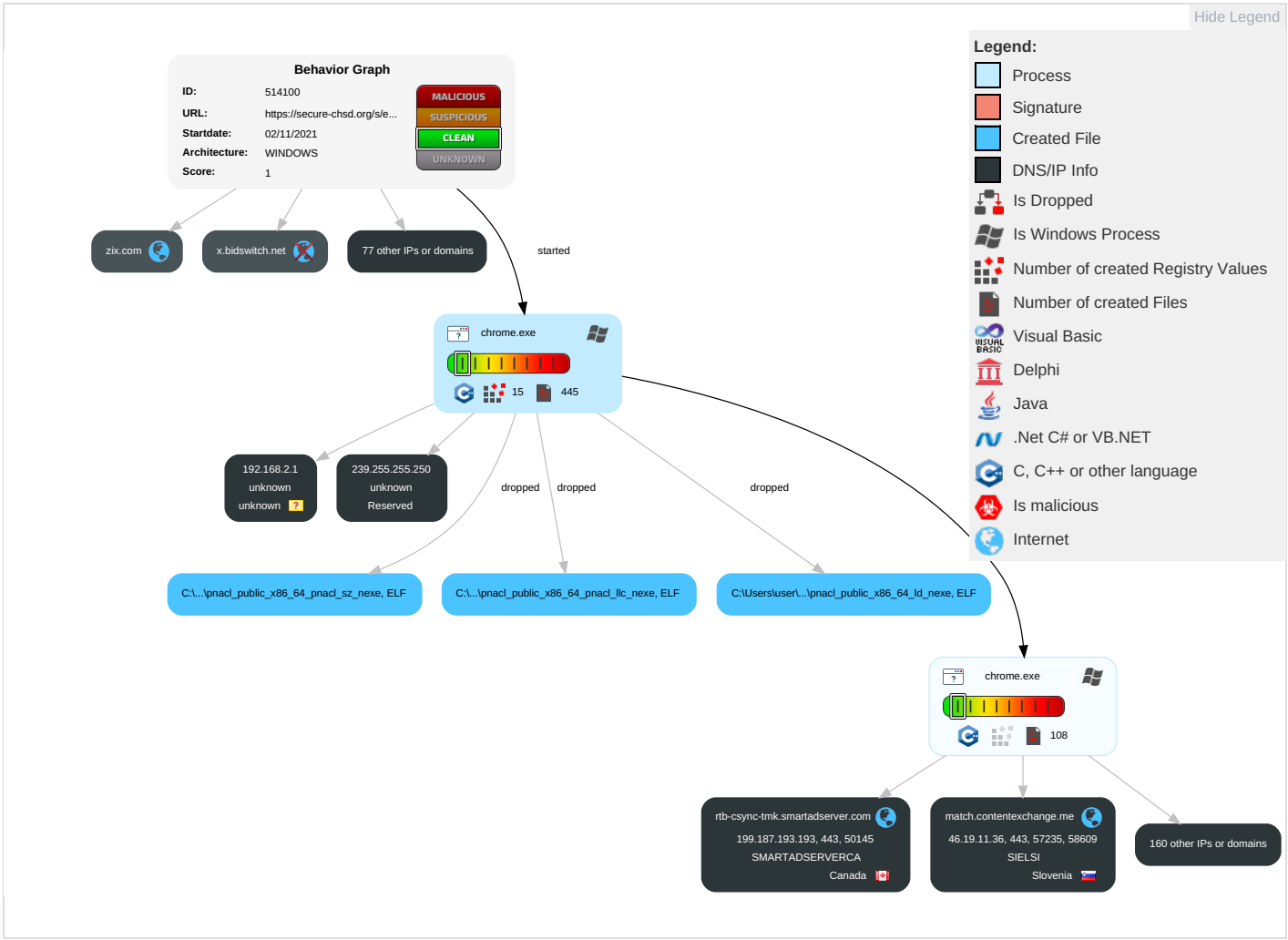
Click to jump to signature section

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

Mitre Att&ck Matrix

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

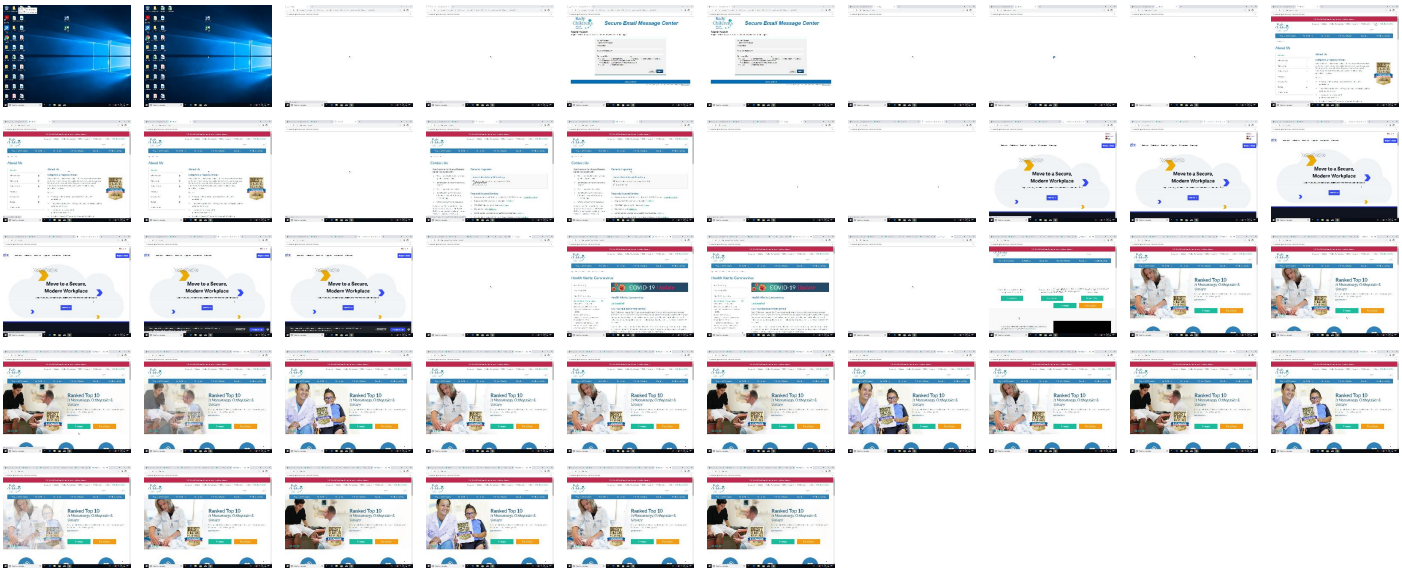
Behavior Graph

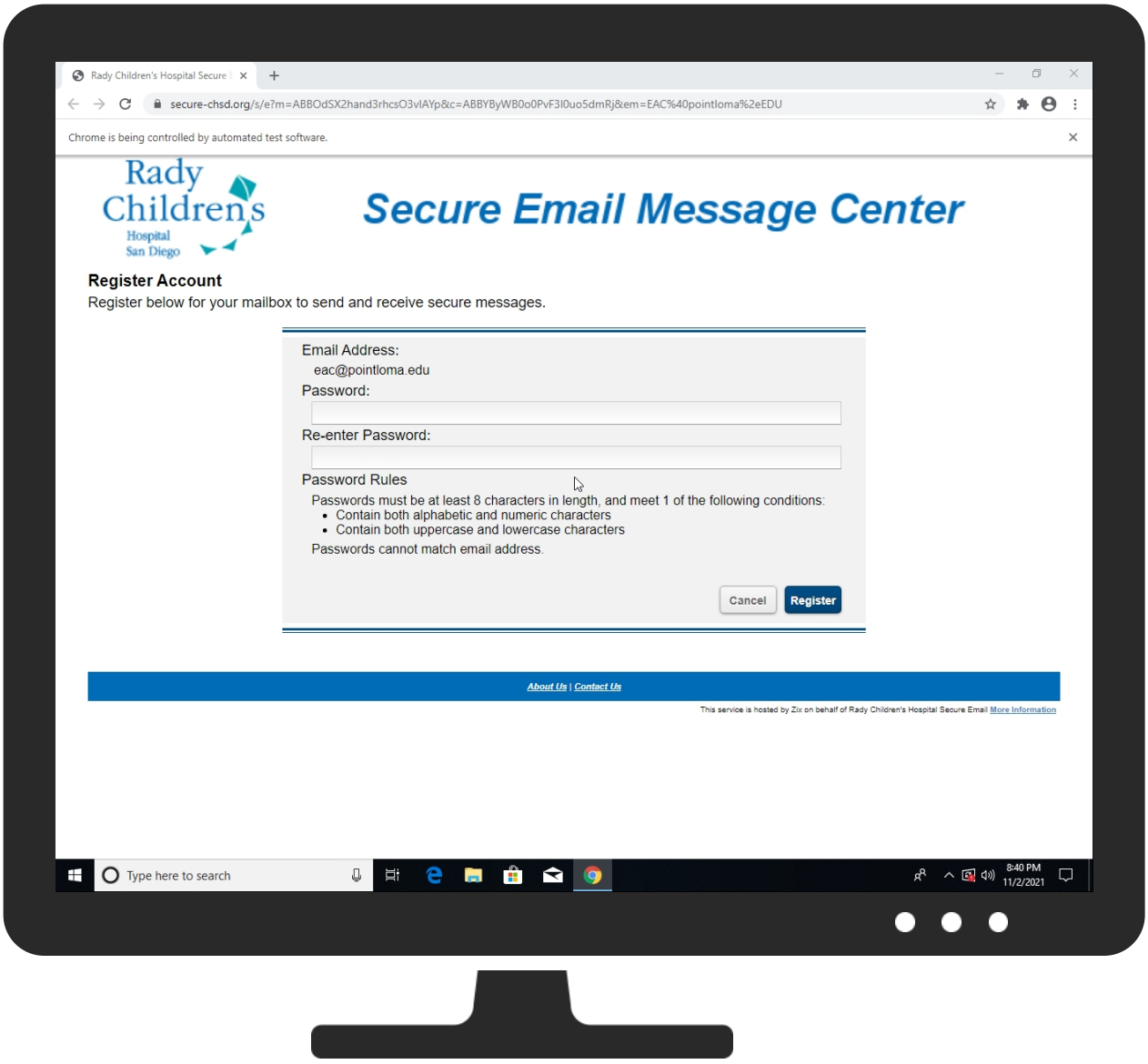


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://secure-chsd.org/s/e?m=ABBOdSX2hand3rhcsO3vIAYp&c=ABBYByWB0o0PvF3l0uo5dmRj&em=EAC%40pointloma%2eEDU	0%	Avira URL Cloud	safe	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\2436_1361747409_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\2436_1361747409_platform_specific\x86_64\pnacl_public_x86_64_ld_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\2436_1361747409_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\2436_1361747409_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\2436_1361747409_platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\2436_1361747409_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://dns.google	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://secure-chsd.org/s/e?m=ABBOdSX2hand3rhcsO3vIAYp&c=ABBYByWB0o0PvF3l0uo5dmRj&em=EAC%40pointloma	0%	Avira URL Cloud	safe	
http://https://www.google.co.uk	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	142.250.203.99	true	false		high
pug-lhr.pubmatic.com	185.64.190.80	true	false		high
segments.company-target.com	143.204.215.100	true	false		unknown
ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com	35.169.187.184	true	false		high
eu-u.openx.net	34.98.64.218	true	false		high
dxedge-prod-lb-1585771072.us-west-2.elb.amazonaws.com	52.89.239.64	true	false		high
eu-eb2.3lift.com	76.223.111.18	true	false		high
b9odqbm.impervadns.net	45.223.138.206	true	false		unknown
ih.adscale.de	35.157.138.20	true	false		high
httplogserver-lb.global.unified-prod.sharethis.net	18.198.109.212	true	false		unknown
elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com	3.120.56.129	true	false		high
sync.crwdcntrl.net	52.30.140.199	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
platform-api.sharethis.com	13.32.22.126	true	false		high
cm.g.doubleclick.net	172.217.168.2	true	false		high
www.google.com	172.217.168.36	true	false		high
rtb-csync-itx4.smartadserver.com	185.86.139.113	true	false		high
tags.adsafety.net	139.162.147.24	true	false		unknown
ads.smartstream.tv	80.82.217.92	true	false		unknown
id.rlcdn.com	35.244.174.68	true	false		high
eu2-ice.360yield.com	3.66.41.54	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
match.adsrvr.org	52.223.40.198	true	false		high
match.contentexchange.me	46.19.11.36	true	false		high
star-mini.c10r.facebook.com	157.240.17.35	true	false		high
d2znr2yi078d75.cloudfront.net	65.9.71.23	true	false		high
match.prod.bidr.io	52.49.53.128	true	false		unknown
stats.l.doubleclick.net	142.250.145.156	true	false		high
uip.semasio.net	77.243.60.138	true	false		high
zix.com	199.30.234.249	true	false		unknown
www.zix.com	199.30.234.249	true	false		unknown
pixel.onaudience.com	146.59.148.16	true	false		unknown
vimeo.com	151.101.0.217	true	false		high
dsp.adfarm1.adition.com	85.114.159.93	true	false		high
redirect.frontend.weborama.fr	35.190.16.14	true	false		high
vimeo.map.fastly.net	151.101.0.217	true	false		unknown
googleads.g.doubleclick.net	142.250.203.98	true	false		high
secure-chsd.org	63.71.15.141	true	false		unknown
www.google.co.uk	142.250.203.99	true	false		unknown
ads4.admatic.com.tr	188.132.147.227	true	false		unknown
clients.l.google.com	172.217.168.78	true	false		high
istrp.adform.net	37.157.2.249	true	false		high
unpkg.com	104.16.122.175	true	false		high
prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com	52.18.60.235	true	false		high
s.w.org	192.0.77.48	true	false		high
googlehosted.l.googleusercontent.com	172.217.168.65	true	false		high
aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com	35.176.195.187	true	false		high
alb-event-1454785217.us-east-1.elb.amazonaws.com	34.234.150.139	true	false		high
sync.1dmp.io	88.99.214.77	true	false		unknown
afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com	34.193.113.164	true	false		high
dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com	3.248.38.136	true	false		high
cm.smartstream.tv	80.85.85.173	true	false		unknown
cm.adsafety.net	80.82.217.100	true	false		unknown
dl7g9llrghqi1.cloudfront.net	143.204.215.88	true	false		high
insight.adsrvr.org	52.223.40.198	true	false		high
pop-edc2.mix.linkedin.com	108.174.11.85	true	false		high
ps.eyeota.net	3.124.210.90	true	false		high
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
tag.demandbase.com	13.32.22.99	true	false		high
a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com	35.174.210.7	true	false		high
rtb-csync-tmk.smartadserver.com	199.187.193.193	true	false		high
idsync.rlcdn.com	35.244.174.68	true	false		high
fresnel.vimeocdn.com	34.120.202.204	true	false		high
pixel.tapad.com	35.227.248.159	true	false		high
s3-eu-west-1.amazonaws.com	52.218.96.10	true	false		high
accounts.google.com	216.58.215.237	true	false		high
www-google-analytics.l.google.com	142.250.203.110	true	false		high
ws.zoominfo.com	104.16.168.82	true	false		high
prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud	18.184.201.8	true	false		unknown
a.audrte.com	34.206.192.53	true	false		unknown
www-googletagmanager.l.google.com	142.250.186.136	true	false		high
adstax-match-proxy.adrtx.net	52.211.146.69	true	false		high
dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com	18.197.87.177	true	false		high
embeds.driftcdn.com	143.204.215.111	true	false		unknown
pug22000nf.pubmatic.com	185.64.189.110	true	false		high
partnerad.l.doubleclick.net	142.250.203.98	true	false		high
global.ib-ibi.com	64.58.232.179	true	false		unknown
s.ad.smaato.net	13.32.22.27	true	false		high
outspot2-ams.adx.opera.com	82.145.213.8	true	false		high
api.company-target.com	143.204.215.82	true	false		unknown
load-euw1.exelator.com	54.78.254.47	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud	18.156.0.31	true	false		unknown
ib.anycast.adnxs.com	37.252.173.215	true	false		high
d3i42lyttuj6qr.cloudfront.net	65.9.71.36	true	false		high
vimeo-video.map.fastly.net	151.101.114.109	true	false		unknown
metrics.api.drift.com	unknown	unknown	false		high
id5-sync.com	unknown	unknown	false		unknown
i.vimeocdn.com	unknown	unknown	false		high
ads.stickyadstv.com	unknown	unknown	false		unknown
stats.g.doubleclick.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
js.driftt.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
token.rubiconproject.com	unknown	unknown	false		high
loada.exelator.com	unknown	unknown	false		high
c1.adform.net	unknown	unknown	false		high
dmp.adform.net	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
bootstrap.api.drift.com	unknown	unknown	false		high
pixel.mathtag.com	unknown	unknown	false		high
t.adx.opera.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.rchsd.org/health-safety/health-alerts/	false		high
http://https://player.vimeo.com/video/398648333?portrait=0&byline=0&title=0	false		high
http://https://player.vimeo.com/video/604357845?portrait=0&byline=0&title=0	false		high
http://https://www.rchsd.org/about-us/	false		high
http://https://player.vimeo.com/video/447845914?portrait=0&byline=0&title=0	false		high
http://https://zix.com/	false		unknown
http://https://js.driftt.com/core/chat?region=US&driftEnableLog=false&pageLoadStartTime=1635910884675	false		high
http://https://pixel.mathtag.com/sync/iframe?mt_uuid=ec1d6181-9483-4f00-986f-209dd10e1e79&no_iframe=1&mt_adid=248701&source=mathtag	false		high
http://https://www.rchsd.org/contact-us/	false		high
http://https://www.rchsd.org/	false		high
http://https://js.driftt.com/core?embedId=65e63pi6mu5c®ion=US&forceShow=false&skipCampaigns=false&sessionId=9a70df5a-b6b4-4e0a-a14c-9a57b6fcaf5a&sessionStarted=1635910895.08&campaignRefreshToken=ef7078d7-33ef-4af8-b357-ba59b7cf0368&hideController=false&pageLoadStartTime=1635910884675&mode=CHAT&driftEnableLog=false	false		high
http://https://c1.adform.net/imatch/pixels?uid=3680121232683396984&agencyId=6276&advertiserId=2105093&src=tp&rnd=139481	false		high
http://https://secure-chsd.org/s/e?m=ABBOdSX2hand3rhcsO3vIAYp&c=ABBYByWB0o0PvF3l0uo5dmRj&em=EAC%40pointloma%2eEDU	false		unknown
http://https://a2.adform.net/serving/container/?pm=2463533&lid=100856282&ctype=0&media=0&PageName=Rady+Childrens+Hospital+Homepage&rnd=1844193108&cpref=&loc=https%3a%2f%2fwww.rchsd.org%2f	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.122.175	unpkg.com	United States		13335	CLOUDFLARENETUS	false
216.58.215.237	accounts.google.com	United States		15169	GOOGLEUS	false
50.16.7.188	unknown	United States		14618	AMAZON-AESUS	false
157.240.17.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false
185.64.190.80	pug-lhr.pubmatic.com	United Kingdom		62713	AS-PUBMATICUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.248.38.136	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
64.58.232.179	global.ib-ibi.com	United States		13649	ASN-VINSUS	false
3.124.210.90	ps.eyeota.net	United States		16509	AMAZON-02US	false
35.227.248.159	pixel.tapad.com	United States		15169	GOOGLEUS	false
52.218.96.10	s3-eu-west-1.amazonaws.com	United States		16509	AMAZON-02US	false
65.9.71.36	d3i42lyttuj6qr.cloudfront.net	United States		16509	AMAZON-02US	false
35.174.210.7	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com	United States		14618	AMAZON-AESUS	false
3.66.41.54	eu2-ice.360yield.com	United States		16509	AMAZON-02US	false
52.30.140.199	sync.crwdcntrl.net	United States		16509	AMAZON-02US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
18.156.0.31	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud	United States		16509	AMAZON-02US	false
143.204.215.111	embeds.driftcdn.com	United States		16509	AMAZON-02US	false
35.244.174.68	id.rlcdn.com	United States		15169	GOOGLEUS	false
80.82.217.100	cm.adsafety.net	Germany		24961	MYLOC-ASIPBackboneofmyLocmanagedITAGDE	false
35.190.16.14	redirect.frontend.weborama.fr	United States		15169	GOOGLEUS	false
52.49.53.128	match.prod.bidr.io	United States		16509	AMAZON-02US	false
188.132.147.235	unknown	Turkey		42910	PREMIERDC-VERI-MERKEZI-ANONIM-SIRKETIPREMIERDC-SHTR	false
63.71.15.141	secure-chsd.org	United States		13380	ASN-CUSTUS	false
88.99.214.77	sync.1dmp.io	Germany		24940	HETZNER-ASDE	false
54.78.254.47	load-euw1.exelator.com	United States		16509	AMAZON-02US	false
52.18.60.235	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
65.9.71.23	d2znr2yi078d75.cloudfront.net	United States		16509	AMAZON-02US	false
45.223.138.206	b9odqbm.impervadns.net	United States		327849	ROCKETNETZA	false
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
13.32.22.99	tag.demandbase.com	United States		7018	ATT-INTERNET4US	false
172.217.168.65	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
143.204.215.100	segments.company-target.com	United States		16509	AMAZON-02US	false
3.120.56.129	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
188.132.147.227	ads4.admatic.com.tr	Turkey		42910	PREMIERDC-VERI-MERKEZI-ANONIM-SIRKETIPREMIERDC-SHTR	false
142.250.186.136	www-googletagmanager.l.google.com	United States		15169	GOOGLEUS	false
34.120.202.204	fresnel.vimeocdn.com	United States		15169	GOOGLEUS	false
37.157.2.249	istrp.adform.net	Denmark		198622	ADFORMDK	false
199.30.234.249	zix.com	United States		13380	ASN-CUSTUS	false
13.32.22.27	s.ad.smaato.net	United States		7018	ATT-INTERNET4US	false
18.198.109.212	httplogserver-lb.global.unified-prod.sharethis.net	United States		16509	AMAZON-02US	false
172.217.168.78	clients.l.google.com	United States		15169	GOOGLEUS	false
46.19.11.36	match.contentexchange.me	Slovenia		51790	SIELSI	false
143.204.215.82	api.company-target.com	United States		16509	AMAZON-02US	false
143.204.215.88	dl7g9llrghqi1.cloudfront.net	United States		16509	AMAZON-02US	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
80.85.85.173	cm.smartstream.tv	United Kingdom		63949	LINODE-APLinodeLLCUS	false
52.89.239.64	dxedge-prod-lb-1585771072.us-west-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
54.147.21.139	unknown	United States		14618	AMAZON-AESUS	false
151.101.0.217	vimeo.com	United States		54113	FASTLYUS	false
80.82.217.92	ads.smartstream.tv	Germany		24961	MYLOC-ASIPBackboneofmyLocmanagedITAGDE	false
34.206.192.53	a.audrte.com	United States		14618	AMAZON-AESUS	false
77.243.60.138	uip.semasio.net	Denmark		42697	NETIC-ASDK	false
34.234.150.139	alb-event-1454785217.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
108.174.11.85	pop-edc2.mix.linkedin.com	United States		14413	LINKEDINUS	false
142.250.203.98	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
142.250.203.99	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
52.223.40.198	match.adsrvr.org	United States		8987	AMAZONEXPANSIONGB	false
82.145.213.8	outspot2-ams.adx.opera.com	United Kingdom		39832	NO-OPERANO	false
51.195.5.232	unknown	France		16276	OVHFR	false
35.169.187.184	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
37.252.173.215	ib.anycast.adnxs.com	European Union		29990	ASN-APPNEXUS	false
139.162.147.24	tags.adsafety.net	Netherlands		63949	LINODE-APLinodeLLCUS	false
13.32.22.126	platform-api.sharethis.com	United States		7018	ATT-INTERNET4US	false
52.211.146.69	adstax-match-proxy.adrtx.net	United States		16509	AMAZON-02US	false
85.114.159.93	dsp.adfarm1.adition.com	Germany		24961	MYLOC-ASIPBackboneofmyLocmanagedITAGDE	false
146.59.148.16	pixel.onaudience.com	Norway		16276	OVHFR	false
18.184.201.8	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud	United States		16509	AMAZON-02US	false
76.223.111.18	eu-eb2.3lift.com	United States		16509	AMAZON-02US	false
35.176.195.187	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false
54.173.95.250	unknown	United States		14618	AMAZON-AESUS	false
151.101.114.109	vimeo-video.map.fastly.net	United States		54113	FASTLYUS	false
35.157.138.20	ih.adscale.de	United States		16509	AMAZON-02US	false
142.250.145.156	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
172.217.168.36	www.google.com	United States		15169	GOOGLEUS	false
104.16.168.82	ws.zoominfo.com	United States		13335	CLOUDFLARENETUS	false
34.98.64.218	eu-u.openx.net	United States		15169	GOOGLEUS	false
199.187.193.193	rtb-csync-tmk.smartadserver.com	Canada		47043	SMARTADSERVERCA	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	514100
Start date:	02.11.2021
Start time:	20:39:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs

