ID: 453277
Cookbook: browseurl.jbs
Time: 17:23:08
Date: 23/07/2021
Version: 33.0.0 White Diamond

Table of Contents

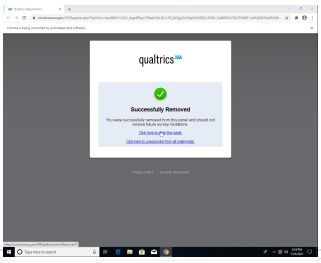
Windows Analysis Report https://covid.census.gov/CP/...

Overview

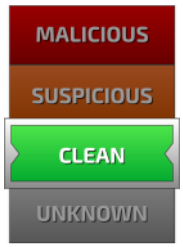
General Information

Sample URL:	https://covid.census.gov/CP/Register.php?OptOut=true&RID=CGC_daprBTqzoTB4ek...R_0ix3gy2rnDlg56J&DID=EMD_SqN0lR2ri39yTOI&BT=dXNjZW5zdXNidXJlYXVjb3ZpZA&_=1
Analysis ID:	453277
Infos:	

Most interesting Screenshot:



Detection

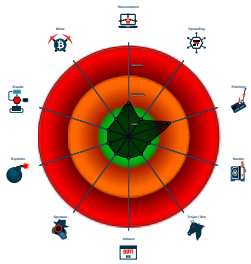


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Found iframes
- HTML body contains low number of ...
- Invalid T&C link found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5336 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://covid.census.gov/CP/Register.php?OptOut=true&RID=CGC_daprBTqzoTB4ekC&LID=UR_0ix3gy2rnDlg56J&DID=EMD_SqN0lR2ri39yTOI&BT=dXNjZW5zdXNidXJlYXVjb3ZpZA&_=1' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 1724 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1640,2244722290038112252,7691160406664226266,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1960 /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

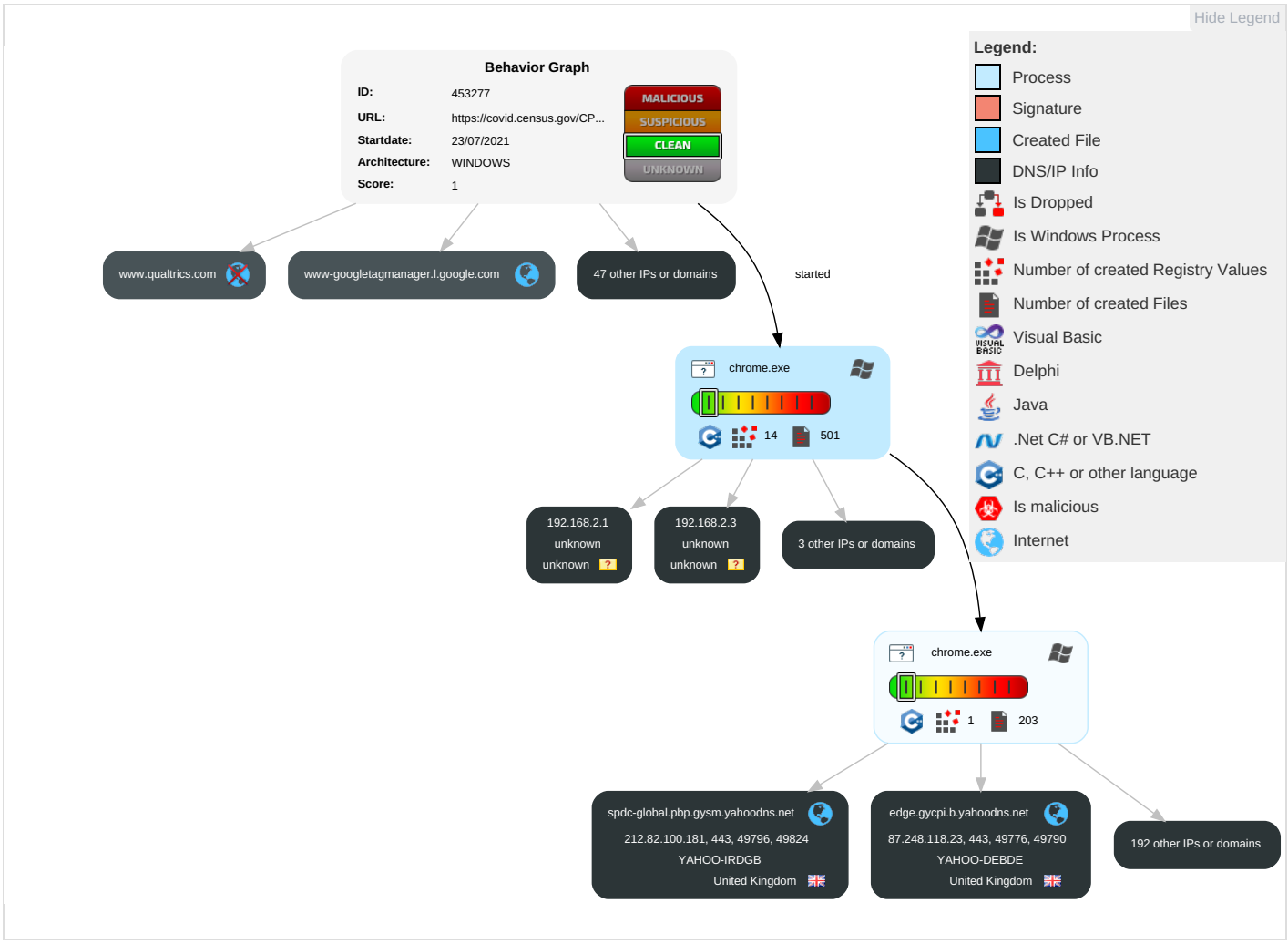
Click to jump to signature section

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	I
Drive-by Compromise 1	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	N S F
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	D L
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	D D D

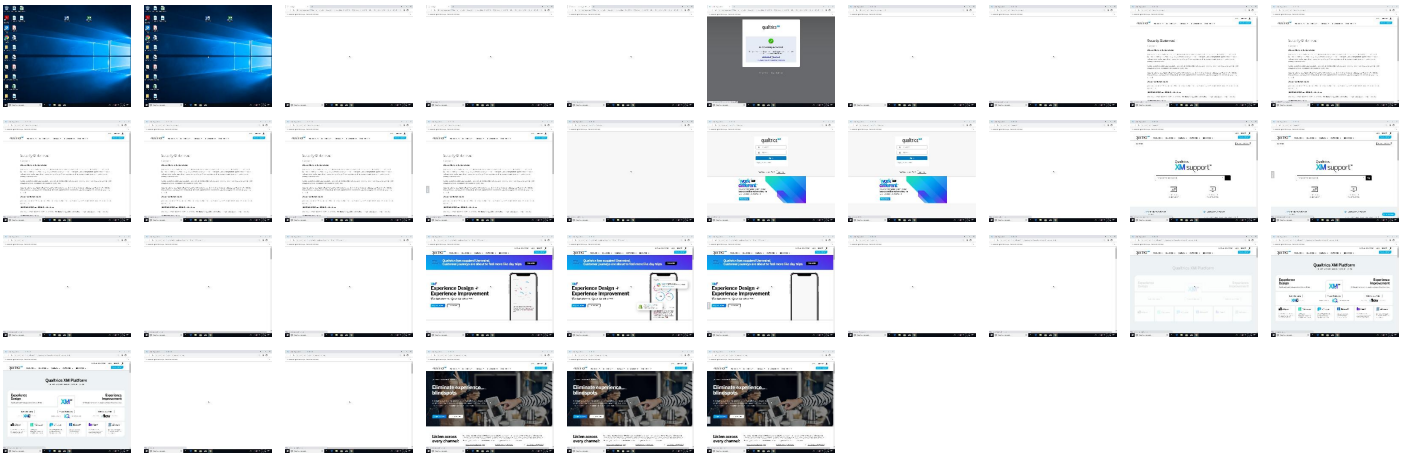
Behavior Graph

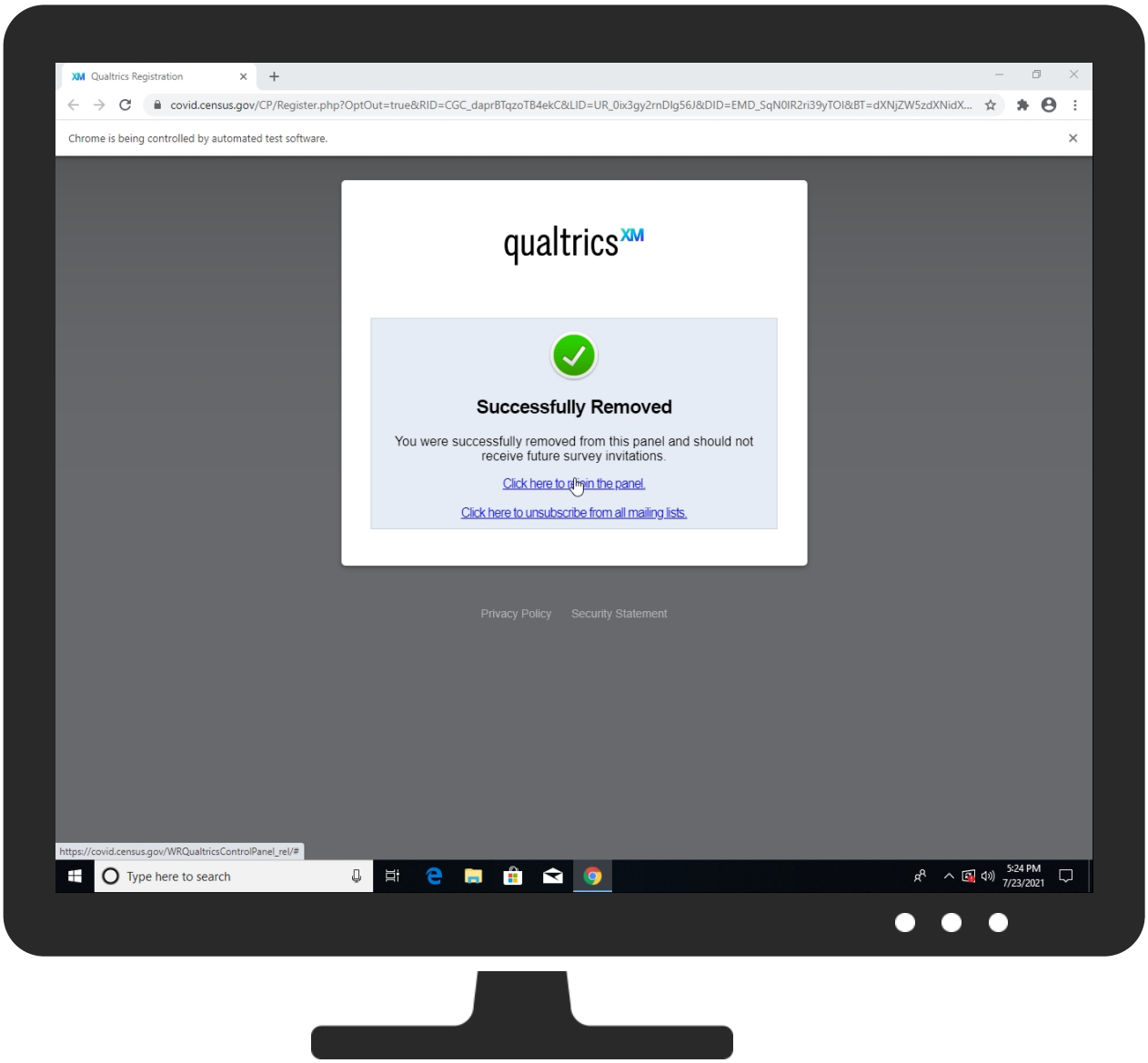


Screenshots

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://covid.census.gov/CP/Register.php?OptOut=true&RID=CGC_daprBTqzoTB4ekC&LID=UR_0ix3gy2rnDlg56J&DID=EMD_SqN0IR2ri39yTOI&BT=dXNjZW5zdXNidXJlYXVjb3ZpZA&_=1	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://solve-widget.forethought.ai/npm.axios.876e878df7f583768084.js	0%	Avira URL Cloud	safe	
http://https://solve-widget.forethought.ai/npm.scheduler.0a4db3c5c8b3c6633028.js	0%	Avira URL Cloud	safe	
http://https://solve-widget.forethought.ai/npm.react.5928087d96bed9c46ed1.js	0%	Avira URL Cloud	safe	
http://https://forethought.ai/xWI	0%	Avira URL Cloud	safe	
http://https://solve-widget.forethought.ai/npm.react-dom.17ddddd2ea32a3d625dc.js	0%	Avira URL Cloud	safe	
http://https://solve-widget.forethought.ai/npm.hoist-non-react-statics.6eafd57b7318f8700355.js	0%	Avira URL Cloud	safe	
http://https://images.mutinycdn.com/82c2f64a-2ad8-4c9d-819a-65a86ff93827/isaac-struna-DMaIZgRq810-unsplash.	0%	Avira URL Cloud	safe	
http://https://solve-widget.forethought.ai/npm.logrocket.c8a35bba1d76c27c027b.js	0%	Avira URL Cloud	safe	
http://https://images.mutinycdn.com/82c2f64a-2ad8-4c9d-819a-65a86ff93827/ABSA.png)	0%	Avira URL Cloud	safe	
http://https://solve-widget.forethought.ai/npm.sentry.de09e17d58473edd0364.js	0%	Avira URL Cloud	safe	
http://https://solve-widget.forethought.ai/npm.react-transition-group.6eee8c21c2073b48ad95.js	0%	Avira URL Cloud	safe	
http://https://munchkin.marketo.net/160/munchkin.js	0%	Avira URL Cloud	safe	
http://https://login.qualtrics.comh	0%	Avira URL Cloud	safe	
http://https://images.mutinycdn.com/82c2f64a-2ad8-4c9d-819a-65a86ff93827/edgar-soto-gb0BZGae1Nk-unsplash.jp	0%	Avira URL Cloud	safe	
http://https://solve-widget.forethought.ai/npm.react-redux.b148dff1aa15fd61b4dc.js	0%	Avira URL Cloud	safe	
http://https://images.mutinycdn.com/82c2f64a-2ad8-4c9d-819a-65a86ff93827/insurance	0%	Avira URL Cloud	safe	
http://https://cdn.lr-ingest.io/logger-1.min.js	0%	Avira URL Cloud	safe	
http://https://client.mutinycdn.com/mutiny-client/8.2.1.0.js	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	172.217.168.3	true	false		high
player-telemetry.vimeo.com	34.120.202.204	true	false		high
lga-bh-bgp.contextweb.com	198.148.27.140	true	false		high
pixel-a.sitescout.com	66.155.71.25	true	false		high
client.mutinycdn.com	52.84.174.89	true	false		unknown
s3.amazonaws.com	52.217.64.246	true	false		high
www.google.com	172.217.168.68	true	false		high
idaas6.cph.liveintent.com	3.209.93.152	true	false		high
bcp.crwdcntrl.net	34.251.130.56	true	false		high
bam.nr-data.net	162.247.242.21	true	false		unknown
vimeo.map.fastly.net	151.101.0.217	true	false		unknown
542-fmf-412.mktoresp.com	192.28.147.68	true	false		unknown
googleads.g.doubleclick.net	172.217.168.66	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
partners-alb-1113315349.us-east-1.elb.amazonaws.com	34.199.218.203	true	false		high
prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com	34.246.41.247	true	false		high
s.w.org	192.0.77.48	true	false		high
googlehosted.l.googleusercontent.com	142.250.203.97	true	false		high
aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com	3.10.35.49	true	false		high
sync.navdmp.com	104.16.14.243	true	false		unknown
public-prod-dspcookiematching.dmxleo.com	34.120.25.144	true	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com	63.32.159.255	true	false		high
o185886.ingest.sentry.io	34.120.195.249	true	false		high
adservice.google.com	172.217.168.2	true	false		high
oeu.vap.lijit.com	72.251.249.14	true	false		high
consent.linksynergy.com	35.241.23.116	true	false		high
dl7g9llrghqi1.cloudfront.net	52.222.174.22	true	false		high
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
idsync.rlcdn.com	35.244.174.68	true	false		high
script.hotjar.com	52.84.174.19	true	false		high
rtb-csync-eqx.smartadserver.com	185.86.137.131	true	false		high
fresnel.vimeocdn.com	34.120.202.204	true	false		high
c.deployads.com	52.51.116.157	true	false		high
intljs.rmtag.com	34.102.147.248	true	false		unknown
thrtle.com	52.86.201.23	true	false		unknown
www.google.de	172.217.168.3	true	false		high
pixel.tapad.com	35.227.248.159	true	false		high
pagead46.l.doubleclick.net	142.250.203.98	true	false		high
accounts.google.com	172.217.168.45	true	false		high
pop-esv5.mix.linkedin.com	108.174.11.37	true	false		high
tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com	18.194.175.178	true	false		high
sentry.io	35.188.42.15	true	false		high
fei.pro-market.net	107.178.240.89	true	false		high
embeds.driftcdn.com	52.222.174.56	true	false		unknown
vars.hotjar.com	52.84.174.22	true	false		high
tags-cluster.rd.linksynergy.com	34.98.67.3	true	false		high
centro.vo.llnwd.net	178.79.242.16	true	false		high
newrelic.map.fastly.net	151.101.1.27	true	false		unknown
d3tnn7lar6ozas.cloudfront.net	52.222.196.201	true	false		high
ib.anycast.adnxs.com	37.252.173.62	true	false		high
prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud	3.126.56.137	true	false		unknown
edge.gycpi.b.yahoodns.net	87.248.118.23	true	false		unknown
sjp.mktossl.com	104.17.70.206	true	false		unknown
vimeo-video.map.fastly.net	151.101.114.109	true	false		unknown
jsdelivr.map.fastly.net	151.101.1.229	true	false		unknown
pug-lhr.pubmatic.com	185.64.190.80	true	false		high
ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com	54.164.185.154	true	false		high
solve-widget.forethought.ai	104.17.177.49	true	false		unknown
cdn.lr-ingest.io	104.21.50.127	true	false		unknown
eu-eb2.3lift.com	76.223.111.18	true	false		high
cm.g.doubleclick.net	172.217.168.34	true	false		high
idaas-ext.cph.liveintent.com	54.85.213.120	true	false		high
sync.1rx.io	213.19.147.45	true	false		high
api.segment.io	52.38.120.169	true	false		high
api.retargetly.com	104.22.17.141	true	false		high
static-cdn.hotjar.com	52.222.174.118	true	false		high
star-mini.c10r.facebook.com	157.240.17.35	true	false		high
us-u.openx.net	34.98.64.218	true	false		high
stats.l.doubleclick.net	108.177.126.155	true	false		high
vimeo.com	151.101.64.217	true	false		high
consent.trustarc.com	52.222.174.42	true	false		high
s3-w.us-east-1.amazonaws.com	52.217.18.236	true	false		high
insight-566961044.eu-west-1.elb.amazonaws.com	52.30.148.233	true	false		high
www3.l.google.com	142.250.203.110	true	false		high
ams01.sync.search.spotxchange.com	185.94.180.126	true	false		high
prod-ash-usermatch-1919559762.us-east-1.elb.amazonaws.com	34.236.226.59	true	false		high
unpkg.com	104.16.126.175	true	false		high
dart.l.doubleclick.net	216.58.215.230	true	false		high
alb-event-1454785217.us-east-1.elb.amazonaws.com	34.234.150.139	true	false		high
ut.ra.linksynergy.com	35.241.23.116	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com	50.16.7.188	true	false		high
a97adde81b00f2ca4.awsglobalaccelerator.com	76.223.111.131	true	false		unknown
e1.emxdgt.com	18.195.155.181	true	false		unknown
cm.t.tailtarget.com	34.102.185.99	true	false		high
spdc-global.pbp.gysm.yahoodns.net	212.82.100.181	true	false		unknown
d296je7bbdd650.cloudfront.net	52.84.178.125	true	false		high
api.forethought.ai	104.18.223.46	true	false		unknown
a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com	35.174.210.7	true	false		high
pixel.sitescout.com	66.155.71.149	true	false		high
pixel.33across.com	208.100.17.176	true	false		high
cse.google.com	142.250.203.110	true	false		high
epsilon.6sense.com	3.65.155.204	true	false		high
www-google-analytics.l.google.com	216.58.215.238	true	false		high
prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud	18.184.153.186	true	false		unknown
www-googletagmanager.l.google.com	172.217.168.8	true	false		high
gentle-meadow-3800.shrouded-lake-4691.herokuspace.com	34.210.130.159	true	false		unknown
load-euw1.exelator.com	54.78.254.47	true	false		high
match-eu-central-1-ecs.sharethrough.com	35.158.176.66	true	false		high
metrics.api.drift.com	unknown	unknown	false		high
zncydxfem8jrupnsj-qwebsite.siteintercept.qualtrics.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://tags.rd.linksynergy.com/pix/8373?type=pos&pt=home&href=https%3A%2F%2Fwww.qualtrics.com%2Fuk%2F%3Frid%3Dip%26prevsite%3Den%26newsite%3Duk%26geo%3DIT%26geomatch%3Duk&referrer=https%3A%2F%2Fwww.qualtrics.com%2F&_rm_fire3p=true	false		high
http://https://www.qualtrics.com/uk/?rid=ip&prevsite=en&newsite=uk&geo=IT&geomatch=uk	false		high
http://https://10784251.fls.doubleclick.net/activityi;dc_pre=CPeoz4PA-fECFYeRhQodLwQIIg;src=10784251;type=rtlnw0;cat=qualt00;ord=9428917481774;gtm=2wg7l1;auiddc=1029000693.1627086256;~oref=https%3A%2F%2Fwww.qualtrics.com%2Flogin-banners%2F%3Flang%3DEN?	false		high
http://https://10784251.fls.doubleclick.net/activityi;dc_pre=CJ6mkoPA-fECFcEQGwodsXcJMA;src=10784251;type=rtlnw0;cat=qualt00;ord=8757211931121;gtm=2wg7l1;auiddc=1029000693.1627086256;~oref=https%3A%2F%2Fwww.qualtrics.com%2Flogin-banners%2F%3Flang%3DEN?	false		high
http://https://10784251.fls.doubleclick.net/activityi;dc_pre=CPLyzfq_-fECFQIaGwodny0IZA;src=10784251;type=rtlnw0;cat=qualt00;ord=6910467301176;gtm=2wg7l1;auiddc=1029000693.1627086256;~oref=https%3A%2F%2Fwww.qualtrics.com%2Fsecurity-statement%2F?	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.246.41.247	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
216.58.215.238	www-google-analytics.l.google.com	United States		15169	GOOGLEUS	false
151.101.64.217	vimeo.com	United States		54113	FASTLYUS	false
52.222.174.118	static-cdn.hotjar.com	United States		16509	AMAZON-02US	false
216.58.215.230	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false
157.240.17.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false
34.236.226.59	prod-ash-usermatch-1919559762.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
185.64.190.80	pug-lhr.pubmatic.com	United Kingdom		62713	AS-PUBMATICUS	false
52.84.174.19	script.hotjar.com	United States		16509	AMAZON-02US	false
35.227.248.159	pixel.tapad.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.22.17.141	api.retargetly.com	United States		13335	CLOUDFLARENETUS	false
172.217.168.2	adservice.google.com	United States		15169	GOOGLEUS	false
52.51.116.157	c.deployads.com	United States		16509	AMAZON-02US	false
37.252.173.62	ib.anycast.adnxs.com	European Union		29990	ASN-APPNEXUS	false
104.21.50.127	cdn.lr-ingest.io	United States		13335	CLOUDFLARENETUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
52.84.174.89	client.mutinycdn.com	United States		16509	AMAZON-02US	false
35.244.174.68	idsync.rlcdn.com	United States		15169	GOOGLEUS	false
108.174.11.37	pop-esv5.mix.linkedin.com	United States		14413	LINKEDINUS	false
66.155.71.149	pixel.sitescout.com	Canada		13768	COGECO-PEER1CA	false
142.250.186.46	unknown	United States		15169	GOOGLEUS	false
34.210.130.159	gentle-meadow-3800.shrouded-lake-4691.herokuspace.com	United States		16509	AMAZON-02US	false
104.17.70.206	sjp.mktossl.com	United States		13335	CLOUDFLARENETUS	false
54.78.254.47	load-euw1.exelator.com	United States		16509	AMAZON-02US	false
34.251.130.56	bcp.crwdcntrl.net	United States		16509	AMAZON-02US	false
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
172.217.168.68	www.google.com	United States		15169	GOOGLEUS	false
192.28.147.68	542-fmf-412.mktoresp.com	United States		53580	MARKETOUS	false
162.247.242.21	bam.nr-data.net	United States		23467	NEWRELIC-AS-1US	false
208.100.17.176	pixel.33across.com	United States		32748	STEADFASTUS	false
172.217.168.66	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
3.65.155.204	epsilon.6sense.com	United States		16509	AMAZON-02US	false
34.98.67.3	tags-cluster.rd.linksynergy.com	United States		15169	GOOGLEUS	false
185.86.137.131	rtb-csync-eqx.smartadserver.com	France		201081	SMARTADSERVERFR	false
34.120.202.204	player-telemetry.vimeo.com	United States		15169	GOOGLEUS	false
18.184.153.186	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud	United States		16509	AMAZON-02US	false
66.155.71.25	pixel-a.sitescout.com	Canada		13768	COGECO-PEER1CA	false
104.17.177.49	solve-widget.forethought.ai	United States		13335	CLOUDFLARENETUS	false
35.241.23.116	consent.linksynergy.com	United States		15169	GOOGLEUS	false
52.217.18.236	s3-w.us-east-1.amazonaws.com	United States		16509	AMAZON-02US	false
34.102.185.99	cm.t.tailtarget.com	United States		15169	GOOGLEUS	false
18.194.175.178	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
52.84.178.125	d296je7bbdd650.cloudfront.net	United States		16509	AMAZON-02US	false
52.222.174.22	dl7g9llrghqi1.cloudfront.net	United States		16509	AMAZON-02US	false
34.120.195.249	o185886.ingest.sentry.io	United States		15169	GOOGLEUS	false
34.199.218.203	partners-alb-1113315349.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
151.101.0.217	vimeo.map.fastly.net	United States		54113	FASTLYUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.203.97	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
108.177.126.155	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
108.177.126.154	unknown	United States		15169	GOOGLEUS	false
104.18.223.46	api.forethought.ai	United States		13335	CLOUDFLARENETUS	false
54.85.213.120	idaas-ext.cph.liveintent.com	United States		14618	AMAZON-AESUS	false
52.222.196.201	d3tnn7lar6ozas.cloudfront.net	United States		16509	AMAZON-02US	false
76.223.111.131	a97adde81b00f2ca4.awsglobalaccelerator.com	United States		16509	AMAZON-02US	false
52.86.201.23	thrtle.com	United States		14618	AMAZON-AESUS	false
34.102.147.248	intljs.rmtag.com	United States		15169	GOOGLEUS	false
52.30.148.233	insight-566961044.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
3.126.56.137	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud	United States		16509	AMAZON-02US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.209.93.152	idaas6.cph.liveintent.com	United States		14618	AMAZON-AESUS	false
212.82.100.181	spdc-global.pbp.gysm.yahoodns.net	United Kingdom		34010	YAHOO-IRDGB	false
52.222.174.42	consent.trustarc.com	United States		16509	AMAZON-02US	false
52.38.120.169	api.segment.io	United States		16509	AMAZON-02US	false
3.10.35.49	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
185.94.180.126	ams01.sync.search.spotxchange.com	Netherlands		35220	SPOTX-AMSNL	false
172.217.168.8	www-googletagmanager.l.google.com	United States		15169	GOOGLEUS	false
172.217.168.3	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
35.158.176.66	match-eu-central-1-ecs.sharethrough.com	United States		16509	AMAZON-02US	false
76.223.111.18	eu-eb2.3lift.com	United States		16509	AMAZON-02US	false
151.101.1.229	jsdelivr.map.fastly.net	United States		54113	FASTLYUS	false
198.148.27.140	lga-bh-bgp.contextweb.com	United States		19189	PULSEPOINTUS	false
107.178.240.89	fei.pro-market.net	United States		15169	GOOGLEUS	false
151.101.114.109	vimeo-video.map.fastly.net	United States		54113	FASTLYUS	false
178.79.242.16	centro.vo.llnwd.net	European Union		22822	LLNWUS	false
151.101.1.27	newrelic.map.fastly.net	United States		54113	FASTLYUS	false
87.248.118.23	edge.gycpi.b.yahoodns.net	United Kingdom		203220	YAHOO-DEBDE	false
172.217.168.34	cm.g.doubleclick.net	United States		15169	GOOGLEUS	false
52.84.174.22	vars.hotjar.com	United States		16509	AMAZON-02US	false
63.32.159.255	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
34.98.64.218	us-u.openx.net	United States		15169	GOOGLEUS	false
52.217.64.246	s3.amazonaws.com	United States		16509	AMAZON-02US	false
72.251.249.14	oeu.vap.lijit.com	United States		29791	VOXEL-DOT-NETUS	false
104.16.126.175	unpkg.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
192.168.2.7
192.168.2.3
192.168.2.6
192.168.2.5
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	453277
Start date:	23.07.2021
Start time:	17:23:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://covid.census.gov/CP/Register.php?OptOut=true&RID=CGC_daprBTqzoTB4ekC&LID=UR_0ix3gy2rnDlg56J&DID=EMD_SqN0lR2ri39yTOI&BT=dXNjZW5zdXNidXJlYXVjb3ZpZA&_=1
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:	11