Sample URL:	http://https://secure-chsd.org/s/e?m=ABBOdSX2hand3rhcsO3vIAYp&c=ABBYByWB0o0PvF3l0uo5dmRj&em=EAC%40pointloma.EDU
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:	CLEAN
Classification:	clean1.win@38/210@161/79
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://www.rchsd.org/about-us/ • Browse: https://www.rchsd.org/contact-us/ • Browse: https://www.zix.com/ • Browse: https://www.rchsd.org/health-safety/health-alerts/ • Browse: https://www.rchsd.org/
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 GM DS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\06aab188-1cb2-4c06-ae29-fd21b950abb4.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):	184977
Entropy (8bit):	6.076883243243446
Encrypted:	false
SSDEEP:	3072:Ikof0L/3HqW0ZbXc+ImuK3HXlLA7bV/nYorVcI8XIssElYTRt:n40b3KW0ZbXc3RlgbV/njhcI8II6Rt
MD5:	6E8BA1D91C4E99CF46C0028919D114A7
SHA1:	884B4D88B265A7A1225EB1CCC0A897AE8B43B40B
SHA-256:	8826B69B4141B28408799E353D3469A02C1571CC37BA3CC05E5EFBDE60633B44
SHA-512:	71638C5830E6ADB204779F3B6276A86AC8296B42EBD1F257460652963E3BDFDA0A6601B2C7E26454E0BD286A77E1B79DC53D85D95DD7E20BD5B6939FE58D01A
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":1.635910854109817e+12,"network":1.635882055e+12,"ticks":122084492.0,"uncertainty":3854697.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909820208"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\07e99566-98f1-4590-9222-0ba425797855.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7517107559976637
Encrypted:	false
SSDEEP:	384:RrfMIihLa1yEVZrofNUrFvw83/MaXHi/GrerZ+wCxveGi5r1kmh2NOsEwPOK2sNj:hWqVJmS3voeTGga4nrqcK+UY9z
MD5:	0EC932C8E9768737986D0F8B6EA7A147
SHA1:	88263A95B9D8DB9D771A1B34EE322FBC43AFA169
SHA-256:	A608BCD1B74615142F1F2BB50F58ABDFE876B9591BC859167A5E48C946A72906
SHA-512:	A34A70C55E47B518CD98F6587E0C0ADF8289D437FC308F4A7BCD851C179BC5CF0AFC5A31CBA8B7746B86A59371BB94A31D356786FAF44F2B00268AF65E659AD2
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...#J8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\20d58fdf-02db-4fa5-b471-1c124fa9d28b.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):	176506
Entropy (8bit):	6.047474742011752
Encrypted:	false
SSDEEP:	3072:Pf0L/3HqW0ZbXc+lmuK3HXlLA7bV/nYorVcI8XIssElYTRt:30b3KW0ZbXc3RlgbV/njhcI8II6Rt
MD5:	79276DD246FE0A7DACB0BD98A1F746BD
SHA1:	3009CF7044A03FE7299D41D73911D4E36E87A1F7
SHA-256:	3FAD53C6699B9FC1AB6EAA1B953B087A744C4D417B1E3832FC74E9FF65256814
SHA-512:	68156A8DD7214D3878E55BA03588DE793CD691B7400B1888E14E35C007A39124D261DF25783A092BB5F0EE41A8FB10D6757E08F9954AED3280C7EC76FE5D9DA
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":1.635910854109817e+12,"network":1.635882055e+12,"ticks":122084492.0,"uncertainty":3854697.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909004089"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\2a0c7f0b-5960-432a-b74f-2df219f66613.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):	184978
Entropy (8bit):	6.076882173537572
Encrypted:	false
SSDEEP:	3072:XkOf0L/3HqW0ZbXc+lmuK3HXlLA7bV/nYorVcI8XIssElYTRt:Ua0b3KW0ZbXc3RlgbV/njhcI8II6Rt
MD5:	310DF352224EA3B41C18A5B7AF31AC5E
SHA1:	5500BAF118D55670BBC3F4F913E0449F1932C5A4
SHA-256:	F015A41F1D0AF250B1038CF50B4CBD6B832B80B90616A8480C6CC847219C4E53
SHA-512:	08F8E2651B6F109E38F1DD1AB4AA494E2DE3FF9ADB1DFAD6D7E9D84E6568B1394832398FCE437D38B523FC70A534F0D601B5A490BF0FD55632F12A7F8740E44
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":1.635910854109817e+12,"network":1.635882055e+12,"ticks":122084492.0,"uncertainty":3854697.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909004089"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\4272dc74-cf44-442c-966e-409e68574aea.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):	184977
Entropy (8bit):	6.076881220530727
Encrypted:	false
SSDEEP:	3072:Ik9f0L/3HqW0ZbXc+lmuK3HXlLA7bV/nYorVcI8XIssElYTRt:nZ0b3KW0ZbXc3RlgbV/njhcI8II6Rt
MD5:	1523F988DF0D4B2F4690664997A39002
SHA1:	725D40EB464ED72A594438B49B3671EFCADFBE73
SHA-256:	E81DB8AAF6A82FC98D6EA3BA759D62DC0F6B81D998DABDE2C756EEC55AFB748D
SHA-512:	6BD31216C36C85C76DB069EC0C025F8BC235F78791992185B0E9B11CBA2E34912CB357F3F86FAB3E5153BEA3D0AFC8CD8E5C45501AA12C822AC2B37A9BEA7ED7
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":1.635910854109817e+12,"network":1.635882055e+12,"ticks":122084492.0,"uncertainty":3854697.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909820208"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\5e6f0284-56e8-4b13-a198-c95416ed412f.tmp

C:\Users\user\AppData\Local\Google\Chrome\User Data\5e6f0284-56e8-4b13-a198-c95416ed412f.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):	184978
Entropy (8bit):	6.0768821163677345
Encrypted:	false
SSDEEP:	3072:Ikpf0L/3HqW0ZbXc+lmuK3HXlLA7bV/nYorVcI8XIssElYTRt:n10b3KW0ZbXc3RlgbV/njhcI8II6Rt
MD5:	B6156102B032D4C4DF6518004139BB05
SHA1:	072D5F074B3B3C68C5C79CA6B4CAD4CE34252A43
SHA-256:	2E3AB5D4993C0FF74F8BCBE41FD4E319D4266627C3F5AF5CC03B838E8B7A920D
SHA-512:	2C03EFC5057442AADDF84DF9A15FFD47574D79CFD156CC4D369E928C13DE74F9F7BE116BB11E298C9587ACD925C0B0103AD979FE36DA6B4618A0E9784563B38
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":1.635910854109817e+12,"network":1.635882055e+12,"ticks":122084492.0,"uncertainty":3854697.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETlkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909820208"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\696815b0-d876-4ac5-8b97-cd940fb82cbd.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):	176506
Entropy (8bit):	6.047475150324646
Encrypted:	false
SSDEEP:	3072:1f0L/3HqW0ZbXc+lmuK3HXlLA7bV/nYorVcI8XIssElYTRt:B0b3KW0ZbXc3RlgbV/njhcI8II6Rt
MD5:	337AAF4FB1ECB65B382A5799B65CCFE6
SHA1:	68E4E46E3B518C5F6044AC3EC9102E9934AFCC7E
SHA-256:	61247F806B2C5EB1E6F84BCBB2883E940CE2553781101152550 82AC677D4F8FD
SHA-512:	1C3B5078CCE3DD6658B03A0CDD90220950BE728E69D3D4E068A3D8B8C43197221B5536BE57D807F79318549C8165EFCB4D8C4BD2584864C080E96FB0D4EB5F2
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":1.635910854109817e+12,"network":1.635882055e+12,"ticks":122084492.0,"uncertainty":3854697.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETlkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909004089"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\7d70bdc6-f41d-4961-b072-777901e00478.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):	176600
Entropy (8bit):	6.047750335495459
Encrypted:	false
SSDEEP:	3072:Wf0L/3HqW0ZbXc+lmuK3HXlLA7bV/nYorVcI8XIssElYTRt:S0b3KW0ZbXc3RlgbV/njhcI8II6Rt
MD5:	EAFE189618F86BEF54459FEEAD3AD1FD
SHA1:	9F4C07DCA372BD49A7172887C2EECF60226AF636
SHA-256:	93B3A5C9598B5C8781A04B20DBF65591CE1BDD50D4B492FE58037EA21E2C09E1
SHA-512:	695915FAA18D66A8358EE6DCC81270592C05F61BF5F3ED2CF0528FA3038B8FE67C99A4CB404EA990D431A6C0C74420581DB9F5600058E21A034122D44C0D66B6
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":1.635910854109817e+12,"network":1.635882055e+12,"ticks":122084492.0,"uncertainty":3854697.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETlkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909004089"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\8b601928-1d09-4ea8-984b-02dffaef5edc.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\8b601928-1d09-4ea8-984b-02dffaef5edc.tmp

File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	176506
Entropy (8bit):	6.047474742011752
Encrypted:	false
SSDEEP:	3072:Pf0L/3HqW0ZbXc+lmuK3HXlLA7bV/nYorVcI8XIssElYTRt:30b3KW0ZbXc3RlgbV/njhcI8II6Rt
MD5:	79276DD246FE0A7DACB0BD98A1F746BD
SHA1:	3009CF7044A03FE7299D41D73911D4E36E87A1F7
SHA-256:	3FAD53C6699B9FC1AB6EAA1B953B087A744C4D417B1E3832FC74E9FF65256814
SHA-512:	68156A8DD7214D3878E55BA03588DE793CD691B7400B1888E14E35C007A39124D261DF25783A092BB5F0EE41A8FB10D6757E08F9954AED3280C7EC76FE5D9DA
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":1.635910854109817e+12,"network":1.635882055e+12,"ticks":122084492.0,"uncertainty":3854697.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909004089"},"plugins":{"metadata":{"adobe-flash-player":{"disp

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXJFlsz6I:+rJJ
MD5:	CE74DBAFA9F4B2CE737AF2E3003A3465
SHA1:	2F58FDA138667FA4941DE1AA201DD70EFF4AAC75
SHA-256:	896C9BD2EDA0D6EEA85229BA58AB7E423D179FD5567CBF0DC9B7EBC1D0539E1D
SHA-512:	8A377209C5DB20248067D2B8283610B58370F6EB8A8AAB1741674414AC07B124678A89A5D85AFA563D09CD526114DA0EE534BDF36A35E43D4DA7FC2D63977D5
Malicious:	false
Reputation:	low
Preview:	sdPC.....@.*.L..nM._bM

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0bfa846f-7f2b-447d-b05b-00b7f02a94e3.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):	5.536073965477386
Encrypted:	false
SSDEEP:	384:209tNLlNKXH1kXqKf/pUZNCgVLH2HfDvrUi4HGOnTFphkGVr4u:bLl6H1kXqKf/pUZNCgVLH2HfDrUisGO/
MD5:	4323B29689F075DB5B55088CE702A7F2
SHA1:	13D4EA1A8DDFDB26FCBE97E05893DA05F6AB8072
SHA-256:	342C1C9EC455624C4011724A38FB7512941E219ECDED87050A159D641810BB9D
SHA-512:	A1DFC685EEC89477F12237F459A14623353B2C66751C3FE4AEEC88321C51378C5382EAD00D18DC73036E470F0C315B1C166171DC69C5E369C54DD8228667423
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":"13280384451977519","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\0f6fdc72-0039-45da-9754-65b2db937691.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):	5189
Entropy (8bit):	4.98292699557884
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0f6fdc72-0039-45da-9754-65b2db937691.tmp	
SSDEEP:	96:n/3hA51l9pYKIwik0JCKL8ckR1LbOTQVuwn:nfhcl9pY6k4KJkRp
MD5:	B9443CBD7E8FF6F03D9B5BF0C4E54712
SHA1:	C791BB0819E36CE51F1EDBEB598DFE1DC07B7599
SHA-256:	4251B1948E8E21C5D1B69B3FC2F6E7B603525898E64800381684AA519122D43D
SHA-512:	CB10C44F9525E18AE289210A663E319C8401DBB6C02001111BCE509677464D334401D39FFA709913E4249A52BB774CE0411A816E42B235898A5B5E10DFB8212A
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280384452686033","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\39e1b833-af68-41e1-b4d9-0bc310436bda.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):	5217
Entropy (8bit):	4.987288131734973
Encrypted:	false
SSDEEP:	96:n/3huEV1l9pYKIkik0JCKL8ckR1gbOTQVuwn:nfhuml9pYek4KJkRQ
MD5:	E580F4CC08F714DFAFF9DE0CCF8FBED2
SHA1:	36A1FA43FA1EE358D7A0876E220202C735CB8871
SHA-256:	16F2E2A68D2383A986D4065D480382D7FC45681CF4C41A6C58D09D8AD376B9E8
SHA-512:	1E682705794F51622D3FBEDE4ED8D3127F69905A6D45CDBECA0FAD3D59442C4478A29D2799455BAEE9D73035049F9BB7CEF7694B65BFDD116DF185AC36E39FB
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280384452686033","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\60d1765d-f5ba-436e-a0ad-7aca6a309fc0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.5777151742118685
Encrypted:	false
SSDEEP:	384:209tULlNKXH1kXqKf/pUZNCgVLH2HfDvrUt2hkmVr4Pl:iLl6H1kXqKf/pUZNCgVLH2HfDrUgDNS
MD5:	2983FECFE7144D2832F6906663F252E7
SHA1:	9F9E2CC94DBCBE9A1D9C981036553B25BAA024D8
SHA-256:	EBFB6299CAB07BB279BA709EE9944E1F54CAC48E6F83AE3E5FAA084F5030702A
SHA-512:	2A6D1BB4ED9432D121E45AFD641ED6440014FA1C5C18347E38314AA610DA85CBDA8CBE49F58DAAE4A9E25D6723F7F029F0384AB388C6D14FAF7C5E70769D1D8
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":"13280384451977519","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\70ef5a4d-5fda-4df5-9f0b-a5534478002f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	203
Entropy (8bit):	5.376032779001182
Encrypted:	false
SSDEEP:	6:YAQNN1jS9RfSHJR8wXwlmUUAnIMp5bIsSQ:Yw9RAJ9+UAnI1Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\70ef5a4d-5fda-4df5-9f0b-a5534478002f.tmp	
MD5:	5F777B860C00BF49542200584F755AE7
SHA1:	B8F113A427873F129AEFAFA03DFBB959226FFDBE
SHA-256:	8E1CA8475CA9312EEC18FE40461E00E1E0B425B3C3581875DDEF69982B4591BC
SHA-512:	E3FCA5AA400C062AA1409CC4EDB2EBE34DBA17B0B063408C95928ED78F10C2E147C3FBE464DBA1ED5437832CC22CBB64B881065C1BABD6FCA0F91088012DE517
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1667446877.915472,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1635910877.915479}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\731cb0a9-891b-4cbc-a09d-2b3daca1f26d.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):	6030
Entropy (8bit):	5.199555967680918
Encrypted:	false
SSDEEP:	96:n/3huEs1l9xHbNLgEYKIkik0JCKL8ckR11Ikfh0bOTQVuwn:nfhutl9xHhYek4KJkRMkfE
MD5:	FBB59A47B81B2A728604EF2E2E78F418
SHA1:	98618BAF5202852EFC5F7B86BBB82533162523C9
SHA-256:	07C8ED5BD315B71292767DBC3E2C590BCC06AB6F6BCA8B267AA8A42458741952
SHA-512:	A843DBD909EFFFCC87ECB7777BD985E5841A521C96C5BFBFABA1D24DE2302F77D97AD26A209B1E5E64F130458819613B86D49260BCCDB2369BFE8341B38AE2A0
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280384452686033","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\74e0311c-bc39-4e29-8439-e10b46d645c7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	17092
Entropy (8bit):	5.583272428784405
Encrypted:	false
SSDEEP:	384:209tNLlNKXH1kXqKf/pUZNCgVLH2HfDvrU1phkoVr45:bLl6H1kXqKf/pUZNCgVLH2HfDrUrJN6
MD5:	66359CF86DB560B04114540F6C792F72
SHA1:	770B9BE15D8670C07617977C09601CB80E6DF764
SHA-256:	C11A18245C29E70050BCB9EA02FC4C1D6244062A568BF035FFD6F1BFEEF3A227
SHA-512:	B447F6C61B25295AEB33F091B23B683C6A2ADA9D21CC99F8D054BFD320E4B412DDAB5E37FC536AD3CF4D292F70F253D178868FBFDB4CE98DF833849A506A6EDF
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":"13280384451977519","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\7629fe09-8f4f-4857-a76e-7f840ed793fc.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2724
Entropy (8bit):	4.858756821586387
Encrypted:	false
SSDEEP:	48:YXsPMHi5s7MHgKsSMH/zs8MHIs51tFsL6zsbWsdCshDysuMHCLsKMH9swIMHlYhm:XGiQGBGFGJ12LLHDwGyGkGihm
MD5:	7AFFAA83A7FEFFB198C390FD9C7A8C4E
SHA1:	E768AF801A60E0B5486B08F6DCEE0CA51F262BD7
SHA-256:	2B88886C774450BC405A17760BF8FF3FA0A196EB31284040143E486ABC9CA198

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7629fe09-8f4f-4857-a76e-7f840ed793fc.tmp	
SHA-512:	07FF1417DAF313391C05D023CBD81FFE9ECF9CAD2030AA083BFDC260E4018999C200177B315F74D9ECF59ECDB37CB3F34869D7D79073B9998537351A5B7B101
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544495618845","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31528},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345624305","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":26637},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345531701","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":53820},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345601356","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":36228},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7a4d6bfd-86bb-4151-ada6-fdd982ecb833.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2724
Entropy (8bit):	4.858441642519087
Encrypted:	false
SSDEEP:	48:YXsPMHi5s7MHgKsSMH/zs8MHIs51tFsL6zsbWsdCshDysuMHCLsKMH9swIMHlYhj:XGiQGBGFGJ12LLHDwGyGkGihj
MD5:	9E0C31BCE1C83C78981EB86A29E2879B
SHA1:	3973E5D4DA1BC0BB99B78D1DFA7BEA045C85E173
SHA-256:	3D1BDA968D1CFF79DBD0C4B9D2A22367E9D9B8374622CD4263BD39137D8FE584
SHA-512:	D196B2993F4A46AFFD38DBA59866B048221D5CF6EAB1574846D1799B748BD71B09BE28D8154B16D97AEA300C7EE13719DC2E5034EC9D8913C6A6B399BDEBC2E
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544495618845","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31528},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345624305","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":26637},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345531701","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":53820},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544345601356","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":36228},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7bb9de8b-9790-47b2-b37e-f712bade65d6.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):	5189
Entropy (8bit):	4.9812403520199515
Encrypted:	false
SSDEEP:	96:n/3hMq/9pYKIBik0JCKL8ckR1LbOTQVuwn:nfh99pYPk4KJkRp
MD5:	D5E3742FF2F799824CC5718B4D324AA0
SHA1:	FADCB2A410F7BF9ED1139393FBE1F2D5776E52A7
SHA-256:	A470335450BFA613C77385A0FDD06E9B350624FB69BD45FA28E12B5ADAF6DCCD
SHA-512:	ED647C0BB0CBDE374F4C8AF660783C8E251719A9B49BC58200E5B5345CBAB57A15F85B417941B81F5264CB0B136851C32162461B5E7C223F937518F8332F0732
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280384452686033","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7e2b4015-2a63-438b-ae5d-d9b9a9e0db54.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7e2b4015-2a63-438b-ae5d-d9b9a9e0db54.tmp	
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8647d2f5-e2a3-437d-ba06-f62213f5cbae.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):	5.5703347378221455
Encrypted:	false
SSDEEP:	384:209tNLlNKXH1kXqKf/pUZNCgVLH2HfDvrUi4HGFphkMVr4n:bLl6H1kXqKf/pUZNCgVLH2HfDrUisG7A
MD5:	66C65AD10C55DB77FC30187189EA55DC
SHA1:	BD059E03BA3900514672A8D7AAB7C76985520358
SHA-256:	6FAC58D422AE4FD82CD3D4C2BD7F8B159F6984BCE1290F3538E0CB294EFA5D67
SHA-512:	6D760DB722A4DF6ED640539E81CD338CA775C3C1E36B7BFEABD9B1EB9210B3CAE63D6B7C272BD7EC685AB84B0CD435C990D850B3EB5477B42D1FB3A14C0C D7A
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13280384451977519","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\89b99dc9-af82-4da7-b5ad-fec9e1117db0.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):	705
Entropy (8bit):	5.568954551746554
Encrypted:	false
SSDEEP:	12:YaMM+j4HH+UAnIb3Rsty9RAJ9+UAnIKcJVDMpL/fN+UAnIRcLrNgmh4r+UAnIkVQ:YIyKeUh3Uy9RAeUA2KrfwUXSG1KUEQ
MD5:	874ACCF5F38EA45DAC3844F6C609C50E
SHA1:	3648E4358070D485DA51C309AD641FBC2F76AB7D
SHA-256:	021989B6616EACE919F7F9F40740F0FEBF47873C92B62A8F5EA761349E6D67D5
SHA-512:	53D5DA10A34E8EF162F8632FE9A189A0EC5F599FA9E75C45DC4E5FB1DB01EE4769147A319050D61B92B911222A4A966AE6B091A0BECF0F63FFECA6B9B673EB A9
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1646797292.866353,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains" :true,"sts_observed":1635910892.866358},{"expiry":1667446912.537166,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_in clude_subdomains":true,"sts_observed":1635910912.537174},{"expiry":1667446886.955972,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force- https","sts_include_subdomains":true,"sts_observed":1635910886.955977},{"expiry":1667446884.678897,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2O kgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1635910884.678903}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9b46ea77-bd9a-458c-ac46-8c6841577861.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):	5189
Entropy (8bit):	4.982954276114193
Encrypted:	false
SSDEEP:	96:n/3hA51l9pYKIXik0JCKL8ckR1LbOTQVuwn:nfhcl9pY5k4KJkRp
MD5:	60A3267752C6D44643ADB38D28DB69E2
SHA1:	E9D9E772F4A4D942EA083D961FB42E86159C9BE5
SHA-256:	2B198C1443966B8D6EA8342638268A3C9AC88D42EEB33D5FD0B889F8AE2C1A10
SHA-512:	A6B28643935BA1D04897C6CF7AE715D7EACD801A373E7D774CA58E472FB44936E2FB0D96E0EC2D56E11090951FD0AF3E412292C36363C47BA022E54126C323B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9b46ea77-bd9a-458c-ac46-8c6841577861.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280384452686033","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQIOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUscllJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkIjEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrIVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=","eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKnMKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9uqQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhIktCK62v2P3OZQAWupWsYzCnvk=","L

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
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):	377
Entropy (8bit):	5.21097014423374
Encrypted:	false
SSDEEP:	6:m8wm+q2PcNwi23iKKdK25+Xqx8chI+IFUtHwFZmwxU2VkwOcNwi23iKKdK25+Xqp:5+vLZ5KkTXfchI3FUtg/e2V54Z5KkTXc
MD5:	066BDEF61FB14C1627E9D421EB4AB169
SHA1:	6A1D0474FA62E4FE517293FDCD10050C8F528608
SHA-256:	9185769833A4603E7D97B7FD008F20F8AD5ECDBF22CCF5D2E9B81F4E8909363D
SHA-512:	DC70EBF2817749361EAA73EC9D21AC05E657DE0CDA568AB97845CDAF864ABAFA425D19C5C6DCF3D6670AE92F945B3E8FC41AE952FF674374EC3199E8B185C 29
Malicious:	false
Reputation:	low
Preview:	2021/11/02-20:41:12.722 b4c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MAN IFEST-000001.2021/11/02-20:41:12.729 b4c Recovering log #3.2021/11/02-20:41:12.737 b4c 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.oldYT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	377
Entropy (8bit):	5.21097014423374
Encrypted:	false
SSDEEP:	6:m8wm+q2PcNwi23iKKdK25+Xqx8chI+IFUtHwFZmwxU2VkwOcNwi23iKKdK25+Xqp:5+vLZ5KkTXfchI3FUtg/e2V54Z5KkTXc
MD5:	066BDEF61FB14C1627E9D421EB4AB169
SHA1:	6A1D0474FA62E4FE517293FDCD10050C8F528608
SHA-256:	9185769833A4603E7D97B7FD008F20F8AD5ECDBF22CCF5D2E9B81F4E8909363D
SHA-512:	DC70EBF2817749361EAA73EC9D21AC05E657DE0CDA568AB97845CDAF864ABAFA425D19C5C6DCF3D6670AE92F945B3E8FC41AE952FF674374EC3199E8B185C 29
Malicious:	false
Reputation:	low
Preview:	2021/11/02-20:41:12.722 b4c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MAN IFEST-000001.2021/11/02-20:41:12.729 b4c Recovering log #3.2021/11/02-20:41:12.737 b4c 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):	1375
Entropy (8bit):	5.668522270671351
Encrypted:	false
SSDEEP:	24:HDCdxt9XDZkGl9IRukoj0GgGjMXe892dtthVa9yBDOxo7nQBrxzkr25wNiyJsyw7:OLXDZkGlhSGppjdtaJFEwSzw6JLCZ
MD5:	74981161EDD13237035E8E910BAB9529
SHA1:	4B4BDEE527CEB6F92464CE88D2D4E012877CD2A4
SHA-256:	5F6A2939DD1B4FC9B8626CE64E096A4CB7518A1621A6BF9A8AF0F1BBEB524E94
SHA-512:	2894DF460C788ACFA4BA45CA6FC683A82C9FA4E4703B15D972A0607A2A6DDFD5AB7F043CD354447148D45AFDB8B6828F21E6A4B2D53FF7E6556BB1433FA1962 2
Malicious:	false
Reputation:	low
Preview:	....."....about..https..org..rchsd..us..www..abbodsx2hand3rhcso3viayp..abbybywb0o0pvf3l0uo5dmrj..c..children's..chsd..e..eac..edu..em..email..hospital..m..point loma..rady..registration..s..secure*.....abbodsx2hand3rhcso3viayp.....abbybywb0o0pvf3l0uo5dmrj.....about.....c.....children's.....chsd.....e.....eac.....edu.....em..... .email.....hospital.....https.....m.....org.....pointloma.....rady.....rchsd.....registration.....s.....secure.....us.....www..2.....'.....0.....2.....3.....5.....a..... ..b.....c.....d.....e.....f.....g.....h.....i.....j.....l.....m.....n.....o.....p.....r.....s.....t.....u.....v..... .w.....x.....y.....:

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5217
Entropy (8bit):	4.987288131734973
Encrypted:	false
SSDEEP:	96:n/3huEV1l9pYKIkik0JCKL8ckR1gbOTQVuwn:nfhuml9pYek4KJkRQ
MD5:	E580F4CC08F714DFAFF9DE0CCF8FBED2
SHA1:	36A1FA43FA1EE358D7A0876E220202C735CB8871
SHA-256:	16F2E2A68D2383A986D4065D480382D7FC45681CF4C41A6C58D09D8AD376B9E8
SHA-512:	1E682705794F51622D3FBEDE4ED8D3127F69905A6D45CDBECA0FAD3D59442C4478A29D2799455BAEE9D73035049F9BB7CEF7694B65BFDD116DF185AC36E39FB
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280384452686033","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5189
Entropy (8bit):	4.98292699557884
Encrypted:	false
SSDEEP:	96:n/3hA51l9pYKIwik0JCKL8ckR1LbOTQVuwn:nfhcl9pY6k4KJkRp
MD5:	B9443CBD7E8FF6F03D9B5BF0C4E54712
SHA1:	C791BB0819E36CE51F1EDBEB598DFE1DC07B7599
SHA-256:	4251B1948E8E21C5D1B69B3FC2F6E7B603525898E64800381684AA519122D43D
SHA-512:	CB10C44F9525E18AE289210A663E319C8401DBB6C02001111BCE509677464D334401D39FFA709913E4249A52BB774CE0411A816E42B235898A5B5E10DFB8212A
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280384452686033","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferencesv (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):	5189

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferencesv (copy)	
Entropy (8bit):	4.982954276114193
Encrypted:	false
SSDEEP:	96:n/3hA51l9pYKIXik0JCKL8ckR1LbOTQVuwn:nfhcl9pY5k4KJkRp
MD5:	60A3267752C6D44643ADB38D28DB69E2
SHA1:	E9D9E772F4A4D942EA083D961FB42E86159C9BE5
SHA-256:	2B198C1443966B8D6EA8342638268A3C9AC88D42EEB33D5FD0B889F8AE2C1A10
SHA-512:	A6B28643935BA1D04897C6CF7AE715D7EACD801A373E7D774CA58E472FB44936E2FB0D96E0EC2D56E11090951FD0AF3E412292C36363C47BA022E54126C323B
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280384452686033","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferencesw. (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):	5189
Entropy (8bit):	4.9812403520199515
Encrypted:	false
SSDEEP:	96:n/3hMq/9pYKIBik0JCKL8ckR1LbOTQVuwn:nfh99pYPk4KJkRp
MD5:	D5E3742FF2F799824CC5718B4D324AA0
SHA1:	FADCB2A410F7BF9ED1139393FBE1F2D5776E52A7
SHA-256:	A470335450BFA613C77385A0FDD06E9B350624FB69BD45FA28E12B5ADAF6DCCD
SHA-512:	ED647C0BB0CBDE374F4C8AF660783C8E251719A9B49BC58200E5B5345CBAB57A15F85B417941B81F5264CB0B136851C32162461B5E7C223F937518F8332F0732
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280384452686033","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure 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):	19181
Entropy (8bit):	5.5703347378221455
Encrypted:	false
SSDEEP:	384:209tNLlNKXH1kXqKf/pUZNCgVLH2HfDvrUi4HGFphkMVr4n:bLl6H1kXqKf/pUZNCgVLH2HfDrUisG7A
MD5:	66C65AD10C55DB77FC30187189EA55DC
SHA1:	BD059E03BA3900514672A8D7AAB7C76985520358
SHA-256:	6FAC58D422AE4FD82CD3D4C2BD7F8B159F6984BCE1290F3538E0CB294EFA5D67
SHA-512:	6D760DB722A4DF6ED640539E81CD338CA775C3C1E36B7BFEABD9B1EB9210B3CAE63D6B7C272BD7EC685AB84B0CD435C990D850B3EB5477B42D1FB3A14C0CD7A
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":"13280384451977519","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure PreferencesMP (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19182
Entropy (8bit):	5.5702925022425065
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure PreferencesMP (copy)	
SSDEEP:	384:209tNLlNKXH1kXqKf/pUZNCgVLH2HfDvrUi4HGAphkfVr45:bLl6H1kXqKf/pUZNCgVLH2HfDrUisGq/
MD5:	BDFBEB5635EAF8B323C1E30FED82B5C2
SHA1:	B3D3BA4632A5013E0C578712F26F09D2BA46FC0D
SHA-256:	6AF57FB9506D38FBAD16D5AECD964C87B4A680C25DBB6F916411B5A7205CA443
SHA-512:	4FB91C200BE09A12C74EF46A2BA3951F911EDD56F373F111530FCC71528D9E5ED1DF960287C0152A06F1645AB32753EE5752984CA6DE9A5749225CE0081F1245
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":"13280384451977519","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 Preferencesrc (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.5777151742118685
Encrypted:	false
SSDEEP:	384:209tULlNKXH1kXqKf/pUZNCgVLH2HfDvrUt2hkmVr4Pl:iLl6H1kXqKf/pUZNCgVLH2HfDrUgDNS
MD5:	2983FECFE7144D2832F6906663F252E7
SHA1:	9F9E2CC94DBCBE9A1D9C981036553B25BAA024D8
SHA-256:	EBFB6299CAB07BB279BA709EE9944E1F54CAC48E6F83AE3E5FAA084F5030702A
SHA-512:	2A6D1BB4ED9432D121E45AFD641ED6440014FA1C5C18347E38314AA610DA85CBDA8CBE49F58DAAE4A9E25D6723F7F029F0384AB388C6D14FAF7C5E70769D1D8
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":"13280384451977519","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\81845bdb-4489-46cb-8745-1eb6b4d95f84.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.957371343316884
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5hsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sd7sBdLJlyH7E4f3K33y
MD5:	363D9EBEDB5030036B53B6B28E8A8EA5
SHA1:	1C7C9012156AC8295EB465BC774430A866096832
SHA-256:	466FE09323B709A587648157D77298132B29F7CD916CD68EF6B28A0FC5EE355B
SHA-512:	9C9A230BAF627B8A9856C0AC66E4EA262C304BBC2272662F4213EB617297DFE222E0CCC4FC0F22B04FAFB3125D55D774174700B381EA3FF90B8C3D11926E023
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544335120983","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\91adff0b-dae8-46e3-b259-1408c3267668.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):	4.95811465076361
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5hsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRKXk1Yn:YHO8sd7sBdLJlyH7E4f3K3X
MD5:	1AF1134949163D4A7CF67ECC19FA5A08
SHA1:	45658A19010DA3AAF326344BB13CC255C33D7E53

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\91adff0b-dae8-46e3-b259-1408c3267668.tmp	
SHA-256:	5BDDE35D93B9EB9BEBF4CC76246A909ECB019746371DD87B0AB64B26185BB59B
SHA-512:	3BB06987F2F5E57E1FA3EDB0308BA64EDE7E7D88905109BBFB18D42C97185A00042DA17E7B69D678E58C2C14877FA0150F8E2DC170F6065CB7AD9BBFFADB8B9F
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544335120983","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"3G"}}}

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:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E889858
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.95811465076361
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5hsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRKXk1Yn:YHO8sd7sBdLJlyH7E4f3K3X
MD5:	1AF1134949163D4A7CF67ECC19FA5A08
SHA1:	45658A19010DA3AAF326344BB13CC255C33D7E53
SHA-256:	5BDDE35D93B9EB9BEBF4CC76246A909ECB019746371DD87B0AB64B26185BB59B
SHA-512:	3BB06987F2F5E57E1FA3EDB0308BA64EDE7E7D88905109BBFB18D42C97185A00042DA17E7B69D678E58C2C14877FA0150F8E2DC170F6065CB7AD9BBFFADB8B9F
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544335120983","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"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):	4.957371343316884
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5hsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sd7sBdLJlyH7E4f3K33y
MD5:	363D9EBEDB5030036B53B6B28E8A8EA5
SHA1:	1C7C9012156AC8295EB465BC774430A866096832
SHA-256:	466FE09323B709A587648157D77298132B29F7CD916CD68EF6B28A0FC5EE355B
SHA-512:	9C9A230BAF627B8A9856C0AC66E4EA262C304BBC2272662F4213EB617297DFE222E0CCC4FC0F22B04FAFB3125D55D774174700B381EA3FF90B8C3D11926E023
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544335120983","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\6bc793fe-8b45-4e39-8be7-c1b73ab9686d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.96345415074364
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5Z0WlyhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sd/0WCsBdLJlyH7E4f3K33y
MD5:	1FE877DDE8B96DED122AC08BB07A83C5
SHA1:	5BEA5FFAF686474CE8ACA1D95500C29D65007745
SHA-256:	3AD373EB6FF8EA394964EDA2A9E53ADD8DBA11DC9716ED3CA672F10DF369BA4D
SHA-512:	1854F005CD691674FCF27376150ABD6F036A79C42BB4FFECDCCA14A74CB21D8ADF2552CACE631E6E9C92C58E7EF27279CA30CE5648C8EB90B06F2247A462003
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248544342473569","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEllllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898I58
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	435
Entropy (8bit):	5.197482791614491
Encrypted:	false
SSDEEP:	12:SEOvLZ5KkkGHArBFUt5b/wj54Z5KkkGHAryJ:nMl5KkkGgPgq1o5KkkGga
MD5:	8ECED7946CFFD70103D94BC28834A9F5
SHA1:	C25D19228A23AF3292A30F6C4A72459EE90C38C4
SHA-256:	01E5FB43DF24750E2BA047BA3F8E17CB3558296E92728B8555E204EBE63186A6
SHA-512:	804E34A012593AE2182AA4B784B727DB32AD76F97248C9CDFB09909A2BF86A4C47E167A893D9B1D4DB5C556EF0ED5F46ECA7550DDDCC1CD6B788DE043E2A1A6
Malicious:	false
Reputation:	low
Preview:	2021/11/02-20:41:53.627 914 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/11/02-20:41:53.630 914 Recovering log #3.2021/11/02-20:41:53.631 914 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	435
Entropy (8bit):	5.197482791614491
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb\LOG.old (copy)	
SSDEEP:	12:SEOvLZ5KkkGHArBFUt5b/wj54Z5KkkGHAryJ:nMl5KkkGgPgq1o5KkkGga
MD5:	8ECED7946CFFD70103D94BC28834A9F5
SHA1:	C25D19228A23AF3292A30F6C4A72459EE90C38C4
SHA-256:	01E5FB43DF24750E2BA047BA3F8E17CB3558296E92728B8555E204EBE63186A6
SHA-512:	804E34A012593AE2182AA4B784B727DB32AD76F97248C9CDFB09909A2BF86A4C47E167A893D9B1D4DB5C556EF0ED5F46ECA7550DDDCC1CD6B788DE043E2A1A6
Malicious:	false
Reputation:	low
Preview:	2021/11/02-20:41:53.627 914 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/MANIFEST-000001.2021/11/02-20:41:53.630 914 Recovering log #3.2021/11/02-20:41:53.631 914 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	437
Entropy (8bit):	5.2355125708317525
Encrypted:	false
SSDEEP:	12:UvLZ5KkkGHArqiuFUtyHh/z54Z5KkkGHArq2J:el5KkkGgCgMbo5KkkGg7
MD5:	EBA66423B0160EF1C3FAFF5CCB8ABE51
SHA1:	3ED44968DE23E8694BA6979AC9B51E483ADAF22A
SHA-256:	165D650E7E2D24C589CB1252FFF5BF5E2E6A3ED07FD842944221D2DF012465C2
SHA-512:	A9FEDE28B3FFCF2C84B95930338ADB89F8FD0399D9C7A1909A4F0A79D832AF8F5597FD718ED2F8FF5E35DFAF7E2BFE5CB2C30EAC4F0260E5C97C7E3BCED4CF54
Malicious:	false
Reputation:	low
Preview:	2021/11/02-20:41:53.654 8b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/11/02-20:41:53.657 8b0 Recovering log #3.2021/11/02-20:41:53.658 8b0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG.old.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	437
Entropy (8bit):	5.2355125708317525
Encrypted:	false
SSDEEP:	12:UvLZ5KkkGHArqiuFUtyHh/z54Z5KkkGHArq2J:el5KkkGgCgMbo5KkkGg7
MD5:	EBA66423B0160EF1C3FAFF5CCB8ABE51
SHA1:	3ED44968DE23E8694BA6979AC9B51E483ADAF22A
SHA-256:	165D650E7E2D24C589CB1252FFF5BF5E2E6A3ED07FD842944221D2DF012465C2
SHA-512:	A9FEDE28B3FFCF2C84B95930338ADB89F8FD0399D9C7A1909A4F0A79D832AF8F5597FD718ED2F8FF5E35DFAF7E2BFE5CB2C30EAC4F0260E5C97C7E3BCED4CF54
Malicious:	false
Reputation:	low
Preview:	2021/11/02-20:41:53.654 8b0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/11/02-20:41:53.657 8b0 Recovering log #3.2021/11/02-20:41:53.658 8b0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Malicious:	false
Reputation:	low
Preview:	*...#.....version.1..namespace-..&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	426
Entropy (8bit):	5.158091839504587
Encrypted:	false
SSDEEP:	12:s+vLZ5KkkGHArAFUtPtW/TiV54Z5KkkGHArfJ:9l5KkkGgkgVNo5KkkGgV
MD5:	DDF3DA9D5A1F51257CE30E9F1B21F42E
SHA1:	6A0DA7922C6D53FE88F1CA47E00C42BA12725E1F
SHA-256:	5CE0A7F7312599F942375C3DEE876250AF410B540058E5808FD1BEE2A95E721F
SHA-512:	2B39D2D2E243B07562A2E1C7497F215B986D88B736216E45E74E2BF6940D71DDBB0EEF292D7D114EABA2FB131FBDA1FDE5241891C14C7E6E23665F07A814C78F
Malicious:	false
Reputation:	low
Preview:	2021/11/02-20:42:09.717 145c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/11/02-20:42:09.719 145c Recovering log #3.2021/11/02-20:42:09.720 145c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	426
Entropy (8bit):	5.158091839504587
Encrypted:	false
SSDEEP:	12:s+vLZ5KkkGHArAFUtPtW/TiV54Z5KkkGHArfJ:9l5KkkGgkgVNo5KkkGgV
MD5:	DDF3DA9D5A1F51257CE30E9F1B21F42E
SHA1:	6A0DA7922C6D53FE88F1CA47E00C42BA12725E1F
SHA-256:	5CE0A7F7312599F942375C3DEE876250AF410B540058E5808FD1BEE2A95E721F
SHA-512:	2B39D2D2E243B07562A2E1C7497F215B986D88B736216E45E74E2BF6940D71DDBB0EEF292D7D114EABA2FB131FBDA1FDE5241891C14C7E6E23665F07A814C78F
Malicious:	false
Reputation:	low
Preview:	2021/11/02-20:42:09.717 145c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/11/02-20:42:09.719 145c Recovering log #3.2021/11/02-20:42:09.720 145c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	410
Entropy (8bit):	5.321286848135815
Encrypted:	false
SSDEEP:	12:6D+vLZ5KkkOrsFUtUiAW/Si3V54Z5KkkOrzJ:6gl5Kk+gU754o5Kkn
MD5:	39E6D32B55D08D97CDE8C34B166EA5EB
SHA1:	4EE9DB7F23233ED955FF4A584A2DEBA139CD41C0
SHA-256:	298E3076CDF3715B54079588280A618F4851137A9786AF1B0E3518FDD148AB1F
SHA-512:	CC54830555B97D2086B1A82A34130651FBFEA282AB97234972535E7D836341DB443212B5AA7B45499D1CCC39D5E614A8AD79E2D1458CCCB7A5326E2C6D867F9
Malicious:	false
Reputation:	low
Preview:	2021/11/02-20:42:58.735 145c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/11/02-20:42:58.736 145c Recovering log #3.2021/11/02-20:42:58.736 145c 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\TransportSecurityMP (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurityMP (copy)	
Size (bytes):	705
Entropy (8bit):	5.568403774115274
Encrypted:	false
SSDEEP:	12:YaMM+j4HH+UAnIb3RFH9RAJ9+UAnItvcJVDMpL/fN+UAnIRcLrNgmh4r+UAnIkVQ:YIyKeUh3v9RAeUCKrfwUXSG1KUEQ
MD5:	7123178CFF2CD9C6E28A832FA772A222
SHA1:	7FA4BEE34B03B865E5F04AF879BB5933C6997C0C
SHA-256:	4FEE86E6862B39A0C8D59E6E379717AAA0E576B2D2275B0581057CCD6375CACC
SHA-512:	ABB6B94EF3571BFC7542CF40F877AEDD5A6219355F76AF4E7D90350D5F98764396FF020BC5ED42FABD2C65D6FB1A1B6DA69E26ADD0CCBDCC17E776929ABC775
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1646797292.866353,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1635910892.866358},{"expiry":1667446886.900434,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1635910886.900438},{"expiry":1667446886.955972,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1635910886.955977},{"expiry":1667446884.678897,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1635910884.678903}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a725d6bb-ac14-4d90-9721-d33e29b2a4f2.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):	5.5702925022425065
Encrypted:	false
SSDEEP:	384:209tNLlNKXH1kXqKf/pUZNCgVLH2HfDvrUi4HGAphkfVr45:bLl6H1kXqKf/pUZNCgVLH2HfDrUisGq/
MD5:	BDFBEB5635EAF8B323C1E30FED82B5C2
SHA1:	B3D3BA4632A5013E0C578712F26F09D2BA46FC0D
SHA-256:	6AF57FB9506D38FBAD16D5AECD964C87B4A680C25DBB6F916411B5A7205CA443
SHA-512:	4FB91C200BE09A12C74EF46A2BA3951F911EDD56F373F111530FCC71528D9E5ED1DF960287C0152A06F1645AB32753EE5752984CA6DE9A5749225CE0081F1245
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":"13280384451977519","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\ae0456c6-a287-4813-ae2b-435f44766f70.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):	705
Entropy (8bit):	5.568403774115274
Encrypted:	false
SSDEEP:	12:YaMM+j4HH+UAnIb3RFH9RAJ9+UAnItvcJVDMpL/fN+UAnIRcLrNgmh4r+UAnIkVQ:YIyKeUh3v9RAeUCKrfwUXSG1KUEQ
MD5:	7123178CFF2CD9C6E28A832FA772A222
SHA1:	7FA4BEE34B03B865E5F04AF879BB5933C6997C0C
SHA-256:	4FEE86E6862B39A0C8D59E6E379717AAA0E576B2D2275B0581057CCD6375CACC
SHA-512:	ABB6B94EF3571BFC7542CF40F877AEDD5A6219355F76AF4E7D90350D5F98764396FF020BC5ED42FABD2C65D6FB1A1B6DA69E26ADD0CCBDCC17E776929ABC775
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1646797292.866353,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1635910892.866358},{"expiry":1667446886.900434,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1635910886.900438},{"expiry":1667446886.955972,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1635910886.955977},{"expiry":1667446884.678897,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1635910884.678903}],"version":2}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b4a9d5dc-169b-46ef-92ed-b1b44b9c8696.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5190
Entropy (8bit):	4.9831935867897235
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b4a9d5dc-169b-46ef-92ed-b1b44b9c8696.tmp	
SSDEEP:	96:n/3huE51l9pYKIGik0JCKL8ckR1LbOTQVuwn:nfhuwl9pY8k4KJkRp
MD5:	28B6C391FC34C0B061634D0F2D8C5AD3
SHA1:	AB34549899294A11967ECDF5859F1DE48E26F9F3
SHA-256:	754AF7CB52F28FE1183D267081E0C43C27EFD2295D1C27661D8D96E300261A00
SHA-512:	19EB30E2BFCBBFE05DC3DB65569D3A1E0D4451868360648811EA74B021A46F101FE0C0561F1A9DB571293ABB4CD8611D2BBCCDEF8469D3E846BFDC61F62C81 CA
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13280384452686033","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952329814949","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952502420488","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355952"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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\CURRENT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f2ceeec2-35ec-46a5-9257-6fb7597513a9.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):	4492
Entropy (8bit):	4.917559834499067
Encrypted:	false
SSDEEP:	96:JDHXTOazJ+9ZrsQ3GlG9GaG7GjDGMVwGuGoWGpEvGJGaBDcGftGeYoGsj:JDHXTOazJ+9Z/30+BMGTVwJ7WDvO/BQ4
MD5:	3147D6315C9E347E6A9380DD164AA235
SHA1:	5BF241AB9AFC4F9D53BA1C7EF9D79FFD30CB7B29
SHA-256:	00A3F1C792E4EE95871D7375F650AF8B96AFAAA0D955C83A314D54C1654440E1
SHA-512:	9634F8561F8B1E3BD8CC1045A26DC45B7ED92F4115DF607CA14F79FD06AA908108D008FE199F76BEE1176A1C25F1B0B48B7F1C28829719AD287014154D127D68
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f2ceeec2-35ec-46a5-9257-6fb7597513a9.tmp	
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13282976454349667","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13282976454395644","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13282976454487986","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"e

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\f52db802-6859-45b7-8928-df25f066b2bd.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):	3911
Entropy (8bit):	4.9232040254513985
Encrypted:	false
SSDEEP:	96:JDHXTOazJ+9ZrsQjD6VzGCYOM45cjMW1ELtKPzo6j:JDHXTOazJ+9Z/f6VzzYOM42jMWKJcEo
MD5:	5B82C5CF27453F63175033AD222746F8
SHA1:	411174B60221611869DBE5A179C74DFC59A2E4D8
SHA-256:	4177C0E28EA14A46F43A29EF91734811D8086F7A8EB580ED5725CEDAAE059FF5
SHA-512:	A2343487ECCD61DEBD5AF82CC83F90FB17155B295AA01485BAABF6F670F5169805CDEA8E06590A34741F24A84B6BE6991E4CA2C3FF5EC7F8D23DCE9F40D81E29
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13282976454349667","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13282976454395644","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13282976454487986","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"e