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@50/404@160/90
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: http://www.qualtrics.com/security-statement.html • Browse: https://login.qualtrics.com/login?lang=en • Browse: https://www.qualtrics.com/support/ • Browse: https://www.qualtrics.com/ • Browse: https://www.qualtrics.com/platform/ • Browse: https://www.qualtrics.com/platform/ultimate-listening/
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:24:22	API Interceptor	2x Sleep call for process: chrome.exe modified

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

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	61020
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	1536:IZ/FdeYPeFusuQszEfL0/NfXfdl5lNQbGxO4EBJE:0tdeYPiuWAVtlLBGm
MD5:	2902DE11E30DCC620B184E3BB0F0C1CB
SHA1:	5D11D14A2558801A2688DC2D6DFAD39AC294F222
SHA-256:	E6A7F1F8810E46A736E80EE5AC6187690F28F4D5D35D130D410E20084B2C1544
SHA-512:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2FA0
Malicious:	false
Reputation:	low
Preview:	MSCF....\.....,.....I.....I.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,.=.I.D.....3...3WW.....y...9..w..D.yM10....`.0.e.._.'..a0xN....)F.C..t .z.,.O20.1``L.....m?H..C..X>Oc..q.....%.!^v%<...O...-..@/.....H.J.W..... T...Fp..2.|$...._.Y..Y`&..s.1.....s.{..,."':o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.` =*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...I.....D0.....Ba...Z.0.o..l.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)... .....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f|.*...'^K`\..e.....j/..|..)..&i...wEj.w...o..r<.$.....C.....}.x...L..&..).r..\...>....v.....7...^..L!.$..'m...*,*.....7F$..~..S.6$S.-y....|.!.....x ...~k...Q/.w.e...h.[...9<x...Q.x.[]}*_%Z..K.).3..'....M.6QkJ.N.....Y..Q.n.[.(.... ...Bg..33..[...S..[... .Z..<i.-.]...po.k.,...X6.....y3^.t[.Dw.]ts. R..L..`..ut_F....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\A4B782275DC1682E4DC39E697A49B151	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1236
Entropy (8bit):	7.139560346502974
Encrypted:	false
SSDEEP:	24:Ky1nita8l2Ymnit2FwlZ7lPo6h7s3aV9unDa1VywVAVwVm7XqyzwsoQc3:KWnita8anitxzlX43vadGVvqyvRS
MD5:	96C25031BC0DC35CFBA723731E1B4140
SHA1:	27AC9369FAF25207BB2627CEFACCBE4EF9C319B8
SHA-256:	973A41276FFD01E027A2AAD49E34C37846D3E976FF6A620B6712E33832041AA6
SHA-512:	42C5B22334CD08C727FDEC4ACA8DF6EC645AFA8DD7FC278D26A2C800C81D7CFF86FC107E6D7F28F1A8E4FAF0216FD4D2A9AF22D69714CA9099E457D1B2D518A
Malicious:	false
Reputation:	low
Preview:	0...0.....0...*.H.....0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.110/..U...(Go Daddy Root Certificate Authority - G20...110503070000Z..310503070000Z0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.1-0+..U...$http://certs.godaddy.com/repository/1301..U...*Go Daddy Secure Certificate Authority - G20..."0...*.H.....0.....v..b.0d...l...b../.>e..b.<R...EKU.xkc.b...il.....L.E3....+..a.yW....?0<]G.....7.AQ..KT.(....08..&.fGcm.q&G.8GS.F .....E...q.o....0:yO_LG...[..`;..C..3N..'O.%.....t.dW..DU.-*:>....2...d..:P.J..y3.. .....9.i.lcR.w...t....PT5KiN.;.I....R.....0...0...U.....0....0...U.....0...U.....@.'..4.0.3..l..,. .0...U.#..0...:....g(.....An .....04..+.....(0&0$..+....0...http://ocsp.godaddy.com/05..U....0,0*.(.&.$http://crl.godaddy.com/gdroot-g2.crl0F..U. .?0=0;..U. .0301..+.....%https://certs.godaddy.com/repository/0...*.H.....~I...8....K._O..I>

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	326

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Entropy (8bit):	3.136889839281767
Encrypted:	false
SSDEEP:	6:kKWtqdoW+N+SkQlPlEGYRMY9z+4KlDA3RUeIlD1Ut:B5kPlE99SNxAhUe0et
MD5:	3CC107BA6A2DE5B44C4F8688ADDEB544
SHA1:	5FD501A83A5A392E3CCDF1C6E4E15C1DD2B6C837
SHA-256:	DA2F41FF92F5678EE36665FC8C6DF7443DB2854030D822E58B835862511C8FA6
SHA-512:	CAE7D4B46F911C30B4ED3200ED5967EE2648FBA8DBB570000D6411097FC2DDC067BBEACBE8B16C2DC67192261C26E60D8FE3B274BEC73148894E51C7220F5F FD
Malicious:	false
Reputation:	low
Preview:	p..... .....<N.@"...(..... .....T'._.....$.....\...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..".0.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\A4B782275DC1682E4DC39E697A49B151	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	262
Entropy (8bit):	2.9209116395050425
Encrypted:	false
SSDEEP:	3:kkFkl4ZVHlyEttfllXlE/jb8V/Hll/XlRDr3wIL9CQBkYcQlA+iYl+XylRBUXl5V:kKhTTt6sjgIcQGQuf1K7OlGm
MD5:	A63D9D84F4932550481FF09AA8AFBE22
SHA1:	D92E44CDB1CD5E3BAA191C195EF7E3950DDE535D
SHA-256:	57000A619CF47E612D40E03F9123CB1064F5715CEA6B33BA570E50745908A2A2
SHA-512:	9F1C3EC42C088665883B1B62F259EEC3FFBDAA37ED8E1EE6280E0E05721F4D83138354020E5C561208ED205925426A8876141A1B1A8E56B6B50B94509B3B433C
Malicious:	false
Reputation:	low
Preview:	p..... ....j....Q.p"...(..... .....Fe[.c.....(.....h.t.t.p.:././.c.e.r.t.i.f.i.c.a.t.e.s...g.o.d.a.d.d.y...c.o.m./.r.e.p.o.s.i.t.o.r.y./.g.d.i.g.2...c.r.t..".4.d.4.-.5.c.4.f.9.c.0.9.d.7.a.4.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\22b80c42-a7e9-4d53-beee-fe995c531caf.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7511960113120746
Encrypted:	false
SSDEEP:	384:dbonXNqwF2xNV2criNDrYvf13wPhwHpsG0zr+ZXvxohNtsr2bmGSRaFbH7QOhBf9:JSKVVqNB4UejD9xUnbOFKrFHhD
MD5:	DABA3D61C900B3BC8CB4FD175959CF65
SHA1:	FB0C6FBDA8396E0E4B33D6CC333AB0E611AEDB6E
SHA-256:	5B81F4EF3DC9CD9260003C0C91D48AEF8C9FCBA1215974AED58D238E7206B23A
SHA-512:	9F54D17D87D00BBD7C2FA44C1D70550A7A1D2E5505559201F9A913797410A9219D224057AD61478C734EA01D98F25D45C496EF0A5C1A4A9670A4149A75922FF8
Malicious:	false
Reputation:	low
Preview:	.t.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{}...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....@8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\32971b41-453a-4254-9e0a-41eb702bad7f.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):	377837
Entropy (8bit):	6.049172121916324
Encrypted:	false
SSDEEP:	6144:blBLBtL/F1CfV2G0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinE:B9bbCfcGNPUZ+w7wJHyEtAWx
MD5:	7AB45D6C2E3364BB56F22B65574CBD44
SHA1:	82B90D171A12A223E3C76887D00CB6B85258679C
SHA-256:	C0C8ACA1011A014F6239BF7D83FAB93238F81343DF9B1E246D5BE822F74DF301
SHA-512:	68DF0120074FB75A5EFD6162A913AF900CB9C1C9273A6116F223B07DC54A1BED787645BE3E5EE43FB19897A1A66260727020F130F85B4DE7F83A541238B248FA
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\32971b41-453a-4254-9e0a-41eb702bad7f.tmp	
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":1.627086247104856e+12,"network":1.627053849e+12,"ticks":4011790733.0,"uncertainty":4360399.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAABYJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488666680"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\5d92d10d-1646-4ae3-af82-b966025dac92.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):	377837
Entropy (8bit):	6.049171949737805
Encrypted:	false
SSDEEP:	6144:ClBLBtL/F1CfV2G0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinE:C9bbCfcGNPUZ+w7wJHyEtAWx
MD5:	0096463EABFC5E4D7E0F3ED8AA6F6832
SHA1:	FC56CE7CD9A7F02B22D7BB9BECB187BE5D241191
SHA-256:	B2F366927F84EE957F9AFD58908C6200F077DEDB54EBA026C8CE506296783A1E
SHA-512:	D21FA4E3263C874608E0AA3BB51E74810C6718A9F17FF69094C323C1C0AA0112C8F1C5A16370EB16CB7C09F45BB42E43449FB77DE523C883E09CFA36E07CEBE1
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":1.627086247104856e+12,"network":1.627053849e+12,"ticks":4011790733.0,"uncertainty":4360399.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAABYJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\5fc4a909-4655-4882-8fb4-942b99f9ca10.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.750714104219658
Encrypted:	false
SSDEEP:	384:DbonXNqwxx2riNDrYvf13wPhwHpsG0zr+ZXvxohNtsr2bmGRaFbH7QOhBfN+1TqY:gKVVqNw4UejD9xUnbOFKrFHhC
MD5:	6F1957AA2A94578F974707539C12306F
SHA1:	6F69BAB16FBA9F652EA94E88E167E6281C6945B4
SHA-256:	3A84A5A92337119F8D64F8EF75CCE97D42C0475994B5884BCE97ABAA3DFF3F71
SHA-512:	1F1898777FE8E8B871862F5E43E672553F61DF80689E6A1DD3808E8059B1F87C2A15D33824C0D0976250571DC51B9BAA090D4B435B0014BA61F7F611DB1675D9
Malicious:	false
Reputation:	low
Preview:	0j.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....@8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\672ac732-fdff-466b-9f01-06201aaea995.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.751155142079015
Encrypted:	false
SSDEEP:	384:tbonXNqwF2xNV2criNDrYvf13wPhwHpsG0zr+ZXvxohNtsr2bmGRaFbH7QOhBfNk:5SKVVqNw4UejD9xUnbOFKrFHhc
MD5:	B028F9D2815C7783164173AA80FAD0FC
SHA1:	240F19DFFA7FE5DE1324D0B325595F0F651B89F4
SHA-256:	B67ACC05A0E8C3A0F4ECE0ACEB647BAA8E2C9930405C07B06DD2B9C3CAD23EB8
SHA-512:	7A0D092DE65A1A73326DBBF2A7D22C25D1A8F04671BFBB7E41560BAE647C573BB038ADD4A341B4B3C989989CE4BBA7EC60F375752953E441B3FC9B7DC3B47455
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\672ac732-fdff-466b-9f01-06201aaea995.tmp	
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....@8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\67909b7b-2c2c-49da-993c-d48f3f8268f9.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):	369364
Entropy (8bit):	6.027974980250614
Encrypted:	false
SSDEEP:	6144:b9lBLBtL/F1CfV2G0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinE:b/9bbCfcGNPUZ+w7wJHyEtAWx
MD5:	87205436BBBA51AA658A8F9B6F8FC5D2
SHA1:	4CE3A0D7878A093F2C630EAA9BE550694A560BD9
SHA-256:	5CFF1D3A3C824610857F576ECB28B59BF2D80505B51C83B7C61E4E30CF5A3295
SHA-512:	A3C1C490BBB150ACB75A87F47DE9B042A62E66BBE73BB454368BB228E53BFDEA76638948FC2851894730BD3DFB7CCC27C99106F46D9595862D73BFD17359DD B
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":1.627086247104856e+12,"network":1.627053849e+12,"ticks":4011790733.0,"uncertainty":4360399.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488666680"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\8927e5f7-c58e-4c4b-8416-6fe0ab12c587.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):	369364
Entropy (8bit):	6.027974980250614
Encrypted:	false
SSDEEP:	6144:b9lBLBtL/F1CfV2G0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinE:b/9bbCfcGNPUZ+w7wJHyEtAWx
MD5:	87205436BBBA51AA658A8F9B6F8FC5D2
SHA1:	4CE3A0D7878A093F2C630EAA9BE550694A560BD9
SHA-256:	5CFF1D3A3C824610857F576ECB28B59BF2D80505B51C83B7C61E4E30CF5A3295
SHA-512:	A3C1C490BBB150ACB75A87F47DE9B042A62E66BBE73BB454368BB228E53BFDEA76638948FC2851894730BD3DFB7CCC27C99106F46D9595862D73BFD17359DD B
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":1.627086247104856e+12,"network":1.627053849e+12,"ticks":4011790733.0,"uncertainty":4360399.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488666680"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\8c6ffddc-20e6-4559-8b9c-eeccdb71b3c8.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):	377837
Entropy (8bit):	6.049171554972433
Encrypted:	false
SSDEEP:	6144:olBLBtL/F1CfV2G0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinE:s9bbCfcGNPUZ+w7wJHyEtAWx
MD5:	B3DBA30A58E21A68BFB6D90A5ECD6323
SHA1:	A0418CD911FCF84BBC2D76DEB450B61B022F9266
SHA-256:	097AFF05FD4361371C8AF6266CD630ECAF83F4B17E923F4BC3400B3B067B3D65
SHA-512:	90BC2BB6DFB32EECCCF88479BB5F296364E464683F97F13A51CEB6CA4BA99CD1B2C8EAACD2E272D57F279AB6549AE7119F854A874C9245E115951BF2823447E D
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\8c6ffddc-20e6-4559-8b9c-eeccdb71b3c8.tmp	
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":1.627086247104856e+12,"network":1.627053849e+12,"ticks":4011790733.0,"uncertainty":4360399.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488666680"},"plugins":{"metadata":{"adobe-flash-player":{"dis

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):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXEwozZHGftEwozZHGftEwozZHn:+EwozZHGVEwozZHGVEwozZHn
MD5:	4829695F153A750ADF50C6E979E8E8F3
SHA1:	2F697EF207460D03671E4B59670BC73328D60D6E
SHA-256:	1AACF1304FD42C84FF41DDD2F2252E5C0EDE7362352661B7957648F2EA4C2683
SHA-512:	6D16A6EF4BB20B25B1B14757C475E9F8C3A40D6181F718D563A628BA41DA9426E1B586C472D4F8729FD65FCA014151B7D46FBFAAE171BFF9A6D937DB7A7A2C02
Malicious:	false
Reputation:	low
Preview:	sdPC.....y3..M.Y.NbD.sdPC.....y3..M.Y.NbD.sdPC.....y3..M.Y.NbD.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0cd45e79-64a0-4c80-9579-2299c42daa48.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):	22595
Entropy (8bit):	5.536235086455508
Encrypted:	false
SSDEEP:	384:m+Tt9LlBjXu1kXqKf/pUZNCgVLH2HfDHrUNHGKnTs7m3i49:LLlBu1kXqKf/pUZNCgVLH2HfzrUxGKnR
MD5:	D1193256015C833BB0A8B7AFD0E3A6FF
SHA1:	618FE31CED5156509240067BB50C4C2767893809
SHA-256:	0E59E11C7A75EF59DCF6B20E725E0FF23E0AA0219EDEA46EA417DD1D13D54B99
SHA-512:	B9AFEAE72F56E2FC4FA2A4EA0BD2E5D54728E55E3909E59076F6B050B3506E5BC042B788A21E902B9E8FFC5C8101F12212999C2D39A9D3B4FAA349F8D3498F8
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":"13271559842625225","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\12b29832-b9a7-4c37-90a1-c7ead731583a.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):	8387
Entropy (8bit):	5.596576628960132
Encrypted:	false
SSDEEP:	192:/UYUIUo7UqUrUyUdYUlU1eURUlU/U75eUAUUa7UdUR7U+IUUUbUQUTUShUwUhQUQ:/jpJ7/sxaY2VYaUWw85gY7IJG/qrh9xb
MD5:	4271B075A9C8315D45E306201719F199
SHA1:	5A201A6465AF193C496E71DBBB69B3EFFE71F6D0
SHA-256:	7A9D9AE417F8B4AA96C3C933C7559A834E3344794646F00DEF22CDB76D84F094
SHA-512:	1E2DB3B44E90F39313683FFC5E1D81624F68361F48CD797F9C8815C9292F81164F9960E4741933D4649AA715B05E2A27586FE9023C56CCCFB9A49578C23778EC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\12b29832-b9a7-4c37-90a1-c7ead731583a.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1658622339.899859,"host":"Aa4GU0FxuqcjoAXZTmDr1vDKrMq1S6I5XChQWQN9I08=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086339.899865},{"expiry":1658622308.721496,"host":"AzBeBX1x4HNBjIA5bPS3feRO+Htj81hHpqjnutroB/I=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086308.721501},{"expiry":1642854319.413936,"host":"BBOugrewRBSrzXkoKc6fle0sVpb0Ep+WZj0hzmox9d0=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086319.41394},{"expiry":1658622326.231798,"host":"B33dNWuWc3elp/rqxbaViYp8VufHqjSms9l6Z0xI7lk=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086326.231804},{"expiry":1627107924.781298,"host":"FyyYYyYz9Eg39ft5yUHhafcjMRpvNWI/vbTSVMs7KmQ=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086324.781303},{"expiry":1627107943.123225,"host":"HQ2YsxhOgJnZ2Kgo8kUjwIJ/qNRZ7nu5hXy/7m5rHKA=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\15e5eae2-32ed-43bf-8dd7-f31f2a170e33.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):	2825
Entropy (8bit):	4.86435102445835
Encrypted:	false
SSDEEP:	48:YALtdpBeMsNMHK5sJDysACs37sHWsd5/sSYMHCKs/MHCzsSOMHwsSJtFsX3RLs9D:HQxGKWDS1i/5vYGmGqOGKJ03QshS
MD5:	95488A82D5073BDAAFC1480073FF801F
SHA1:	E2E979B6D4A3EE16A815115C414D0A98E1DFA93F
SHA-256:	C091AE68AFCD5EC632B2C324B983D70F722463CB4D05A3CE8D52E07AA7E5A5D6
SHA-512:	D536466352320C5D394130A59B605617580050CDF325C4B3392D87D384C246E9D8C54FC16A247FF4B379F162536304E0D312D7781FFE245C643C5081B8BE08CD
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952675493","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":32613},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952813644","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952748754","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952634896","port":443,"protocol_str":"quic"}],"isolation":[],"server"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\224ab5fb-3f8f-4f6d-9e6a-26835797bf31.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):	8888
Entropy (8bit):	5.593555883622779
Encrypted:	false
SSDEEP:	192:qUWUIUc7UGUrUyUKEYUXUVeU3UgUaU75eUAUUarD+U8UrUR7U+FUaUPUQUTUShU2:qFp177sxCYIp6NhWw8lD+h+Y7FfW/qrB
MD5:	57EA134FCB74E0D0CA75075FFE567163
SHA1:	F386C91F1AA1678758E247A96513930B0AE3C2E9
SHA-256:	105EB2A58DE3F233535F4568BE69165F97FC4DA61E779E7004B93954566D105D
SHA-512:	0899EE955221775D4AD87BB3F1D34DA3A79D6210DB5A0A51FC43A24792938C535C6C0479B5181C0E5FAF242353D2DAD8F0921E410D4639A487AD0646263D8598
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1658622378.364951,"host":"Aa4GU0FxuqcjoAXZTmDr1vDKrMq1S6I5XChQWQN9I08=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086378.364955},{"expiry":1658622308.721496,"host":"AzBeBX1x4HNBjIA5bPS3feRO+Htj81hHpqjnutroB/I=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086308.721501},{"expiry":1642854319.413936,"host":"BBOugrewRBSrzXkoKc6fle0sVpb0Ep+WZj0hzmox9d0=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086319.41394},{"expiry":1658622378.005943,"host":"B33dNWuWc3elp/rqxbaViYp8VufHqjSms9l6Z0xI7lk=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086378.005976},{"expiry":1627107924.781298,"host":"FyyYYyYz9Eg39ft5yUHhafcjMRpvNWI/vbTSVMs7KmQ=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086324.781303},{"expiry":1627107943.123225,"host":"HQ2YsxhOgJnZ2Kgo8kUjwIJ/qNRZ7nu5hXy/7m5rHKA=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\260d8418-57e3-4f6a-b8fb-d28035f38b96.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):	7060
Entropy (8bit):	5.594555617409998
Encrypted:	false
SSDEEP:	192:sUq8UIUF7UHUsU3UkYUsU1eUeUDU75eUAUUaw7U+0UKUpU0UtU9UhQURUiU/U4Uq:sH8ps72LqjY/VvUWw8e70jAdgwx4xOBD
MD5:	9E91FD3D273B3B45A7A87B75FFA01886
SHA1:	AE6412C6A36BEF8A32D6E2DE1374E890ACC45911
SHA-256:	FE10F648A04A9419903096ED87B35FAD20EE9A18C5095D9791C80AD0FD72FFCE
SHA-512:	624A4D24762E92FEA124B3220ECEF85884746CAF5354CFB0B3B9F2763D8EEB472212E08D485537B259D82E2D62A2C55FE116DFF23213979F02BBEA219A4E747B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\260d8418-57e3-4f6a-b8fb-d28035f38b96.tmp