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tblolIrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State (copy)	
Category:	dropped
Size (bytes):	176506
Entropy (8bit):	6.047474742011752
Encrypted:	false
SSDEEP:	3072:Pf0L/3HqW0ZbXc+lmuK3HXlLA7bV/nYorVcI8XIssElYTRt:30b3KW0ZbXc3RlgbV/njhcI8II6Rt
MD5:	79276DD246FE0A7DACB0BD98A1F746BD
SHA1:	3009CF7044A03FE7299D41D73911D4E36E87A1F7
SHA-256:	3FAD53C6699B9FC1AB6EAA1B953B087A744C4D417B1E3832FC74E9FF65256814
SHA-512:	68156A8DD7214D3878E55BA03588DE793CD691B7400B1888E14E35C007A39124D261DF25783A092BB5F0EE41A8FB10D6757E08F9954AED3280C7EC76FE5D9DA
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":1.635910854109817e+12,"network":1.635882055e+12,"ticks":122084492.0,"uncertainty":3854697.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETlkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909004089"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Local StatetS (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):	176506
Entropy (8bit):	6.047475150324646
Encrypted:	false
SSDEEP:	3072:1f0L/3HqW0ZbXc+lmuK3HXlLA7bV/nYorVcI8XIssElYTRt:B0b3KW0ZbXc3RlgbV/njhcI8II6Rt
MD5:	337AAF4FB1ECB65B382A5799B65CCFE6
SHA1:	68E4E46E3B518C5F6044AC3EC9102E9934AFCC7E
SHA-256:	61247F806B2C5EB1E6F84BCBB2883E940CE2553781101152550 82AC677D4F8FD
SHA-512:	1C3B5078CCE3DD6658B03A0CDD90220950BE728E69D3D4E068A3D8B8C43197221B5536BE57D807F79318549C8165EFCB4D8C4BD2584864C080E96FB0D4EB5F2
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":1.635910854109817e+12,"network":1.635882055e+12,"ticks":122084492.0,"uncertainty":3854697.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETlkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0I1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909004089"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7514599466125884
Encrypted:	false
SSDEEP:	384:BrfMIihLa1yEVZrofNUrFvw83/MaXHi/GrerZ+wCxveGi5r1kmhtjNOsEwPOK2sw:xWqVJmSsvoeTGga4nrqcK+UY9O
MD5:	43E81CBD3A2BBA157724A0B94887005D
SHA1:	60E9DF5FE70697842341FC74AA9CA4C02429D2D6
SHA-256:	9A1FFEA98E8EB2DD7A5C88827389261B0562515F46C1BE858C70A8F5784DB47E
SHA-512:	2928A5BB776BBAC06E318A78814EAE5614D7B8CA3B090158CCAADD61EEE49B2DA92745B48A7E91279C3DD3F794DBB2E4AE24F9554AF6EE397B1DB7DEEE241FA8
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...#J8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache\p (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cache\p (copy)	
Size (bytes):	94708
Entropy (8bit):	3.7517107559976637
Encrypted:	false
SSDEEP:	384:RrfMIihLa1yEVZrofNUrFvw83/MaXHi/GrerZ+wCxveGi5r1kmh2NOsEwPOK2sNj:hWqVJmS3voeTGga4nrqcK+UY9z
MD5:	0EC932C8E9768737986D0F8B6EA7A147
SHA1:	88263A95B9D8DB9D771A1B34EE322FBC43AFA169
SHA-256:	A608BCD1B74615142F1F2BB50F58ABDFE876B9591BC859167A5E48C946A72906
SHA-512:	A34A70C55E47B518CD98F6587E0C0ADF8289D437FC308F4A7BCD851C179BC5CF0AFC5A31CBA8B7746B86A59371BB94A31D356786FAF44F2B00268AF65E659AD2
Malicious:	false
Reputation:	low
Preview:	.q.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...#J8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Module Info Cachees (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.751107734011847
Encrypted:	false
SSDEEP:	384:/rfMIihLmy9ofNUrFvw83/MaXHi/GrerZ+wCxveGi5r1kmh2NOsEwPOK2sNd1cFk:RqVJmS3voeTGga4nrqcK+UY95
MD5:	573384B0DC53A3AB9E0714485D172280
SHA1:	980E6620E5AD0FE17250E475253E80411A6FB6E4
SHA-256:	40B3DD5284977231EC1B9DBEBD46ED13AA44C6B74206CC04EC701E5DA35FDE7B
SHA-512:	C3600FDD9CD57D5C82270EFD1DE3D74A89519D4092C4E1370E621C435C2E4ED9A4AAE129D6D80EE67F0883AC91D6F71B6505C9EE179390DEF74E2B3CBD913B7
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...#J8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\b30ef004-77c7-4fb1-8cbd-2b46f4c2b917.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):	176600
Entropy (8bit):	6.047750335495459
Encrypted:	false
SSDEEP:	3072:Wf0L/3HqW0ZbXc+lmuK3HXlLA7bV/nYorVcI8XIssElYTRt:S0b3KW0ZbXc3RlgbV/njhcI8II6Rt
MD5:	EAFE189618F86BEF54459FEEAD3AD1FD
SHA1:	9F4C07DCA372BD49A7172887C2EECF60226AF636
SHA-256:	93B3A5C9598B5C8781A04B20DBF65591CE1BDD50D4B492FE58037EA21E2C09E1
SHA-512:	695915FAA18D66A8358EE6DCC81270592C05F61BF5F3ED2CF0528FA3038B8FE67C99A4CB404EA990D431A6C0C74420581DB9F5600058E21A034122D44C0D66B6
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":1.635910854109817e+12,"network":1.635882055e+12,"ticks":122084492.0,"uncertainty":3854697.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAAD5yRpyxHTvRo045wUdD0XcAAAAAAIAAAAAABBmAAAAAQAAIAAAABLbexqB/oExTFJmpcENOvX+bVETIkvlcZMf3oIBvp2bAAAAAA6AAAAAAgAAIAAAAAb9GGQ1QmHgGBymkKDudOpZA89StPbsfruaqqGAbN50MAAAALDWaloNNJZN9rwnlUq/XLN9khJ9Jz9md9VO4rX+Yg+g8mRS88Enlg3B2TpBYYNjwkAAAACddQYw45aj+S/8dGnDKvRWon1T/sv/0i6HXgLXg0l1kMUaef/c6zqkTQ7ehiG3nkSfg6dR/4o1ZLALr+MYbEZ2"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951909004089"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\b6657594-5af5-4017-bf28-4576982ce1cc.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724

C:\Users\user\AppData\Local\Google\Chrome\User Data\b6657594-5af5-4017-bf28-4576982ce1cc.tmp	
Entropy (8bit):	3.751107734011847
Encrypted:	false
SSDEEP:	384:/rfMIihLmy9ofNUrFvw83/MaXHi/GrerZ+wCxveGi5r1kmh2NOsEwPOK2sNd1cFk:RqVJmS3voeTGga4nrqcK+UY95
MD5:	573384B0DC53A3AB9E0714485D172280
SHA1:	980E6620E5AD0FE17250E475253E80411A6FB6E4
SHA-256:	40B3DD5284977231EC1B9DBEBD46ED13AA44C6B74206CC04EC701E5DA35FDE7B
SHA-512:	C3600FDD9CD57D5C82270EFD1DE3D74A89519D4092C4E1370E621C435C2E4ED9A4AAE129D6D80EE67F0883AC91D6F71B6505C9EE179390DEF74E2B3CBD913 B7
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...#J8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\faed375a-b496-4a30-aa58-f407f99e71f1.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7514599466125884
Encrypted:	false
SSDEEP:	384:BrfMIihLa1yEVZrofNUrFvw83/MaXHi/GrerZ+wCxveGi5r1kmhtjNOsEwPOK2sw:xWqVJmSsvoeTGga4nrqcK+UY9O
MD5:	43E81CBD3A2BBA157724A0B94887005D
SHA1:	60E9DF5FE70697842341FC74AA9CA4C02429D2D6
SHA-256:	9A1FFEA98E8EB2DD7A5C88827389261B0562515F46C1BE858C70A8F5784DB47E
SHA-512:	2928A5BB776BBAC06E318A78814EAE5614D7B8CA3B090158CCAADD61EEE49B2DA92745B48A7E91279C3DD3F794DBB2E4AE24F9554AF6EE397B1DB7DEEE241 FA8
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.... ...g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....* ...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...#J8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\..... .m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o .g.r.a.m.

C:\Users\user\AppData\Local\Temp\2436_1361747409_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:	37048EF8FADF62A26CAEC6EE90AC192429AB1E99424E5C68FACA90C0DAD68642C761FDCAC03FC38FA930841F91FA145A6943EC7F168D4F2FA426F1F092C2F5 2
Malicious:	false
Reputation:	low
Preview:	[{"description":"treehash per file","signed_content":{"payload":"eyJjb250ZW50X2hhc2hlcyI6W3siYmxvY2tfc2l6ZSI6NDA5NiwiZGlnZXN0Ijoic2hhMjU2IiwiZmlsZXMiO lt7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY19wbmFjbF9qc29uIiwicm9vdF9oYXNoIjoiVkNUSHNJVHNUSXVncWNhV2ctWHVpTU1 sdWloV1FSTE1sQnpTTGprdGhETSJ9LHsicGF0aCI6Il9wbGF0Zm9ybV9zcGVjaWZpYy94ODZfNjQvcG5hY2xfcHVibGljX3g4Nl82NF9jcnRiZWdpbl9mb3JfZWhfbyIs nJvb3RfaGFzaCI6ImxINWt2a1BvSVZZczZKVHhyOHc5Q2MxXzloVEJCX3lVSlF6VDZseVVNd0kifSx7InBhdGgiOiJfcGxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWN sX3B1YmxpY194ODZfNjRfY3J0YmVnaW5fbyIsInJvb3RfaGFzaCI6IkVuLVFQTW1HUm1xbG9Ud1gzOTAzckpsMkw0R25sQmdET1FhZlNKaHJ4Nk0ifSx7InBhdGgiOiJfc GxhdGZvcm1fc3BlY2lmaWMveDg2XzY0L3BuYWNsX3B1YmxpY194ODZfNjRfY3J0ZW5kX28iLCJyb290X2hhc2giOiJkT2lJVzRmdEdGNW9FY0k1UXYyYjBmd XNrUlYyaUVtdmxhbmV6MlpFc3VvIn0seyJwYXRoIjoiX3BsYXRmb3JtX3NwZWNpZmljL3g4Nl82NC9wbmFjbF9wdWJsaWNfeDg2XzY0X2xkX25leGUiLCJyb290X2hhc2g iOiIzNEU5QU9EMmpqLWNoMzZQZ0NVV0YtMUpYWVhVdlNGY1I4bks1aWppcWNjIn0seyJwYXRoIjoiX3B

C:\Users\user\AppData\Local\Temp\2436_1361747409_platform_specific\x86_64\pnacl_public_pnacl_json	
Entropy (8bit):	4.68252584617246
Encrypted:	false
SSDEEP:	12:TjLJ7qaVgPPd8bdzQBXefosmc5T9+n6e1Cetm1JXcAwA:TJ7jViPOd8wfHmZ6RP15
MD5:	35D5F285F255682477F4C50E93299146
SHA1:	FB58813C4D785412F05962CD379434669DE79C2B
SHA-256:	5424C7B084EC4C8BA0A9C69683E5EE88C325BA28564112CC941CD22E392D8433
SHA-512:	59DF2D5F2684FACC80C72F9C4B7E280F705776076C9D843534F772D5A3D578BEE04289AEE81320F23FB4D743F3969EDF5BA53FEBBAC8A4D27F3BC53BCF271C E
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 prev ent ", . "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\2436_1361747409_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:	85B1EDA4C473E00034EE627B7ABB894A77E521BC6A91A91A4A3744CA7511CB0AF10B9723D9ECC2CE3378DD70B659DF842D8C11875958CB77070CF01EC0A158 0
Malicious:	false
Reputation:	low
Preview:	.ELF.....>.....@.....@.....PH.....,$J.l=....J.$<A[..@.A...M..A..ffffff.....PH.....,$J.l=....J.$<A[..D..A...M..A..ffffff..... ....PH..1..,$J.l=....J.$<A[.....A...M..A..ffffff.....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\2436_1361747409_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
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..ffffff.....PH.....,$J.l=....J.$<A[..D..A...M..A..ffffff..... ....PH..1..,$J.l=....J.$<A[.....A...M..A..ffffff.....PH..,$J.l=....J.$<A[f.....A...M..A..ffffff.....PH..,$J.l=....J.$<A[f.....A...M..A..ffffff.....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\2436_1361747409_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

C:\Users\user\AppData\Local\Temp\2436_1361747409_platform_specific\x86_64\pnacl_public_x86_64_crtend_o	
SHA-512:	FE3F86E926759E71494F2060C4ED3C883EBCAF20CB129A5AD7F142766C33FAB10B5FABC3C7C938E0E895E27EA0AC03CBFE8D0EEABF5300A4AD07F67FD96CC253
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\2436_1361747409_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:	8EF8689E00E4B210A30444D18ED6247F364995ABEB2FD272064C3AF671EEDB4D9B8B67CA56F72FEBF8F56896D4EA7EC4B10CB445FFA1C710C1F312E9DA0E486
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\2436_1361747409_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
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.n acl_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_4 xi32_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\2436_1361747409_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

C:\Users\user\AppData\Local\Temp\2436_1361747409_platform_specific\x86_64\pnacl_public_x86_64_libgcc_a	
SHA-512:	01281DE92B281FB29E1ACA96AA64B740B65CC3A9097307827F0D8DB9E1C164C56AFCDFA0BF138EA670A596D55CE2C8D722760744E9FC9343BB6514417BF333E A
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.__div moddi4.__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\2436_1361747409_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:	46116B8BABC719676D68FD40D2AC82F38A3D13D8A482ADFC6FC32A99170AC3420E52CC33242CCD0FA723ABF4FA5EDBB9CE16A09C729BF04AE4AFBB2F67A1E 38B
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 ce163f dd0f16b4481e5cf77a16d45e9b4dc8300e) (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\2436_1361747409_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
SSDEEP:	24:MOcpdhWE5O/bZbmT3296bmT3TwQwDnvD/+R3:MHuECdaTS6aTTwXDvD/+l
MD5:	F950F89D06C45E63CE9862BE59E937C9
SHA1:	9CFAD34139CC428CE0C07A869C15B71A9632365D
SHA-256:	945B1C8A1666CBF05E8B8941B70D9D044BAAFB59B006F728F8995072DE7C4C40
SHA-512:	F9AFBB800A875EDCC63DEA4986179E73632B3182951A99C8B3D37DB454EFD7CC7192ECA5AC87514918A858BAD6DAEAB59548CA2E90EADA9900EF5B9F08E62 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\2436_1361747409_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:	0B4FF60B5428F81B8B1BCF3328CF80CBD88D8CE5E8BDBC236B06D5A54E7CF26168A3ABB348D87423DA613AB3F0B4D9B37CB5180804839F1CA158EC2B315DDF 00

C:\Users\user\AppData\Local\Temp\2436_1361747409_platform_specific\x86_64\pnacl_public_x86_64_pnacl_llc_nexe	
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	.ELF.....>..... .....@.....@.8...@.....$.....I.....I.....'.....G..... .....@.....@.....P.td.....D.....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\2436_1361747409_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\2436_1361747409\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
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\2436_1361747409\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

C:\Users\user\AppData\Local\Temp\2436_1361747409\manifest.json	
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\31ee74f6-483d-4a16-9061-7c973bbd367e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\547848f5-3b3a-45d9-aa6e-1fdf87495b09.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.$.....I-m.....ni...`..W.....R.p.b.+...+.\k.R$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\e1f1d19e-22c3-4008-85bf-b10acfd88a2f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Temp\e2524fb5-dae4-4dc3-89db-84c45e773e98.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Google Chrome extension, version 3
Category:	dropped
Size (bytes):	248531

C:\Users\user\AppData\Local\Temp\e2524fb5-dae4-4dc3-89db-84c45e773e98.tmp	
Entropy (8bit):	7.963657412635355
Encrypted:	false
SSDEEP:	3072:r+nmRykNgoldZ8GjJCiUXZSk+QSVh85PxEalRVHmcld9R6yYfEp4ABUGDcaKklrv:k3oF4Z4h45P99Fld9RBQYBVcaxlnfL
MD5:	541F52E24FE1EF9F8E12377A6CCAE0C0
SHA1:	189898BB2DCAE7D5A6057BC2D98B8B450AFAEBB6
SHA-256:	81E3A4D43A73699E1B7781723F56B8717175C536685C5450122B30789464AD82
SHA-512:	D779D78A15C5EFCA51EBD6B96A7CCB6D718741BDF7D9A37F53B2EB4B98AA1A78BC4CFA57D6E763AAB97276C8F9088940AC0476690D4D46023FF4BF52F3326C88
Malicious:	false
Reputation:	low
Preview:	Cr24.....0..."0...*.H.....0.....\7c.<.....Fto.8.2'5..qk...%....2...C.F.9.#..e.xQ.....[...L|....3>/....u.:T.7...(.yM...?V.<?.....1.a...O?d.....A.H..'.MpB..T.m..Vn Ip..>k.|1..n.<Fb..f..*Q1.....s..2..{*.6....Pp....obM..1.....b1.....(.u^.'z.....v.F.W.X4."-*eu...b.....\..F!...b...l5....zJ.q.....L].....w[T0.6....E.....r..%Z.vFm.9..5!,.~g5...;.t...']....+A.....u....k...e..&..l.6r[yU...%..f.....N..V.....<+.....l..}.{...z...)y.n..'..).....,.b....5.08K%..O.g..D.S.F5o..<(....>....\f..X..I..2."l...w....7f|.~.c.4.E.....0..0...*.H.....0.....).'..b.*$w\$.q&.]zF_2..;...?.U,..W..L1.2...R..#....W.....c1k.$W..$.J....+M!.Hz.n`U.I)N.\|b.l....{.K@]6.LIP/....](.A.....I...).H....IQ.y.;MG.d..ix..#f.Z$|..|.?...0K...t"i..s...Y..%.Ky....0...{.!+.~v.;....J.....Z....).(6..@?v.;~..2..c....[0Y0...*.H.=....*.H.=....B.....r...2..+Y.I...k..bR.j5Sl..8.....H"i.-l..`.Q.{...F0D. .0...|!..A..L.+.=...kP.!.1..

C:\Users\user\AppData\Local\Temp\scoped_dir2436_1737230934\CRX_INSTALL_locales\bg\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	796
Entropy (8bit):	4.864931792423268
Encrypted:	false
SSDEEP:	12:1HEJMLkSlwZGGMLkSlwZ+WYpU34f145Gb+dgoxTyO8ZpU34f1L0frhmJ03OyZnLt:1HE7n4gn8WYpYrbhz8ZpotHOGAOf6aD
MD5:	6F8E288A9AD5B1ED8633B430E2B4D4CA
SHA1:	F671D3D4BEFA431D1946D706F4192D44E29B6F08
SHA-256:	A114E2783D0E9B12155017323BA70838F0F82A71C7EE8DC1F115AE36991241F8
SHA-512:	0F87F3F0D115B872288949E59ACD3CD41B1FBC64A622D8FDA6D71FAFC5A900D92ADFBB0E7EB926F2A8759BBAA0896D48728FB719BBF5EF54AC21027328F770C
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "..... . ... Chrome".. },.. "app_name": {.. "message": "..... . ... Chrome".. },.. "craw_app_unavailable": {.. "message": "..... ....".. },.. "craw_connect_to_network": {.. "message": "...., ...".. },.. "iap_unavailable": {.. "message": "..... ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "...., ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2436_1737230934\CRX_INSTALL_locales\ca\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	4.536753193530313
Encrypted:	false
SSDEEP:	12:1HEJ0gbbGG0gbb+WYpU34g3YbiLO+dgyGFoO8ZpU34+puiPmb03OyZnLAOfTYABk:1HE5baib6WYpm31Lt0Z8Zp8pxOGAOfKD
MD5:	1FDAFC926391BD580B655FBAF46ED260
SHA1:	C95743C3F43B2B099FEBEBC5BD850F0C20E820AC
SHA-256:	C67898B67F9C9209EAFDA6532B62D5789863CFB855998DD6A70E7775316CEC20
SHA-512:	39D95D45C5746DA3BAA7AE6A3344EA17D7A7C3569C2A56959FF119261DA08C747A320FCF701AC72B8DBDBF8BF06FD8B239017A282CDDA444F3826D4EC672CEB4
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagaments de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Ara mateix aquesta aplicaci. no est. disponible.".. },.. "craw_connect_to_network": {.. "message": "Connecteu-vos a una xarxa.".. },.. "iap_unavailable": {.. "message": "La funci. Pagaments a l'aplicaci. no est. disponible actualment.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicieu la sessi. a Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2436_1737230934\CRX_INSTALL_locales\cs\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	641
Entropy (8bit):	4.698608127109193
Encrypted:	false
SSDEEP:	12:1HEJfZGGfZ+WYpU34OBh+dgN/O8ZpU34j05U03OyZnLAOfTYWc:1HEl4G8WYpdt8Zpq5TOGAOfW
MD5:	76DEC64ED1556180B452A13C83171883
SHA1:	CFB1E56FD587BCDC459C1D9A683B71F9849058F9

C:\Users\user\AppData\Local\Temp\scoped_dir2436_1737230934\CRX_INSTALL_locales\cs\messages.json	
SHA-256:	32290D69A90E6BAAC428B10382C99221B12773BB9A184F3B93DFB48A4F6D7A40
SHA-512:	5230A217968D5DC463E2E92D704544311A721E5CEF65C3125CBD8DEB9C0293D3BFB5C820A6011ABF77095FDEE7DAF67D541DC202B0C9CDB0908CBB85D84885B
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "app_name": {.. "message": "Platby Internetov.ho obchodu Chrome".. },.. "craw_app_unavailable": {.. "message": "Aplikace v sou.asn. dob. nen. dostupn..".. },.. "craw_connect_to_network": {.. "message": "P.ipojte se pros.m k s.ti.".. },.. "iap_unavailable": {.. "message": "Platby v aplikaci aktu.ln. nejsou k dispozici.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed .".. },.. "please_sign_in": {.. "message": "P.ihlaste se do Chromu.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2436_1737230934\CRX_INSTALL_locales\da\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	4.5289746475384565
Encrypted:	false
SSDEEP:	12:1HEJJMKKFZGGJMKKFZ+WYpU34OHu+dgxlCZO8ZpU34J4Wu03OyZnLAOfTYzD:1HErMKfqMKVWYpM6lL8ZpDNOGAOfiD
MD5:	238B97A36E411E42FF37CEFAF2927ED1
SHA1:	4E47AC90BA24C8F4724D9293FA40CFD4ADA66FE0
SHA-256:	4977D4A053542FF66967FAED6B06585DD70E68E20BFEB533B66FE3287F9655D9
SHA-512:	FD0742D47B5F5AB9AAD9B4C3D57F63CB693E060EECE123A72036C6E92156D099495C7E9E9CC6DC83EEBCDDCC4B4C81FB47E4C9559DA3EBA024780FFF10C53E0A
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Betalinger i Chrome Webshop".. },.. "app_name": {.. "message": "Betalinger i Chrome Webshop".. },.. "craw_app_unavailable": {.. "message": "Appen er ikke tilg.ngelig i .jeblikket.".. },.. "craw_connect_to_network": {.. "message": "Opret forbindelse til et netv.rk.".. },.. "iap_unavailable": {.. "message": "Betaling i appen er ikke tilg.ngelig i .jeblikket.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Log ind p. Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2436_1737230934\CRX_INSTALL_locales\de\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	651
Entropy (8bit):	4.583694000020627
Encrypted:	false
SSDEEP:	12:1HEJQ1ZGGQ1Z+WYpU34pCEMT+dgJMlCTO8ZpU34p6FK603OyZnLAOfTYJ6K:1HEzWWYp3Bewv8Zp7k4OGAOfQj
MD5:	6B3E916E8C1991AA0453CBA00FEDCAAA
SHA1:	D6366D15912E40CA107FD42BFE9579C3336A51F9
SHA-256:	A62FFAB910E31531758EEE48B2CC71A8857BEC3021DEAD50B668CBA3C8667053
SHA-512:	87EA4311B61F29543B13F3E17DFA919D0C320B4FE370CC152E0B1514BCA79B0ABB526DDCF08621D6EBFA48923EE8FB4C667EFB120A72BD9583EEBEE7BFB80552
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store-Zahlungen".. },.. "app_name": {.. "message": "Chrome Web Store-Zahlungen".. },.. "craw_app_unavailable": {.. "message": "Die App ist momentan nicht verf.gbar.".. },.. "craw_connect_to_network": {.. "message": "Bitte stellen Sie eine Verbindung zu einem Netzwerk her.".. },.. "iap_unavailable": {.. "message": "In-App-Zahlungen sind momentan nicht m.glich.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Bitte melden Sie sich in Chrome an.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2436_1737230934\CRX_INSTALL_locales\el\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	787
Entropy (8bit):	4.973349962793468
Encrypted:	false
SSDEEP:	24:1HEw+aZ+6WYpbWZe80A08ZpCGyDVWlOGAOf+XD:WguYpCZnpEZbGoD
MD5:	05C437A322C1148B5F78B2F341339147
SHA1:	AB53003A678E44A170E73711FBD9949833BBF3AA
SHA-256:	A052C32B4FCAC61152EB0ADB2C260FB6A8256AD104AA0013DB93E9798D41A070
SHA-512:	C36CB9202A34356DD06D377E2A088F428D0B8EBE7D2E54F8380485E9D94A0598D7F651C1E7A2FD55BE481D49C02B0812F2BA335E08611EC85EE0BD60784A6B4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\scoped_dir2436_1737230934\CRX_INSTALL_locales\el\messages.json	
Preview:	{.. "app_description": {.. "message": "..... ... Chrome Web Store".. },.. "app_name": {.. "message": "..... ... Chrome Web Store".. },.. "craw_app_unavail able": {.. "message": ". ....".. },.. "craw_connect_to_network": {.. "message": "..... .. ..".. },.. "iap_unavailable": {.. "message": ".. ....".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "..... ... Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2436_1737230934\CRX_INSTALL_locales\en\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2436_1737230934\CRX_INSTALL_locales\en_GB\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	593
Entropy (8bit):	4.483686991119526
Encrypted:	false
SSDEEP:	12:1HEJ6GG6+WYpU34OuFpR+dgGfFZO8ZpU34aEGFpR03OyZnLAOfTYdD:1HEVSWYpVp0JS8Zp5KpaOGAOfuD
MD5:	91F5BC87FD478A007EC68C4E8ADF11AC
SHA1:	D07DD49E4EF3B36DAD7D038B7E999AE850C5BEF6
SHA-256:	92F1246C21DD5FD7266EBFD65798C61E403D01A816CC3CF780DB5C8AA2E3D9C9
SHA-512:	FDC2A29B04E67DDBBD8FB6E8D2443E46BADCB2B2FB3A850BBD6198CDCCC32EE0BD8A9769D929FEEFE84D1015145E6664AB5FEA114DF5A864CF963BF98A65FFD9
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Chrome Web Store Payments".. },.. "app_name": {.. "message": "Chrome Web Store Payments".. },.. "craw_app_unava ilable": {.. "message": "App currently unavailable.".. },.. "craw_connect_to_network": {.. "message": "Please connect to a network.".. },.. "iap_unavailable": {.. "message": "In-App Payments is currently unavailable.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Please sign into Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2436_1737230934\CRX_INSTALL_locales\es\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	661
Entropy (8bit):	4.450938335136508
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34lPbdlVo03OyZnLAOfTY6xjD:1HEvaC6WYpcDeEFxq8ZpNl5OGAOffD
MD5:	82719BD3999AD66193A9B0BB525F97CD
SHA1:	41194D511F1ACC16C1CA828AC81C18C8C6B47287
SHA-256:	4DB9B2721E625C18B9E05C04B31AF5D9694712F1CAAF6219ABE34BB08E5DB1C7
SHA-512:	D4C49B43427799B6292CEED11CACB1D76F7CE43EBF402B43B638A6EB2B414ED0981E386CB8CDF0B51D1BD9552934FE25B2F6392266BB73D8C9A691F65BCE018
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "Los pagos en la aplicaci.n no est.n disponibles en este momento.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Inicia sesi.n en Chrome.".. }..}..

C:\Users\user\AppData\Local\Temp\scoped_dir2436_1737230934\CRX_INSTALL_locales\es_419\messages.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	637
Entropy (8bit):	4.47253983486615
Encrypted:	false
SSDEEP:	12:1HEJHlbGGHlb+WYpU34ubdDH+dgxbFxTO8ZpU34GLO03OyZnLAOfTYiJD:1HEvaC6WYpcDeEFxq8Zp4LlOGAOfvD
MD5:	6B2583D8D1C147E36A69A88009CBEBC7
SHA1:	4D4DEEB4BE6AA0181825F3371A761ABC5B4D5937
SHA-256:	6659BC3705311D7641A73995DCFEA80C7734F2F4EBBC3787B3892A240348324F
SHA-512:	37F0DBFCC1B5A2B8E4C92C49D2D9DEEF25616421350324F57E0149A45A6CCB437F5E3CBE97412C4B5DBBF2593783C7DF71E9C25A851AEAE6E4764C545723FA3
Malicious:	false
Reputation:	low
Preview:	{.. "app_description": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "app_name": {.. "message": "Sistema de pagos de Chrome Web Store".. },.. "craw_app_unavailable": {.. "message": "Esta aplicaci.n no est. disponible en este momento.".. },.. "craw_connect_to_network": {.. "message": "Con.ctate a una red.".. },.. "iap_unavailable": {.. "message": "En este momento, Pagos En-Apps no est. disponible.".. },.. "jwt_retrieve_failed": {.. "message": "The transaction could not be completed.".. },.. "please_sign_in": {.. "message": "Accede a Chrome.".. }..}..