Preview:	{"expect_ct":[],"sts":[{"expiry":1658622315.604081,"host":"Aa4GU0FxuqcjoAXZTmDr1vDKrMq1S6I5XChQWQN9I08=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086315.604086},{"expiry":1658622308.721496,"host":"AzBeBX1x4HNBjIA5bPS3feRO+Htj81hHpqjnutroB/I=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086308.721501},{"expiry":1642854319.413936,"host":"BBOugrewRBSrzXkoKc6fle0sVpb0Ep+WZj0hzmox9d0=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086319.41394},{"expiry":1658622323.848136,"host":"B33dNWuWc3elp/rqxbaViYp8VufHqjSms9l6Z0xI7lk=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086323.848141},{"expiry":1627107924.781298,"host":"FyyYYyYz9Eg39ft5yUHhafcjMRpvNWI/vbTSVMs7KmQ=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086324.781303},{"expiry":1627107922.924835,"host":"HQ2YsxhOgJnZ2Kgo8kUjwIJ/qNRZ7nu5hXy/7m5rHKA=","mode":"force-https","sts_include_subdomains":false,"sts_o

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\264fd5a9-10a6-4312-b048-699c058b6da5.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):	5763
Entropy (8bit):	5.187087723227767
Encrypted:	false
SSDEEP:	96:nj4XbysdMKJNaAKInxk0JCKL82hkw1frbOTQVuwn:nj4XbZMK9D4KTkwB/
MD5:	F32BE550776F3515D240A761B3DD2182
SHA1:	53FE14A1F13E1ED7C371CA18C8C2DAF87A9BD55D
SHA-256:	72BF89B473C98315098660CDBE78EDE3F6268E44CD26674CDA3C655F73A5F9A2
SHA-512:	4B69F32BDD272488694D1F99682CC77D3015486747268B1F284F81329B78ED8DFABC9B6279FF022D53BB6BC5C258D87F835AFB23BDE9B9A3EDF725EF3CFB285
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271559842807032","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\33885b5d-9683-4c99-9ce3-4a48866b4565.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):	6217
Entropy (8bit):	5.592534357167967
Encrypted:	false
SSDEEP:	192:dUJUF7UupUBUsYUleU2UCU7TeUnuUUaw7U+IUyUSU0UtU9UhQUNiUmUhUtUsKU4m:dmA7BpgDY3jBWyue7IdXdgwxVXUmdKdm
MD5:	875D24F9522201A767FBC41BC677A7D4
SHA1:	B712AC0AB9BE1014D3F8816F5D7D771FDFC77CED
SHA-256:	EA26C2727BAAF195E51EE934905A4040CDB78452146911E5AB41E0B0F22AC0F8
SHA-512:	FA34AE7CDEDEB44FFCE166F904DC28F155AC9B310124F0F1499EC3975B003D8D1E1BACDB5F5A6BB3558164436C752E4D74172C9DBA94CC809F4C1E954807AA AB
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1658622261.647083,"host":"Aa4GU0FxuqcjoAXZTmDr1vDKrMq1S6I5XChQWQN9I08=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086261.647089},{"expiry":1658622308.721496,"host":"AzBeBX1x4HNBjIA5bPS3feRO+Htj81hHpqjnutroB/I=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086308.721501},{"expiry":1658622315.278594,"host":"B33dNWuWc3elp/rqxbaViYp8VufHqjSms9l6Z0xI7lk=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086315.2786},{"expiry":1627107912.523965,"host":"HQ2YsxhOgJnZ2Kgo8kUjwIJ/qNRZ7nu5hXy/7m5rHKA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086312.523969},{"expiry":1658622307.44047,"host":"Hi4bEdMq563Qsqn4sVyUls/uVk7U80IxMa3wyWVUqWU=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086307.440474},{"expiry":1642638312.792527,"host":"Imip1Y7nHfPZTYQgI7EifDZOyiqlFeRT0HU8heztW1Q=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\38a0a2c8-ce2a-4f07-8de9-4b810425afcd.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):	2042
Entropy (8bit):	5.58398077514853
Encrypted:	false
SSDEEP:	48:YmieUo2c6UUhcz1mU2UoK+MAOUGKUe3UogUo4JUFxaUeSwUNkhUew:9ieUo2lUUakU2UoKAOUGKUgUogURJUFJ
MD5:	0D47FE749A553A29D3F8848E8B34006B
SHA1:	A3203A8D119D14CEAC04D2CB97693798CF9B4F8A
SHA-256:	354390BDB36E32E175CBA940C050864F7E3BAC7B3FEDEC2B8EFD638740CFE6D8
SHA-512:	1A6ACDFF5D7D3BA563BA2AFFAB74B19C19AE27119FAA671D341CA450A132E99D606D90FFF5FE5A389128D52255FCFC85CE1C68CE77D1CD5260E922E6CF9A4 F8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\38a0a2c8-ce2a-4f07-8de9-4b810425afcd.tmp

Preview:	{"expect_ct":[],"sts":[{"expiry":1658622254.700859,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086254.700865},{"expiry":1633015352.675531,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601479352.675536},{"expiry":1658622255.044823,"host":"VGQ6545MPscdk7hM9fz9uBzJpl6C/weKwQlKZ0pwY6E=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086255.044828},{"expiry":1658622254.471796,"host":"YM4f//w1CcI/7dx+OeDGnBvwUnMyJZY4cHFMiioO6Vw=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086254.471801},{"expiry":1658622256.89042,"host":"hj2BNNgbcbmO14A6Aijd/hhGxIj9INAjfq11nYDXuMo=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086256.890424},{"expiry":1633015352.520557,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3bada902-d8e4-483c-9289-e8baa23141ac.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5154
Entropy (8bit):	4.977050227393555
Encrypted:	false
SSDEEP:	96:nj4XbaoqmMpaAKIOxk0JCKL82hkw1frbOTQVuwn:nj4XbimMp944KTkwB/
MD5:	D3A87DCF104860ED09BCB14EE97018F5
SHA1:	8F67A065A5021C22DB564F6CB154F687E12FA2BE
SHA-256:	82D0963DCE7D181E58F7AFB846BF809CB15B4A72C52B23B9B8E1CB1E8214D85A
SHA-512:	695C02718831FA9D98D8AF35D684A36A12D9F8F328FB7B3A6642A6E19AB88158444FC7F60F316F3EE8DE772769F5ACF06FE758C8B648C0CF5A06C47016A09B5C
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271559842807032","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\50e556e9-2ece-4bdd-ab0a-90890272cd20.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\58628bc6-7340-4ed3-86e2-65d071aee781.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):	2825
Entropy (8bit):	4.86435102445835
Encrypted:	false
SSDEEP:	48:YALtdpBeMsNMHK5sJDysACs37sHWsd5/sSYMHCKs/MHCzsSOMHwsSJtFsX3RLs9D:HQxGKWDS1i/5vYGmGqOGKJ03QshS
MD5:	95488A82D5073BDAAFC1480073FF801F
SHA1:	E2E979B6D4A3EE16A815115C414D0A98E1DFA93F
SHA-256:	C091AE68AFCD5EC632B2C324B983D70F722463CB4D05A3CE8D52E07AA7E5A5D6
SHA-512:	D536466352320C5D394130A59B605617580050CDF325C4B3392D87D384C246E9D8C54FC16A247FF4B379F162536304E0D312D7781FFE245C643C5081B8BE08CD
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"broken_alternative_services":[{"broken_count":1,"host":"accounts.google.com","isolation":[],"port":443,"protocol_str":"quic"},{"broken_count":1,"host":"www.google.com","isolation":[],"port":443,"protocol_str":"quic"}],"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952675493","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":32613},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952813644","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952748754","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248544952634896","port":443,"protocol_str":"quic"}],"isolation":[],"server"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5d444e53-67b7-4803-ae94-3c0ec25ae3ca.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):	3379
Entropy (8bit):	5.59523210703569
Encrypted:	false
SSDEEP:	96:dUFUmYU8eUpieU7UUa+UMUxUoSUi0AOUGKUgUoBFUUURJUFxaUiUNCUFUL:dUFUmYU8eUXU7UUa+UMUxUoSU3UGKUgw
MD5:	806EC6317112F7C27A61E09A8DFDB45A
SHA1:	D2BCF1A4E08093EE171CA2F4C69D5F469622A3D0
SHA-256:	3EEF58D6DA8324BD77E95321CAB3312A1F44DBA3923F3FA35B4695A17644C0E1
SHA-512:	7E2F5ACF559DD8900E159B07E2AF80577406773146CC905E70001D4B95588AC1CE80B95B092DD707DEBAF8217C3285C4200673350D56FB81A8E5D7F093318560
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1658622261.647083,"host":"Aa4GU0FxuqcjoAXZTmDr1vDKrMq1S6I5XChQWQN9I08=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086261.647089},{"expiry":1627107858.992875,"host":"HQ2YsxhOgJnZ2Kgo8kUjwIJ/qNRZ7nu5hXy/7m5rHKA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086258.99288},{"expiry":1642638260.102414,"host":"Imip1Y7nHfPZTYQgI7EifDZOyiqlFeRT0HU8heztW1Q=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086260.102418},{"expiry":1637972660.964112,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086260.964117},{"expiry":1658622258.671913,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086258.671918},{"expiry":1633015352.675531,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6186b98c-132d-4507-a8b0-201c4c2df5cd.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):	5.536235366797616
Encrypted:	false
SSDEEP:	384:m+Tt9lBjXu1kXqKf/pUZNCgVLH2HfDHrUNHGFnTs7i3i4h:LLlBu1kXqKf/pUZNCgVLH2HfzrUxGFnh
MD5:	EF27D3CE462822B53B772467E6CEA3D7
SHA1:	27B056BD07B7A50BD2E00C9DDC67ADF3F52EAB2D
SHA-256:	0EE689DE80CDF174E0CB227481289271785CEE429A54108E412BB583F73E8789
SHA-512:	E4E16A7636C9214323B077833AF9F08C0906995BDF0D77DF5229FDDB8E12D6361ACECD8B4A56017190E0A54CC349C176417ACEBC787D552BB531D50C1E7E818
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":"13271559842625225","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\6b2e227d-5548-41f9-b424-5d478bb0b256.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):	7890
Entropy (8bit):	5.599501537040441
Encrypted:	false
SSDEEP:	192:HUiUIUo7UqU7UbUXYUNU1eU1UPUzU75eUAUUaeUI7U+iU6UkUrUvUShUwUhQUxUo:HDpJ7/I2gYUVqKIWw8897i5R6+rh9xMr
MD5:	DD9889E016192A54DF50DB549814F163
SHA1:	CEBD423E1C19DC2D0A63A4763FC0077F92F8CF8B
SHA-256:	085DF9A535DE090AE44956ECA292BE8984705C80043B8B5958A51BBF92847B36
SHA-512:	8288701764EBB1AFA7549CC1A196D1514F462E44CAB292197D06313F48367EA7C54BBF0361994E943AFA265CC6082F5A32C015BF8B4A26ECC3E25E18AC660FE9
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1658622327.399404,"host":"Aa4GU0FxuqcjoAXZTmDr1vDKrMq1S6I5XChQWQN9I08=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086327.39941},{"expiry":1658622308.721496,"host":"AzBeBX1x4HNBjIA5bPS3feRO+Htj81hHpqjnutroB/I=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086308.721501},{"expiry":1642854319.413936,"host":"BBOugrewRBSrzXkoKc6fle0sVpb0Ep+WZj0hzmox9d0=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086319.41394},{"expiry":1658622326.231798,"host":"B33dNWuWc3elp/rqxbaViYp8VufHqjSms9l6Z0xl7lk=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1627086326.231804},{"expiry":1627107924.781298,"host":"FyyYYyYz9Eg39ft5yUHhafcjMRpvNWI/vbTSVMs7KmQ=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627086324.781303},{"expiry":1627107933.595612,"host":"HQ2YsxhOgJnZ2Kgo8kUjwIJ/qNRZ7nu5hXy/7m5rHKA=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9b1e467e-616d-4125-99c5-b95c177da121.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9b1e467e-616d-4125-99c5-b95c177da121.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5789
Entropy (8bit):	5.189589629533208
Encrypted:	false
SSDEEP:	96:nj4Xby/dMKJNaAKIqxk0JCKL82hkw1fCbOTQVuwn:nj4Xb4MK984KTkwB4
MD5:	3740A710B9FF2563FC5FE18E0FFD9921
SHA1:	21B3E1E8200F1C6122F0BDB6AD3A3DF1DA056A7D
SHA-256:	ABB36767949DD80B658D167E5E33CDF7140A07AB9D22C6BAA05E60033E4C852C
SHA-512:	7C7BF5722C59C729CC29BCFA003E1F26E562B6D03EB3FDC25E53B2EAC743EC55D7BDC0A32C7C64E5F6AE17C90FD7AC4FA8FA690EB0C6121AA72F4AD3C2D3B96
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271559842807032","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","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","1501624"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	340
Entropy (8bit):	5.210098193262282
Encrypted:	false
SSDEEP:	6:mfdg/+q2PN723iKKdK9RXXTZIFUtpOdB/ZmwPOdnUVctVkwON723iKKdK9RXX5LJ:bGvVa5Kk7XT2FUtpW//PFVg5Oa5Kk7XH
MD5:	D2F0A9E8683A8B63F8BBB532A73223EB
SHA1:	132043E2C8FA4086BB89C21B79159B6CDB31627D
SHA-256:	498BA7DD4C28E64135B2C458550E8143E51B5EC42D683CB8C439842C02A82297
SHA-512:	0F9108E352DE35440D46061B4B7AB27150D8FFCE666DE6A819EDB572AE7363C7715F41A04C31C45EC8ADD9026EB3076FE69A18C271BFCADFCE1A120EE1F06FD
Malicious:	false
Reputation:	low
Preview:	2021/07/23-17:24:23.175 1098 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/07/23-17:24:23.183 1098 Recovering log #3.2021/07/23-17:24:23.185 1098 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.219042314813676
Encrypted:	false
SSDEEP:	6:mf32N3+q2PN723iKKdKyDZIFUtpO3l5ZmwPO3ltVkwON723iKKdKyJLJ:NNOvVa5Kk02FUtpC/Pu5Oa5KkWJ
MD5:	8D04BE2EE705FEBE37CA7C1F787BF820
SHA1:	8FF5277031F26F2F3A55930F200AC23565E6E294
SHA-256:	CE703EDCC05D256D17898FF5C943DA043E6548DB82F323DAC8444D81D85F3A45
SHA-512:	5DF8855F5CD162756418F42AE089A13D01AFDA1AB48AD39F107E82011A91184F8AE0B20370F47A7F987C368F52BF16CED3B8083F89ABCCC055D48A60BE94F353
Malicious:	false
Reputation:	low
Preview:	2021/07/23-17:24:22.945 1098 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/07/23-17:24:22.946 1098 Recovering log #3.2021/07/23-17:24:22.946 1098 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0057b96b1d8f0164_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	888
Entropy (8bit):	5.520318896139994
Encrypted:	false
SSDEEP:	12:BMfD5FM0HYFvs7u5tVhjrIM+lfctDUYqr3fD5FM0HcEp6J+hcfcIfik0y3Mvsy:BML34ICjzhqr3L32PRikd83

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0057b96b1d8f0164_0	
MD5:	9E41AB40863A3DC6902209E0A4458D8D
SHA1:	085B63455BD95C97053EB7CD2BEA265490ACF0C0
SHA-256:	1D9D14D73D2DF889823AADACDC567BA15B5F5D438789104C96B7448019D25A30
SHA-512:	B1C8AC7E4A8C35047F07D2D0D097AA82B4426641C7D10A9FF36A713527910D7B12AC5E06CD8842F576E9DBD92D600EAFA1764CCF612EC65D6AD90930E81793E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...U....._keyhttps://www.qualtrics.com/assets/dist/js/libraries/teknkl-simpledto-1.0.4.js .https://qualtrics.com/.4..i&/.....Z.....mp...^..;..r}.U..ul4.6...._-.A..Eo.....C.....A..Eo.....4..i&/.H.....'.....O.....dD.....h.....(S.D..`@.....L`.....L`.....(S.....laP...u....P..q=.....*.....d.....QdZ.)e....SimpleDTO...E.@.-....XP.Q.....L...https://www.qualtrics.com/assets/dist/js/libraries/teknkl-simpledto-1.0.4.jsa.....D`....D`....D`.....4...`....&...&..A..D`$...DI]d.....`.....Q.@..o.....window.....K`....Dk.....&.'..a9.....&....&.-...'..%.....$Rc.....`.....Ib.....&.....b..... ...1.d.....mp...^..;..r}.U..ul4.6...._-.A..Eo.....:..T.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\014d4c92b4dbbd55_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	96592
Entropy (8bit):	5.827553714385367
Encrypted:	false
SSDEEP:	1536:TE8P4jLCUqd0cPMVGWrEIZzHJV8PpPRO+OaSbKrqcDIVVVyZnUOFjSPfnq:w4md1r7ZAY1JBsm/q
MD5:	584305A3E4BFA867808371099AE6AE55
SHA1:	53E32D08C66E4EB18FAAC524EC62C7A88AB3B4F7
SHA-256:	C95C72F9F8B96FDE8E4D8638B10B9828D80FC160B9ABC2175D9BC01497747E00
SHA-512:	B9C4978392874CB5751C323E8F7EC7AD1CDCCA41D154E9FB4E4B973E52C80B1579145BF28C3F9E5A858A8411384352FB4CE67F218C35DF80020166E8A1C9C6B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....8E89BA0D40F7B80B4AFB73B3795A21042FB97D7DBB9EE06473E84DF0C55601CA.....'.WX....O!....w..M.....%.....4.....H.....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....Qb.`.....t...`....I`....Da....j.....Q.@.....module....Q.@..!.....exports..Qc..z.....document.(S.....5.a.....a.....a.....A....a.....a.....Pc.....exportsa..../...l.....@.-....TP.A.....F...https://www.qualtrics.com/assets/dist/js/libraries/jquery-3.4.0.min.js..a.....D`....D`@...D`.....]...`....&...&..!.&....&.(S....%..``K.....L`.....Rcd.....*.....QbbG4|....C.....Qb.`.....E.....Qb..)....r.....Qb..J.....s.....R.....S...Qbf.'Q....n.....Qb..C.....o....Qb..vf....v.....M...Qbb.._....l.....Qb.....y.....Qbv.....m.....Qb^u'.....x.....Qb...,....c.....O...Qbn.1.....w.....Qb.....k.....Qb..x.....p....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\042c86523873eb37_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.540278934820386
Encrypted:	false
SSDEEP:	6:maYGLKfDhHyiTL1UM3ugdsuforryfablMrK6t:GfD5zH1UCXPord4
MD5:	B50768A2E3F053396334E8CE08A8B708
SHA1:	80BB21F90864BC36E51FD47BE82CD051A4824CE7
SHA-256:	148BCD629D2B9D88E79A1FDB7D45B316B739D5B2889DB67A5160FE3279A46413
SHA-512:	AB52B54D0DA75BA5B285549D0DFAA9702BA65D2245770946FEFEF0E06E7012634D04CA1B974AC2CC9F39AF9E5E9458CE0E5243571602F862E87C832FBBCE15D0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`.....K1...._keyhttps://www.qualtrics.com/assets/dist/js/modules/main-nav_v1.js?v=53 .https://qualtrics.com/W*..i&/.....8.....$.....j....WQs.T..`lU.s.A..Eo.....j".&.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\047ae0d77132df40_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	111776
Entropy (8bit):	5.691918666322761
Encrypted:	false
SSDEEP:	1536:RBn67BMcqfysejpa22psZkCUsaoITYzpdUlr67UHZH:CFMhqxWgpW5ZH
MD5:	161EF90083C0049E71635239BCD1EF00
SHA1:	DBC8EB15CF4A2F2E05E95AEE90DE4A7CDE5903A5
SHA-256:	0211ADABD084F6500A4AC4A93933BE752A5E1E089BD8F01F9BEB74DE332F1410
SHA-512:	FD5873760624FB494BEFD10F188A68CEA90270EBB1AB7E890C991D7F2D9301C0D444FC4CFBAE7E538E62505D1B7EDB1C391BFFC2CE208E35EFB1ADEADEAE699A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\047ae0d77132df40_0	
Preview:	0\r..m.....@.....!.....7BFE937E5CC1160DEEE6003D7ABC865582E76D5FAFCCC4507CB5CE0BF3B16A9D.....'.r.....O%...8..... .....D.....(S.0..`.....L`....(S....`.....1.L`....@Rc.....QbN>b....t.....QbZ.P.....e.....Qb..=G....n...b.....I`....Da. .....(S.h.`.....L`.....Q.@V%.....exports.....a.....3...a.....K`....Dt8.....&.%.*..&...(.....&.}...&.0..'....&.%.*..&.(...&...&.'..W....(.....,Rc.....0`....Da.I...I....a/....d... .....0.....@.-....LP.!.....?...https://www.qualtrics.com/assets/dist/js/modules/styles.js?v=51.a.....D`....D`2...D`.....y....`8...&...&....&.(S.,..`.....L`.....(S.H.`J.....L`.....q.. Q f..d.... is not a function....K`....Dl.....%.s.....&....&.]...&...4..&.]....%....,Rc.....l`.....Pd.....t.exports...al.....a/....c.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\049bc53fabe1795a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	255168
Entropy (8bit):	5.976944101422575
Encrypted:	false
SSDEEP:	3072:3tPvMwhtSbANHVOfFw7LTNg/N/q2jD/ZOOPxQwkTIdvJ+dl/N3oNAdum4wzTCHTc:3tPvcbCbEZS78iebbg
MD5:	976674382E0708AD633C79528612D7DF
SHA1:	703349A3F156EFD095A46F3EB8F79253CA2CFD02
SHA-256:	DFCA2F889AE49FCB522900D2523A91EEEE7923A622FD07D5349E2083737D80DD
SHA-512:	949452E9D462B5AD8793E08865935446E788AE0D1D35B9710B9E3B8A61B2C7087A499E6AB70020772AB7AE04BAA30FC2997BE5391380C7F3734797AC73DB68D7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....69FF934884BCEBD14FBDB94EBDF6062601E08457C345956DA5F3848C58119C65.....'..{....OK.....X..... .....<...`.....H.....(S.0..`. .....L`.....(S....`.....i.L`0....@Rc.....Qb&%.....o.....QbZ.P.....e.....M.b.....I`....Da.....(S.h.`.....L`.....Q.@V%.....exports.....a.....7...a.....K`....Dt8..... ..&.%.*..&...(.....&.}...&.0...'....&.%.*..&.(...&...&.'..W....(.....,Rc.....`....Da.....3....d.....0.....@.-....LP.!.....@...https://www.qualtrics.com/assets/dist/js/modules/marketo.js?v=54a.....D`....D`4...D`.....y....`8...&...&....&.(S.,..`.....L`.....(S.H.`J.....L`.....q.. Qf..d.... is not a function...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\051bd93171dc2e8e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.454185769530797
Encrypted:	false
SSDEEP:	3:m+loCQs8RzY/LJN9qLJB27l/M842+ll/lHCD//S3wQb+nLoWhww/MmlKlpK5kt:myQ9YD8FBM/wgGAQb+nnhwWnlUK6t
MD5:	CF9C8941F56218107E14A171FC07A049
SHA1:	01C32209BEBFF81D920A26CC79F6ACFB51BEB209
SHA-256:	26691A269A588CA47CA5FE6F1BF7AC385A8BE776CE2F032C1A28704FD61EE6F7
SHA-512:	53BAA5B5A97F594D90C9D05DC19536EAAEAB597A7D90274BEA15D4FD30924A03536C76F79F59EF1BE3FC04F7A2DA138E33CCE5AFD4667EBE4AEF83EC764CC 247
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H....._keyhttps://solve-widget.forethought.ai/embed.js .https://qualtrics.com/.]2.i&/.....#..=U....GrU$..k..u.....R.&.M.A..Eo.....9.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\07ec88d8e9dac3cb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	40116
Entropy (8bit):	5.757589132499802
Encrypted:	false
SSDEEP:	768:evnE97pdQ4sTNkA0ALWTEcMY5KF5xLueOr2ngM1+I:6EBpdQ4WkkVe5Y5VLOr2P+I
MD5:	B0C2C9A94113BEEE5A8D36FC2D4082FD
SHA1:	E7FE055C4EF23FEA1DF45127E2AD0A86374E268E
SHA-256:	BECFA9C2DAB81AC01BB989FA1AA29AFAB3D2FDCE1DC4B3AB67F11AEEEAEA8FED
SHA-512:	7A37C391E008DB7B4F7C3BE31B1D4BABB6F316043B002B2D34EDB95F98D23289F03C87E09808E07853A2A4314146808EB5ABDD0204EF27A4FE502BAE9578D18
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d...gM...._keyhttps://cdn.krxd.net/ctjs/controltag.js.0631b7d64dbbd3656a8b7368ad227a04 .https://qualtrics.com/=;..i&/.....F.....n..`.....0D...w.+R.....9..... ....A..Eo.....dg.....A..Eo.....'.....O.....}}M.....4.....T.....(S.....`N.....L`.....(S.`.`z.... L`.....@Rc.....Qb.`.....t.... Qf..`M....__webpack_require__...Qbv.....e...b$.....I`....Da....&....(S...`.....L`.....Q.@..!.....exports..$..a.....a'...a.....Qbz.....id..C..Qc.....loaded..H..q(..Qb..{.....call... (..K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&...&.'..W.....-...(.....,Rc.....a#`....Da....T.....!"....e..... P.....@....@.- ....TP.A.....H...https://cdn.krxd.net/ctjs/controltag.js.0631b7d64dbbd3656a8b7368ad227a04a.....D`....D`R...D`.....`....&...&....&..!$&...(S.0..`.....L`...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0a83620de7a6fb57_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0a83620de7a6fb57_0	
File Type:	data
Category:	dropped
Size (bytes):	279
Entropy (8bit):	5.892831265846954
Encrypted:	false
SSDEEP:	6:mdX6EYWVBMGDLwGNeB/6mpeQ6dTrgyttL4WK6t:kzVBMGXcB/6mMQIv3
MD5:	51F72949E25BCFA136D30EFB10351771
SHA1:	A335876716FCE6E140ED0219702D10E53F213172
SHA-256:	366255720798B8268A5BB327ECD932CD104098DFBC265917DF6C3B4D47852259
SHA-512:	4C5F06136173346B1E19AFC319FD1A6EA58AEE4967249AB491A416746A231E9A71AEB516D34A4F16FFB766489D9DB167FAA3E8808CE6E0D1188312DD8630A25F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T...._keyhttps://siteintercept.qualtrics.com/dxjsmodule/12.f5ece31f48e9c7ec490e.chunk.js?Q_CLIENTVERSION=1.56.0&Q_CLIENTTYPE=web .https://qualtrics.com/Q.k.i&/.....C.i@.`q.....},.wdC"..h..."..A..Eo.....^F.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0aee9548ba24a462_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	223
Entropy (8bit):	5.47606240216891
Encrypted:	false
SSDEEP:	3:m+l7Ds/l08RzYrSLKfcIhHWPTaQUxxj/McSJl/lHCfnlXgWaboMsI78BkoMmB/lB:mys/PYGLKfDhHyoxjfqgPdYoBbK6t
MD5:	7186E6BD0A60A2E7C15EDBF408BEAD99
SHA1:	EE13DF3EA5D7FAA82236E36606E342DD9CDB1EEF
SHA-256:	15053DA3B23B86624B3D28E0E6E9E62C9395678A3E502FE896EAC0B1EB15FEE2
SHA-512:	35EE79DE5A092C9A371D8F20D760498853CAE3C29511136675C42CDCBCC2A28720A216385C28C74C8EC73B7166C81FD24BE8BE67C6C7A7DBD602DCAEA0D5D75
Malicious:	false
Reputation:	low
Preview:	0\r..m.....[...Pf3....._keyhttps://www.qualtrics.com/assets/dist/js/modules/styles.js?v=32 .https://qualtrics.com/u...i&/.....@.....}).0`...*...-.....A..Eo.....W?.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0ba4a747ccde2352_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.620636532713655
Encrypted:	false
SSDEEP:	6:mwYZDtLUA0k6vaLKvNjnGvtgK8KzcH4CDK6t:qLUAl6vaL0BKzcF
MD5:	6229716AB3380386D46EC7D04F5D72F8
SHA1:	E21CB98591BB4B98AB49A3ACE6D2839221AEB25F
SHA-256:	0DF5A55D5E81C8C2F7688F532E66B15BFAC74F773C28806E83FA5B9D32EAA6A5
SHA-512:	326A769D33165E43C706BCB9F9486EF9A03084532A76ADBB180B0E286DAADD07D563904EC0BBFFD99E3D130F6E9B06264BC12C57AF2BC89EA4FD8F6E5C6C1E13
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W...I....._keyhttps://js.driftt.com/include/1627086600000/z7vv59u6ahv3.js .https://qualtrics.com/x1j.i&/.....V.....We.)I#...(.<%...^.`.Y.I.)./{..H.A..Eo.....!.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0d46afaf093754da_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	233
Entropy (8bit):	5.5361724080841626
Encrypted:	false
SSDEEP:	6:mmrNYD8/J5v++vOG+lHgiRnqqpko5OhK6t:y8/J5VmG+ZRLkX
MD5:	F618C055F08BE399ED7D3F53D7267B65
SHA1:	2F0C4E2675F32127E7B55377E52AC04C11D5FA55
SHA-256:	37119F89A4D4017A866B9F26DB5C5B2C5D344B4B5E27D56353ACADBA007E0206
SHA-512:	5C29FCFE15AAA410F218298A8A96F4C454E2E99FDBD23E2592329154F227B62A4346D88E88E9CA2B7FD6D005CBCAC99BECF9C941FA1BB3441BB2800641B0525

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0d46afaf093754da_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e...-....._keyhttps://solve-widget.forethought.ai/npm.react-is.b9533b2b3a0ac0182179.js .https://forethought.ai/dNI.i&/.....,...,.0.....?...6.1.....m6.A..Eo.....>.&.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0d501bcb1918354a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	789
Entropy (8bit):	5.830387262296428
Encrypted:	false
SSDEEP:	24:sSUXFKWNh/ltnuyAyyJSu1FJzrsLxR07WiANYc:qFK+DnursQJkL0c
MD5:	ECFBFE73F7261614B1C3980C80B2C153
SHA1:	980A33881C25B2005E72239C5C84BF2D1D41320A
SHA-256:	534C4989598912D09B35D760903DD48F14619AE4EB5C70D83FBDD80CFD2AD010
SHA-512:	EBA10A979E4044892E3622FD0767D053F8B8E193F6EC796678B05257C6AE1B222FAD7A1FF068EA1E35832027A6B64167BA0A86B83B62F457F645F0CC67C3458A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....).!...._keyhttps://www.googleadservices.com/pagead/conversion/1026978278/?random=1627086290815&cv=9&fst=1627086290815&num=1&value=0&label=wX24CLq7jPwBEObj2ekD&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=2&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2wg7l1&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fwww.qualtrics.com%2Fuk%2F%3Frid%3Dip%26prevsite%3Den%26newsite%3Duk%26geo%3DIT%26geomatch%3Duk&ref=https%3A%2F%2Fwww.qualtrics.com%2F&tiba=Qualtrics%20XM%20%2F%2F%20The%20Leading%20Experience%20Management%20Software&auid=1029000693.1627086256&hn=www.googleadservices.com&bttype=purchase&async=1&rfmt=3&fmt=4 .https://qualtrics.com/...i&/.....#.....e.....J...t#.I....w... .:.CT.A..Eo.....yo.~.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\104909bf8604211e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	105536
Entropy (8bit):	5.7191102574270145
Encrypted:	false
SSDEEP:	1536:eWX7bsTT+ULh1/c2KFJEhBkL7wkChRdEubEe3/mXS:DguUdCnBgOug5S
MD5:	5FE9F703DA0C861A67D5D4CF2B4FF4E1
SHA1:	125B2F2E5E9DE7B5C1631D17BBFBF4460B15DE8F
SHA-256:	8EBA85D05FD7E8241CC8A364D65C6152B524727A0E8D015C9FF6A296A3597748
SHA-512:	FE64B684FAC871DEF3B1ADFCEF5267F5C47F25F63CD4F1843CB7507425E879650B764DB825680018AC59E1A2EFED49AB6DB0569046B23B216C3C1CFA167F390
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....sl.....3651D8C15701CF196D3D5861A5348E4D6118EC4BCC9D21E377F3FBB9EEBAF199.....'.....O$.....r.....H.....(S.0..`.....L`.....(S.-..`.....5.L`.....@Rc.....Qb.~.....t.....Qb*.....e.....Qb...,...n...b.....I`....Da.....(S.h.`.....L`.....Q.@.A.j....exports.....a.....3...a.....K`....Dt8.....&.%.*..&...(.....&.}...&.0...'....&.%.*..&.(...&...&.'..W....(.....,Rc.....11`....Da.k..~l..../....d.....0.....@.-....PP.1.....D...https://www.qualtrics.com/assets/dist/js/modules/main-nav_v1.js?v=54a.....D`....D`*...D`.....U....`&...&...&....&.(S.,..`.....L`.....(S.H.`J.....L`.....q.. Qfj..... is not a function....K`....Dl.....%.s.....&....&.]...&...4..&.]....%....,Rc.....I`.....Pd.....t.exports...al...../....c.....<...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1161c276fb29f36e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1631
Entropy (8bit):	5.771090413638735
Encrypted:	false
SSDEEP:	24:5IDXDIDDRDIDl8DDIDRkDIDrDID0DIDZurvS1:5IDXDIDlDIDyDDIDODIDrDID0DIDZuS
MD5:	31A94182E92F301311DD2C1BC41B56DB
SHA1:	49B0482199A966B70D0E183921A133F05972F3E6
SHA-256:	E0CFE8D0954B781BB81F12AD7848A4E2691D3A0F3D9ABA82D0D4076A02B7CF22
SHA-512:	A283AE5B17BFCE99180CBC6FED8B577A5438DF8A24B02DAE47F76EED985B626FE6B80F64395E480D129490E7B38CB64A914E02C3ECA3CB6FFDF831820C3BFFE6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1161c276fb29f36e_0	
Preview:	0\r..m.....e...]....._keyhttps://www.googletagmanager.com/gtag/js?id=G-Z0RM4JK167&l=dataLayer&cx=c .https://qualtrics.com/.3..i&/.....#..._.....@..38.....&...A..Eo.....o.....A..Eo.....0\r..m.....e...]....._keyhttps://www.googletagmanager.com/gtag/js?id=G-Z0RM4JK167&l=dataLayer&cx=c .https://qualtrics.com/?...i&/.....#..._.....@..38.....&....A..Eo.....A..Eo.....0\r..m.....e...]....._keyhttps://www.googletagmanager.com/gtag/js?id=G-Z0RM4JK167&l=dataLayer&cx=c .https://qualtrics.com/..1.i&/.....(.....#..._.....@..38.....&....A..Eo.....O.I.....A..Eo.....0\r..m.....e...]....._keyhttps://www.googletagmanager.com/gtag/js?id=G-Z0RM4JK167&l=dataLayer&cx=c .https://qualtrics.com/.j..i&/.....;.....#..._.....@..38.....&....A..Eo...../".....A..Eo.....0\r..m.....e...]....._keyhttps://www.googletagmanager.com/gtag/js

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\11e3b80c57293106_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	234
Entropy (8bit):	5.554907510700875
Encrypted:	false
SSDEEP:	6:mEX6EYD8/jH1Ln1ldFgWDlSn+4n5l/bK6t:ts8/5L1lpQ+er
MD5:	2A2B678E1ED57A5B32A3FF7B6BA3BA62
SHA1:	D00C673C7B21D6B1E2D68C064442E5B6F098528B
SHA-256:	9386D2D4634C37990F084EACED606B26E6449DB2086AF7E124C9435EB6AF06E2
SHA-512:	933D4E1B0DC2CD084C44DF5D82FD1C8471036C0D12C1AA8C85D2D11132F8DE7FAAAFC6C94EF7DBAF42D74CCAACCCD3C1C6D5AEA5B9F368D108B5F7547D973CF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f...j.}....._keyhttps://solve-widget.forethought.ai/npm.react-dom.17ddddd2ea32a3d625dc.js .https://forethought.ai/..I.i&/.....^.9.QD"S..._ebR'.y..V.\..2.d...m.A..Eo.....(..I.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1277e856134e2dec_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.412983969781285
Encrypted:	false
SSDEEP:	6:mUV9YZDtVcmWyAq3VFJDiKFgS4QQ6zA/9K6t:rV6Vx0GbViKKE0
MD5:	EDB45F8770C368AF99D791EEEF850CE6
SHA1:	8A2142245451954FE04D4FD661F0B9ED1106297A
SHA-256:	611D88813E194716B694A253DA1B03A7C37E97FDE74DC8D9376B0211EE54B971
SHA-512:	E4107E80C722C0EEA77ECDF291AD2C78D813BB8BDA4CD9BC50ACF8F92622383A1F8AA39600EB9905B070A27B1C745A60CE2CBB4E8A67DD36D6D9A09AA312ED66
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....._keyhttps://js.driftt.com/core/assets/js/25.788dec0b.chunk.js .https://driftt.com/l...i&/.....i.....\a....5..@.A..X../...n...8..?..A..Eo.....E/c.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\151ce477c6211907_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.67420988828452
Encrypted:	false
SSDEEP:	3:m+lW6S78RzY/LJN9qLT+dieNR7nLpll/lHC0tzZGcHnXwfeg6g4mw95///pK5kt:ma/YD8/i7N1tg0JDHnXwRLr2hK6t
MD5:	EAA39755706B3488A5F9DCC85DFAFAC5
SHA1:	D69CFFD05A5B6F77F098B1AAFA19B2889BAD5E6C
SHA-256:	27E541D9390C503CE18C8F17F52E7026E9A8D35305022FA14DED7076CCF61F62
SHA-512:	79D2019B4DE614383132ECD464FFB41460C3163E9D8CEB3F7AD520990A43B8424CD6DA5E0D44D6C8AA014B3D4D9D21F9E19D3980A21FF4B17BCF9A044EBC2DBE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b...._....._keyhttps://solve-widget.forethought.ai/npm.react.5928087d96bed9c46ed1.js .https://forethought.ai/(HI.i&/.....-..O.c..4.{Mk.....*.#U..R.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\171d665dec25f7fc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\171d665dec25f7fc_0	
Size (bytes):	4693
Entropy (8bit):	5.615686292257367
Encrypted:	false
SSDEEP:	96:BWZ403qKsLL0+oXrXlRw0iKG+kttt30oztmj:B+4xLDoXrXLwnKG+ktz/Q
MD5:	8ACC96F8726425DA52047BB25EF31951
SHA1:	42F797503B8E6DB7793A70E08CC9220D051468FC
SHA-256:	5276B72F67D6DA34CDF207834BF8E579428302DEB7427F73F0B7DE781F5E0750
SHA-512:	7051BC5BDE78C5501D14F2C02D0BCC29302A649FF4BC1C4CC33D4345C02A982B9C58E662A6C4EC07F1DA5A33E8212F7A93944CF35A6B46A99F321DF1C90208E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m..._....._keyhttps://cdn.jsdelivr.net/npm/intersection-observer@0.7.0/intersection-observer.js .https://qualtrics.com/._..i&/.....Y..1...s,....4....jX.:}'"Y....A..Eo.....P.....A..Eo.....'..W....O.....A.....p.....(S.0..`.....L`.....(S.)..`.....L`z.....Rc@.....Qc.....document..Qc.t.....registry.(Qh.....IntersectionObserverEntry.....Qb.).0....now...Qc...I....throttle..Qc..#.....addEvent..Qd.....removeEvent..$Qg>P\|.....computeRectIntersection..$Qg...=....getBoundingClientRect.....Qd.'mQ....getEmptyRect..Qd.&.....containsDeep..Qe.x.....getParentNode...k.....I`....Da....P....(S.....IaT.....@.-....`P.q....Q...https://cdn.jsdelivr.net/npm/intersection-observer@0.7.0/intersection-observer.js...a.....D`....D`(...D`.....`P...&...&....&.(S.....5.a.....a.....a.....e...Pb.....geta.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1723e5332b47c8a4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1494
Entropy (8bit):	5.869672886124122
Encrypted:	false
SSDEEP:	24:0Tq+65gT+Tqe0p+TqkHkn+Tq2ek+Tqc7X+TqAL:0TqbyT+Tqe0p+TqVn+Tqxk+TqQX+TqAL
MD5:	83D082BDF72134A943B769F590983100
SHA1:	90998B9B052877FE118852766FE505A7FA21D5D5
SHA-256:	A5252FA60DEEB6B794878793F53616B13A63DE4D8F279A02B87191124D7F3AC9
SHA-512:	A500CFC7DE6A76F24817D87345E6492AF5E5DE3825DFEF1EC9DE821F9F7F1ACDA77A6DB4E92D48714897AF97D04CF90405B50291EA3BBD5DACB9C5F8D6F1AC5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....u.....(...._keyhttps://www.google-analytics.com/gtm/js?id=GTM-TBK3K53&cid=1619834339.1627086260&aip=true .https://qualtrics.com/....i&/.....Lx.K..Z.g.....E?`...."E.K.C..A..Eo.....,;.....A..Eo.....0\r..m.....u.....(...._keyhttps://www.google-analytics.com/gtm/js?id=GTM-TBK3K53&cid=1619834339.1627086260&aip=true .https://qualtrics.com/x...i&/.....Lx.K..Z.g.....E?`...."E.K.C..A..Eo.....!8.....A..Eo.....0\r..m.....u.....(...._keyhttps://www.google-analytics.com/gtm/js?id=GTM-TBK3K53&cid=1619834339.1627086260&aip=true .https://qualtrics.com/..3.i&/.....9.....Lx.K..Z.g.....E?`...."E.K.C..A..Eo.....,!.....A..Eo.....0\r..m.....u.....(...._keyhttps://www.google-analytics.com/gtm/js?id=GTM-TBK3K53&cid=1619834339.1627086260&aip=true .https://qualtrics.com/....i&/.....C%....Lx.K..Z.g.....E?`...."E.K.C..A..Eo...../-.....A..Eo.....0\r.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1780796995a5f2db_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.511163631714824
Encrypted:	false
SSDEEP:	6:m+LXYZDtVcmWyz9u0JDlugGfaefAMK6t:pMVxrVVm5
MD5:	6906620B546A86D8912A54D1B8BA536F
SHA1:	02CB2FC7227B022C931035CDBC76D15F21A22D16
SHA-256:	979887CEA9652E9185E8B108AF3A519353EB4CB80EE7D1235068612BF721A317
SHA-512:	AB8F6186A37BBB715C7A10D77FF438BA235B23B3A2F82DBC504936C11409C9137C57BA39FF88B780C28CC0F43DA733E341C176BD6DB35AF9923C57CBC3871A99
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...k....._keyhttps://js.driftt.com/core/assets/js/18.5dcdfb92.chunk.js .https://driftt.com/....i&/.....Th.....[.$p....z....I....U;....3tYO.A..Eo.....Q.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\17c37e61cbd438c2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	565
Entropy (8bit):	5.778799980983275
Encrypted:	false
SSDEEP:	12:WOE3aXFKmdNTd3ux2pHgyye3CMxtfdfyL0ECNjO6LjKqGd8:WOEKXFKmdNTd3uyAyyeSu1qLNCNjhLjr