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 2, 2021 20:40:53.783828974 CET	192.168.2.7	8.8.8.8	0x7359	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:40:53.796571016 CET	192.168.2.7	8.8.8.8	0x99d0	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:40:53.831850052 CET	192.168.2.7	8.8.8.8	0x5798	Standard query (0)	secure-chsd.org	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:01.616506100 CET	192.168.2.7	8.8.8.8	0x6d0a	Standard query (0)	www.rchsd.org	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:06.850986004 CET	192.168.2.7	8.8.8.8	0xc940	Standard query (0)	s.w.org	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:09.095388889 CET	192.168.2.7	8.8.8.8	0x2452	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:09.751718998 CET	192.168.2.7	8.8.8.8	0x1396	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:09.755501032 CET	192.168.2.7	8.8.8.8	0x6c52	Standard query (0)	insight.adsrvr.org	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:09.756248951 CET	192.168.2.7	8.8.8.8	0x22ed	Standard query (0)	pubads.g.doubleclick.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:10.809367895 CET	192.168.2.7	8.8.8.8	0xce36	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:10.809416056 CET	192.168.2.7	8.8.8.8	0x9e67	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:10.810094118 CET	192.168.2.7	8.8.8.8	0x75b9	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 2, 2021 20:41:11.203772068 CET	192.168.2.7	8.8.8.8	0x799f	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:12.458092928 CET	192.168.2.7	8.8.8.8	0xdd2c	Standard query (0)	www.rchsd.org	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:12.472821951 CET	192.168.2.7	8.8.8.8	0x19ee	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:12.602035999 CET	192.168.2.7	8.8.8.8	0xeaed	Standard query (0)	pubads.g.doubleclick.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:21.659471989 CET	192.168.2.7	8.8.8.8	0x956	Standard query (0)	www.zix.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:22.575943947 CET	192.168.2.7	8.8.8.8	0x9604	Standard query (0)	zix.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:24.496227980 CET	192.168.2.7	8.8.8.8	0x7e8c	Standard query (0)	use.typekit.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:25.348715067 CET	192.168.2.7	8.8.8.8	0xb049	Standard query (0)	p.typekit.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:26.443759918 CET	192.168.2.7	8.8.8.8	0x5cdc	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:26.451841116 CET	192.168.2.7	8.8.8.8	0xdb49	Standard query (0)	unpkg.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:26.498209953 CET	192.168.2.7	8.8.8.8	0x3abb	Standard query (0)	platform-api.sharethis.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:27.191203117 CET	192.168.2.7	8.8.8.8	0xc1f4	Standard query (0)	buttons-config.sharethis.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:27.204389095 CET	192.168.2.7	8.8.8.8	0x5961	Standard query (0)	l.sharethis.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:31.558037996 CET	192.168.2.7	8.8.8.8	0x5dc	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:31.572889090 CET	192.168.2.7	8.8.8.8	0x3643	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:31.585844994 CET	192.168.2.7	8.8.8.8	0xc398	Standard query (0)	tag.demandbase.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:31.626329899 CET	192.168.2.7	8.8.8.8	0x1284	Standard query (0)	ws.zoominfo.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:31.932640076 CET	192.168.2.7	8.8.8.8	0xb6ee	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:32.504019976 CET	192.168.2.7	8.8.8.8	0xbfbc	Standard query (0)	match.prod.bidr.io	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:32.508421898 CET	192.168.2.7	8.8.8.8	0x3c58	Standard query (0)	id.rlcdn.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:32.509900093 CET	192.168.2.7	8.8.8.8	0xddfd	Standard query (0)	api.company-target.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:32.515151978 CET	192.168.2.7	8.8.8.8	0x4689	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:33.006690025 CET	192.168.2.7	8.8.8.8	0xb4cd	Standard query (0)	segments.company-target.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:34.501096010 CET	192.168.2.7	8.8.8.8	0x6350	Standard query (0)	zix.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:34.599018097 CET	192.168.2.7	8.8.8.8	0x5030	Standard query (0)	js.driftt.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:34.720832109 CET	192.168.2.7	8.8.8.8	0x905e	Standard query (0)	match.prod.bidr.io	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:34.727720022 CET	192.168.2.7	8.8.8.8	0x9a1e	Standard query (0)	id.rlcdn.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:35.170736074 CET	192.168.2.7	8.8.8.8	0x541	Standard query (0)	segments.company-target.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:35.318789005 CET	192.168.2.7	8.8.8.8	0x6207	Standard query (0)	customer.api.drift.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:35.318866014 CET	192.168.2.7	8.8.8.8	0x24c4	Standard query (0)	conversation.api.drift.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:35.319572926 CET	192.168.2.7	8.8.8.8	0xb06	Standard query (0)	metrics.api.drift.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:35.341105938 CET	192.168.2.7	8.8.8.8	0x7fec	Standard query (0)	targeting.api.drift.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:36.459095001 CET	192.168.2.7	8.8.8.8	0x1177	Standard query (0)	bootstrap.api.drift.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:38.004719019 CET	192.168.2.7	8.8.8.8	0xfd95	Standard query (0)	embeds.driftcdn.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:40.245879889 CET	192.168.2.7	8.8.8.8	0xa4da	Standard query (0)	presence.api.drift.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 2, 2021 20:41:40.246649027 CET	192.168.2.7	8.8.8.8	0x92d6	Standard query (0)	115079-29.chat.api.drift.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:40.249185085 CET	192.168.2.7	8.8.8.8	0x403e	Standard query (0)	event.api.drift.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:45.440679073 CET	192.168.2.7	8.8.8.8	0x54f	Standard query (0)	player.vimeo.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:46.243664980 CET	192.168.2.7	8.8.8.8	0x8d19	Standard query (0)	f.vimeocdn.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:46.244623899 CET	192.168.2.7	8.8.8.8	0x91c0	Standard query (0)	fresnel.vimeocdn.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:46.245548010 CET	192.168.2.7	8.8.8.8	0xd6b1	Standard query (0)	i.vimeocdn.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:46.535880089 CET	192.168.2.7	8.8.8.8	0x8c8	Standard query (0)	vimeo.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:52.677207947 CET	192.168.2.7	8.8.8.8	0x53e9	Standard query (0)	s2.adform.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:53.427761078 CET	192.168.2.7	8.8.8.8	0xc058	Standard query (0)	a2.adform.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.461534023 CET	192.168.2.7	8.8.8.8	0xac7a	Standard query (0)	a1.seadform.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.464148045 CET	192.168.2.7	8.8.8.8	0xe4fd	Standard query (0)	c1.adform.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.702841997 CET	192.168.2.7	8.8.8.8	0x26fe	Standard query (0)	ad.360yield.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.735692978 CET	192.168.2.7	8.8.8.8	0x495e	Standard query (0)	ad.yieldlab.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.735735893 CET	192.168.2.7	8.8.8.8	0xa9bd	Standard query (0)	token.rubiconproject.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.739659071 CET	192.168.2.7	8.8.8.8	0x4585	Standard query (0)	ih.adscale.de	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.759017944 CET	192.168.2.7	8.8.8.8	0xaa20	Standard query (0)	pixel.advertising.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.759219885 CET	192.168.2.7	8.8.8.8	0x6405	Standard query (0)	rtb-csync.smartadserver.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.761516094 CET	192.168.2.7	8.8.8.8	0xad69	Standard query (0)	ads.stickyadstv.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.778213024 CET	192.168.2.7	8.8.8.8	0xa40f	Standard query (0)	x.bidswitch.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.782170057 CET	192.168.2.7	8.8.8.8	0x5ee3	Standard query (0)	dsum-sec.casalemedia.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.878669977 CET	192.168.2.7	8.8.8.8	0xfdc8	Standard query (0)	uipglob.semasio.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.909073114 CET	192.168.2.7	8.8.8.8	0x5a59	Standard query (0)	loadm.exelator.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.909795046 CET	192.168.2.7	8.8.8.8	0xc150	Standard query (0)	ps.eyeota.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.937604904 CET	192.168.2.7	8.8.8.8	0xe250	Standard query (0)	idsync.rlcdn.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.020139933 CET	192.168.2.7	8.8.8.8	0xd089	Standard query (0)	sync.crwdcntrl.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.066603899 CET	192.168.2.7	8.8.8.8	0x9d83	Standard query (0)	tags.bluekai.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.119415998 CET	192.168.2.7	8.8.8.8	0x7f95	Standard query (0)	eu-u.openx.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.164144039 CET	192.168.2.7	8.8.8.8	0x6571	Standard query (0)	pixel.mathtag.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.171313047 CET	192.168.2.7	8.8.8.8	0x8709	Standard query (0)	api.adrtx.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.304128885 CET	192.168.2.7	8.8.8.8	0x8864	Standard query (0)	ads4.admatic.com.tr	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.308151007 CET	192.168.2.7	8.8.8.8	0xdc39	Standard query (0)	ups.analytics.yahoo.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.321611881 CET	192.168.2.7	8.8.8.8	0x97ed	Standard query (0)	pixel.onaudience.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.407643080 CET	192.168.2.7	8.8.8.8	0x8f1f	Standard query (0)	cm.adsafety.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.422447920 CET	192.168.2.7	8.8.8.8	0x9a7f	Standard query (0)	s3-eu-west-1.amazonaws.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.439789057 CET	192.168.2.7	8.8.8.8	0x7c11	Standard query (0)	beacon.krxd.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.463157892 CET	192.168.2.7	8.8.8.8	0xe882	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 2, 2021 20:41:55.473356009 CET	192.168.2.7	8.8.8.8	0xa8f5	Standard query (0)	loada.exelator.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.556703091 CET	192.168.2.7	8.8.8.8	0x5f6e	Standard query (0)	secure.adnxs.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.609395027 CET	192.168.2.7	8.8.8.8	0xbe7b	Standard query (0)	simage2.pubmatic.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.739423037 CET	192.168.2.7	8.8.8.8	0x4a09	Standard query (0)	pdw-adf.userreport.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.754066944 CET	192.168.2.7	8.8.8.8	0x4b19	Standard query (0)	a.audrte.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.757190943 CET	192.168.2.7	8.8.8.8	0xb2d3	Standard query (0)	dpm.demdex.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.876470089 CET	192.168.2.7	8.8.8.8	0x7a21	Standard query (0)	aa.agkn.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.926717043 CET	192.168.2.7	8.8.8.8	0x3dee	Standard query (0)	dsp.adfarm1.adition.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:56.713335991 CET	192.168.2.7	8.8.8.8	0x4182	Standard query (0)	ads3.admatic.com.tr	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:56.718564987 CET	192.168.2.7	8.8.8.8	0x75a8	Standard query (0)	tags.adsafety.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:56.766385078 CET	192.168.2.7	8.8.8.8	0x2966	Standard query (0)	dmp.adform.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:56.867250919 CET	192.168.2.7	8.8.8.8	0x5842	Standard query (0)	match.adsrvr.org	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:56.942439079 CET	192.168.2.7	8.8.8.8	0xf6a3	Standard query (0)	pm.w55c.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.011730909 CET	192.168.2.7	8.8.8.8	0xfe1e	Standard query (0)	ads.smartstream.tv	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.107764006 CET	192.168.2.7	8.8.8.8	0x78a3	Standard query (0)	global.ib-ibi.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.158628941 CET	192.168.2.7	8.8.8.8	0xd109	Standard query (0)	id5-sync.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.162314892 CET	192.168.2.7	8.8.8.8	0xfff9	Standard query (0)	redirect.frontend.weborama.fr	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.196938038 CET	192.168.2.7	8.8.8.8	0xd109	Standard query (0)	id5-sync.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.205626011 CET	192.168.2.7	8.8.8.8	0x5f65	Standard query (0)	sync.teads.tv	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.220618010 CET	192.168.2.7	8.8.8.8	0xb42f	Standard query (0)	sync.1dmp.io	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.352658987 CET	192.168.2.7	8.8.8.8	0x6e10	Standard query (0)	s.ad.smaato.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.495282888 CET	192.168.2.7	8.8.8.8	0xea14	Standard query (0)	pixel.tapad.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.543217897 CET	192.168.2.7	8.8.8.8	0xf17d	Standard query (0)	match.contentexchange.me	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.686033964 CET	192.168.2.7	8.8.8.8	0x8c1b	Standard query (0)	eb2.3lift.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.270953894 CET	192.168.2.7	8.8.8.8	0x7466	Standard query (0)	t.adx.opera.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.275722027 CET	192.168.2.7	8.8.8.8	0x470c	Standard query (0)	cm.smartstream.tv	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.383501053 CET	192.168.2.7	8.8.8.8	0x1dbd	Standard query (0)	c1.adform.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.396703959 CET	192.168.2.7	8.8.8.8	0xf0f0	Standard query (0)	rtd-tm.everesttech.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.402633905 CET	192.168.2.7	8.8.8.8	0xe76f	Standard query (0)	ad.360yield.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.411381960 CET	192.168.2.7	8.8.8.8	0xcee3	Standard query (0)	ad.yieldlab.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.419636965 CET	192.168.2.7	8.8.8.8	0xbd7f	Standard query (0)	token.rubiconproject.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.426711082 CET	192.168.2.7	8.8.8.8	0x31d5	Standard query (0)	ih.adscale.de	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.438700914 CET	192.168.2.7	8.8.8.8	0xfdc7	Standard query (0)	rtb-csync.smartadserver.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.446959972 CET	192.168.2.7	8.8.8.8	0xcc35	Standard query (0)	pixel.advertising.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.450506926 CET	192.168.2.7	8.8.8.8	0x30e9	Standard query (0)	ads.stickyadstv.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.457380056 CET	192.168.2.7	8.8.8.8	0x467e	Standard query (0)	x.bidswitch.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 2, 2021 20:41:58.461932898 CET	192.168.2.7	8.8.8.8	0x5048	Standard query (0)	dsum-sec.casalemedia.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.471395016 CET	192.168.2.7	8.8.8.8	0x4a59	Standard query (0)	uipglob.semasio.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.476670027 CET	192.168.2.7	8.8.8.8	0x3b18	Standard query (0)	ps.eyeota.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.481070995 CET	192.168.2.7	8.8.8.8	0xd4b5	Standard query (0)	loadm.exelator.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.493041039 CET	192.168.2.7	8.8.8.8	0xa675	Standard query (0)	sync.crwdcntrl.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.504467964 CET	192.168.2.7	8.8.8.8	0xc086	Standard query (0)	idsync.rlcdn.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.518632889 CET	192.168.2.7	8.8.8.8	0x6686	Standard query (0)	tags.bluekai.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.533526897 CET	192.168.2.7	8.8.8.8	0x9965	Standard query (0)	eu-u.openx.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.555239916 CET	192.168.2.7	8.8.8.8	0xfbc4	Standard query (0)	api.adrtx.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.565524101 CET	192.168.2.7	8.8.8.8	0xf6d	Standard query (0)	pixel.onaudience.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.567801952 CET	192.168.2.7	8.8.8.8	0x1dde	Standard query (0)	cm.adsafety.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.575974941 CET	192.168.2.7	8.8.8.8	0x459e	Standard query (0)	beacon.krxd.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.588910103 CET	192.168.2.7	8.8.8.8	0xbe0c	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.667292118 CET	192.168.2.7	8.8.8.8	0x7034	Standard query (0)	secure.adnxs.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.688349962 CET	192.168.2.7	8.8.8.8	0x9612	Standard query (0)	simage2.pubmatic.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.700340986 CET	192.168.2.7	8.8.8.8	0x3d78	Standard query (0)	pdw-adf.userreport.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.714617014 CET	192.168.2.7	8.8.8.8	0x2ca8	Standard query (0)	ups.analytics.yahoo.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.723232985 CET	192.168.2.7	8.8.8.8	0xaa5	Standard query (0)	a.audrte.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.001647949 CET	192.168.2.7	8.8.8.8	0xf667	Standard query (0)	tags.adsafety.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.040720940 CET	192.168.2.7	8.8.8.8	0x5421	Standard query (0)	pixel.mathtag.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.070000887 CET	192.168.2.7	8.8.8.8	0x5ddb	Standard query (0)	s3-eu-west-1.amazonaws.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.074821949 CET	192.168.2.7	8.8.8.8	0x2870	Standard query (0)	dpm.demdex.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.126693010 CET	192.168.2.7	8.8.8.8	0x217c	Standard query (0)	aa.agkn.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.131819010 CET	192.168.2.7	8.8.8.8	0xe65	Standard query (0)	loada.exelator.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.157489061 CET	192.168.2.7	8.8.8.8	0xbf94	Standard query (0)	dsp.adfarm1.adition.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.298386097 CET	192.168.2.7	8.8.8.8	0x9448	Standard query (0)	ads.smartstream.tv	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.301667929 CET	192.168.2.7	8.8.8.8	0x6519	Standard query (0)	match.adsrvr.org	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.319462061 CET	192.168.2.7	8.8.8.8	0xc198	Standard query (0)	dmp.adform.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.335189104 CET	192.168.2.7	8.8.8.8	0x743d	Standard query (0)	pm.w55c.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.726686954 CET	192.168.2.7	8.8.8.8	0x4d17	Standard query (0)	global.ib-ibi.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.787348032 CET	192.168.2.7	8.8.8.8	0x5466	Standard query (0)	id5-sync.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.815323114 CET	192.168.2.7	8.8.8.8	0x64f2	Standard query (0)	redirect.frontend.weborama.fr	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.828393936 CET	192.168.2.7	8.8.8.8	0x5466	Standard query (0)	id5-sync.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.988436937 CET	192.168.2.7	8.8.8.8	0x8215	Standard query (0)	sync.teads.tv	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:00.058967113 CET	192.168.2.7	8.8.8.8	0xf42e	Standard query (0)	sync.1dmp.io	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:00.115111113 CET	192.168.2.7	8.8.8.8	0xd40a	Standard query (0)	s.ad.smaato.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 2, 2021 20:42:00.290793896 CET	192.168.2.7	8.8.8.8	0x311d	Standard query (0)	pixel.tapad.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:00.307540894 CET	192.168.2.7	8.8.8.8	0x6967	Standard query (0)	match.contentexchange.me	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:00.321866989 CET	192.168.2.7	8.8.8.8	0xefea	Standard query (0)	eb2.3lift.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:00.519985914 CET	192.168.2.7	8.8.8.8	0x355e	Standard query (0)	rtd-tm.everesttech.net	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:41.214855909 CET	192.168.2.7	8.8.8.8	0x5f88	Standard query (0)	115079-29.chat.api.drift.com	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:42.552562952 CET	192.168.2.7	8.8.8.8	0xf819	Standard query (0)	presence.api.drift.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:40:53.811501026 CET	8.8.8.8	192.168.2.7	0x7359	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:40:53.811501026 CET	8.8.8.8	192.168.2.7	0x7359	No error (0)	clients.l.google.com		172.217.168.78	A (IP address)	IN (0x0001)
Nov 2, 2021 20:40:53.822891951 CET	8.8.8.8	192.168.2.7	0x99d0	No error (0)	accounts.google.com		216.58.215.237	A (IP address)	IN (0x0001)
Nov 2, 2021 20:40:54.224409103 CET	8.8.8.8	192.168.2.7	0x5798	No error (0)	secure-chsd.org		63.71.15.141	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:01.793407917 CET	8.8.8.8	192.168.2.7	0x6d0a	No error (0)	www.rchsd.org	b9odqbm.impervadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:01.793407917 CET	8.8.8.8	192.168.2.7	0x6d0a	No error (0)	b9odqbm.impervadns.net		45.223.138.206	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:02.907269955 CET	8.8.8.8	192.168.2.7	0x6521	No error (0)	www-google-tagmanager.l.google.com		142.250.186.136	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:03.711867094 CET	8.8.8.8	192.168.2.7	0x61b5	No error (0)	gstaticadssl.l.google.com		142.250.203.99	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:06.869927883 CET	8.8.8.8	192.168.2.7	0xc940	No error (0)	s.w.org		192.0.77.48	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:09.117459059 CET	8.8.8.8	192.168.2.7	0x2452	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:09.117459059 CET	8.8.8.8	192.168.2.7	0x2452	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:09.770378113 CET	8.8.8.8	192.168.2.7	0x1396	No error (0)	googleads.g.doubleclick.net		142.250.203.98	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:09.772895098 CET	8.8.8.8	192.168.2.7	0x6c52	No error (0)	insight.adsrvr.org		52.223.40.198	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:09.772895098 CET	8.8.8.8	192.168.2.7	0x6c52	No error (0)	insight.adsrvr.org		35.71.131.137	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:09.772895098 CET	8.8.8.8	192.168.2.7	0x6c52	No error (0)	insight.adsrvr.org		15.197.193.217	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:09.772895098 CET	8.8.8.8	192.168.2.7	0x6c52	No error (0)	insight.adsrvr.org		3.33.220.150	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:09.774872065 CET	8.8.8.8	192.168.2.7	0xd07b	No error (0)	www-google-analytics.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:09.783189058 CET	8.8.8.8	192.168.2.7	0x22ed	No error (0)	pubads.g.doubleclick.net	partnerad.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:09.783189058 CET	8.8.8.8	192.168.2.7	0x22ed	No error (0)	partnerad.l.doubleclick.net		142.250.203.98	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:10.828233004 CET	8.8.8.8	192.168.2.7	0xce36	No error (0)	www.google.com		172.217.168.36	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:10.828600883 CET	8.8.8.8	192.168.2.7	0x9e67	No error (0)	www.google.co.uk		142.250.203.99	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:10.828838110 CET	8.8.8.8	192.168.2.7	0x75b9	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:10.828838110 CET	8.8.8.8	192.168.2.7	0x75b9	No error (0)	star-mini.c10r.facebook.com		157.240.17.35	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:11.221311092 CET	8.8.8.8	192.168.2.7	0x799f	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:11.221311092 CET	8.8.8.8	192.168.2.7	0x799f	No error (0)	stats.l.doubleclick.net		142.250.145.156	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:11.221311092 CET	8.8.8.8	192.168.2.7	0x799f	No error (0)	stats.l.doubleclick.net		142.250.145.154	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:11.221311092 CET	8.8.8.8	192.168.2.7	0x799f	No error (0)	stats.l.doubleclick.net		142.250.145.155	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:11.221311092 CET	8.8.8.8	192.168.2.7	0x799f	No error (0)	stats.l.doubleclick.net		142.250.145.157	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:12.477787971 CET	8.8.8.8	192.168.2.7	0xdd2c	No error (0)	www.rchsd.org	b9odqbm.impervadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:12.477787971 CET	8.8.8.8	192.168.2.7	0xdd2c	No error (0)	b9odqbm.impervadns.net		45.223.138.206	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:12.492281914 CET	8.8.8.8	192.168.2.7	0x19ee	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:12.492281914 CET	8.8.8.8	192.168.2.7	0x19ee	No error (0)	googlehosted.l.googleusercontent.com		172.217.168.65	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:12.629956961 CET	8.8.8.8	192.168.2.7	0xeaed	No error (0)	pubads.g.doubleclick.net	partnerad.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:12.629956961 CET	8.8.8.8	192.168.2.7	0xeaed	No error (0)	partnerad.l.doubleclick.net		142.250.203.98	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:21.779032946 CET	8.8.8.8	192.168.2.7	0x956	No error (0)	www.zix.com		199.30.234.249	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:22.695264101 CET	8.8.8.8	192.168.2.7	0x9604	No error (0)	zix.com		199.30.234.249	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:24.544368029 CET	8.8.8.8	192.168.2.7	0x7e8c	No error (0)	use.typekit.net	use-stls.adobe.com.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:25.368119955 CET	8.8.8.8	192.168.2.7	0xb049	No error (0)	p.typekit.net	p.typekit.net-v3.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:26.468314886 CET	8.8.8.8	192.168.2.7	0x5cdc	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:26.468314886 CET	8.8.8.8	192.168.2.7	0x5cdc	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:26.473136902 CET	8.8.8.8	192.168.2.7	0xdb49	No error (0)	unpkg.com		104.16.122.175	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:26.473136902 CET	8.8.8.8	192.168.2.7	0xdb49	No error (0)	unpkg.com		104.16.125.175	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:26.473136902 CET	8.8.8.8	192.168.2.7	0xdb49	No error (0)	unpkg.com		104.16.126.175	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:26.473136902 CET	8.8.8.8	192.168.2.7	0xdb49	No error (0)	unpkg.com		104.16.124.175	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:26.473136902 CET	8.8.8.8	192.168.2.7	0xdb49	No error (0)	unpkg.com		104.16.123.175	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:26.519886017 CET	8.8.8.8	192.168.2.7	0x3abb	No error (0)	platform-api.sharethis.com		13.32.22.126	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:26.519886017 CET	8.8.8.8	192.168.2.7	0x3abb	No error (0)	platform-api.sharethis.com		13.32.22.86	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:26.519886017 CET	8.8.8.8	192.168.2.7	0x3abb	No error (0)	platform-api.sharethis.com		13.32.22.44	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:26.519886017 CET	8.8.8.8	192.168.2.7	0x3abb	No error (0)	platform-api.sharethis.com		13.32.22.102	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:27.215097904 CET	8.8.8.8	192.168.2.7	0xc1f4	No error (0)	buttons-config.sharethis.com	d2znr2yi078d75.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:27.215097904 CET	8.8.8.8	192.168.2.7	0xc1f4	No error (0)	d2znr2yi078d75.cloudfront.net		65.9.71.23	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:27.215097904 CET	8.8.8.8	192.168.2.7	0xc1f4	No error (0)	d2znr2yi078d75.cloudfront.net		65.9.71.8	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:27.215097904 CET	8.8.8.8	192.168.2.7	0xc1f4	No error (0)	d2znr2yi078d75.cloudfront.net		65.9.71.124	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:27.215097904 CET	8.8.8.8	192.168.2.7	0xc1f4	No error (0)	d2znr2yi078d75.cloudfront.net		65.9.71.97	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:27.234350920 CET	8.8.8.8	192.168.2.7	0x5961	No error (0)	l.sharethis.com	httplogserver-lb.global.unified-prod.sharethis.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:27.234350920 CET	8.8.8.8	192.168.2.7	0x5961	No error (0)	httplogserver-lb.global.unified-prod.sharethis.net		18.198.109.212	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:27.234350920 CET	8.8.8.8	192.168.2.7	0x5961	No error (0)	httplogserver-lb.global.unified-prod.sharethis.net		3.124.181.115	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:27.234350920 CET	8.8.8.8	192.168.2.7	0x5961	No error (0)	httplogserver-lb.global.unified-prod.sharethis.net		52.29.0.64	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:31.576930046 CET	8.8.8.8	192.168.2.7	0x5dc	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:31.593519926 CET	8.8.8.8	192.168.2.7	0x3643	No error (0)	snap.licdn.com	od.linkedin.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:31.608930111 CET	8.8.8.8	192.168.2.7	0xc398	No error (0)	tag.demandbase.com		13.32.22.99	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:31.608930111 CET	8.8.8.8	192.168.2.7	0xc398	No error (0)	tag.demandbase.com		13.32.22.85	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:31.608930111 CET	8.8.8.8	192.168.2.7	0xc398	No error (0)	tag.demandbase.com		13.32.22.12	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:31.608930111 CET	8.8.8.8	192.168.2.7	0xc398	No error (0)	tag.demandbase.com		13.32.22.30	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:31.650249004 CET	8.8.8.8	192.168.2.7	0x1284	No error (0)	ws.zoominfo.com		104.16.168.82	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:31.650249004 CET	8.8.8.8	192.168.2.7	0x1284	No error (0)	ws.zoominfo.com		104.16.101.12	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:31.954076052 CET	8.8.8.8	192.168.2.7	0xb6ee	No error (0)	px.ads.linkedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:31.954076052 CET	8.8.8.8	192.168.2.7	0xb6ee	No error (0)	mix.linkedin.com	glb-na.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:31.954076052 CET	8.8.8.8	192.168.2.7	0xb6ee	No error (0)	glb-na.mix.linkedin.com	pop-edc2.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:31.954076052 CET	8.8.8.8	192.168.2.7	0xb6ee	No error (0)	pop-edc2.mix.linkedin.com		108.174.11.85	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:32.526557922 CET	8.8.8.8	192.168.2.7	0xbfbc	No error (0)	match.prod.bidr.io		52.49.53.128	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:32.526557922 CET	8.8.8.8	192.168.2.7	0xbfbc	No error (0)	match.prod.bidr.io		34.248.204.54	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:32.526557922 CET	8.8.8.8	192.168.2.7	0xbfbc	No error (0)	match.prod.bidr.io		54.77.6.213	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:32.526557922 CET	8.8.8.8	192.168.2.7	0xbfbc	No error (0)	match.prod.bidr.io		52.16.214.249	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:32.526557922 CET	8.8.8.8	192.168.2.7	0xbfbc	No error (0)	match.prod.bidr.io		52.215.67.80	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:32.526557922 CET	8.8.8.8	192.168.2.7	0xbfbc	No error (0)	match.prod.bidr.io		52.30.222.33	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:32.526557922 CET	8.8.8.8	192.168.2.7	0xbfbc	No error (0)	match.prod.bidr.io		52.49.238.187	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:32.526557922 CET	8.8.8.8	192.168.2.7	0xbfbc	No error (0)	match.prod.bidr.io		52.212.206.16	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:32.534166098 CET	8.8.8.8	192.168.2.7	0x4689	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:32.534327030 CET	8.8.8.8	192.168.2.7	0x3c58	No error (0)	id.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:32.549993038 CET	8.8.8.8	192.168.2.7	0xddfd	No error (0)	api.company-target.com		143.204.215.82	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:32.549993038 CET	8.8.8.8	192.168.2.7	0xddfd	No error (0)	api.company-target.com		143.204.215.77	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:32.549993038 CET	8.8.8.8	192.168.2.7	0xddfd	No error (0)	api.company-target.com		143.204.215.78	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:32.549993038 CET	8.8.8.8	192.168.2.7	0xddfd	No error (0)	api.company-target.com		143.204.215.129	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:33.028970003 CET	8.8.8.8	192.168.2.7	0xb4cd	No error (0)	segments.company-target.com		143.204.215.100	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:33.028970003 CET	8.8.8.8	192.168.2.7	0xb4cd	No error (0)	segments.company-target.com		143.204.215.97	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:33.028970003 CET	8.8.8.8	192.168.2.7	0xb4cd	No error (0)	segments.company-target.com		143.204.215.101	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:33.028970003 CET	8.8.8.8	192.168.2.7	0xb4cd	No error (0)	segments.company-target.com		143.204.215.69	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:34.623395920 CET	8.8.8.8	192.168.2.7	0x5030	No error (0)	js.driftt.com	dl7g9llrghqi1.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:34.623395920 CET	8.8.8.8	192.168.2.7	0x5030	No error (0)	dl7g9llrghqi1.cloudfront.net		143.204.215.88	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:34.623395920 CET	8.8.8.8	192.168.2.7	0x5030	No error (0)	dl7g9llrghqi1.cloudfront.net		143.204.215.62	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:34.623395920 CET	8.8.8.8	192.168.2.7	0x5030	No error (0)	dl7g9llrghqi1.cloudfront.net		143.204.215.12	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:34.623395920 CET	8.8.8.8	192.168.2.7	0x5030	No error (0)	dl7g9llrghqi1.cloudfront.net		143.204.215.107	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:34.638746023 CET	8.8.8.8	192.168.2.7	0x6350	No error (0)	zix.com		199.30.234.249	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:34.743551016 CET	8.8.8.8	192.168.2.7	0x905e	No error (0)	match.prod.bidr.io		52.49.238.187	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:34.743551016 CET	8.8.8.8	192.168.2.7	0x905e	No error (0)	match.prod.bidr.io		52.16.229.21	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:34.743551016 CET	8.8.8.8	192.168.2.7	0x905e	No error (0)	match.prod.bidr.io		54.77.6.213	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:34.743551016 CET	8.8.8.8	192.168.2.7	0x905e	No error (0)	match.prod.bidr.io		52.215.67.80	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:34.743551016 CET	8.8.8.8	192.168.2.7	0x905e	No error (0)	match.prod.bidr.io		52.30.222.33	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:34.743551016 CET	8.8.8.8	192.168.2.7	0x905e	No error (0)	match.prod.bidr.io		52.16.151.94	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:34.743551016 CET	8.8.8.8	192.168.2.7	0x905e	No error (0)	match.prod.bidr.io		52.215.67.233	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:34.743551016 CET	8.8.8.8	192.168.2.7	0x905e	No error (0)	match.prod.bidr.io		52.215.68.151	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:34.747747898 CET	8.8.8.8	192.168.2.7	0x9a1e	No error (0)	id.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:35.193964005 CET	8.8.8.8	192.168.2.7	0x541	No error (0)	segments.company-target.com		143.204.215.101	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:35.193964005 CET	8.8.8.8	192.168.2.7	0x541	No error (0)	segments.company-target.com		143.204.215.69	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:35.193964005 CET	8.8.8.8	192.168.2.7	0x541	No error (0)	segments.company-target.com		143.204.215.97	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:35.193964005 CET	8.8.8.8	192.168.2.7	0x541	No error (0)	segments.company-target.com		143.204.215.100	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:35.338107109 CET	8.8.8.8	192.168.2.7	0x24c4	No error (0)	conversation.api.drift.com	istio.api.drift.