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\17c37e61cbd438c2_0	
MD5:	0A37F8DAFB66E643E8FAAF35CA932668
SHA1:	D8A40F48EFD26A8CAB95C99EB8B162B77F667555
SHA-256:	42B4AFDBFC8A5E34A5570FC323D11EEF62E9DED1723AFD9D0472931BCDB4770F
SHA-512:	A7F124A1CC5DAD60D4A1755DC7E53F95CCBF67534CF394E748CE4244A5E765C020DAC41EA33C90FD02032C7CD252F42F15F4A8B4A709126F36C62FD6F15C3E7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z.b....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/1026978278/?random=1627086282782&cv=9&fst=1627086282782&num=1&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2wg7l1&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fwww.qualtrics.com%2Fsupport%2F&tiba=Qualtrics%20Support&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://qualtrics.com/.G6.i&/.....T.....Z.?W.yL.3.I..hT..Y4..F.S.....6.A..Eo.....X.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\197eb3c4b5d2ded9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	564
Entropy (8bit):	5.81599694067912
Encrypted:	false
SSDEEP:	12:qE3jmfyITJux2pHgyye3CMxtfdfyL0ECk2qY0BO7Ap:qEzm6ITJuyAyyeSu1qLNCkVq0p
MD5:	4C3DE1D9E24755BBB4CD82A42C17AF12
SHA1:	4F4D6876AD3E960244F241027A1A176F93476416
SHA-256:	CC934D195A4894E71F32DBC531496F779EE9D4956AADF61A74F909EF6500C9A6
SHA-512:	9ECD61BE61FCF1BAC208409DCC23AAEB08CFB549C4942EC787128FD53D2CBE12FB62E4997A24766B87DA28E3A5311DE2F3569CF53E36E4E6CE270FB1F3BF7ACB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....KK.H...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/875348540/?random=1627086282728&cv=9&fst=1627086282728&num=1&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2wg7l1&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fwww.qualtrics.com%2Fsupport%2F&tiba=Qualtrics%20Support&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://qualtrics.com/.l5.i&/.....e^.7.^.M!..3\g..b..$.Z.j.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1a4cf728f54a63c6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12590
Entropy (8bit):	5.661926973546898
Encrypted:	false
SSDEEP:	384:HkSeaXk+XALAifDKmc72emv3BLQEarWUB/AOIUmJLuXds8YElx:Hk/2k4AmdYElx
MD5:	3E848B7B17F8BF683DE7BE893E912862
SHA1:	B03851C10F60602FFAE138A038713BA2BE503C44
SHA-256:	82BDF1719DCE19F430085989A977B8E6477B03F57996E89E126819B4B4BE1AF4
SHA-512:	52FA769D388C495270208A8D9ED1EC294FA3F62C895B0C6710AD4B7073B5114A32FD5549008C4BCD713415279A8D60C36274BB000E529C4640649F716DBB3CD2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....^...6....._keyhttps://www.qualtrics.com/assets/dist/js/libraries/vimeo-player.js .https://qualtrics.com/.R..i&/.....Oj....5...K.9... ...f.v....A..Eo.....-2@)..A..Eo.....'..?....O...../...hA.....(S.<..`4.....L`.....(S...`.....$L`.....Q.@V%.....exports...Q.@RU.!....module....Q.@.<>"....define.....Qb>.g.....amd...Qbr.....self..Q.@f*.....Vimeo.....Qc.<.....Player....K`....D}.....s.....s.....&.\..&.-...%..G...s.....&.(.....&.]....*%.....&.(...'....~-...(...&.\..&.-...%.....(Rc.....l`....Da....6.... ..f.....`...p...@... .....@.-....PP.1.....B...https://www.qualtrics.com/assets/dist/js/libraries/vimeo-player.js..a.....D`....D`:...D`.....-....`....&...&....&.(S....`.....L`H.....Rc\.....&.....Qb.U.(....r.....S...Qb.....s.....Qb&%.....o.....M...QbB.@.....l.....Qb.c.....f.....Qb...Y....c.....Qb.....d.....Qb:.Z.....h.....Qbr

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1d230ff31e2b1a8c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1494
Entropy (8bit):	5.76791979423724
Encrypted:	false
SSDEEP:	24:zwo+nZtktxVwo+8tITVwo+4ytcVwo+ltQTVwo+EaStdVwo+Fth:zwo+nZtkDVwo+8mTVwo+4y2Vwo+lOVwr
MD5:	90DC8997D3786CB757280D75C6327555
SHA1:	382EAD1A2E2E156252BCCA5B2178FA1C5DD7A933
SHA-256:	D17E62592719F8EC3D19EFF4F2997C68E5A621A1FBCF3360FA82089818340DE4
SHA-512:	9AD524BA559216BF419E878F42FC9B6C1126DD68D6A2A99F916F19D48DAD113EFF284422F4A981E005149907A05A05D76976195CF7997E143E94A6A257B12957
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1d230ff31e2b1a8c_0	
Preview:	0\r..m.....u...kVs....._keyhttps://cdn.segment.com/analytics.js/v1/8OWg9yQBTSrD1lfR6cCeGsSpAhB3t0PA/analytics.min.js .https://qualtrics.com/....i&/.....M..... ..w.....C!.Q...L.=?....O..9.A..Eo.....d.....A..Eo.....0\r..m.....u...kVs....._keyhttps://cdn.segment.com/analytics.js/v1/8OWg9yQBTSrD1lfR6cCeGsSpAhB 3t0PA/analytics.min.js .https://qualtrics.com/+...i&/.....w.....C!.Q...L.=?....O..9.A..Eo.....3.t.....A..Eo.....0\r..m.....u...kVs....._keyhttps://cdn.segment.com/analytics.js/v1/8OWg9yQBTSrD1lfR6cCeGsSpAhB3t0PA/analytics.min.js .https://qualtrics.com/..C.i&/.....w.....C!.Q...L.=?....O..9.A..Eo.....$.....A..Eo... .....0\r..m.....u...kVs....._keyhttps://cdn.segment.com/analytics.js/v1/8OWg9yQBTSrD1lfR6cCeGsSpAhB3t0PA/analytics.min.js .https://qualtrics.com/.}..i&/.....'... .....w.....C!.Q...L.=?....O..9.A..Eo.....t.....A..Eo.....0\r.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1dc84d34104e76b8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	49892
Entropy (8bit):	6.080032103106183
Encrypted:	false
SSDEEP:	768:L4aBg5uzSHDutmk62hDaUr9pe0AZ6SnftcjfTudR94enE:8EcHqmqheyG0AICtcjG9pnE
MD5:	69D339CBDFF40EB19D50DAFB4A5D7F63
SHA1:	5707D812ECD54AF4E8BA340B824891D301EF65B0
SHA-256:	FE5A343E171E5C0DDD355883E8BFA09D3352C9CD61C88E9BC534B5443E1FBDB4
SHA-512:	667D567422A945AE26E9B130E10ADF55C3A6EE4A2863033595B759F92CE1C2D04B703182CAC54CD650DC2FE20CD460602D1E11BC7E299CEA5141D20B7E6739E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T....._keyhttps://consent.trustarc.com/asset/notice.js/v/v1.7-8690 .https://qualtrics.com/8...i&/...../..p*v..O.FS..OfEI....~.j.Pe..A..Eo.....=..... ...A..Eo.....'." ....O....0....%o.....,.....d.....(S.\..`t....L`.....L`.....(S...-..`. .....%.L`.....LRc".....R..... d.....Qd...3...._truste_eu..`....Da&....?...(S....`^.....L`T....4Rc.....Qb:.Z.....h...`.....`....Da@…2.....Q.@.:.n....truste....Qb*.OE....eu....Qc>j.....bindMap...Q b..].....feat..Qd.6.....crossDomain.. Qf.....isConsentRetrieved...u...Qb.H/.....ccpa..QdZ..4....initialize....QbB.....dnt...Qb..C\....gcm...Qbr.....gpc..(S.....QbB.@.....l...a....7. ....!&... .@.-....DP.....8...https://consent.trustarc.com/asset/notice.js/v/v1.7-8690a.....D`....D`R...D`.....`h...&...&....&..!.&..A%&.(S....`.....,L`.....Y...Qc.P^-.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1f48e9599133dde1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	309
Entropy (8bit):	5.581276986517725
Encrypted:	false
SSDEEP:	6:mLGYZDtVcmWyX0L+yC6SJDAHgN3t/A+DjGvAVK6tcfHgQlA+DjGvA:IVxA6yzSVAo31DDjHWfbDDj
MD5:	AF576714CC9AD16EB67ADC4FD174308B
SHA1:	0384297FA49988593CC49850914BE522D74D04BD
SHA-256:	B27527980DA57710A0A48CD81C1ABDF5047EC25B6D09B5CB45D5CC27CD705504
SHA-512:	A6F692B18302D43C5911655A92EB24CA3FD61C362CA58C55A5CB2F99F0B02B168FB0C9A5088ED7A585AE4BF2F1F3B3F97FBF198F76AD0EBB26B9D9989ED23CB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]...j..?...._keyhttps://js.driftt.com/core/assets/js/main~50ba91a7.4529f001.chunk.js .https://driftt.com/N...i&/.....Y.....&p.av...5...5.....Q..A..Eo..... .....A..Eo.....N...i&/.....Y.....&p.av...5...5.....Q..A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1f4f1ba04892ebd0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	298
Entropy (8bit):	5.457942873634544
Encrypted:	false
SSDEEP:	6:mLlllgEYZDtVcmWybuOSJDyVXygWXZi8rJ0ZK6tWigCXZi8rx:BVxvuOSVy2i8axi89
MD5:	5AA68F4DAA56AB51364E9F8C9B3D4F80
SHA1:	F1824C3829E0F0B0ECE7543E9BF7F0B70D3E903A
SHA-256:	D67A9C3951BAF713089068DF522E58C6236C9EB8640DB84DC27CE40FD75999C3
SHA-512:	EBD1F10A36F2342923DE2CC347CF7A08AD90FACA06F98535B3422D316DA1F30EA7054D427A7F669E1C71072E368E68720156148111329 3A7E6C36B5154103786
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...d....._keyhttps://js.driftt.com/core/assets/js/32.a09dc9c3.chunk.js .https://driftt.com/...i&/.....dX.....b..{.9...`..QuR7..dIp;/..v..S....A..Eo.....@..=..... A..Eo.....i&/.....pX.....b..{.9...`..QuR7..dIp;/..v..S....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\207689dcb9dc70b0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\207689dcb9dc70b0_0	
Category:	dropped
Size (bytes):	213
Entropy (8bit):	5.407290798654462
Encrypted:	false
SSDEEP:	6:mRBgEYZDtVcmWyH9FOSJD/gkW6ELt45zrt/ZK6t:wSVxh0SVjW6EO5F
MD5:	37E2780E8845B8EFA9811D23F8ABB3F8
SHA1:	AC973DA97C386291AAE6C48A7CE7403D5E2994BF
SHA-256:	E2C31EBA314FD62FAC3FB7E87662D4E7E972CC8C99BF0BDDB7A34EFC05A04A59
SHA-512:	3152BE306B5ECB3FDD86E0C61EA612A3CC8D7057DACC1D6A47517EC1EF2F5DBA0CCAE18D0D8DB0A40DA653E78334518266CB308EA919F83896F0FCE537C2F71
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q.....*....._keyhttps://js.driftt.com/core/assets/js/0.4b8a868c.chunk.js .https://driftt.com/>d..i&/.....h.....jU,.C^@E6..".e.:F7.c$.....u.y.Z.A..Eo.....%.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\23c60a2ffb1f7a19_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	298
Entropy (8bit):	5.379650706712271
Encrypted:	false
SSDEEP:	6:mCtYZDtVcmWyIQNJDwQr+1tgglTlzE4AjNnK6tYr1tgglTlzE4AjN:HqVxc0Vwh/lpzEpih/lpzE
MD5:	A5444B1A5985BE882EDB80C54840817A
SHA1:	C5BC51CED1714435321A97579988DAA4A4A5C5B2
SHA-256:	A9E122959438AA3512AF92386ACD61BB869E4E732ACC18C61B7CBC51FF40725F
SHA-512:	7208C8CB5C77BAA9576E94279823956E4E25EFCAFAAF3CC186A93D53B1FD96985039D22AC40F7BDD63D33D22EA468EA45FFD8FB60B81F420D21AE62F9C586E3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....._keyhttps://js.driftt.com/core/assets/js/26.99c92d86.chunk.js .https://driftt.com/u...i&/.....[.....3.8.@i.1.u.o...Ai6.aq)..-Zv.;..A..Eo.....~.....A..Eo.....u...i&/.....[.....3.8.@i.1.u.o...Ai6.aq)..-Zv.;..A..Eo.....~.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\24ace19ef85dd2c1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2579
Entropy (8bit):	5.708783225691595
Encrypted:	false
SSDEEP:	48:rb2DvoynJ/l/jpb28rGq20tFPiwD8XcFdzAtsF+bDTkXvL:ryDvlxpy8rGqTF7DdEuXvL
MD5:	7D3F2764752BEABA5126982DE7836697
SHA1:	1D816C77B80146ED3C03A9CF4B9D565053E8FC18
SHA-256:	5892A0E1EF08577F928B510A1DF72F5D54AAF6633410820240F36790005193C7
SHA-512:	5420455CF7BB4C6667CE8D964F4481CEFA62B8F6BC71C0F2E80CB1FC4FFBFF0A9D5F5289E6A65BAFCDA050BAFF5BB415E07093C9551EE697E41BB7A112FFD48B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I.At...._keyhttps://siteintercept.qualtrics.com/dxjsmodule/16.f3fa4a6e94a4c8016f98.chunk.js?Q_CLIENTVERSION=1.56.0&Q_CLIENTTYPE=web .https://qualtrics.com/.$G.i&/.....6Z]KBV<.....A.E&..U*>w....._'.A..Eo.....P.....A..Eo.....$G.i&/.....'.....O....x.....(S....`R....0L`.....Q.@v.....window...4Q..f.L.%...WAFQualtricsWebpackJsonP-cloud-1.56.0.....Qb.[M.....push.....`.....L`.....`.....Ma.... ...`.....b.....j...C`.....(S...`.....8L`.....PRc$.....S..Qb&%.....o.....Qb.....d.....Qb.U.(....r.....M.d.....Qb.....53..`.....Pc.....push.53.a.....(S.(.`.....L`.....(S....Ia.....I.....@.-.....P.....w...https://siteintercept.qualtrics.com/dxjsmodule/16.f3fa4a6e94a4c8016f98.chunk.js?Q_CLIENTVERSION=1.56.0&Q_CLIENTTYPE=web.a.....D`....D`....D`.....0...`....&...&..!.&..q.&....&.(S.(..`....]..K`....Dd.....,Rc.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\24e081ff6bb503eb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	298
Entropy (8bit):	5.488883524121045
Encrypted:	false
SSDEEP:	6:maIEYZDtVcmWybnoJDyigfMpJqsPyABnK6tHgTMpJqsPyANl:wVxXoVrpJXPyQpVpJXPyW
MD5:	7EF303477DAC76CC352F3E4C8429DA1D
SHA1:	55F39CD838E2E07D7F9C5C5FA5BA56A7D049C2F9

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\24e081ff6bb503eb_0	
SHA-256:	66119F809CBC05CDA6D1263FA462C26C25F2C9661B57BFE708881F5FA59B09F9
SHA-512:	3D5BFC8B8BB576A045D7199013380D78949CEFF247A38120BFE3769A8C9EE00A955B2171DE503079E9E6A17E0338FB5358D840C0113B02A74444391B4ACC176A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....._keyhttps://js.driftt.com/core/assets/js/12.744a3ffe.chunk.js .https://driftt.com/.`..i&/.....X.....;c.K.2..'.>..p..)....r"a...M..A..Eo.....|.....A..Eo..... .....`..i&/.....X.....;c.K.2..'.>..p..)....r"a...M..A..Eo.....w.6.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\273a104cf1af3806_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	10688
Entropy (8bit):	6.072354294777068
Encrypted:	false
SSDEEP:	192:NJ2nYynVvHOh2UfLDoCTc8XMDiZJyLJdHpGdj7trToFbrpPu:NJ2npVvuhRf/rTuiXyLHpGdj7VmBPu
MD5:	5C44747288A86CA139C983085674B183
SHA1:	E4C2BC3D8419D7D56B60735FCB4C7C0287D2AC6C
SHA-256:	AD14079965DBCB9E4A34C30B48784E312F862E9281E4BF48B9AF70C3C6CFAB57
SHA-512:	3FA2B658197AD5B6DA4F1AD8922443062F4B65FDDDE347F346AF5D9F2EB4326F217743B4810AFA66C8475DC29747346FB2129EDDE03FB5CA222C26B27FD9360
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L....._keyhttps://static.hotjar.com/c/hotjar-84529.js?sv=7 .https://qualtrics.com/....i&/.....@$.Y.S..# .*8.oB.6~L....T...A..Eo.....`.....A..Eo..... .....0\r..m.....L....._keyhttps://static.hotjar.com/c/hotjar-84529.js?sv=7 .https://qualtrics.com/..i&/.....@$.Y.S..# .*8.oB.6~L....T...A..Eo.....`.k{.....A..Eo..... .....0\r..m.....L....._keyhttps://static.hotjar.com/c/hotjar-84529.js?sv=7 .https://qualtrics.com/.....'.Y.....O....x%.....t...$.....(S.d..`..... L`.....Qc..;... .window....Q.`.....hjSiteSettings.....aZ.....Qc2xc.....site_id.`b.....QbZydU....r.....Xa .^.=..?..Qd.p.....rec_value...`.....$Qg...1....state_change_listen_mode..QcN..... manual....Qc.}a6....record..G.(Qh.oA.....continuous_capture_enabled..G.(Qh.....recording_capture_keystrokesG..Qe."u....anonymize_digitsH..Qe.fO.....anonymize _emailsG..Qd.f2.....suppress_allH..Qe&'

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\29879f09295102cf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	383
Entropy (8bit):	5.862942231218658
Encrypted:	false
SSDEEP:	6:mkHYFBKbHYVzi1xCJgRR3zBf68RWmAbm+X3R6KYWU0MSjWUIXLFgBAY3J5+40K6t:5eKbtKgndfdOb7UBSqUMS53J5e
MD5:	B22390266EC5D114C9392AB3C25D9359
SHA1:	B7EA04CFF0F324F35AE6A51DD8805414CAD5BEA8
SHA-256:	B859FCA63F6055CC2B5041B59FCB796AC1D8D8ADE3D49A4EA653CB3FB3283B92
SHA-512:	6F9D6F424CA71DEFF4973DFB585E819DC07F5C923E64B5D71BBE4BD8E6A185336FCD4BE75ADEC3428A34E1E63111E20AED83DE4C353806924441EC23BC9999 A3
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://success.qualtrics.com/index.php/form/getForm?munchkinId=542-FMF-412&form=7836&url=https%3A%2F%2Fwww.qualtrics.com% 2Fplatform%2Fultimate-listening%2F&callback=jQuery112403565566282629513_1627086313479&_=1627086313480 .https://qualtrics.com/....i&/.....$t.....f..Q.D. ...L.;...r...J..w..%V...A..Eo.....#o.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\298f5c72f76110a9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	564
Entropy (8bit):	5.830327071220887
Encrypted:	false
SSDEEP:	12:GQgE3oTpmRcOTR1ux2pHgyye3CMxtfdfyL0ECbZctN:GEopmtTXuyAyyeSu1qLNCar
MD5:	4FB73B9E93F80D9519FA02F099293682
SHA1:	0D4CE7D1E1CF1C8CA3EC8EE5DEB753BFD99D8B46
SHA-256:	5FB1FF194482782A572BEE8FBAAE97E9BDC130CD5A569E8C75F3B74BD29900E0
SHA-512:	439E1FDB73AE82C2AC88271DE22427BD6519A95EFF49726D8B128E174F63AA654E0662DB742CBDC3BBFB6DEFF47FE406138B5A78F4D86E2260DB883E8FC12A 3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\298f5c72f76110a9_0	
Preview:	0\r..m.....<S....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/857073434/?random=1627086282744&cv=9&fst=1627086282744&num=1&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2wg7l1&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fwww.qualtrics.com%2Fsupport%2F&tiba=Qualtrics%20Support&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://qualtrics.com/..5.i&/.....K.....P...^.....M.D\....</.@.jl.4h.A..Eo.....u.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2b4f818ea5a7b69e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	640
Entropy (8bit):	5.772419370730281
Encrypted:	false
SSDEEP:	12:kE3jScFpcvux2pHgyye3CMxtKadfGRXUHQE5IHyq6uCCNMub:kEzScFpcvuyAyyeSuKCOeyx5CCNME
MD5:	BBEE2261FB251FE423E5AD7A8034A720
SHA1:	48BFE97E0519F45E4972E501B21F6B88DAA451E7
SHA-256:	7A99146E777B293562C67A938E41ADFEAEB65ED33A5720D9AF92A073D32534D8
SHA-512:	2D02941DDE8746DE99D0D0F42E86543B1B935B3A504BEF6619A8E944393FB50C91596F8230DEF15C2F3E469C8E72A40AB78DFDCF5B47543C6CB34290AF6FFC1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....8...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/875348540/?random=1627086276913&cv=9&fst=1627086276913&num=1&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2wg7l1&sendb=1&ig=1&frm=2&url=https%3A%2F%2Fwww.qualtrics.com%2Flogin-banners%2F%3Flang%3DEN&ref=https%3A%2F%2Flogin.qualtrics.com%2Flogin%3Flang%3Den&tiba=Qualtrics%20Banners&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://qualtrics.com/....i&/.....\c2.i\sOj….s.....W&....]S._G~.A..Eo.....ue.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2bfeab7566364c53_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1800
Entropy (8bit):	5.89889560874633
Encrypted:	false
SSDEEP:	48:ZEhopsrPEhNtEhnbEhPWEhLAEh6Ez9Ehn7BEhS:UEQ
MD5:	F6BEE221AD54CC2195129ED528FA8681
SHA1:	8F7CB7EC84E6D6C67F6FEA9DA2050AF54F3FF788
SHA-256:	728B41874E14F1C79887FBF895EC29D5E3B8FCD5CA8B1D211FEFFE35922C8307
SHA-512:	EA8545324CF31176EA546A00602F4D4FADD49A843DC7E87138DFAA693869D3F848C01926BC8F2BB8CB4A54CFD401AE9DB0703FE5B8A8CF4F23A27504D7ACF8E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q...- ....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-W6F8HX .https://qualtrics.com/Q3..i&/.....W.....x....8.OH}!E..c.p..-...").....A..Eo.....6.....A..Eo.....0\r..m.....Q...- ....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-W6F8HX .https://qualtrics.com/hA..i&/.....h.....x....8.OH}!E..c.p..-...").....A..Eo.....Z.....A..Eo.....0\r..m.....Q...- ....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-W6F8HX .https://qualtrics.com/a.,.i&/.....x....8.OH}!E..c.p..-...").....A..Eo.....A..Eo.....0\r..m.....Q...- ....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-W6F8HX .https://qualtrics.com/P..i&/.....x....8.OH}!E..c.p..-...").....A..Eo.....z./.....A..Eo.....0\r..m.....Q...- ....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-W6F8HX .https://qualtrics.com/P..i&/..T..FEB5810056E41146CB725CB0070B679

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2c3ffd832f287d94_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.4373305987251985
Encrypted:	false
SSDEEP:	6:mekXYZDtVcmWyMCzSJDZ6HgDSGjjlJhYwwTV4VfbK6t:JkgVx4CzSVE+j/ubWfN
MD5:	4EFE441E9BD5E2D761783A8FDFDF1ED0
SHA1:	E40C58A7C5CDA32C1F1F5CFAE34142236BCAEA09
SHA-256:	86026D112ECD6CA3203D9706B8BD2869DA808143738C2B8579ACA0645E98130B
SHA-512:	BCB434068DB1D96A0FBE94ED89B8693768EF6E8969FFB3F43BD9665FEA207FC1AFD911E515899F97A8C9BB5D2BEEDB458849B4ECE0A9C96BC90CCCD7B5315FD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R.....M....._keyhttps://js.driftt.com/core/assets/js/29.9b16991a.chunk.js .https://driftt.com/....i&/.....&h.....(^...f.a..Q\..Zc.....g.y.O..A..Eo.....>=^.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2d8e602c0c1f3146_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	33325
Entropy (8bit):	6.049343258633729
Encrypted:	false
SSDEEP:	768:UGDUGsGaqEVEdEzT2PqCKPpYLbZleoeSYAHTqS+8qASQuhTsnE:i/VNa3opYLlk8qoE
MD5:	387C41F7030E1428403547A8527679AA
SHA1:	E4E5E493C377A0CD9BDB00BA040E86BE620B59B0
SHA-256:	A93F9E9D76055ED2B7A3B8208E4E33BE55EA05929AC5E6FECD642F54D6A27218
SHA-512:	A129CBD0EAD64B3EAA889ECA2EBF3E81CEA2B5BD65966ACB2D92D90A1A45E06061FE89A75A05C4EE42687852F9408B4E3002120A251E69CF49EA5B5BF2F03677
Malicious:	false
Reputation:	low
Preview:	0\r..m.....C.....[...._keyhttps://cdn.krxd.net/controltag/wdd070r9h.js .https://krxd.net/..(.i&/.....1)...c/2.F..IZ\.y.@...G.A..Eo.....w.....A..Eo.....0\r..m.....C.....[...._keyhttps://cdn.krxd.net/controltag/wdd070r9h.js .https://krxd.net/;p..i&/.....e.....1)...c/2.F..IZ\.y.@...G.A..Eo.....W=X.....A..Eo.....0\r..m.....C.....[...._keyhttps://cdn.krxd.net/controltag/wdd070r9h.js .https://krxd.net/.....'..e....O.....H.....(S.@..`<.....L`.....(S....`X.....L`@.....HRc .....Qb..:.....w.....Qd.\.,....debugging.....Qb...F....log...Qc..#.....config..c$.....I`....Da....T.... Qf...z....Twitter for iPhone....Qb.../....test..Qd..g....navigator.....Qd..t.....userAgent...I..Qc:.Q.....kxdebug...Qc.t.....location.(S.t.`..... L`.....Qc..S.....console.....Qc".!.....slice.....Qb.....call.....K...K`....Dw0.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\30d85c3efd15fab4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	612
Entropy (8bit):	5.564783073425274
Encrypted:	false
SSDEEP:	6:meo6EYFEDL5VTqvMggPUV2cIQTAqgK6tWeo6EYFEDL5VTqGtgLqPUV2cIQTAR/h8:nnMWwUjzYNnM26UjzG/7NnMZcUjzz
MD5:	FE4B5D011D4D40DB3F4C131713E4131B
SHA1:	39051065161CD80DA30773C9C6D874A6EB86AE42
SHA-256:	A6CCFD5BFF88C603D7AC259898588D83B2D391FC8AF7D9C127752E34D105DD3C
SHA-512:	F51720E859D460FB243253A79270E984FDC69E7FA2E02E1D50A64BFA1F7987CD55CB608F1D1884C4A636CBCB5E85F6E3B7D400AEDDCCDBD2EE043513F0423FE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H.... S....._keyhttps://js-agent.newrelic.com/nr-1209.min.js .https://qualtrics.com/..9.i&/.....|.....F.2Uf..rC.....A..Eo.....5Po.....A..Eo.....0\r..m.....H.... S....._keyhttps://js-agent.newrelic.com/nr-1209.min.js .https://qualtrics.com/...i&/.....F.2Uf..rC.....A..Eo.....P.E.....A..Eo.....0\r..m.....H.... S....._keyhttps://js-agent.newrelic.com/nr-1209.min.js .https://qualtrics.com/%7!.i&/.....F.2Uf..rC.....A..Eo.....,.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\30e4a8a144320c5f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.606260086651443
Encrypted:	false
SSDEEP:	3:m+lWfL6v8RzY/LJN9qLTFJStvdUqyTdvD7nLKC+vll/lHCD5/qWYBKVkevg4m5/R:mmEYD8/mtuqyZvX+HgD4oke4rzbK6t
MD5:	747F17DB267E64EB6A65AC8066001106
SHA1:	9678B3DDD0DEA11B5A1184FC2B43230FE48FC5F0
SHA-256:	57FB5482E95197C206E8CA7952647F4447E83F7F8855C7B24C5E9D344B79A388
SHA-512:	866024B7151F940122F66C179BD3E68D1885FA912428E2EE97FA005FE48D7A47965942BE128147C875051240806B432A1EE7D3001A22E17CF4FF617FC24694E2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b...td:>...._keyhttps://solve-widget.forethought.ai/npm.redux.7aa0e181921351cb640e.js .https://forethought.ai/.EI.i&/.....&.....9.^....e.M.....L..7...2."BX.t..A..Eo.....'.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\331396fbc7887f8f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.5742720061815145
Encrypted:	false
SSDEEP:	3:m+leOK8RzYTuCAugWALua8mhucEVNVZ/MI2vlll/lHCyl/lMGgZam9bD6CB2MmEH:mcnYKCRgruaFOjL2FgylCDNgnEDK6t
MD5:	4B421DDED5097917755F0A7C547F5605

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\331396fbc7887f8f_0	
SHA1:	DC57239D001230F58FFB7A1DF6DAF757713C76D9
SHA-256:	BA9E79F351A9E4931E40621D8ECE00049A5C23DD7A71B5070251FD53353630AF
SHA-512:	200CE4F1BA68BDF9FE72EBDC3FE7303FD957491220D5D221E9900B44471D3849350CEB441E7D47C7DD492C691CECD634E92BF6271542F288B895B8B85D16244
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N...uF.z...._keyhttps://cse.google.com/cse.js?cx=1b2c273955de6993f .https://qualtrics.com/a6-.i&/.....mlH..,V;..I.|...X@$&.....g.A..Eo.....5.d..... ...A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\351a5472c87eed38_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	346
Entropy (8bit):	5.939562131452504
Encrypted:	false
SSDEEP:	6:mEdLPYhDbCxwVk6xSzSuzPBgNR1z8Z7D+MoeSfvNzVQgRKKj3u+4GK6t:6VkASmNR1IHuHNRV++n
MD5:	10BE928F38CB87871BD44E5CF243FEF0
SHA1:	B01D89E0558E7902A8B7B20ED25D9A846B8351DE
SHA-256:	A24ACF69D61BFEF9ABE13FC234D0BD26DF92F2F597AD4BEA8A06C5D79E75921C
SHA-512:	4CEE47D44243A3FA076659B7C0AEAA3BD2C5807790112AB4996F0FB18259FFF2545E68D5303FD2D5968F178CCAA851CD8FA596EE3D6BBE625C692BFBC6D654 3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U..:...._keyhttps://zncydxfem8jrupnsj-qwebsite.siteintercept.qualtrics.com/WRSiteInterceptuser/?Q_ZID=ZN_cYDxfeM8jruPnSJ&Q_LOC=https%3A%2F%2Flog in.qualtrics.com%2Flogin%3Flang%3Den&t=1627086278791 .https://qualtrics.com/...i&/.....s.....('..-U7...=..~.1p..T.?W$(n.mB..A..Eo.....bX.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\35f99f3ccb147235_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	367
Entropy (8bit):	5.840383783980375
Encrypted:	false
SSDEEP:	6:muEYFBKbHYVzi1xCJgRR3zBfJPLvbm+XIiYWERmFSjWECZrKtgcJeImOok4nK6t:JvKbtKgndfJmG4bqGtMItoD
MD5:	9648FCA88376372CA448D22D17B4A8E3
SHA1:	99813862E001DB3E2162F99F9EA630DAC63E9C04
SHA-256:	95E4FBDC99E49EC1ED84F0EA4C6CBA8FB57EC79EB62B7F1B7C1BB9A5CB798FA5
SHA-512:	3EDE345CD75AC5CB05D7C888515D2EE5BC18D1979AA1E18F7AD4606003378B5DF6208332704B74AB88F691186211CA02CA584060CB523A9550AF6AFD21641ED
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<..H...._keyhttps://success.qualtrics.com/index.php/form/getForm?munchkinId=542-FMF-412&form=7836&url=https%3A%2F%2Fwww.qualtrics.com% 2Fuk%2Fplatform%2F&callback=jQuery112405971744821627878_1627086304584&_=1627086304585 .https://qualtrics.com/s...i&/.....aP.....6..c.D.cQ..tL04Vv1#. !....(Q.0.A..Eo.....F.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3ba0d59b2336e054_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	298
Entropy (8bit):	5.514730571399984
Encrypted:	false
SSDEEP:	6:moUEYZDtVcmWyyVRSJDdDKtg71XhJcHT+ck4jJhK6tctgyJcHT+ck4:OVxmLSVdDpSHK9+78SHK9
MD5:	9AF72D4FB0D830EB3E69C7DDD14B98AB
SHA1:	82C15B2F105A9CE024D54A00D476F0A4EECB8DAC
SHA-256:	6DD7270EBD8738206A1D975940EEA417A53285E05DC38B5E34E47F197F7C2706
SHA-512:	4C81C233188CD9571C18A5B3572B7F68675E1FC4075E440BF09D63011AD542A0F8EBC395BFC849885C149393F99CE939EB12C4B62AB5313F86EAA61D245F1FBE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...X....._keyhttps://js.driftt.com/core/assets/js/16.053b05ea.chunk.js .https://driftt.com/....i&/.....W.....)g..0l.1..yk...Mg_.g...\..$...I.A..Eo.....K].....A ..Eo.....i&/.....W.....)g..0l.1..yk...Mg_.g...\..$...I.A..Eo.....-.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3cdf39d43fad418f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3cdf39d43fad418f_0	
File Type:	data
Category:	dropped
Size (bytes):	70560
Entropy (8bit):	6.083544527050046
Encrypted:	false
SSDEEP:	1536:poXqYwrN5LakzIRYp0Rl+yGpENhIbcRjVF9dz2:maLe0Xp0RRQSuIRjVF9M
MD5:	70EA31003B1DCF8D78D12AA628C1FCE0
SHA1:	767D86762B4B6B2B30736E528620965520B32E91
SHA-256:	726CB413067BDDF251EF4ABB5D0911BE64F86ED449E67D26DBD431CADC44C640
SHA-512:	02B4CE6883FDADA9FC78B61593F5F0562F8F900FB9165FA57BB5177C8321290BD9717A60D533C7DC1B5370A03E153FB75A477B1218FED277526D52CF7728446E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....BFBD1B3177C17B3B8A8ABEF6BA9339782F8FBDBF06C65301CCCF593EB2383AFC.....'.....O....h....9j.....4.....D..... .....(S.D..`B....L`.....(S.]..`p....L``....u.Rc.....R.....Qb.3z2....n.....Qb.....q.....QbZydU....r.....Qbn.u.....t.....Qb...o....v.....Qb..G.....x.....Qb^{jV.... y.....Qb.....z.....Qb.....A.....QbFu.....B.....Qb..|....C.....Qb.&.....F.....Qb.....E.....Qb*C.1....D.....Qb.Z....G.....Qb..+.....H.....Qb..|.....J.....Qb.i.....I.....Qb.L.6....K.....Qb.l. G....aa....Qb.Z-.....L.....Qb.y.U....N.....Qbj.....O.....Qb.e.....P.....Qb.....M.....Qb.....da....Qb.....ea....Qb...$....Q.....QbB0.....S.....Qb.:`....R.....Qb..P{....ia....Qb.[.F....U.... .QbJ.U.....ha....Qbv.....T.....Qb..}....V.....Qb.G.....W.....Qb..5.....Z.....Qb.b2J....Y.....QbN.y.....X.....Qb..|.....ba....Qbf..S....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3d5900f755529cdc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	739
Entropy (8bit):	5.791117076449713
Encrypted:	false
SSDEEP:	12:HE3j4P/KHP+fPux2pHgyyTt3CMxtfdfJDri2ZzJdfGR7p0fNCsIzJR:HEzwyv+XuyAyyJSu1xJzruR7SfNCsGJR
MD5:	47075DCC40A55E3243CA45E9D7D9BE08
SHA1:	C1DC8F042E30E131CFF1B6998FFCB7308CD581F4
SHA-256:	528C1CAFF24823179042DE77238336F3A0534FD198CC5A7096D84AD5F2B34D1A
SHA-512:	02E3DA3FE8ACFF59A366DC382D8FBB8B3AED05D57361724C433E18FE002523C103368EF8983B327B8DEE7ED40BF88B6D9B1160F57E8B7AD3E9F1CA00E589CC BC
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...,]....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/875348540/?random=1627086303987&cv=9&fst=1627086303987&nu m=1&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=2&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2& gtm=2wg7l1&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fwww.qualtrics.com%2Fuk%2Fplatform%2F%3Frid%3Dip%26prevsite%3Den%26newsite%3Duk%26g eo%3DIT%26geomatch%3Duk&ref=https%3A%2F%2Fwww.qualtrics.com%2Fplatform%2F&tiba=The%20Experience%20Management%20Software%20Platform %20%7C%20Qualtrics&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://qualtrics.com/E.}.i&/.....eO.....5.6.^kM..Bs....<.d..,.w...Q.A..Eo..... ..A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3e037aa5d2226c98_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	609
Entropy (8bit):	5.796446481801899
Encrypted:	false
SSDEEP:	12:7wE3aXFK4UiPHUYux2pHgyye3CMxtfdfAYUwdNC6lY2rSMkDKLf7:kEKXFKePuyAyyeSu1ovwdNCOYcSMkQf7
MD5:	CE205551F172BD379B66A66454E9FAF3
SHA1:	CD593642EA72F4461F92F55FAEDB8C752B975935
SHA-256:	0ADB00B410177C1272CC0C832DA2E78E25B0AC23E5809DB910D66B572877E0C4
SHA-512:	66502C3CAF14A4ED2B7B77B914020D889221271CDC535CB5C7521332858FEC0F41DF3B857F084AC1C38DBC3DC81B8ACCEDDCD1B97C5CFD7884DAAE192755(BA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.3K...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/1026978278/?random=1627086314326&cv=9&fst=1627086314326&n um=1&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2 &gtm=2wg7l1&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fwww.qualtrics.com%2Fplatform%2Fultimate-listening%2F&tiba=Ultimate%20Listening%20%2F%2F%20Q ualtrics&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://qualtrics.com/#...i&/.....v.....k...L,...;t.>.<."~}(:Ny....A..Eo.....,.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3f603955b56b791f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	267
Entropy (8bit):	5.522201850626634

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3f603955b56b791f_0	
Encrypted:	false
SSDEEP:	6:mmLyPYGLKfVVOlAkFayGlHlsrj6tgkGBT3OyjRK6t:2Sf1GayKFeKcJr
MD5:	5A6F478992BAF838747AE831B5B62684
SHA1:	5FCABC03BFA8C9D09582427150D7E1289229B419
SHA-256:	369BF6FAC91735730BD6538C2FCC97B8ABF3EF1C13581E17D8A1CBC124C01334
SHA-512:	C3A4EBDCDD9628F03EC6311DED2E7F7D3A6B16E8FB247C87168A22D406DD69012C9FCD03294B82A01ADF29DF1FD5F7184CAD9559FE04E66CD58163216FBAC84
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M.G...._keyhttps://www.qualtrics.com/wp-content/themes/qualtrics/components/language-routing/q-language-routing.js?v=1 .https://qualtrics.com/A.j.i&/.....G.....NL.Ixg.B..n.|T. ..''.B.. ...A..Eo.....Z.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\411c60ce258c96af_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	249
Entropy (8bit):	5.679489062169585
Encrypted:	false
SSDEEP:	6:mjlXYGLIgcZbEhyjL2lJHgon/ywkTPtihA/bK6t:0loBZ/unHKwkTPb/N
MD5:	0D247594636C5EED43F699461E018045
SHA1:	6E76530FD1B727AEFD3A8F1D78C8A6AB99CCC5C4
SHA-256:	E19A5D83E4981F1DEAA676D6C16C58412B085260294D2262039786EDE7B958D1
SHA-512:	0FC34F77AC28C17911FED80A2FC8CEB016C119C936F053585CBB01B4BC11ED83E6ADA64934516E5B41C8212E10ECC2B7849386B7196051624783FAA8D0A0D98
Malicious:	false
Reputation:	low
Preview:	0\r..m.....u...{....._keyhttps://www.google.com/cse/static/element/b54a745638da8bbb/cse_element__en.js?usqp=CAI%3D .https://qualtrics.com/f.=.i&/..... ..2u%V.~....W..f.....r..A..Eo.....b._.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\426bd77de8a308fe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1125
Entropy (8bit):	5.6164369188976115
Encrypted:	false
SSDEEP:	24:U63iOR+1y6yOR6wy6aORGy6nSywOR6y6D7ORH:UvyRwyDy8SJyKa
MD5:	5DF75C65B4661EA63A801C3876C3B193
SHA1:	4780DA3C582A88FB027A83601262C20BE2220D5C
SHA-256:	E294AEFE522DA7D2A7FFDF3C2C53F3CC7EF9497AEEB8ECB5102151C516649A55
SHA-512:	310EFF06F220944F712A2648AB71BB62C8C594A9129554A32C91ADE5C2A0F6DFF62CE4095ACE468547A7E3ED442292FAF04557D55027770321276DD4C7417065
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]...`c....._keyhttps://connect.facebook.net/signals/plugins/identity.js?v=2.9.43 .https://qualtrics.com/B...i&/.....Hw-*'..E....B.*.....q..Pijz..A..Eo.....?~.. .....A..Eo.....0\r..m.....]...`c....._keyhttps://connect.facebook.net/signals/plugins/identity.js?v=2.9.43 .https://qualtrics.com/.]3.i&/.....%.....Hw-*'..E....B.* .....q..Pijz..A..Eo.....$\.....A..Eo.....0\r..m.....]...`c....._keyhttps://connect.facebook.net/signals/plugins/identity.js?v=2.9.43 .https://qualtrics.com/....i&/.....#. .....Hw-*'..E....B.*.....q..Pijz..A..Eo.....`.....A..Eo.....0\r..m.....]...`c....._keyhttps://connect.facebook.net/signals/plugins/identity.js?v=2.9.43 .https://qualtr ics.com/G>~.i&/.....lO.....Hw-*'..E....B.*.....q..Pijz..A..Eo.....A..Eo.....0\r..m.....]...`c....._keyhttps://connect.facebook.net/signals/plugins/identity.js?v=2. 9.43 .https

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\42b7c017e3dc2d2d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6744
Entropy (8bit):	5.749621047076554
Encrypted:	false
SSDEEP:	192:0b5cs1YlDmLE8LU3h6Ul4c30WypghZig5RfVBZG:0lJ1YleHY3h6PA0lgZ7tPG
MD5:	5AE45F3D262CE235E6BE920801720161
SHA1:	F2714DB164A11378F501EF70F4AAEC381DBA548A
SHA-256:	5700CED11EDAB7E81D249448DCB00570EDC475C468117B919A62798B3D1CF49D
SHA-512:	593A23A45D8B38D376438C5E0A9A4B5AB04CC877344CB218A0C2E73DE1B41EE01C30E792E607451F5BD221B5D716059CED68D79497BD4A88B7DCDB4534F35B4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\42b7c017e3dc2d2d_0	
Preview:	0\r..m.....H...3.N...._keyhttps://munchkin.marketo.net/160/munchkin.js .https://qualtrics.com/....i&/.....<...B2oy...9._..5.....d..| ....A..Eo.....`.^.....A..Eo.....'.f+....O.....[.....(S.4..`$.....L`.....(S.Y..`j.....L`x....q.Rc.....R.....Qb:.Z.....h.....QbB.@.....I.....Qb..'a....q.....Qb.2.....D.....Qb.r.5....A.....R....QbN>b.....t.....QbZ.....E.....Qb..%a....x.....Qb..-.....F.....Qbr.....v.....Qb.H.....V.....Qb.c.....f.....Qb.....G.....QbB .....W.....Qb.U.(....r.....Qb.x.....H.....Qbb.....I.....Qb.__,...J.....Qb.2k.....K.....Qb...L.....L.....Qbn[.*....y.....QbZ.P.....e.....Qb.....m.....Qb.1Y....p.....Qb2.....X.....QbF..t....B.....Qbn._....C.....Qb.)8.....M.....Qb.....Y.....Qb...K....Q.....Qb.r.....Z.....Qb:.~\|....R.....Qbrq.....w.....Qb.....S.....Qb.)&.....z.....Qb.n.3....T.....Qb.....N.....Qb...^....U.....Qb.....O.....$.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\436864cf0cb947e7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	77864
Entropy (8bit):	5.903653072700037
Encrypted:	false
SSDEEP:	1536:UYy5UNh2SzyASwQoMAmTLOwGCHNDO5XiNzCezMFWih:UYy5whDxSwxMWyg
MD5:	3B11BD1E7CC79220D07397BAF925D0A1
SHA1:	9B12EAA1558E0C3326163A2EDBCA7F6522F51A7E
SHA-256:	F408234DF937097A46CDF82A903A03757F99C472AD419661B2064E05D4FE6ECB
SHA-512:	74D1818B9D16DA02872CC9732446DCF6B85FF0E7E7F3ABB0A7BA5D098E50C2110ADCF23802BB6B8DDA66E65E5734A757C7D0D0C4BD799373D94D8890F420ED9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...RM.k....DB6FF2450FB679D5705B41DCBFE6DB76504D2E6793F645541FE989C883589F1E.....'..+....O.....,.....t.....@.....(S.=...`.....L`Z....(S.`.`x.... L`.....@Rc.....Qbn.u.....t.....Qbr.....e.....Qb.3z2....n...b$.....I`....Da.....(S...`.....L`.....Q.@".&.....exports..$..a.....!....a.....QbF_.....id..C..Qc.....loaded..H..1...Qb..P%....call..q...K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&.(...&...&.'..W.....-...(.....,Rc.....a.`....Da....<.....!.....e..... P.....@....@.-....4P.....%...https://intljs.rmtag.com/119359.ct.js...a.....D`....D`p...D`.....-...`....&...&....&....&.(S.8..`(.....L`.....0Rc.....`$...I`....Da.....(S..`.....L`.....QdF8.$....isTesting.....Qb...t....main..K`....D.a.....&..(&.]....&..*&.]...&.(