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:35.338107109 CET	8.8.8.8	192.168.2.7	0x24c4	No error (0)	istio.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:35.338107109 CET	8.8.8.8	192.168.2.7	0x24c4	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:35.338107109 CET	8.8.8.8	192.168.2.7	0x24c4	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		50.16.7.188	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:35.338107109 CET	8.8.8.8	192.168.2.7	0x24c4	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:35.338107109 CET	8.8.8.8	192.168.2.7	0x24c4	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		54.147.21.139	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:35.340516090 CET	8.8.8.8	192.168.2.7	0x6207	No error (0)	customer.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:35.340516090 CET	8.8.8.8	192.168.2.7	0x6207	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		54.147.21.139	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:35.340516090 CET	8.8.8.8	192.168.2.7	0x6207	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:35.340516090 CET	8.8.8.8	192.168.2.7	0x6207	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		50.16.7.188	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:35.340516090 CET	8.8.8.8	192.168.2.7	0x6207	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:35.341383934 CET	8.8.8.8	192.168.2.7	0xb06	No error (0)	metrics.api.drift.com	istio.api.drift.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:35.341383934 CET	8.8.8.8	192.168.2.7	0xb06	No error (0)	istio.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:35.341383934 CET	8.8.8.8	192.168.2.7	0xb06	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		54.147.21.139	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:35.341383934 CET	8.8.8.8	192.168.2.7	0xb06	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:35.341383934 CET	8.8.8.8	192.168.2.7	0xb06	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		50.16.7.188	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:35.341383934 CET	8.8.8.8	192.168.2.7	0xb06	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:35.360223055 CET	8.8.8.8	192.168.2.7	0x7fec	No error (0)	targeting.api.drift.com	istio.api.drift.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:35.360223055 CET	8.8.8.8	192.168.2.7	0x7fec	No error (0)	istio.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:35.360223055 CET	8.8.8.8	192.168.2.7	0x7fec	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		50.16.7.188	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:35.360223055 CET	8.8.8.8	192.168.2.7	0x7fec	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		54.147.21.139	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:35.360223055 CET	8.8.8.8	192.168.2.7	0x7fec	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:35.360223055 CET	8.8.8.8	192.168.2.7	0x7fec	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:36.480762959 CET	8.8.8.8	192.168.2.7	0x1177	No error (0)	bootstrap.api.drift.com	istio.api.drift.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:36.480762959 CET	8.8.8.8	192.168.2.7	0x1177	No error (0)	istio.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:36.480762959 CET	8.8.8.8	192.168.2.7	0x1177	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		54.147.21.139	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:36.480762959 CET	8.8.8.8	192.168.2.7	0x1177	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:36.480762959 CET	8.8.8.8	192.168.2.7	0x1177	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		50.16.7.188	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:36.480762959 CET	8.8.8.8	192.168.2.7	0x1177	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:38.027745008 CET	8.8.8.8	192.168.2.7	0xfd95	No error (0)	embeds.driftcdn.com		143.204.215.111	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:38.027745008 CET	8.8.8.8	192.168.2.7	0xfd95	No error (0)	embeds.driftcdn.com		143.204.215.110	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:38.027745008 CET	8.8.8.8	192.168.2.7	0xfd95	No error (0)	embeds.driftcdn.com		143.204.215.48	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:38.027745008 CET	8.8.8.8	192.168.2.7	0xfd95	No error (0)	embeds.driftcdn.com		143.204.215.26	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:40.265500069 CET	8.8.8.8	192.168.2.7	0xa4da	No error (0)	presence.api.drift.com	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:40.265500069 CET	8.8.8.8	192.168.2.7	0xa4da	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		35.174.210.7	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:40.265500069 CET	8.8.8.8	192.168.2.7	0xa4da	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		54.85.240.191	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:40.265500069 CET	8.8.8.8	192.168.2.7	0xa4da	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		54.173.95.250	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:40.265500069 CET	8.8.8.8	192.168.2.7	0xa4da	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		52.0.218.127	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:40.268389940 CET	8.8.8.8	192.168.2.7	0x403e	No error (0)	event.api.drift.com	alb-event-1454785217.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:40.268389940 CET	8.8.8.8	192.168.2.7	0x403e	No error (0)	alb-event-1454785217.us-east-1.elb.amazonaws.com		34.234.150.139	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:40.268389940 CET	8.8.8.8	192.168.2.7	0x403e	No error (0)	alb-event-1454785217.us-east-1.elb.amazonaws.com		34.231.2.68	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:40.268490076 CET	8.8.8.8	192.168.2.7	0x92d6	No error (0)	115079-29.chat.api.drift.com	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:40.268490076 CET	8.8.8.8	192.168.2.7	0x92d6	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		35.169.187.184	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:40.268490076 CET	8.8.8.8	192.168.2.7	0x92d6	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		34.203.97.57	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:40.268490076 CET	8.8.8.8	192.168.2.7	0x92d6	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		54.221.22.199	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:40.268490076 CET	8.8.8.8	192.168.2.7	0x92d6	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		54.237.186.175	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:40.268490076 CET	8.8.8.8	192.168.2.7	0x92d6	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		3.219.62.124	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:40.268490076 CET	8.8.8.8	192.168.2.7	0x92d6	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		18.204.103.191	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:40.268490076 CET	8.8.8.8	192.168.2.7	0x92d6	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		52.3.165.219	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:40.268490076 CET	8.8.8.8	192.168.2.7	0x92d6	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		34.225.177.96	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:45.460001945 CET	8.8.8.8	192.168.2.7	0x54f	No error (0)	player.vimeo.com	vimeo.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:45.460001945 CET	8.8.8.8	192.168.2.7	0x54f	No error (0)	vimeo.map.fastly.net		151.101.0.217	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:45.460001945 CET	8.8.8.8	192.168.2.7	0x54f	No error (0)	vimeo.map.fastly.net		151.101.64.217	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:45.460001945 CET	8.8.8.8	192.168.2.7	0x54f	No error (0)	vimeo.map.fastly.net		151.101.128.217	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:45.460001945 CET	8.8.8.8	192.168.2.7	0x54f	No error (0)	vimeo.map.fastly.net		151.101.192.217	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:46.261941910 CET	8.8.8.8	192.168.2.7	0x91c0	No error (0)	fresnel.vimeocdn.com		34.120.202.204	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:46.262471914 CET	8.8.8.8	192.168.2.7	0x8d19	No error (0)	f.vimeocdn.com	vimeo-video.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:46.262471914 CET	8.8.8.8	192.168.2.7	0x8d19	No error (0)	vimeo-video.map.fastly.net		151.101.114.109	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:46.264194965 CET	8.8.8.8	192.168.2.7	0xd6b1	No error (0)	i.vimeocdn.com	vimeo-video.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:46.264194965 CET	8.8.8.8	192.168.2.7	0xd6b1	No error (0)	vimeo-video.map.fastly.net		151.101.114.109	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:46.554738998 CET	8.8.8.8	192.168.2.7	0x8c8	No error (0)	vimeo.com		151.101.0.217	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:46.554738998 CET	8.8.8.8	192.168.2.7	0x8c8	No error (0)	vimeo.com		151.101.128.217	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:46.554738998 CET	8.8.8.8	192.168.2.7	0x8c8	No error (0)	vimeo.com		151.101.64.217	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:46.554738998 CET	8.8.8.8	192.168.2.7	0x8c8	No error (0)	vimeo.com		151.101.192.217	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:52.696464062 CET	8.8.8.8	192.168.2.7	0x53e9	No error (0)	s2.adform.net	s2.adformnet.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:52.696464062 CET	8.8.8.8	192.168.2.7	0x53e9	No error (0)	istrp.adform.net		37.157.2.249	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:52.696464062 CET	8.8.8.8	192.168.2.7	0x53e9	No error (0)	istrp.adform.net		37.157.2.248	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:52.696464062 CET	8.8.8.8	192.168.2.7	0x53e9	No error (0)	istrp.adform.net		37.157.2.247	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:53.448795080 CET	8.8.8.8	192.168.2.7	0xc058	No error (0)	a2.adform.net	track-us.adformnet.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:54.481915951 CET	8.8.8.8	192.168.2.7	0xe4fd	No error (0)	c1.adform.net	track.adformnet.akadns.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:54.482472897 CET	8.8.8.8	192.168.2.7	0xac7a	No error (0)	a1.seadform.net	a1.adformnet.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:54.724297047 CET	8.8.8.8	192.168.2.7	0x26fe	No error (0)	ad.360yield.com	ice.360yield.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:54.724297047 CET	8.8.8.8	192.168.2.7	0x26fe	No error (0)	ice.360yield.com	eu2-ice.360yield.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:54.724297047 CET	8.8.8.8	192.168.2.7	0x26fe	No error (0)	eu2-ice.360yield.com		3.66.41.54	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.724297047 CET	8.8.8.8	192.168.2.7	0x26fe	No error (0)	eu2-ice.360yield.com		52.28.38.50	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.724297047 CET	8.8.8.8	192.168.2.7	0x26fe	No error (0)	eu2-ice.360yield.com		54.93.66.232	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.724297047 CET	8.8.8.8	192.168.2.7	0x26fe	No error (0)	eu2-ice.360yield.com		35.157.220.171	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.724297047 CET	8.8.8.8	192.168.2.7	0x26fe	No error (0)	eu2-ice.360yield.com		52.28.69.126	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.724297047 CET	8.8.8.8	192.168.2.7	0x26fe	No error (0)	eu2-ice.360yield.com		52.28.122.36	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.724297047 CET	8.8.8.8	192.168.2.7	0x26fe	No error (0)	eu2-ice.360yield.com		3.123.215.135	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.724297047 CET	8.8.8.8	192.168.2.7	0x26fe	No error (0)	eu2-ice.360yield.com		52.58.67.48	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.754842043 CET	8.8.8.8	192.168.2.7	0x495e	No error (0)	ad.yieldlab.net	yieldlab.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:54.755731106 CET	8.8.8.8	192.168.2.7	0xa9bd	No error (0)	token.rubiconproject.com	pixel.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:54.758500099 CET	8.8.8.8	192.168.2.7	0x4585	No error (0)	ih.adscale.de		35.157.138.20	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.758500099 CET	8.8.8.8	192.168.2.7	0x4585	No error (0)	ih.adscale.de		18.193.208.211	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.758500099 CET	8.8.8.8	192.168.2.7	0x4585	No error (0)	ih.adscale.de		54.93.80.4	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.778068066 CET	8.8.8.8	192.168.2.7	0xaa20	No error (0)	pixel.advertising.com	prod.ups-adcom.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:54.778068066 CET	8.8.8.8	192.168.2.7	0xaa20	No error (0)	prod.ups-adcom.aolp-ds-prd.aws.oath.cloud	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:54.778068066 CET	8.8.8.8	192.168.2.7	0xaa20	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.184.201.8	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.778068066 CET	8.8.8.8	192.168.2.7	0xaa20	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		3.120.13.220	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.778068066 CET	8.8.8.8	192.168.2.7	0xaa20	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.159.140.98	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.778068066 CET	8.8.8.8	192.168.2.7	0xaa20	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		54.93.162.63	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.778068066 CET	8.8.8.8	192.168.2.7	0xaa20	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.156.147.57	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.778068066 CET	8.8.8.8	192.168.2.7	0xaa20	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.197.47.23	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:54.778068066 CET	8.8.8.8	192.168.2.7	0xaa20	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.159.118.206	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.778068066 CET	8.8.8.8	192.168.2.7	0xaa20	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.184.95.242	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.778110981 CET	8.8.8.8	192.168.2.7	0x6405	No error (0)	rtb-csync.smartadserver.com	rtb-csync-geo.usersync-prod-sas.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:54.778110981 CET	8.8.8.8	192.168.2.7	0x6405	No error (0)	rtb-csync-tmk.smartadserver.com		199.187.193.193	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.778110981 CET	8.8.8.8	192.168.2.7	0x6405	No error (0)	rtb-csync-tmk.smartadserver.com		199.187.193.166	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.778110981 CET	8.8.8.8	192.168.2.7	0x6405	No error (0)	rtb-csync-tmk.smartadserver.com		199.187.193.192	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.778110981 CET	8.8.8.8	192.168.2.7	0x6405	No error (0)	rtb-csync-tmk.smartadserver.com		199.187.193.185	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.782460928 CET	8.8.8.8	192.168.2.7	0xad69	No error (0)	ads.stickyadstv.com	ip1.ads.stickyadstv.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:54.795458078 CET	8.8.8.8	192.168.2.7	0xa40f	No error (0)	x.bidswitch.net	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:54.795458078 CET	8.8.8.8	192.168.2.7	0xa40f	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		3.120.56.129	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.795458078 CET	8.8.8.8	192.168.2.7	0xa40f	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		35.156.121.212	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.795458078 CET	8.8.8.8	192.168.2.7	0xa40f	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		3.122.152.23	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.795458078 CET	8.8.8.8	192.168.2.7	0xa40f	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		18.157.70.90	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.795458078 CET	8.8.8.8	192.168.2.7	0xa40f	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		18.196.176.125	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.795458078 CET	8.8.8.8	192.168.2.7	0xa40f	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		18.193.230.138	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.795458078 CET	8.8.8.8	192.168.2.7	0xa40f	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		3.126.38.41	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.795458078 CET	8.8.8.8	192.168.2.7	0xa40f	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		18.192.95.190	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.803129911 CET	8.8.8.8	192.168.2.7	0x5ee3	No error (0)	dsum-sec.casalemedia.com	dsum-sec.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:54.898272038 CET	8.8.8.8	192.168.2.7	0xfdc8	No error (0)	uipglob.semasio.net	uipglob.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:54.898272038 CET	8.8.8.8	192.168.2.7	0xfdc8	No error (0)	uip.semasio.net		77.243.60.138	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.930367947 CET	8.8.8.8	192.168.2.7	0x5a59	No error (0)	loadm.exelator.com	loadus.tm.ssl.exelator.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:54.930367947 CET	8.8.8.8	192.168.2.7	0x5a59	No error (0)	loadus.tm.ssl.exelator.com	eu-west.load.exelator.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:54.930367947 CET	8.8.8.8	192.168.2.7	0x5a59	No error (0)	eu-west.load.exelator.com	load-euw1.exelator.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:54.930367947 CET	8.8.8.8	192.168.2.7	0x5a59	No error (0)	load-euw1.exelator.com		54.78.254.47	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.931263924 CET	8.8.8.8	192.168.2.7	0xc150	No error (0)	ps.eyeota.net		3.124.210.90	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:54.959428072 CET	8.8.8.8	192.168.2.7	0xe250	No error (0)	idsync.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.041493893 CET	8.8.8.8	192.168.2.7	0xd089	No error (0)	sync.crwdcntrl.net		52.30.140.199	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.041493893 CET	8.8.8.8	192.168.2.7	0xd089	No error (0)	sync.crwdcntrl.net		52.19.22.209	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.041493893 CET	8.8.8.8	192.168.2.7	0xd089	No error (0)	sync.crwdcntrl.net		52.215.102.174	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.041493893 CET	8.8.8.8	192.168.2.7	0xd089	No error (0)	sync.crwdcntrl.net		52.209.129.133	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.041493893 CET	8.8.8.8	192.168.2.7	0xd089	No error (0)	sync.crwdcntrl.net		52.30.14.23	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.041493893 CET	8.8.8.8	192.168.2.7	0xd089	No error (0)	sync.crwdcntrl.net		63.35.242.195	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.041493893 CET	8.8.8.8	192.168.2.7	0xd089	No error (0)	sync.crwdcntrl.net		52.17.84.146	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.041493893 CET	8.8.8.8	192.168.2.7	0xd089	No error (0)	sync.crwdcntrl.net		54.194.226.253	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.090358973 CET	8.8.8.8	192.168.2.7	0x9d83	No error (0)	tags.bluekai.com	tags.bluekai.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:55.136197090 CET	8.8.8.8	192.168.2.7	0x7f95	No error (0)	eu-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.136197090 CET	8.8.8.8	192.168.2.7	0x7f95	No error (0)	eu-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.185136080 CET	8.8.8.8	192.168.2.7	0x6571	No error (0)	pixel.mathtag.com	pixel.mathtag.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:55.190375090 CET	8.8.8.8	192.168.2.7	0x8709	No error (0)	api.adrtx.net	adstax-match-proxy.adrtx.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:55.190375090 CET	8.8.8.8	192.168.2.7	0x8709	No error (0)	adstax-match-proxy.adrtx.net		52.211.146.69	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.190375090 CET	8.8.8.8	192.168.2.7	0x8709	No error (0)	adstax-match-proxy.adrtx.net		54.77.170.127	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.323533058 CET	8.8.8.8	192.168.2.7	0x8864	No error (0)	ads4.admatic.com.tr		188.132.147.227	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.323533058 CET	8.8.8.8	192.168.2.7	0x8864	No error (0)	ads4.admatic.com.tr		188.132.147.235	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.323533058 CET	8.8.8.8	192.168.2.7	0x8864	No error (0)	ads4.admatic.com.tr		188.132.147.228	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:55.323533058 CET	8.8.8.8	192.168.2.7	0x8864	No error (0)	ads4.admatic.com.tr		188.132.147.236	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.326919079 CET	8.8.8.8	192.168.2.7	0xdc39	No error (0)	ups.analytics.yahoo.com	prod.ups-ats.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:55.326919079 CET	8.8.8.8	192.168.2.7	0xdc39	No error (0)	prod.ups-ats.aolp-ds-prd.aws.oath.cloud	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:55.326919079 CET	8.8.8.8	192.168.2.7	0xdc39	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		18.156.0.31	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.326919079 CET	8.8.8.8	192.168.2.7	0xdc39	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		3.126.56.137	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.340255022 CET	8.8.8.8	192.168.2.7	0x97ed	No error (0)	pixel.onaudience.com		146.59.148.16	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.340255022 CET	8.8.8.8	192.168.2.7	0x97ed	No error (0)	pixel.onaudience.com		51.222.80.231	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.340255022 CET	8.8.8.8	192.168.2.7	0x97ed	No error (0)	pixel.onaudience.com		51.210.112.63	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.340255022 CET	8.8.8.8	192.168.2.7	0x97ed	No error (0)	pixel.onaudience.com		51.79.83.225	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.340255022 CET	8.8.8.8	192.168.2.7	0x97ed	No error (0)	pixel.onaudience.com		51.210.112.236	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.427094936 CET	8.8.8.8	192.168.2.7	0x8f1f	No error (0)	cm.adsafety.net		80.82.217.100	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.427094936 CET	8.8.8.8	192.168.2.7	0x8f1f	No error (0)	cm.adsafety.net		85.90.246.246	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.427094936 CET	8.8.8.8	192.168.2.7	0x8f1f	No error (0)	cm.adsafety.net		139.162.172.91	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.427094936 CET	8.8.8.8	192.168.2.7	0x8f1f	No error (0)	cm.adsafety.net		85.90.244.253	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.427094936 CET	8.8.8.8	192.168.2.7	0x8f1f	No error (0)	cm.adsafety.net		139.162.152.253	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.427094936 CET	8.8.8.8	192.168.2.7	0x8f1f	No error (0)	cm.adsafety.net		212.71.252.71	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.427094936 CET	8.8.8.8	192.168.2.7	0x8f1f	No error (0)	cm.adsafety.net		85.90.246.38	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.427094936 CET	8.8.8.8	192.168.2.7	0x8f1f	No error (0)	cm.adsafety.net		80.82.217.101	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.427094936 CET	8.8.8.8	192.168.2.7	0x8f1f	No error (0)	cm.adsafety.net		212.71.237.162	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.427094936 CET	8.8.8.8	192.168.2.7	0x8f1f	No error (0)	cm.adsafety.net		80.82.217.103	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.427094936 CET	8.8.8.8	192.168.2.7	0x8f1f	No error (0)	cm.adsafety.net		80.82.217.102	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.427094936 CET	8.8.8.8	192.168.2.7	0x8f1f	No error (0)	cm.adsafety.net		139.162.146.37	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.427094936 CET	8.8.8.8	192.168.2.7	0x8f1f	No error (0)	cm.adsafety.net		139.162.159.252	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.427094936 CET	8.8.8.8	192.168.2.7	0x8f1f	No error (0)	cm.adsafety.net		80.82.217.104	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.427094936 CET	8.8.8.8	192.168.2.7	0x8f1f	No error (0)	cm.adsafety.net		139.162.145.200	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:55.427094936 CET	8.8.8.8	192.168.2.7	0x8f1f	No error (0)	cm.adsafety.net		139.162.147.254	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.427094936 CET	8.8.8.8	192.168.2.7	0x8f1f	No error (0)	cm.adsafety.net		88.80.189.68	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.441490889 CET	8.8.8.8	192.168.2.7	0x9a7f	No error (0)	s3-eu-west-1.amazonaws.com		52.218.96.10	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.458750010 CET	8.8.8.8	192.168.2.7	0x7c11	No error (0)	beacon.krxd.net	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:55.458750010 CET	8.8.8.8	192.168.2.7	0x7c11	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		52.18.60.235	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.458750010 CET	8.8.8.8	192.168.2.7	0x7c11	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		52.31.165.105	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.458750010 CET	8.8.8.8	192.168.2.7	0x7c11	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		34.250.222.102	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.458750010 CET	8.8.8.8	192.168.2.7	0x7c11	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		52.31.166.207	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.458750010 CET	8.8.8.8	192.168.2.7	0x7c11	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		108.128.79.28	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.458750010 CET	8.8.8.8	192.168.2.7	0x7c11	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		54.154.13.77	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.458750010 CET	8.8.8.8	192.168.2.7	0x7c11	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		52.51.5.121	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.458750010 CET	8.8.8.8	192.168.2.7	0x7c11	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		63.35.102.121	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.482541084 CET	8.8.8.8	192.168.2.7	0xe882	No error (0)	cm.g.doubleclick.net		172.217.168.2	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.501761913 CET	8.8.8.8	192.168.2.7	0xa8f5	No error (0)	loada.exelator.com	eu-west.load.exelator.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:55.501761913 CET	8.8.8.8	192.168.2.7	0xa8f5	No error (0)	eu-west.load.exelator.com	load-euw1.exelator.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:55.501761913 CET	8.8.8.8	192.168.2.7	0xa8f5	No error (0)	load-euw1.exelator.com		54.78.254.47	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.575443983 CET	8.8.8.8	192.168.2.7	0x5f6e	No error (0)	secure.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:55.575443983 CET	8.8.8.8	192.168.2.7	0x5f6e	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:55.575443983 CET	8.8.8.8	192.168.2.7	0x5f6e	No error (0)	ib.anycast.adnxs.com		37.252.173.215	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:55.575443983 CET	8.8.8.8	192.168.2.7	0x5f6e	No error (0)	ib.anycast.adnxs.com		37.252.173.27	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.575443983 CET	8.8.8.8	192.168.2.7	0x5f6e	No error (0)	ib.anycast.adnxs.com		37.252.172.249	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.575443983 CET	8.8.8.8	192.168.2.7	0x5f6e	No error (0)	ib.anycast.adnxs.com		37.252.172.36	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.575443983 CET	8.8.8.8	192.168.2.7	0x5f6e	No error (0)	ib.anycast.adnxs.com		37.252.172.45	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.575443983 CET	8.8.8.8	192.168.2.7	0x5f6e	No error (0)	ib.anycast.adnxs.com		37.252.173.22	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.575443983 CET	8.8.8.8	192.168.2.7	0x5f6e	No error (0)	ib.anycast.adnxs.com		37.252.172.38	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.575443983 CET	8.8.8.8	192.168.2.7	0x5f6e	No error (0)	ib.anycast.adnxs.com		37.252.173.62	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.628120899 CET	8.8.8.8	192.168.2.7	0xbe7b	No error (0)	simage2.pubmatic.com	pug-lhrc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:55.628120899 CET	8.8.8.8	192.168.2.7	0xbe7b	No error (0)	pug-lhrc.pubmatic.com	pug-lhr.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:55.628120899 CET	8.8.8.8	192.168.2.7	0xbe7b	No error (0)	pug-lhr.pubmatic.com		185.64.190.80	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.770926952 CET	8.8.8.8	192.168.2.7	0x4b19	No error (0)	a.audrte.com		34.206.192.53	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.770926952 CET	8.8.8.8	192.168.2.7	0x4b19	No error (0)	a.audrte.com		52.86.83.177	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.770926952 CET	8.8.8.8	192.168.2.7	0x4b19	No error (0)	a.audrte.com		34.206.28.97	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.770926952 CET	8.8.8.8	192.168.2.7	0x4b19	No error (0)	a.audrte.com		3.212.173.197	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.770926952 CET	8.8.8.8	192.168.2.7	0x4b19	No error (0)	a.audrte.com		54.236.81.149	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.770926952 CET	8.8.8.8	192.168.2.7	0x4b19	No error (0)	a.audrte.com		3.213.248.174	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.770926952 CET	8.8.8.8	192.168.2.7	0x4b19	No error (0)	a.audrte.com		34.192.120.237	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.770926952 CET	8.8.8.8	192.168.2.7	0x4b19	No error (0)	a.audrte.com		18.215.193.43	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.772927046 CET	8.8.8.8	192.168.2.7	0x4a09	No error (0)	pdw-adf.us erreport.com	d3i42lyttuj6qr.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:55.772927046 CET	8.8.8.8	192.168.2.7	0x4a09	No error (0)	d3i42lyttuj6qr.cloudfront.net		65.9.71.36	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.772927046 CET	8.8.8.8	192.168.2.7	0x4a09	No error (0)	d3i42lyttuj6qr.cloudfront.net		65.9.71.2	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.772927046 CET	8.8.8.8	192.168.2.7	0x4a09	No error (0)	d3i42lyttuj6qr.cloudfront.net		65.9.71.103	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.772927046 CET	8.8.8.8	192.168.2.7	0x4a09	No error (0)	d3i42lyttuj6qr.cloudfront.net		65.9.71.72	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.778033018 CET	8.8.8.8	192.168.2.7	0xb2d3	No error (0)	dpm.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:55.778033018 CET	8.8.8.8	192.168.2.7	0xb2d3	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:55.778033018 CET	8.8.8.8	192.168.2.7	0xb2d3	No error (0)	edge-irl1.demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:55.778033018 CET	8.8.8.8	192.168.2.7	0xb2d3	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		3.248.38.136	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.778033018 CET	8.8.8.8	192.168.2.7	0xb2d3	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.17.185.148	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.778033018 CET	8.8.8.8	192.168.2.7	0xb2d3	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.210.87.143	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.778033018 CET	8.8.8.8	192.168.2.7	0xb2d3	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.214.44.171	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.778033018 CET	8.8.8.8	192.168.2.7	0xb2d3	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.241.100.150	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.778033018 CET	8.8.8.8	192.168.2.7	0xb2d3	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		18.200.165.55	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.778033018 CET	8.8.8.8	192.168.2.7	0xb2d3	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		18.203.8.109	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.778033018 CET	8.8.8.8	192.168.2.7	0xb2d3	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.247.138.82	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.895682096 CET	8.8.8.8	192.168.2.7	0x7a21	No error (0)	aa.agkn.com	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:55.895682096 CET	8.8.8.8	192.168.2.7	0x7a21	No error (0)	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		35.176.195.187	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.895682096 CET	8.8.8.8	192.168.2.7	0x7a21	No error (0)	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		18.168.102.56	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.895682096 CET	8.8.8.8	192.168.2.7	0x7a21	No error (0)	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		3.8.243.222	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.895682096 CET	8.8.8.8	192.168.2.7	0x7a21	No error (0)	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		18.169.90.17	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.945753098 CET	8.8.8.8	192.168.2.7	0x3dee	No error (0)	dsp.adfarm1.adition.com		85.114.159.93	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:55.945753098 CET	8.8.8.8	192.168.2.7	0x3dee	No error (0)	dsp.adfarm1.adition.com		85.114.159.118	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:56.730113029 CET	8.8.8.8	192.168.2.7	0x4182	No error (0)	ads3.admatic.com.tr	ads4.admatic.com.tr		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:56.730113029 CET	8.8.8.8	192.168.2.7	0x4182	No error (0)	ads4.admatic.com.tr		188.132.147.235	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:56.730113029 CET	8.8.8.8	192.168.2.7	0x4182	No error (0)	ads4.admatic.com.tr		188.132.147.227	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:56.730113029 CET	8.8.8.8	192.168.2.7	0x4182	No error (0)	ads4.admatic.com.tr		188.132.147.228	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:56.730113029 CET	8.8.8.8	192.168.2.7	0x4182	No error (0)	ads4.admatic.com.tr		188.132.147.236	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:56.739804029 CET	8.8.8.8	192.168.2.7	0x75a8	No error (0)	tags.adsafety.net		139.162.147.24	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:56.739804029 CET	8.8.8.8	192.168.2.7	0x75a8	No error (0)	tags.adsafety.net		139.162.141.41	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:56.739804029 CET	8.8.8.8	192.168.2.7	0x75a8	No error (0)	tags.adsafety.net		51.77.65.171	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:56.739804029 CET	8.8.8.8	192.168.2.7	0x75a8	No error (0)	tags.adsafety.net		51.77.65.176	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:56.739804029 CET	8.8.8.8	192.168.2.7	0x75a8	No error (0)	tags.adsafety.net		51.77.65.169	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:56.795156956 CET	8.8.8.8	192.168.2.7	0x2966	No error (0)	dmp.adform.net	track.adformnet.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:56.886101961 CET	8.8.8.8	192.168.2.7	0x5842	No error (0)	match.adsrvr.org		52.223.40.198	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:56.886101961 CET	8.8.8.8	192.168.2.7	0x5842	No error (0)	match.adsrvr.org		35.71.131.137	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:56.886101961 CET	8.8.8.8	192.168.2.7	0x5842	No error (0)	match.adsrvr.org		15.197.193.217	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:56.886101961 CET	8.8.8.8	192.168.2.7	0x5842	No error (0)	match.adsrvr.org		3.33.220.150	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:56.961065054 CET	8.8.8.8	192.168.2.7	0xf6a3	No error (0)	pm.w55c.net	dxedge-prod-lb-1585771072.us-west-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:56.961065054 CET	8.8.8.8	192.168.2.7	0xf6a3	No error (0)	dxedge-prod-lb-1585771072.us-west-2.elb.amazonaws.com		52.89.239.64	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:56.961065054 CET	8.8.8.8	192.168.2.7	0xf6a3	No error (0)	dxedge-prod-lb-1585771072.us-west-2.elb.amazonaws.com		44.236.75.167	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:56.961065054 CET	8.8.8.8	192.168.2.7	0xf6a3	No error (0)	dxedge-prod-lb-1585771072.us-west-2.elb.amazonaws.com		52.24.93.99	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:56.961065054 CET	8.8.8.8	192.168.2.7	0xf6a3	No error (0)	dxedge-prod-lb-1585771072.us-west-2.elb.amazonaws.com		35.165.222.68	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:56.961065054 CET	8.8.8.8	192.168.2.7	0xf6a3	No error (0)	dxedge-prod-lb-1585771072.us-west-2.elb.amazonaws.com		54.148.190.121	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:56.961065054 CET	8.8.8.8	192.168.2.7	0xf6a3	No error (0)	dxedge-prod-lb-1585771072.us-west-2.elb.amazonaws.com		52.34.139.214	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.030446053 CET	8.8.8.8	192.168.2.7	0xfe1e	No error (0)	ads.smartstream.tv		80.82.217.92	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.030446053 CET	8.8.8.8	192.168.2.7	0xfe1e	No error (0)	ads.smartstream.tv		80.82.217.94	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.030446053 CET	8.8.8.8	192.168.2.7	0xfe1e	No error (0)	ads.smartstream.tv		145.239.1.221	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.030446053 CET	8.8.8.8	192.168.2.7	0xfe1e	No error (0)	ads.smartstream.tv		80.82.217.93	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.030446053 CET	8.8.8.8	192.168.2.7	0xfe1e	No error (0)	ads.smartstream.tv		80.82.217.91	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.030446053 CET	8.8.8.8	192.168.2.7	0xfe1e	No error (0)	ads.smartstream.tv		80.82.217.90	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.030446053 CET	8.8.8.8	192.168.2.7	0xfe1e	No error (0)	ads.smartstream.tv		145.239.1.219	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:57.030446053 CET	8.8.8.8	192.168.2.7	0xfe1e	No error (0)	ads.smartstream.tv		145.239.1.220	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.125334024 CET	8.8.8.8	192.168.2.7	0x78a3	No error (0)	global.ib-ibi.com		64.58.232.179	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.183414936 CET	8.8.8.8	192.168.2.7	0xfff9	No error (0)	redirect.frontend.weborama.fr		35.190.16.14	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.226805925 CET	8.8.8.8	192.168.2.7	0x5f65	No error (0)	sync.teads.tv	sync.teads.tv.