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4777c499c25aa38f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	234
Entropy (8bit):	5.562583164317594
Encrypted:	false
SSDEEP:	6:m6XYD8/qB09FSSPErHga/I76Tx8rp5xK6t:88/60nSSP8GN5L
MD5:	E94BA1EF3C4ADCC8E570669507EE8916
SHA1:	B7A2C31DE364CAE3B2992693FAE6308AB0BDA1A2
SHA-256:	94F4B55A9AC545D9EB668D63722BC367E733041FEACCF900F071C8EA9F31CA6C
SHA-512:	E2FD519AE593530DF5299233892FCB0C2F146CD8D255343F33E11300B367ED2D968640FC82DEAEE8127788A78941ED55E59BB45183CCC029CD546CA7C8BE363
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f...0.i....._keyhttps://solve-widget.forethought.ai/npm.logrocket.c8a35bba1d76c27c027b.js .https://forethought.ai/.PI.i&/.....).....Z ..3X....?.9...(SX9.....@..rb.A..Eo.....m.<.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\47ae5e91f81262aa_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	83368
Entropy (8bit):	6.067885014665933
Encrypted:	false
SSDEEP:	1536:LQGJ0UF7VdKdsLL7F9wJZsTvr/uGbUBfYNSpEatInlaJ/F9dz5:L/GUFjKG7v2ZsTvrGRmNU1ilaJ/F9D
MD5:	119D0E395F0FA76D241BAA44A73DFE2A
SHA1:	47B0007B722783A662A6E759C9C13D803465DD16
SHA-256:	40A94BB46696D95227265BB2E66A82EF2E41883D749564540A10776ED37E3614
SHA-512:	75C325DED5C9D5F18DFD4C2FA18C125560E69DA0F2A0F9B09927543E6FD757BE31E30A282D2FF3D7287728E30DBA04AB549E0198C99B6F5543673A34F61A08E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....99241F4B4869D51D6EB8BA46A3CA83DF73D949139C26BCFF31E3E17E4D5E38F4.....'.....O....`D..B.....4.....D.....L.....8.....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qb..=G....n.....Qb..'a....q.....Qb.U.(....r.....QbN>b....t....Qbr.....v.....Qb..%a....x.....Qbn[.*....y.....Qb.)&.....z.....Qb.r.5....A.....QbF..t....B.....Qbn._....C.....Qb..-.....F.....QbZ.....E.....Qb.2.....D.....Qb.....G.....Qb.x.....H.....Qb.__,....J.....Qbb.....I.....Qb.2k.....K.....Qb&.....aa....Qb...L....L.....Qb.....N.....Qb.....O.....Qbf!.....P.....Qb.)8.....M.....Qb.....da....Qb.s.8....ea....Qb...K....Q.....Qb.....S.....Qb:.~|....R.....QbV.q.....ia....Qb...^....U.....Qb.....ha....Qb.n.3....T.....Qb.H.....V.....QbB .....W.....Qb.r.....Z.....Qb.....Y.....Qb2.....X.....QbVy.....ba....QbR}a8....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4932a4428abbea52_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4932a4428abbea52_0	
File Type:	data
Category:	dropped
Size (bytes):	329
Entropy (8bit):	5.771399505324892
Encrypted:	false
SSDEEP:	6:myyEYkpWSnjf6tgA7AmcaYzAx5K6tyqTnmp3zUY3mlJAmcaYzA:mUfmAmcLzGbnmxHm2AmcLz
MD5:	29E6C0EDC1AB11593431797A0A7FF242
SHA1:	D77F84EE26B0A139786E4A1E06F3AE2BADFDF180
SHA-256:	B3AF7B6406FA227860E7DBD5A08AE439F2A1AF10123650E5DE14614630DDBFA5
SHA-512:	F61867F9A69E6F7F389DD0E5246E50BE02960786A449054434D5277BBBF1CDFE7A704B4239D61D28363B78C12CFB7FDDF4407AB196216FD8DBE86393CE5A822
Malicious:	false
Reputation:	low
Preview:	0\r..m.....A.....\...._keyhttps://intljs.rmtag.com/119359.ct.js .https://qualtrics.com/.>..i&/.....7.....\t...g...[..%s{..4..r1lzi..#%.'.A..Eo.....N.....A..Eo.....>.. i&/../..DB6FF2450FB679D5705B41DCBFE6DB76504D2E6793F645541FE989C883589F1E.\t...g...[..%s{..4..r1lzi..#%.'.A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4bddf5dfbefc791e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	739
Entropy (8bit):	5.779495127477368
Encrypted:	false
SSDEEP:	12:uE3oTp4PsHPEPux2pHgyyTt3CMxtfdfJDri2ZzJdfGR7p0fNCWyYElARGr:uEopwsvEPuyAyyJSu1xJzruR7SfNCWyT
MD5:	D8F2BE5EFE2250AB8C84DF37BDBECAA9
SHA1:	658E131D1153373BA6F050F6D57DCAA6A06A1C66
SHA-256:	E3311239EA8CF4FF468CAB48385621516BE47066754520301EAE864DCCDD8FB7
SHA-512:	A12101D98800144C44EC7A766D143CBBF70F61C2E341B21663F2174320E39867A07CDFD2997E81841BD94981AA782F4A338B20FA209328E9E2965CAD1B880FFF
Malicious:	false
Reputation:	low
Preview:	0\r..m....._....,_~...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/857073434/?random=1627086303985&cv=9&fst=1627086303985&nu m=1&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=2&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2& gtm=2wg7l1&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fwww.qualtrics.com%2Fuk%2Fplatform%2F%3Frid%3Dip%26prevsite%3Den%26newsite%3Duk%26g eo%3DIT%26geomatch%3Duk&ref=https%3A%2F%2Fwww.qualtrics.com%2Fplatform%2F&tiba=The%20Experience%20Management%20Software%20Platform %20%7C%20Qualtrics&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://qualtrics.com/['z.i&/.....VO.....:&..^.R..l.6.Tg.{0R...eI..8.A..Eo.....}.h.... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4e0db295e0762028_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	11125
Entropy (8bit):	5.298038114920672
Encrypted:	false
SSDEEP:	192:0JwbSaba2HR5uE1aejMKigJeO/4LL/rRQovQdSt6WtE3ZQRm7S5Q2s:Rm4R5Lv5Wkie
MD5:	6790ABC9BC29C85AD99ED46CC0EC4B68
SHA1:	E55C480D9BD99FDF562926904228526F2D92D60E
SHA-256:	C1386FBB89D4EF05B7B93B75A65DB0827524D544FEE6786E010C88370A1A826F
SHA-512:	2DDF2B282634DCCDEA3F9038E369015A0E27582DE62B05911B4FAA5E0E2512791F9C8C6DCC52C0E3F078C41A5E5A009FC5F54F87305FB24FF76036284D85936A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]...k....._keyhttps://www.qualtrics.com/hreflang-routing/managed/definitions.js .https://qualtrics.com/.f..i&/.....y.....J@.5q..`.O..A..Eo.....t8q8.. .....A..Eo.....'.,....O.....).....\.....(S.8..`*.....L`.....L`.....$Qg.....ql_routing_custom_data...,..a.....Qdf.....exclusions.....a..... .Qc.....exact.....a..... Qf...X..../uk/free-account/...`..... Qf.0g]..../au/free-account/...`.....Qc.].....partial..\.a*.....Qb.Q.`..../lp/`.....Qcz..Y..../events/`.....Qe.Cp...../ebooks-guides/.`.....Qd.K...../x4summit/..`.....Qe.. ...../uk/x4europe/...`.....QeV..{..../au/x4sydney/...`.....Qe.S[...../fr/x4europe/...`.....Qd*..+..../es/support/`..... Qf.>...../research-center/...`.....Qd...../resources/.`.....Qd.^.p....geoip_lang.....a.....Qb..h.....AL.....a.....Qb.5C....en.....a.....Qb...6....path..Qb.x.....uk.....QbV.d....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5001de7cb5b35478_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	11042
Entropy (8bit):	5.565989676317368
Encrypted:	false
SSDEEP:	192:qf/e/70zHJlCTpkHLxV1RxwzN3C6B4swgTy7A9xe0D5jANT14coaYBJ:qf/ej0zHrCTpkVv+Zl0F0NZ4daYj
MD5:	0943A960E949493D3DE210D8D78DE52E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5001de7cb5b35478_0	
SHA1:	6BA6A5FC81AD4526C433DA16DAA1BB7B1711A1D7
SHA-256:	F7DDEB3D41AC617D91E3A2BB18CADFE89C2218D2015248D7C6C504010DD3EE72
SHA-512:	78ABA0AEC8CCEB9B3999D04A207D933BD8FC261882343961D15DB121EB52BA37D60C5120F6DADAB6EE38B429D5937305A935C968E4F572D43E0312E47528230
Malicious:	false
Reputation:	low
Preview:	0\r..m.....D....._keyhttps://siteintercept.qualtrics.com/dxjsmodule/1.bc170c7af0103c537cda.chunk.js?Q_CLIENTVERSION=1.56.0&Q_CLIENTTYPE=web .https://qualtrics.com/..G.i&/.....9.J..5..#.. ..N/,.k./Z.X7.....A..Eo.....,S+.....A..Eo.....'..g....O....`)....nU.....@.....$.....(S...`.....<L`.....Q.@v.....window...4Q..f.L.%...WAFQualtricsWebpackJsonP-cloud-1.56.0.....Qb.[M.....push.....`.....L`.....`.....Ma.....`.....0..b.....C`@...C`V...C`Z...C`.....(S.\.`r....$L`.....HRc.....S...Qb..=G....n.....Qb.U.(....r.....Qb&%.....o...c$.....Qb\.....23..`.....Pc.....push.23.a.....(S.....Ia.....d.....@.(.....d.....@.....@.-.....P.....v...https://siteintercept.qualtrics.com/dxjsmodule/1.bc170c7af0103c537cda.chunk.js?Q_CLIENTVERSION=1.56.0&Q_CLIENTTYPE=web..a.....D`....D`....D`.....`....&...&..a.&.(S.....Ia.....I...1.d

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5279e4cbc4657b6e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	39453
Entropy (8bit):	6.256101835894065
Encrypted:	false
SSDEEP:	768:61ARm5YjZDMhznrmCJe7isSG6Z40PCHIzKz6s3tsXgY:6WRUYjxEPmCw7FemXIzKz6wwgY
MD5:	EDD659096C3481D2059ECEFAF5D71718
SHA1:	A4883BCEFDD2A10797463CA407942EFC5F230BA1
SHA-256:	AE99F423DF4DC5CA2E2EE660577C99C3B8ED374569462376D88E919927650FC2
SHA-512:	9F4B8156BF216528EAFB9EA04B9CB32E21CA1913EC33BA217E79B8D917E245BD063C2C6FFB7B61D5F5DE8F7E59A9E84E1BEA3DD87CF9069DDF06E807778DA09E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....7....._keyhttps://bat.bing.com/bat.js .https://qualtrics.com/.O..i&/.....`.....5'.....@';@q..c.n.g.Gp..Cmh..k.A..Eo.....*C.....A..Eo.....0\r..m.....7.....`....._keyhttps://bat.bing.com/bat.js .https://qualtrics.com/ ...i&/.....;.....5'.....@';@q..c.n.g.Gp..Cmh..k.A..Eo.....`.....A..Eo.....0\r..m.....7....._keyhttps://bat.bing.com/bat.js .https://qualtrics.com/x.1.i&/.....5'.....@';@q..c.n.g.Gp..Cmh..k.A..Eo.....d .....A..Eo.....0\r..m.....7....._keyhttps://bat.bing.com/bat.js .https://qualtrics.com/J...i&/.....A.....5'.....@';@q..c.n.g.Gp..Cmh..k.A..Eo.....(.....A..Eo.....0\r..m.....7....._keyhttps://bat.bing.com/bat.js .https://qualtrics.com/.....'.6w....O.....p.....(S.0..`.....L`..... L`.....(S.U..`^.....L`.....<Rc.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5287292456405dd2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	309
Entropy (8bit):	5.593230039959613
Encrypted:	false
SSDEEP:	6:mmZnYZDtVcmWyXWT0ptyIBJDAXtgoWt+TCft0H4SDK6tQtgyl/+TCft0H4:KVx9blVEbOt0HF1wGOt0H
MD5:	60C8495158D09995EDDA8C09D89EDC9D
SHA1:	67737DB4B08310BFB1B9155F8CEEF117F2067E1E
SHA-256:	3D17341774B3D75ED67DE506882B26680EEB6EFFB8881511356E6B91B06331BE
SHA-512:	FA8CC179F0C893D8D90229CE66FB3EA14D8C1AA0917C6B0D5431210F632D6D4CDC75FFFA95CDB26351D08E5E25F58214318EFBD784066F87A3100AC6C1A810
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]...;....._keyhttps://js.driftt.com/core/assets/js/main~53ca99a6.8bfc1b55.chunk.js .https://driftt.com/%-..i&/.....Z.....ykd3..8i.V..U[.#..4.[....#.h...A..Eo.....e^~.....A..Eo.....%-..i&/.....Z.....ykd3..8i.V..U[.#..4.[....#.h...A..Eo.....I.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\53a3aa1de5952d66_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1236
Entropy (8bit):	5.51544611328082
Encrypted:	false
SSDEEP:	24:7e52g5e5yR5e5u6A5e57fE15e5TW5e5n6eV:7KJ5KE5KuZ5K7E15Ky5KnxV
MD5:	DECEEECC958E1AE57C62F58B0FF0D342
SHA1:	DE3671BA25B7C5AB4356ABF372283225165B62C6
SHA-256:	7E6D7E5456C92174071AE08F34123D9A3898DA3F40F9064169F43046AD80F8BF
SHA-512:	D391BDABAF9D2E88BB2AC3E7ED1077AFFE5DCF4C1F9E2CCE6259B3748610FAA652AD8D719AFDBBD4B4797B26C639FFFE249F81CF701FA4FAE59313B52CF05FFE
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\53a3aa1de5952d66_0	
Preview:	0\r..m.....J....-v....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://qualtrics.com/dY..i&/...../.....,.....Sd....n...-..e...Q...&!..A..Eo.....\.....A..Eo..... .....0\r..m.....J....-v....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://qualtrics.com/.]1.i&/.....,.....Sd....n...-..e...Q...&!..A..Eo.....o#G.....A..Eo..... .....0\r..m.....J....-v....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://qualtrics.com/.g..i&/.....,.....Sd....n...-..e...Q...&!..A..Eo.....y.*Y.....A..Eo .....0\r..m.....J....-v....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://qualtrics.com/....i&/.....,.....Sd....n...-..e...Q...&!..A..Eo.....P.Y..... .A..Eo.....0\r..m.....J....-v....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://qualtrics.com/g,r.i&/.....L.....,.....Sd....n...-..e...Q...&!..A..Eo.....C..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5544eddf7848ee75_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	740
Entropy (8bit):	5.798914368691935
Encrypted:	false
SSDEEP:	12:FpE3aXFK4PQHPAaIux2pHgyyTt3CMxtfdfJDri2ZzJdfGR7p0fNCjMtMuMkP:FpEKXFKwQvbIuyAyyJSu1xJzruR7SfN5
MD5:	99535002ECED0AFA9431E8698AB0DF61
SHA1:	2E0B0EDFCA18E1788F7A8079920753E475BE24E7
SHA-256:	0746FCEFD08638252EAF9DE45160F72D94DB4BABAB2C7D56D3739797194350C4
SHA-512:	175D5F3832D24D9BE5386C1A4314F3E568CB3B081BEF521AFA1BB1D502D79B25FFF3A63667E102D4BD5D9ADB8AFFF0D4FD97768CCC28EB79AF2DD176A722D DA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`....Z....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/1026978278/?random=1627086303981&cv=9&fst=1627086303981&n um=1&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=2&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2 &gtm=2wg7l1&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fwww.qualtrics.com%2Fuk%2Fplatform%2F%3Frid%3Dip%26prevsite%3Den%26newsite%3Duk%26 geo%3DIT%26geomatch%3Duk&ref=https%3A%2F%2Fwww.qualtrics.com%2Fplatform%2F&tiba=The%20Experience%20Management%20Software%20Platfor m%20%7C%20Qualtrics&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://qualtrics.com/.Yz.i&/.....RO.....xO.....@]+w...^...6..=."...S..n..A..Eo.....x,-^.. .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\55ad2a779d02c10b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.589675644947499
Encrypted:	false
SSDEEP:	3:m+lvL68RzY/LJN9qLTWoDXLxmEN1VR7nLGvll/lHCH5Hs3UgOyj+/Pg4miU5l1pD:mW3YD8/17xXV1CHgHS3UgOyCQJlDK6t
MD5:	E94792401A230C8B3AC3F590BD870926
SHA1:	E18EFEB07B507AECB8DCD725F92D2BF1262A31C4
SHA-256:	545901C1563BCA34FDEDF11E01E331811992D6E6A4F03B28B1BE4E40FBBE837B
SHA-512:	95138FBE2B8E2A58B5749DE144C9AF4A0DE1BC7BFF229E639B3FCE28CA1F276EE77676CE784C1091EDB7F7B77FA64FA7155F46DC87609973940D8B627AEB29E 3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g.....UG...._keyhttps://solve-widget.forethought.ai/npm.tinycolor2.32e5d98f59e3ee73a28a.js .https://forethought.ai/..I.i&/....."".....2....[....q.+....[.2...mX 6.zf..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5818a042fafbbe68_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.5474064087628605
Encrypted:	false
SSDEEP:	6:m/OYD8/1kz08Gw18gDQbELYtH4dJZK6t:g8/1kzoOsQsHkJT
MD5:	B89B3A72700C488954410188B86811D1
SHA1:	61D3FB5B0C82536FBF9EEECB773C0CF707372988
SHA-256:	73C2DCEA83DE4DBE17343A38A9B011B54A32757C5E3C207019E318C4D88DD4A4
SHA-512:	EEF38753321CA02420978ADEE739ACB5D733D9CEB84D642344894CC1947AC97D02481409905EEBAFB332260EA6FF5455B2480AA5443B1CCF3C12CF667311F30
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....i....._keyhttps://solve-widget.forethought.ai/npm.react-redux.b148dff1aa15fd61b4dc.js .https://forethought.ai/.GI.i&/.....\.eo.`t....U..(..^.Dh....m...y.A. .Eo.....(.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\584a352353d9719d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\584a352353d9719d_0	
File Type:	data
Category:	dropped
Size (bytes):	673
Entropy (8bit):	5.810840122312966
Encrypted:	false
SSDEEP:	12:5lOtnAUXFK4UaOHUqUltJBux2pHgyye3CMxtfdfAYUwdDAniXI/jFM:7OSUXFKLXUltnuyAyyeSu1ovwdkimFM
MD5:	7F39592C8F09BF484D525A515BA2E2F9
SHA1:	C78E29085F6AAC2F857250E03DCA78C608255754
SHA-256:	A4C87B904CA31FB19A14D358AE20C3C7553DDAA0B01BBC254FAD2A455CD6C3DD
SHA-512:	DA35CBB197E944103A147F98F5E58705FED6159D3C49032EAF65EA89E5619AD0639FA6EB9B5A266614D2C3149A748DF292664F52F5F0B8738E288678D34D8501
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O.LK...._keyhttps://www.googleadservices.com/pagead/conversion/1026978278/?random=1627086314365&cv=9&fst=1627086314365&num=1&value=0&label=wX24CLq7jPwBEObj2ekD&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2wg7l1&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fwww.qualtrics.com%2Fplatform%2Fultimate-listening%2F&tiba=Ultimate%20Listening%20%2F%2F%20Qualtrics&auid=1029000693.1627086256&hn=www.googleadservices.com&bttype=purchase&async=1&rfmt=3&fmt=4 .https://qualtrics.com/.]..i&/.....nv.....#.:..?..._.F..uMg..@n.. .P..w.A..Eo.....u..|.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5a552cc262ae94ca_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	725
Entropy (8bit):	5.816632141160553
Encrypted:	false
SSDEEP:	12:yggE3aXFK9cDI2ux2pHgyyTt3CMxtfdfJkWri2ZzJdfEL9CwR07fC4LU+mT:yggEKXFK+DI2uyAyyJSu1FJzrsLxR07C
MD5:	2708AE847690F8927F47C29A06C5AADC
SHA1:	A55BBD82C714F2BF196A014B34471AACEB1EB56F
SHA-256:	2F622637B69E7FCDEC54775EAFB1F1587B81151BA1B5FC538379307EB0011D53
SHA-512:	06A9C51293368826B1243686F311A874EE6E74E11E5BDA2DCE4A2E53B685BC0A61940AE34681031F42B775A56A78B1F03731D18DBDFC7278822E0BB6E61F3D91
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....E....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/1026978278/?random=1627086291288&cv=9&fst=1627086291288&num=1&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=2&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2wg7l1&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fwww.qualtrics.com%2Fuk%2F%3Frid%3Dip%26prevsite%3Den%26newsite%3Duk%26geo%3DIT%26geomatch%3Duk&ref=https%3A%2F%2Fwww.qualtrics.com%2F&tiba=Qualtrics%20XM%20%2F%2F%20The%20Leading%20Experience%20Management%20Software&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://qualtrics.com/C..i&/.....#.....?j$.....;..@@.....#.-b..".Gv.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5ae794d5df51a271_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	224
Entropy (8bit):	5.540283953510105
Encrypted:	false
SSDEEP:	3:m+lU4OA8RzY/LJN9qLVWpfA4eR7nLPsvll/lHCrD/BNYYFvR4guhJaUkoMmS1pK+:mLYD8oA4e1WgrD/3ZV+peYMK6t
MD5:	3CB243EF11EEA9CFE5EF2C8581611E2A
SHA1:	B9F0E2F3668270E108B21EA8ACB833AB6575778C
SHA-256:	A5216406481144CA7D7FF7ED0AC104C1DD90E8A76ED2584D4B0002876D9B903B
SHA-512:	AD724D962F7E56A7562B785D565EAE259CC14ABE0C99D7B533310B783D45BB32E8089332727B1C48D3A6B86A10AF472B51B7A5F5453A29E0F37DF95B79BA083
Malicious:	false
Reputation:	low
Preview:	0\r..m.....\...{..}...._keyhttps://solve-widget.forethought.ai/app.3ae1a9eba3bbfff9e8bf.js .https://forethought.ai/xWI.i&/.....5.....E.mVR...z(.....(3.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6103b5b7f78f61b6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	64188
Entropy (8bit):	6.151178205754315
Encrypted:	false
SSDEEP:	1536:lJbpyhknL27r0fjRl+oIueFKXg2h/DjBAaXHaVCp:P0hAL27r07R8XueFJ2/DjBAa3aVCp
MD5:	926A278BA2F85A59B073C64D1F4D4C7E
SHA1:	2FE9C201EAFA4B6F26F43CAA807B4150758870B8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6103b5b7f78f61b6_0	
SHA-256:	137621E5AA22D8A22CEFB53128025A8F106DCC6B3DDA6820145E57BEEF68FC53
SHA-512:	3E357642E1C907DCBF5872536FF48E40905AD1AEBCF1A580B27D0E548204FC2363492195D0828958A7AB81C083E3BCC3455AECD2CC79D115E7315CF1555F8B1
Malicious:	false
Reputation:	low
Preview:	.....'.....O.....z.....\.....T.....(.....(S.<..`4.....L`.....(S...`.....$L`.....Q.@".&.....exports...Q.@J9].....module....Q. @6.H.....define....Qb^"Y.....amd.....`.....M`.....!...Qb. .:.....self..Qc..;....window....K`....D{.....s.....s.....&.]....F...s.....&.(.....&.z..%&.^....."%.'.....&.(...'....~&.-...]..... (Rc.....I`....Da`..... ..f.....`..`..L.....@.-....<P.....0...https://www.qualtrics.com/m/homepage/gsap.min.jsa.....D`....D`2...D`.....Y....`....&...&....&.(S...]..`p$.....L`| ....Y.Rc.....QeN....._inheritsLoose...$Qg..t...._assertThisInitialized....Qb.3z2....n.....Qb>..h....o.....Qb&^.....p.....Qb.....q.....QbZydU....r.....Qb..K.....s.....Qbn. u.....t.....R....Qb.L.6....K.....Qb.Z-.....L.....Qb.....M.....Qb.y.U....N.....Qbj.....O.....Qb.b2J....Y.....Qb..5.....Z.....QbN....._.....Qb.l.G....aa....Qb..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\611664e4979d2859_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	242
Entropy (8bit):	5.594215068956902
Encrypted:	false
SSDEEP:	6:mGtVYD8/WS7Kk01jgBDFmloBB+Ntl/lnK6t:Dtu8/D5S4RrBB+Qn
MD5:	3C38FC9B18EBD86A800002E97D86189C
SHA1:	A1A589A869883E83C314215CEB4164B94921E343
SHA-256:	AD1E95604143F9870555AAB412C7921D1289D29B712FC1E8E45904FFAA4E809C
SHA-512:	854B4A2B2136B1CAF506AEEE7ED48F236F7B99E54242CDAA96F007EF4DFDE43A25EBE4F017320AB053F5B8D36079CAB493207DB29747E3E7963C147FA7F3C62 5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....n....!...._keyhttps://solve-widget.forethought.ai/npm.styled-components.625ba7f88591c28d1d1a.js .https://forethought.ai/:LI.i&/.....$.....Y=..(.+H..1e.mdl ..."H.1..3.mi.A..Eo.....J.....A..Eo.....

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
Jul 23, 2021 17:24:07.216331005 CEST	192.168.2.6	8.8.8.8	0xf695	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:07.216509104 CEST	192.168.2.6	8.8.8.8	0xbd43	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:07.223121881 CEST	192.168.2.6	8.8.8.8	0xe4f2	Standard query (0)	covid.census.gov	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:13.432615042 CEST	192.168.2.6	8.8.8.8	0x3186	Standard query (0)	www.qualtrics.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:14.679274082 CEST	192.168.2.6	8.8.8.8	0xb49e	Standard query (0)	g1-iad.qualtrics.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:14.797614098 CEST	192.168.2.6	8.8.8.8	0x8f2f	Standard query (0)	www-api.qualtrics.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:14.836215973 CEST	192.168.2.6	8.8.8.8	0xa914	Standard query (0)	success.qualtrics.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 23, 2021 17:24:14.993247032 CEST	192.168.2.6	8.8.8.8	0xe0f0	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:14.995959044 CEST	192.168.2.6	8.8.8.8	0xe605	Standard query (0)	consent.trustarc.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:15.090369940 CEST	192.168.2.6	8.8.8.8	0xc8cb	Standard query (0)	s3.amazonaws.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:16.042299032 CEST	192.168.2.6	8.8.8.8	0x7988	Standard query (0)	s.w.org	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:16.131867886 CEST	192.168.2.6	8.8.8.8	0xcb4a	Standard query (0)	qualtrics-www.s3.amazonaws.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:18.157418013 CEST	192.168.2.6	8.8.8.8	0xbc48	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:18.158921003 CEST	192.168.2.6	8.8.8.8	0xfb04	Standard query (0)	static.hotjar.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:18.163301945 CEST	192.168.2.6	8.8.8.8	0x3d8f	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:19.018646955 CEST	192.168.2.6	8.8.8.8	0x8acf	Standard query (0)	10784251.fls.doubleclick.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:19.022563934 CEST	192.168.2.6	8.8.8.8	0xf643	Standard query (0)	munchkin.marketo.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:19.024753094 CEST	192.168.2.6	8.8.8.8	0xc192	Standard query (0)	s.yimg.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:19.027074099 CEST	192.168.2.6	8.8.8.8	0x302f	Standard query (0)	extend.vimeocdn.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:19.030021906 CEST	192.168.2.6	8.8.8.8	0x740	Standard query (0)	intljs.rmtag.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:19.555660009 CEST	192.168.2.6	8.8.8.8	0x7996	Standard query (0)	j.6sc.co	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:19.566371918 CEST	192.168.2.6	8.8.8.8	0x6975	Standard query (0)	cdn.segment.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:19.569709063 CEST	192.168.2.6	8.8.8.8	0xac94	Standard query (0)	cdn.krxd.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:19.952100992 CEST	192.168.2.6	8.8.8.8	0x92d3	Standard query (0)	adservice.google.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.507575035 CEST	192.168.2.6	8.8.8.8	0xa0fa	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.508172035 CEST	192.168.2.6	8.8.8.8	0xf87a	Standard query (0)	analytics.google.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.511336088 CEST	192.168.2.6	8.8.8.8	0xd161	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.528820992 CEST	192.168.2.6	8.8.8.8	0x82dd	Standard query (0)	script.hotjar.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.529501915 CEST	192.168.2.6	8.8.8.8	0xfcb	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.577657938 CEST	192.168.2.6	8.8.8.8	0x17be	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.651093006 CEST	192.168.2.6	8.8.8.8	0x595e	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.772510052 CEST	192.168.2.6	8.8.8.8	0xa350	Standard query (0)	vars.hotjar.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.772600889 CEST	192.168.2.6	8.8.8.8	0xa19e	Standard query (0)	c.6sc.co	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.904388905 CEST	192.168.2.6	8.8.8.8	0xc54f	Standard query (0)	sp.analytics.yahoo.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.905970097 CEST	192.168.2.6	8.8.8.8	0xe3fc	Standard query (0)	b.6sc.co	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.906323910 CEST	192.168.2.6	8.8.8.8	0x6f5a	Standard query (0)	ut.ra.linksynergy.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.906682014 CEST	192.168.2.6	8.8.8.8	0x97c9	Standard query (0)	consent.linksynergy.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:21.114476919 CEST	192.168.2.6	8.8.8.8	0xd299	Standard query (0)	epsilon.6sense.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:21.219234943 CEST	192.168.2.6	8.8.8.8	0xd15c	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:21.220567942 CEST	192.168.2.6	8.8.8.8	0xab32	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:21.339191914 CEST	192.168.2.6	8.8.8.8	0x2c55	Standard query (0)	542-fmf-412.mktoresp.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:21.469170094 CEST	192.168.2.6	8.8.8.8	0xae68	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:22.423612118 CEST	192.168.2.6	8.8.8.8	0x27b8	Standard query (0)	consumer.krxd.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 23, 2021 17:24:22.573873997 CEST	192.168.2.6	8.8.8.8	0x8586	Standard query (0)	idsync.rlcdn.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:22.931005955 CEST	192.168.2.6	8.8.8.8	0x7bb1	Standard query (0)	api.segment.io	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:23.349499941 CEST	192.168.2.6	8.8.8.8	0x27fc	Standard query (0)	adservice.google.de	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:23.653173923 CEST	192.168.2.6	8.8.8.8	0xcbb5	Standard query (0)	www.qualtrics.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:23.669743061 CEST	192.168.2.6	8.8.8.8	0xd369	Standard query (0)	sp.analytics.yahoo.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.179724932 CEST	192.168.2.6	8.8.8.8	0x259f	Standard query (0)	usermatch.krxd.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.179797888 CEST	192.168.2.6	8.8.8.8	0x117e	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.179877996 CEST	192.168.2.6	8.8.8.8	0x70ce	Standard query (0)	beacon.krxd.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.208414078 CEST	192.168.2.6	8.8.8.8	0x3cf7	Standard query (0)	dpm.demdex.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.210005999 CEST	192.168.2.6	8.8.8.8	0x9c0	Standard query (0)	aa.agkn.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.214879990 CEST	192.168.2.6	8.8.8.8	0x8940	Standard query (0)	up.pixel.ad	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.217434883 CEST	192.168.2.6	8.8.8.8	0x6a89	Standard query (0)	fei.pro-market.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.542181969 CEST	192.168.2.6	8.8.8.8	0x8209	Standard query (0)	pixel.sitescout.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:26.083802938 CEST	192.168.2.6	8.8.8.8	0x9399	Standard query (0)	pixel-sync.sitescout.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:26.278939009 CEST	192.168.2.6	8.8.8.8	0xe281	Standard query (0)	pixel.tapad.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:26.280869007 CEST	192.168.2.6	8.8.8.8	0x982	Standard query (0)	loadm.exelator.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:26.281187057 CEST	192.168.2.6	8.8.8.8	0xb5f3	Standard query (0)	sync.teads.tv	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:26.282593966 CEST	192.168.2.6	8.8.8.8	0x7e98	Standard query (0)	bcp.crwdcntrl.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:26.762453079 CEST	192.168.2.6	8.8.8.8	0x6ff8	Standard query (0)	zn725dkxtvxq847sl-qxm.siteintercept.qualtrics.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:26.763200998 CEST	192.168.2.6	8.8.8.8	0xe424	Standard query (0)	js-agent.newrelic.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:27.037698030 CEST	192.168.2.6	8.8.8.8	0xae4a	Standard query (0)	bam.nr-data.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:27.047858000 CEST	192.168.2.6	8.8.8.8	0xfae0	Standard query (0)	siteintercept.qualtrics.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:27.914262056 CEST	192.168.2.6	8.8.8.8	0x60a4	Standard query (0)	dpm.demdex.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:27.919780016 CEST	192.168.2.6	8.8.8.8	0x46e	Standard query (0)	pixel.tapad.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:27.935858965 CEST	192.168.2.6	8.8.8.8	0x5618	Standard query (0)	loadm.exelator.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:27.958765030 CEST	192.168.2.6	8.8.8.8	0x6df3	Standard query (0)	sync.teads.tv	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:27.966327906 CEST	192.168.2.6	8.8.8.8	0x2d42	Standard query (0)	bcp.crwdcntrl.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:36.007586956 CEST	192.168.2.6	8.8.8.8	0xb0a0	Standard query (0)	login.qualtrics.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:36.643450022 CEST	192.168.2.6	8.8.8.8	0xd8a4	Standard query (0)	use.typekit.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:36.830760956 CEST	192.168.2.6	8.8.8.8	0x6c41	Standard query (0)	p.typekit.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:36.862277031 CEST	192.168.2.6	8.8.8.8	0xfa06	Standard query (0)	unpkg.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:36.868969917 CEST	192.168.2.6	8.8.8.8	0xf818	Standard query (0)	s.qualtrics.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:39.010169029 CEST	192.168.2.6	8.8.8.8	0xf634	Standard query (0)	login.qualtrics.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:39.070707083 CEST	192.168.2.6	8.8.8.8	0xa52c	Standard query (0)	sync.search.spotxchange.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:39.070921898 CEST	192.168.2.6	8.8.8.8	0x909d	Standard query (0)	tags.bluekai.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 23, 2021 17:24:39.071038008 CEST	192.168.2.6	8.8.8.8	0xa254	Standard query (0)	image2.pubmatic.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:39.075270891 CEST	192.168.2.6	8.8.8.8	0x52d	Standard query (0)	us-u.openx.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:39.479959011 CEST	192.168.2.6	8.8.8.8	0xa594	Standard query (0)	zncydxfem8jrupnsj-qwebsite.siteintercept.qualtrics.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:42.459944010 CEST	192.168.2.6	8.8.8.8	0x57f7	Standard query (0)	client-registry.mutinycdn.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:42.608392000 CEST	192.168.2.6	8.8.8.8	0x697f	Standard query (0)	solve-widget.forethought.ai	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:42.681157112 CEST	192.168.2.6	8.8.8.8	0xd058	Standard query (0)	user-data.mutinycdn.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:42.799474001 CEST	192.168.2.6	8.8.8.8	0xea96	Standard query (0)	cse.google.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.447434902 CEST	192.168.2.6	8.8.8.8	0xbd85	Standard query (0)	pixel.advertising.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.447577000 CEST	192.168.2.6	8.8.8.8	0x7ff6	Standard query (0)	su.addthis.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.447967052 CEST	192.168.2.6	8.8.8.8	0x53f5	Standard query (0)	ib.adnxs.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.448088884 CEST	192.168.2.6	8.8.8.8	0xd848	Standard query (0)	match.sharethrough.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.448323011 CEST	192.168.2.6	8.8.8.8	0xc977	Standard query (0)	ce.lijit.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.860620975 CEST	192.168.2.6	8.8.8.8	0xb519	Standard query (0)	client.mutinycdn.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:44.634792089 CEST	192.168.2.6	8.8.8.8	0x3ad	Standard query (0)	clients1.google.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:44.934055090 CEST	192.168.2.6	8.8.8.8	0xa328	Standard query (0)	cdn.lr-ingest.io	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:45.011322021 CEST	192.168.2.6	8.8.8.8	0x7d8c	Standard query (0)	o185886.ingest.sentry.io	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:45.409418106 CEST	192.168.2.6	8.8.8.8	0x1078	Standard query (0)	api-v2.mutinyhq.io	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:45.472182989 CEST	192.168.2.6	8.8.8.8	0x913b	Standard query (0)	api.forethought.ai	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:45.715554953 CEST	192.168.2.6	8.8.8.8	0xb2a7	Standard query (0)	ups.analytics.yahoo.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:46.349642992 CEST	192.168.2.6	8.8.8.8	0x59c0	Standard query (0)	solve-widget.forethought.ai	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:46.431628942 CEST	192.168.2.6	8.8.8.8	0xa839	Standard query (0)	zn85jou57xphaxsod-qxm.siteintercept.qualtrics.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:46.433993101 CEST	192.168.2.6	8.8.8.8	0x6847	Standard query (0)	zn5bvpdtma7urhqyn-qdigitalsupport.siteintercept.qualtrics.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:46.728586912 CEST	192.168.2.6	8.8.8.8	0x3d62	Standard query (0)	d3tnn7lar6ozas.cloudfront.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:47.603146076 CEST	192.168.2.6	8.8.8.8	0x8691	Standard query (0)	siteintercept.qualtrics.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:47.960094929 CEST	192.168.2.6	8.8.8.8	0x3662	Standard query (0)	www.qualtrics.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:48.713157892 CEST	192.168.2.6	8.8.8.8	0xc27a	Standard query (0)	s.w.org	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:49.843764067 CEST	192.168.2.6	8.8.8.8	0xb204	Standard query (0)	rtb-csync.smartadserver.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:49.844218016 CEST	192.168.2.6	8.8.8.8	0xe5c0	Standard query (0)	eb2.3lift.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:49.844749928 CEST	192.168.2.6	8.8.8.8	0xf16	Standard query (0)	bh.contextweb.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:49.845062017 CEST	192.168.2.6	8.8.8.8	0xac19	Standard query (0)	r.casalemedia.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:49.845251083 CEST	192.168.2.6	8.8.8.8	0x91a5	Standard query (0)	partners.tremorhub.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:50.350022078 CEST	192.168.2.6	8.8.8.8	0xd520	Standard query (0)	cdn.krxd.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 23, 2021 17:24:54.212968111 CEST	192.168.2.6	8.8.8.8	0x4fd4	Standard query (0)	tags.rd.linksynergy.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:54.301958084 CEST	192.168.2.6	8.8.8.8	0x57c2	Standard query (0)	cm.t.tailtarget.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:54.304058075 CEST	192.168.2.6	8.8.8.8	0xd962	Standard query (0)	c.deployads.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:54.306348085 CEST	192.168.2.6	8.8.8.8	0x62df	Standard query (0)	i.liadm.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:54.306893110 CEST	192.168.2.6	8.8.8.8	0x8a47	Standard query (0)	pixel.rubiconproject.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.052406073 CEST	192.168.2.6	8.8.8.8	0x3704	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.073283911 CEST	192.168.2.6	8.8.8.8	0x5272	Standard query (0)	d.agkn.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.358377934 CEST	192.168.2.6	8.8.8.8	0xee9a	Standard query (0)	match.adsrvr.org	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.358402967 CEST	192.168.2.6	8.8.8.8	0x45ea	Standard query (0)	insight.adsrvr.org	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.389271021 CEST	192.168.2.6	8.8.8.8	0xd909	Standard query (0)	9876505.fls.doubleclick.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:56.255825043 CEST	192.168.2.6	8.8.8.8	0xef7a	Standard query (0)	i6.liadm.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.984412909 CEST	192.168.2.6	8.8.8.8	0x90c2	Standard query (0)	match.adsrvr.org	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:57.995642900 CEST	192.168.2.6	8.8.8.8	0xdff5	Standard query (0)	idsync.rlcdn.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:58.003175020 CEST	192.168.2.6	8.8.8.8	0x95fb	Standard query (0)	insight.adsrvr.org	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:58.406908035 CEST	192.168.2.6	8.8.8.8	0x6092	Standard query (0)	tags.rd.linksynergy.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:00.828217983 CEST	192.168.2.6	8.8.8.8	0x9cda	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:00.829628944 CEST	192.168.2.6	8.8.8.8	0xc1d7	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:02.906191111 CEST	192.168.2.6	8.8.8.8	0xf599	Standard query (0)	player.vimeo.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:03.387480021 CEST	192.168.2.6	8.8.8.8	0x46c3	Standard query (0)	js.driftt.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:03.730185986 CEST	192.168.2.6	8.8.8.8	0x661c	Standard query (0)	consent.trustarc.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.585588932 CEST	192.168.2.6	8.8.8.8	0x399c	Standard query (0)	api.retargetly.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.588264942 CEST	192.168.2.6	8.8.8.8	0x3d6e	Standard query (0)	ads.stickyadstv.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.588917017 CEST	192.168.2.6	8.8.8.8	0xe11d	Standard query (0)	thrtle.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.589817047 CEST	192.168.2.6	8.8.8.8	0xc933	Standard query (0)	ssc-cms.33across.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.592422009 CEST	192.168.2.6	8.8.8.8	0xe011	Standard query (0)	i.vimeocdn.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.618684053 CEST	192.168.2.6	8.8.8.8	0xe0ed	Standard query (0)	f.vimeocdn.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.619191885 CEST	192.168.2.6	8.8.8.8	0x12b2	Standard query (0)	fresnel.vimeocdn.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.747704983 CEST	192.168.2.6	8.8.8.8	0xbefc	Standard query (0)	vimeo.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:05.065211058 CEST	192.168.2.6	8.8.8.8	0x9f25	Standard query (0)	player-telemetry.vimeo.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:05.509438038 CEST	192.168.2.6	8.8.8.8	0xd711	Standard query (0)	j.6sc.co	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:07.338040113 CEST	192.168.2.6	8.8.8.8	0xa6e	Standard query (0)	b.6sc.co	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:07.711940050 CEST	192.168.2.6	8.8.8.8	0x658f	Standard query (0)	customer.api.drift.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:07.712502003 CEST	192.168.2.6	8.8.8.8	0x5686	Standard query (0)	metrics.api.drift.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:07.712519884 CEST	192.168.2.6	8.8.8.8	0x4deb	Standard query (0)	conversation.api.drift.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:07.750565052 CEST	192.168.2.6	8.8.8.8	0x9f81	Standard query (0)	targeting.api.drift.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:08.488682032 CEST	192.168.2.6	8.8.8.8	0x66c5	Standard query (0)	sentry.io	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:13.223855019 CEST	192.168.2.6	8.8.8.8	0xe079	Standard query (0)	bootstrap.api.drift.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 23, 2021 17:25:13.888611078 CEST	192.168.2.6	8.8.8.8	0x9ace	Standard query (0)	embeds.driftcdn.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:14.118014097 CEST	192.168.2.6	8.8.8.8	0xcc2e	Standard query (0)	jadserve.postrelease.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:14.119714975 CEST	192.168.2.6	8.8.8.8	0x6155	Standard query (0)	public-prod-dspcookiematching.dmxleo.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:14.122217894 CEST	192.168.2.6	8.8.8.8	0x67f6	Standard query (0)	sync.1rx.io	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:14.123085976 CEST	192.168.2.6	8.8.8.8	0x76ff	Standard query (0)	sync.navdmp.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:14.124013901 CEST	192.168.2.6	8.8.8.8	0xaf8d	Standard query (0)	e1.emxdgt.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:14.267962933 CEST	192.168.2.6	8.8.8.8	0x8e65	Standard query (0)	certificates.godaddy.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:14.331608057 CEST	192.168.2.6	8.8.8.8	0x9abb	Standard query (0)	sync.targeting.unrulymedia.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:15.079907894 CEST	192.168.2.6	8.8.8.8	0x1df0	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:16.669410944 CEST	192.168.2.6	8.8.8.8	0xfc17	Standard query (0)	79332-32.chat.api.drift.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:16.672163010 CEST	192.168.2.6	8.8.8.8	0xf13f	Standard query (0)	presence.api.drift.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:16.854897976 CEST	192.168.2.6	8.8.8.8	0xa22c	Standard query (0)	event.api.drift.com	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:17.360019922 CEST	192.168.2.6	8.8.8.8	0x5aff	Standard query (0)	flow.api.drift.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:07.250130892 CEST	8.8.8.8	192.168.2.6	0xbd43	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:07.252125025 CEST	8.8.8.8	192.168.2.6	0xf695	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:07.252125025 CEST	8.8.8.8	192.168.2.6	0xf695	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:07.374072075 CEST	8.8.8.8	192.168.2.6	0xe4f2	No error (0)	covid.census.gov	uscensusbureaucovid.vanity6.gov1.qualtrics.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:07.374072075 CEST	8.8.8.8	192.168.2.6	0xe4f2	No error (0)	uscensusbureaucovid.vanity6.gov1.qualtrics.com	akamaisecure6.qualtrics.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:13.470300913 CEST	8.8.8.8	192.168.2.6	0x3186	No error (0)	www.qualtrics.com	cloudenhanced.qualtrics.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:14.716766119 CEST	8.8.8.8	192.168.2.6	0xb49e	No error (0)	g1-iad.qualtrics.com	cloudenhanced.qualtrics.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:14.836036921 CEST	8.8.8.8	192.168.2.6	0x8f2f	No error (0)	www-api.qualtrics.com	cloudenhanced.qualtrics.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:14.961879015 CEST	8.8.8.8	192.168.2.6	0xa914	No error (0)	success.qualtrics.com	qualtrics.mktoweb.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:14.961879015 CEST	8.8.8.8	192.168.2.6	0xa914	No error (0)	qualtrics.mktoweb.com	sjp.mktossl.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:14.961879015 CEST	8.8.8.8	192.168.2.6	0xa914	No error (0)	sjp.mktossl.com		104.17.70.206	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:14.961879015 CEST	8.8.8.8	192.168.2.6	0xa914	No error (0)	sjp.mktossl.com		104.17.72.206	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:14.961879015 CEST	8.8.8.8	192.168.2.6	0xa914	No error (0)	sjp.mktossl.com		104.17.73.206	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:14.961879015 CEST	8.8.8.8	192.168.2.6	0xa914	No error (0)	sjp.mktossl.com		104.17.74.206	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:14.961879015 CEST	8.8.8.8	192.168.2.6	0xa914	No error (0)	sjp.mktossl.com		104.17.71.206	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:15.021686077 CEST	8.8.8.8	192.168.2.6	0xe0f0	No error (0)	cdn.jsdelivr.net	jsdelivr.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:15.021686077 CEST	8.8.8.8	192.168.2.6	0xe0f0	No error (0)	jsdelivr.map.fastly.net		151.101.1.229	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:15.021686077 CEST	8.8.8.8	192.168.2.6	0xe0f0	No error (0)	jsdelivr.map.fastly.net		151.101.65.229	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:15.021686077 CEST	8.8.8.8	192.168.2.6	0xe0f0	No error (0)	jsdelivr.map.fastly.net		151.101.129.229	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:15.021686077 CEST	8.8.8.8	192.168.2.6	0xe0f0	No error (0)	jsdelivr.map.fastly.net		151.101.193.229	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:15.031322956 CEST	8.8.8.8	192.168.2.6	0xe605	No error (0)	consent.trustarc.com		52.222.174.42	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:15.031322956 CEST	8.8.8.8	192.168.2.6	0xe605	No error (0)	consent.trustarc.com		52.222.174.125	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:15.031322956 CEST	8.8.8.8	192.168.2.6	0xe605	No error (0)	consent.trustarc.com		52.222.174.74	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:15.031322956 CEST	8.8.8.8	192.168.2.6	0xe605	No error (0)	consent.trustarc.com		52.222.174.69	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:15.039719105 CEST	8.8.8.8	192.168.2.6	0x8a9c	No error (0)	www-google tagmanager.l.google.com		172.217.168.8	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:15.118423939 CEST	8.8.8.8	192.168.2.6	0xc8cb	No error (0)	s3.amazonaws.com		52.217.64.246	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:16.068099976 CEST	8.8.8.8	192.168.2.6	0x7988	No error (0)	s.w.org		192.0.77.48	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:16.166424036 CEST	8.8.8.8	192.168.2.6	0xcb4a	No error (0)	qualtrics-www.s3.amazonaws.com	s3-1-w.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:16.166424036 CEST	8.8.8.8	192.168.2.6	0xcb4a	No error (0)	s3-1-w.amazonaws.com	s3-w.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:16.166424036 CEST	8.8.8.8	192.168.2.6	0xcb4a	No error (0)	s3-w.us-east-1.amazonaws.com		52.217.18.236	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:18.186033010 CEST	8.8.8.8	192.168.2.6	0x1c3d	No error (0)	www-google-analytics.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:18.192183971 CEST	8.8.8.8	192.168.2.6	0xbc48	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:18.192183971 CEST	8.8.8.8	192.168.2.6	0xbc48	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:18.197654963 CEST	8.8.8.8	192.168.2.6	0x3d8f	No error (0)	snap.licdn.com	wildcard.licdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:18.198288918 CEST	8.8.8.8	192.168.2.6	0xfb04	No error (0)	static.hotjar.com	static-cdn.hotjar.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:18.198288918 CEST	8.8.8.8	192.168.2.6	0xfb04	No error (0)	static-cdn.hotjar.com		52.222.174.118	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:18.198288918 CEST	8.8.8.8	192.168.2.6	0xfb04	No error (0)	static-cdn.hotjar.com		52.222.174.67	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:18.198288918 CEST	8.8.8.8	192.168.2.6	0xfb04	No error (0)	static-cdn.hotjar.com		52.222.174.96	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:18.198288918 CEST	8.8.8.8	192.168.2.6	0xfb04	No error (0)	static-cdn.hotjar.com		52.222.174.124	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:19.050174952 CEST	8.8.8.8	192.168.2.6	0xc192	No error (0)	s.yimg.com	edge.gycpi.b.yahoodns.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:19.050174952 CEST	8.8.8.8	192.168.2.6	0xc192	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.23	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:19.050174952 CEST	8.8.8.8	192.168.2.6	0xc192	No error (0)