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:57.239479065 CET	8.8.8.8	192.168.2.7	0xb42f	No error (0)	sync.1dmp.io		88.99.214.77	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.239479065 CET	8.8.8.8	192.168.2.7	0xb42f	No error (0)	sync.1dmp.io		136.243.148.229	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.239479065 CET	8.8.8.8	192.168.2.7	0xb42f	No error (0)	sync.1dmp.io		88.99.213.228	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.239479065 CET	8.8.8.8	192.168.2.7	0xb42f	No error (0)	sync.1dmp.io		88.99.149.88	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.239479065 CET	8.8.8.8	192.168.2.7	0xb42f	No error (0)	sync.1dmp.io		78.46.100.125	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.239479065 CET	8.8.8.8	192.168.2.7	0xb42f	No error (0)	sync.1dmp.io		95.216.101.186	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.389467001 CET	8.8.8.8	192.168.2.7	0x6e10	No error (0)	s.ad.smaato.net		13.32.22.27	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.389467001 CET	8.8.8.8	192.168.2.7	0x6e10	No error (0)	s.ad.smaato.net		13.32.22.28	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.389467001 CET	8.8.8.8	192.168.2.7	0x6e10	No error (0)	s.ad.smaato.net		13.32.22.103	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.389467001 CET	8.8.8.8	192.168.2.7	0x6e10	No error (0)	s.ad.smaato.net		13.32.22.118	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.518034935 CET	8.8.8.8	192.168.2.7	0xea14	No error (0)	pixel.tapad.com		35.227.248.159	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.560339928 CET	8.8.8.8	192.168.2.7	0xf17d	No error (0)	match.contentexchange.me		46.19.11.36	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.704878092 CET	8.8.8.8	192.168.2.7	0x8c1b	No error (0)	eb2.3lift.com	eu-eb2.3lift.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:57.704878092 CET	8.8.8.8	192.168.2.7	0x8c1b	No error (0)	eu-eb2.3lift.com		76.223.111.18	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:57.704878092 CET	8.8.8.8	192.168.2.7	0x8c1b	No error (0)	eu-eb2.3lift.com		13.248.245.213	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.290086985 CET	8.8.8.8	192.168.2.7	0x7466	No error (0)	t.adx.opera.com	outspot2-ams.adx.opera.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.290086985 CET	8.8.8.8	192.168.2.7	0x7466	No error (0)	outspot2-ams.adx.opera.com		82.145.213.8	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.294636965 CET	8.8.8.8	192.168.2.7	0x470c	No error (0)	cm.smartstream.tv		80.85.85.173	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.294636965 CET	8.8.8.8	192.168.2.7	0x470c	No error (0)	cm.smartstream.tv		85.90.245.27	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.405515909 CET	8.8.8.8	192.168.2.7	0x1dbd	No error (0)	c1.adform.net	track.adformnet.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.416209936 CET	8.8.8.8	192.168.2.7	0xf0f0	No error (0)	rtd-tm.everesttech.net	rtd.tubemogul.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.416209936 CET	8.8.8.8	192.168.2.7	0xf0f0	No error (0)	rtd.tubemogul.com	h2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:58.424796104 CET	8.8.8.8	192.168.2.7	0xe76f	No error (0)	ad.360yield.com	ice.360yield.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.424796104 CET	8.8.8.8	192.168.2.7	0xe76f	No error (0)	ice.360yield.com	eu2-ice.360yield.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.424796104 CET	8.8.8.8	192.168.2.7	0xe76f	No error (0)	eu2-ice.360yield.com		52.28.122.36	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.424796104 CET	8.8.8.8	192.168.2.7	0xe76f	No error (0)	eu2-ice.360yield.com		52.58.206.142	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.424796104 CET	8.8.8.8	192.168.2.7	0xe76f	No error (0)	eu2-ice.360yield.com		3.68.1.143	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.424796104 CET	8.8.8.8	192.168.2.7	0xe76f	No error (0)	eu2-ice.360yield.com		3.66.71.220	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.424796104 CET	8.8.8.8	192.168.2.7	0xe76f	No error (0)	eu2-ice.360yield.com		18.185.200.55	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.424796104 CET	8.8.8.8	192.168.2.7	0xe76f	No error (0)	eu2-ice.360yield.com		52.58.124.95	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.424796104 CET	8.8.8.8	192.168.2.7	0xe76f	No error (0)	eu2-ice.360yield.com		18.185.206.125	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.424796104 CET	8.8.8.8	192.168.2.7	0xe76f	No error (0)	eu2-ice.360yield.com		3.66.41.54	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.432981968 CET	8.8.8.8	192.168.2.7	0xcee3	No error (0)	ad.yieldlab.net	yieldlab.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.438824892 CET	8.8.8.8	192.168.2.7	0xbd7f	No error (0)	token.rubiconproject.com	pixel.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.443465948 CET	8.8.8.8	192.168.2.7	0x31d5	No error (0)	ih.adscale.de		35.157.138.20	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.443465948 CET	8.8.8.8	192.168.2.7	0x31d5	No error (0)	ih.adscale.de		54.93.80.4	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.443465948 CET	8.8.8.8	192.168.2.7	0x31d5	No error (0)	ih.adscale.de		18.193.208.211	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.457633018 CET	8.8.8.8	192.168.2.7	0xfdc7	No error (0)	rtb-csync.smartadserver.com	rtb-csync-geo.usersync-prod-sas.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.457633018 CET	8.8.8.8	192.168.2.7	0xfdc7	No error (0)	rtb-csync-itx4.smartadserver.com		185.86.139.113	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.457633018 CET	8.8.8.8	192.168.2.7	0xfdc7	No error (0)	rtb-csync-itx4.smartadserver.com		185.86.139.114	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.457633018 CET	8.8.8.8	192.168.2.7	0xfdc7	No error (0)	rtb-csync-itx4.smartadserver.com		185.86.139.89	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.457633018 CET	8.8.8.8	192.168.2.7	0xfdc7	No error (0)	rtb-csync-itx4.smartadserver.com		185.86.139.115	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.468619108 CET	8.8.8.8	192.168.2.7	0xcc35	No error (0)	pixel.advertising.com	prod.ups-adcom.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.468619108 CET	8.8.8.8	192.168.2.7	0xcc35	No error (0)	prod.ups-adcom.aolp-ds-prd.aws.oath.cloud	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.468619108 CET	8.8.8.8	192.168.2.7	0xcc35	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.194.17.206	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.468619108 CET	8.8.8.8	192.168.2.7	0xcc35	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		54.93.133.131	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.468619108 CET	8.8.8.8	192.168.2.7	0xcc35	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.184.95.242	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:58.468619108 CET	8.8.8.8	192.168.2.7	0xcc35	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.159.140.98	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.468619108 CET	8.8.8.8	192.168.2.7	0xcc35	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.197.47.23	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.468619108 CET	8.8.8.8	192.168.2.7	0xcc35	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		3.120.13.220	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.468619108 CET	8.8.8.8	192.168.2.7	0xcc35	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.184.201.8	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.468619108 CET	8.8.8.8	192.168.2.7	0xcc35	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		35.157.177.200	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.471682072 CET	8.8.8.8	192.168.2.7	0x30e9	No error (0)	ads.stickyadstv.com	ip1.ads.stickyadstv.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.476278067 CET	8.8.8.8	192.168.2.7	0x467e	No error (0)	x.bidswitch.net	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.476278067 CET	8.8.8.8	192.168.2.7	0x467e	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		3.120.56.129	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.476278067 CET	8.8.8.8	192.168.2.7	0x467e	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		35.156.121.212	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.476278067 CET	8.8.8.8	192.168.2.7	0x467e	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		3.122.152.23	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.476278067 CET	8.8.8.8	192.168.2.7	0x467e	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		18.157.70.90	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.476278067 CET	8.8.8.8	192.168.2.7	0x467e	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		18.196.176.125	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.476278067 CET	8.8.8.8	192.168.2.7	0x467e	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		18.193.230.138	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.476278067 CET	8.8.8.8	192.168.2.7	0x467e	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		3.126.38.41	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.476278067 CET	8.8.8.8	192.168.2.7	0x467e	No error (0)	elb-aws-fr-bruges-621602890.eu-central-1.elb.amazonaws.com		18.192.95.190	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.483217001 CET	8.8.8.8	192.168.2.7	0x5048	No error (0)	dsum-sec.casalemedia.com	dsum-sec.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.490437031 CET	8.8.8.8	192.168.2.7	0x4a59	No error (0)	uipglob.semasio.net	uipglob.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:58.490437031 CET	8.8.8.8	192.168.2.7	0x4a59	No error (0)	uip.semasio.net		77.243.60.138	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.498667002 CET	8.8.8.8	192.168.2.7	0x3b18	No error (0)	ps.eyeota.net		3.125.70.222	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.502558947 CET	8.8.8.8	192.168.2.7	0xd4b5	No error (0)	loadm.exelator.com	loadus.tm.ssl.exelator.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.502558947 CET	8.8.8.8	192.168.2.7	0xd4b5	No error (0)	loadus.tm.ssl.exelator.com	eu-west.load.exelator.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.502558947 CET	8.8.8.8	192.168.2.7	0xd4b5	No error (0)	eu-west.load.exelator.com	load-euw1.exelator.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.502558947 CET	8.8.8.8	192.168.2.7	0xd4b5	No error (0)	load-euw1.exelator.com		54.78.254.47	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.515280008 CET	8.8.8.8	192.168.2.7	0xa675	No error (0)	sync.crwdcntrl.net		52.215.102.174	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.515280008 CET	8.8.8.8	192.168.2.7	0xa675	No error (0)	sync.crwdcntrl.net		52.208.103.128	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.515280008 CET	8.8.8.8	192.168.2.7	0xa675	No error (0)	sync.crwdcntrl.net		63.35.242.195	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.515280008 CET	8.8.8.8	192.168.2.7	0xa675	No error (0)	sync.crwdcntrl.net		52.209.129.133	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.515280008 CET	8.8.8.8	192.168.2.7	0xa675	No error (0)	sync.crwdcntrl.net		52.30.14.23	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.515280008 CET	8.8.8.8	192.168.2.7	0xa675	No error (0)	sync.crwdcntrl.net		52.30.140.199	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.515280008 CET	8.8.8.8	192.168.2.7	0xa675	No error (0)	sync.crwdcntrl.net		52.17.84.146	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.515280008 CET	8.8.8.8	192.168.2.7	0xa675	No error (0)	sync.crwdcntrl.net		52.19.22.209	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.532628059 CET	8.8.8.8	192.168.2.7	0xc086	No error (0)	idsync.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.540431976 CET	8.8.8.8	192.168.2.7	0x6686	No error (0)	tags.bluekai.com	tags.bluekai.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.552251101 CET	8.8.8.8	192.168.2.7	0x9965	No error (0)	eu-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.552251101 CET	8.8.8.8	192.168.2.7	0x9965	No error (0)	eu-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.574760914 CET	8.8.8.8	192.168.2.7	0xfbc4	No error (0)	api.adrtx.net	adstax-match-proxy.adrtx.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.574760914 CET	8.8.8.8	192.168.2.7	0xfbc4	No error (0)	adstax-match-proxy.adrtx.net		54.77.170.127	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.574760914 CET	8.8.8.8	192.168.2.7	0xfbc4	No error (0)	adstax-match-proxy.adrtx.net		52.211.146.69	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.584544897 CET	8.8.8.8	192.168.2.7	0xf6d	No error (0)	pixel.onaudience.com		51.79.83.225	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.584544897 CET	8.8.8.8	192.168.2.7	0xf6d	No error (0)	pixel.onaudience.com		51.210.112.63	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.584544897 CET	8.8.8.8	192.168.2.7	0xf6d	No error (0)	pixel.onaudience.com		51.210.112.236	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.584544897 CET	8.8.8.8	192.168.2.7	0xf6d	No error (0)	pixel.onaudience.com		51.222.80.231	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.584544897 CET	8.8.8.8	192.168.2.7	0xf6d	No error (0)	pixel.onaudience.com		146.59.148.16	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:58.587091923 CET	8.8.8.8	192.168.2.7	0x1dde	No error (0)	cm.adsafety.net		212.71.237.162	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.587091923 CET	8.8.8.8	192.168.2.7	0x1dde	No error (0)	cm.adsafety.net		139.162.146.37	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.587091923 CET	8.8.8.8	192.168.2.7	0x1dde	No error (0)	cm.adsafety.net		139.162.145.200	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.587091923 CET	8.8.8.8	192.168.2.7	0x1dde	No error (0)	cm.adsafety.net		80.82.217.103	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.587091923 CET	8.8.8.8	192.168.2.7	0x1dde	No error (0)	cm.adsafety.net		139.162.159.252	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.587091923 CET	8.8.8.8	192.168.2.7	0x1dde	No error (0)	cm.adsafety.net		80.82.217.104	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.587091923 CET	8.8.8.8	192.168.2.7	0x1dde	No error (0)	cm.adsafety.net		80.82.217.100	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.587091923 CET	8.8.8.8	192.168.2.7	0x1dde	No error (0)	cm.adsafety.net		85.90.244.253	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.587091923 CET	8.8.8.8	192.168.2.7	0x1dde	No error (0)	cm.adsafety.net		139.162.152.253	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.587091923 CET	8.8.8.8	192.168.2.7	0x1dde	No error (0)	cm.adsafety.net		85.90.246.38	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.587091923 CET	8.8.8.8	192.168.2.7	0x1dde	No error (0)	cm.adsafety.net		139.162.172.91	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.587091923 CET	8.8.8.8	192.168.2.7	0x1dde	No error (0)	cm.adsafety.net		212.71.252.71	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.587091923 CET	8.8.8.8	192.168.2.7	0x1dde	No error (0)	cm.adsafety.net		80.82.217.101	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.587091923 CET	8.8.8.8	192.168.2.7	0x1dde	No error (0)	cm.adsafety.net		85.90.246.246	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.587091923 CET	8.8.8.8	192.168.2.7	0x1dde	No error (0)	cm.adsafety.net		139.162.147.254	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.587091923 CET	8.8.8.8	192.168.2.7	0x1dde	No error (0)	cm.adsafety.net		88.80.189.68	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.587091923 CET	8.8.8.8	192.168.2.7	0x1dde	No error (0)	cm.adsafety.net		80.82.217.102	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.592806101 CET	8.8.8.8	192.168.2.7	0x459e	No error (0)	beacon.krxd.net	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.592806101 CET	8.8.8.8	192.168.2.7	0x459e	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		52.214.241.88	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.592806101 CET	8.8.8.8	192.168.2.7	0x459e	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		63.35.102.121	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.592806101 CET	8.8.8.8	192.168.2.7	0x459e	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		54.76.2.238	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.592806101 CET	8.8.8.8	192.168.2.7	0x459e	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		34.255.77.76	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:58.592806101 CET	8.8.8.8	192.168.2.7	0x459e	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		52.215.41.87	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.592806101 CET	8.8.8.8	192.168.2.7	0x459e	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		18.200.98.193	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.592806101 CET	8.8.8.8	192.168.2.7	0x459e	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		108.128.86.195	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.592806101 CET	8.8.8.8	192.168.2.7	0x459e	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		54.154.13.77	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.606704950 CET	8.8.8.8	192.168.2.7	0xbe0c	No error (0)	cm.g.doubleclick.net		172.217.168.66	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.686253071 CET	8.8.8.8	192.168.2.7	0x7034	No error (0)	secure.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.686253071 CET	8.8.8.8	192.168.2.7	0x7034	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.686253071 CET	8.8.8.8	192.168.2.7	0x7034	No error (0)	ib.anycast.adnxs.com		37.252.173.215	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.686253071 CET	8.8.8.8	192.168.2.7	0x7034	No error (0)	ib.anycast.adnxs.com		37.252.173.27	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.686253071 CET	8.8.8.8	192.168.2.7	0x7034	No error (0)	ib.anycast.adnxs.com		37.252.172.249	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.686253071 CET	8.8.8.8	192.168.2.7	0x7034	No error (0)	ib.anycast.adnxs.com		37.252.172.36	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.686253071 CET	8.8.8.8	192.168.2.7	0x7034	No error (0)	ib.anycast.adnxs.com		37.252.172.45	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.686253071 CET	8.8.8.8	192.168.2.7	0x7034	No error (0)	ib.anycast.adnxs.com		37.252.173.22	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.686253071 CET	8.8.8.8	192.168.2.7	0x7034	No error (0)	ib.anycast.adnxs.com		37.252.172.38	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.686253071 CET	8.8.8.8	192.168.2.7	0x7034	No error (0)	ib.anycast.adnxs.com		37.252.173.62	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.707051992 CET	8.8.8.8	192.168.2.7	0x9612	No error (0)	simage2.pubmatic.com	pug22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.707051992 CET	8.8.8.8	192.168.2.7	0x9612	No error (0)	pug22000nfc.pubmatic.com	pug22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.707051992 CET	8.8.8.8	192.168.2.7	0x9612	No error (0)	pug22000nf.pubmatic.com		185.64.189.110	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.724193096 CET	8.8.8.8	192.168.2.7	0x3d78	No error (0)	pdw-adf.userreport.com	d3i42lyttuj6qr.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.724193096 CET	8.8.8.8	192.168.2.7	0x3d78	No error (0)	d3i42lyttuj6qr.cloudfront.net		65.9.71.2	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.724193096 CET	8.8.8.8	192.168.2.7	0x3d78	No error (0)	d3i42lyttuj6qr.cloudfront.net		65.9.71.103	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.724193096 CET	8.8.8.8	192.168.2.7	0x3d78	No error (0)	d3i42lyttuj6qr.cloudfront.net		65.9.71.36	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:58.724193096 CET	8.8.8.8	192.168.2.7	0x3d78	No error (0)	d3i42lyttu j6qr.cloud front.net		65.9.71.72	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.733911037 CET	8.8.8.8	192.168.2.7	0x2ca8	No error (0)	ups.analyt ics.yahoo.com	prod.ups-ats.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.733911037 CET	8.8.8.8	192.168.2.7	0x2ca8	No error (0)	prod.ups-a ts.aolp-ds-prd.aws.o ath.cloud	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:58.733911037 CET	8.8.8.8	192.168.2.7	0x2ca8	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aw s.oath.cloud		18.156.0.31	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.733911037 CET	8.8.8.8	192.168.2.7	0x2ca8	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aw s.oath.cloud		3.126.56.137	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.742753029 CET	8.8.8.8	192.168.2.7	0xaa5	No error (0)	a.audrte.com		3.213.248.174	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.742753029 CET	8.8.8.8	192.168.2.7	0xaa5	No error (0)	a.audrte.com		52.86.83.177	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.742753029 CET	8.8.8.8	192.168.2.7	0xaa5	No error (0)	a.audrte.com		34.206.28.97	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.742753029 CET	8.8.8.8	192.168.2.7	0xaa5	No error (0)	a.audrte.com		34.192.120.237	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.742753029 CET	8.8.8.8	192.168.2.7	0xaa5	No error (0)	a.audrte.com		3.212.173.197	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.742753029 CET	8.8.8.8	192.168.2.7	0xaa5	No error (0)	a.audrte.com		34.206.192.53	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.742753029 CET	8.8.8.8	192.168.2.7	0xaa5	No error (0)	a.audrte.com		18.215.193.43	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:58.742753029 CET	8.8.8.8	192.168.2.7	0xaa5	No error (0)	a.audrte.com		54.236.81.149	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.027766943 CET	8.8.8.8	192.168.2.7	0xf667	No error (0)	tags.adsaf ety.net		51.77.65.171	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.027766943 CET	8.8.8.8	192.168.2.7	0xf667	No error (0)	tags.adsaf ety.net		51.77.65.176	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.027766943 CET	8.8.8.8	192.168.2.7	0xf667	No error (0)	tags.adsaf ety.net		139.162.141.41	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.027766943 CET	8.8.8.8	192.168.2.7	0xf667	No error (0)	tags.adsaf ety.net		51.77.65.169	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.027766943 CET	8.8.8.8	192.168.2.7	0xf667	No error (0)	tags.adsaf ety.net		139.162.147.24	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.060810089 CET	8.8.8.8	192.168.2.7	0x5421	No error (0)	pixel.math tag.com	pixel.mathtag.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:59.088746071 CET	8.8.8.8	192.168.2.7	0x5ddb	No error (0)	s3-eu-west-1.amazona ws.com		52.218.108.83	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.097377062 CET	8.8.8.8	192.168.2.7	0x2870	No error (0)	dpm.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:59.097377062 CET	8.8.8.8	192.168.2.7	0x2870	No error (0)	gslb-2.dem dex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:59.097377062 CET	8.8.8.8	192.168.2.7	0x2870	No error (0)	edge-irl1. demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:59.097377062 CET	8.8.8.8	192.168.2.7	0x2870	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.am azonaws.com		52.30.48.112	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:59.097377062 CET	8.8.8.8	192.168.2.7	0x2870	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		63.32.159.255	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.097377062 CET	8.8.8.8	192.168.2.7	0x2870	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		108.128.92.179	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.097377062 CET	8.8.8.8	192.168.2.7	0x2870	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		18.200.208.216	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.097377062 CET	8.8.8.8	192.168.2.7	0x2870	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.18.85.49	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.097377062 CET	8.8.8.8	192.168.2.7	0x2870	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.17.95.93	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.097377062 CET	8.8.8.8	192.168.2.7	0x2870	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.51.58.216	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.097377062 CET	8.8.8.8	192.168.2.7	0x2870	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.213.37.66	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.149732113 CET	8.8.8.8	192.168.2.7	0x217c	No error (0)	aa.agkn.com	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:59.149732113 CET	8.8.8.8	192.168.2.7	0x217c	No error (0)	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		18.169.90.17	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.149732113 CET	8.8.8.8	192.168.2.7	0x217c	No error (0)	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		18.168.102.56	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.149732113 CET	8.8.8.8	192.168.2.7	0x217c	No error (0)	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		35.176.195.187	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.149732113 CET	8.8.8.8	192.168.2.7	0x217c	No error (0)	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		3.8.243.222	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.154891968 CET	8.8.8.8	192.168.2.7	0xe65	No error (0)	loada.exelator.com	eu-west.load.exelator.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:59.154891968 CET	8.8.8.8	192.168.2.7	0xe65	No error (0)	eu-west.load.exelator.com	load-euw1.exelator.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:59.154891968 CET	8.8.8.8	192.168.2.7	0xe65	No error (0)	load-euw1.exelator.com		54.78.254.47	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.176678896 CET	8.8.8.8	192.168.2.7	0xbf94	No error (0)	dsp.adfarm1.adition.com		85.114.159.118	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.176678896 CET	8.8.8.8	192.168.2.7	0xbf94	No error (0)	dsp.adfarm1.adition.com		85.114.159.93	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.318240881 CET	8.8.8.8	192.168.2.7	0x9448	No error (0)	ads.smartstream.tv		145.239.1.221	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.318240881 CET	8.8.8.8	192.168.2.7	0x9448	No error (0)	ads.smartstream.tv		80.82.217.93	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.318240881 CET	8.8.8.8	192.168.2.7	0x9448	No error (0)	ads.smartstream.tv		80.82.217.91	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:41:59.318240881 CET	8.8.8.8	192.168.2.7	0x9448	No error (0)	ads.smartstream.tv		80.82.217.94	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.318240881 CET	8.8.8.8	192.168.2.7	0x9448	No error (0)	ads.smartstream.tv		145.239.1.219	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.318240881 CET	8.8.8.8	192.168.2.7	0x9448	No error (0)	ads.smartstream.tv		80.82.217.90	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.318240881 CET	8.8.8.8	192.168.2.7	0x9448	No error (0)	ads.smartstream.tv		145.239.1.220	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.318240881 CET	8.8.8.8	192.168.2.7	0x9448	No error (0)	ads.smartstream.tv		80.82.217.92	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.321409941 CET	8.8.8.8	192.168.2.7	0x6519	No error (0)	match.adsrvr.org		52.223.40.198	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.321409941 CET	8.8.8.8	192.168.2.7	0x6519	No error (0)	match.adsrvr.org		35.71.131.137	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.321409941 CET	8.8.8.8	192.168.2.7	0x6519	No error (0)	match.adsrvr.org		15.197.193.217	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.321409941 CET	8.8.8.8	192.168.2.7	0x6519	No error (0)	match.adsrvr.org		3.33.220.150	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.339040041 CET	8.8.8.8	192.168.2.7	0xc198	No error (0)	dmp.adform.net	track.adformnet.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:59.353898048 CET	8.8.8.8	192.168.2.7	0x743d	No error (0)	pm.w55c.net	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:41:59.353898048 CET	8.8.8.8	192.168.2.7	0x743d	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		18.197.87.177	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.353898048 CET	8.8.8.8	192.168.2.7	0x743d	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		3.127.92.82	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.353898048 CET	8.8.8.8	192.168.2.7	0x743d	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		3.120.29.221	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.353898048 CET	8.8.8.8	192.168.2.7	0x743d	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		3.125.99.7	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.353898048 CET	8.8.8.8	192.168.2.7	0x743d	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		18.185.182.242	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.353898048 CET	8.8.8.8	192.168.2.7	0x743d	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		35.156.135.60	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.353898048 CET	8.8.8.8	192.168.2.7	0x743d	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		3.124.143.99	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.353898048 CET	8.8.8.8	192.168.2.7	0x743d	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		3.126.16.11	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.744307995 CET	8.8.8.8	192.168.2.7	0x4d17	No error (0)	global.ib-ibi.com		64.58.232.176	A (IP address)	IN (0x0001)
Nov 2, 2021 20:41:59.837582111 CET	8.8.8.8	192.168.2.7	0x64f2	No error (0)	redirect.frontend.weborama.fr		35.190.16.14	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:42:00.009651899 CET	8.8.8.8	192.168.2.7	0x8215	No error (0)	sync.teads.tv	sync.teads.tv.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:42:00.076199055 CET	8.8.8.8	192.168.2.7	0xf42e	No error (0)	sync.1dmp.io		78.46.100.125	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:00.076199055 CET	8.8.8.8	192.168.2.7	0xf42e	No error (0)	sync.1dmp.io		88.99.149.88	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:00.076199055 CET	8.8.8.8	192.168.2.7	0xf42e	No error (0)	sync.1dmp.io		88.99.213.228	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:00.076199055 CET	8.8.8.8	192.168.2.7	0xf42e	No error (0)	sync.1dmp.io		88.99.214.77	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:00.076199055 CET	8.8.8.8	192.168.2.7	0xf42e	No error (0)	sync.1dmp.io		95.216.101.186	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:00.076199055 CET	8.8.8.8	192.168.2.7	0xf42e	No error (0)	sync.1dmp.io		136.243.148.229	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:00.148164988 CET	8.8.8.8	192.168.2.7	0xd40a	No error (0)	s.ad.smaato.net		13.32.22.103	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:00.148164988 CET	8.8.8.8	192.168.2.7	0xd40a	No error (0)	s.ad.smaato.net		13.32.22.118	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:00.148164988 CET	8.8.8.8	192.168.2.7	0xd40a	No error (0)	s.ad.smaato.net		13.32.22.28	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:00.148164988 CET	8.8.8.8	192.168.2.7	0xd40a	No error (0)	s.ad.smaato.net		13.32.22.27	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:00.311403036 CET	8.8.8.8	192.168.2.7	0x311d	No error (0)	pixel.tapad.com		35.227.248.159	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:00.326419115 CET	8.8.8.8	192.168.2.7	0x6967	No error (0)	match.contentexchange.me		46.19.11.36	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:00.338881969 CET	8.8.8.8	192.168.2.7	0xefea	No error (0)	eb2.3lift.com	eu-eb2.3lift.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:42:00.338881969 CET	8.8.8.8	192.168.2.7	0xefea	No error (0)	eu-eb2.3lift.com		76.223.111.18	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:00.338881969 CET	8.8.8.8	192.168.2.7	0xefea	No error (0)	eu-eb2.3lift.com		13.248.245.213	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:00.537482977 CET	8.8.8.8	192.168.2.7	0x355e	No error (0)	rtd-tm.everesttech.net	rtd.tubemogul.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:42:00.537482977 CET	8.8.8.8	192.168.2.7	0x355e	No error (0)	rtd.tubemogul.com	h2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:42:41.243488073 CET	8.8.8.8	192.168.2.7	0x5f88	No error (0)	115079-29.chat.api.drift.com	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:42:41.243488073 CET	8.8.8.8	192.168.2.7	0x5f88	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		34.232.153.59	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:41.243488073 CET	8.8.8.8	192.168.2.7	0x5f88	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		18.205.58.198	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:41.243488073 CET	8.8.8.8	192.168.2.7	0x5f88	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		52.54.84.154	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 20:42:41.243488073 CET	8.8.8.8	192.168.2.7	0x5f88	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		52.5.116.97	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:41.243488073 CET	8.8.8.8	192.168.2.7	0x5f88	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		54.166.248.40	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:41.243488073 CET	8.8.8.8	192.168.2.7	0x5f88	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		54.152.150.128	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:41.243488073 CET	8.8.8.8	192.168.2.7	0x5f88	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		52.4.89.98	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:41.243488073 CET	8.8.8.8	192.168.2.7	0x5f88	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		23.21.39.23	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:42.569945097 CET	8.8.8.8	192.168.2.7	0xf819	No error (0)	presence.api.drift.com	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 20:42:42.569945097 CET	8.8.8.8	192.168.2.7	0xf819	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		54.173.95.250	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:42.569945097 CET	8.8.8.8	192.168.2.7	0xf819	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		35.174.210.7	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:42.569945097 CET	8.8.8.8	192.168.2.7	0xf819	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		52.0.218.127	A (IP address)	IN (0x0001)
Nov 2, 2021 20:42:42.569945097 CET	8.8.8.8	192.168.2.7	0xf819	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		54.85.240.191	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 2436 Parent PID: 476

General

Start time:	20:40:50
Start date:	02/11/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "https://secure-chsd.org/s/e?m=ABBOdSX2hand3rhcsO3vIAYp&c=ABBYByWB0o0PvF3l0uo5dmRj&em=EAC%40pointloma%2eEDU
Imagebase:	0x7ff76d1c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 1592 Parent PID: 2436

General

Start time:	20:40:51
Start date:	02/11/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1536,1080383137737942703,10415530265892783596,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1920 /prefetch:8
Imagebase:	0x7ff76d1c0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis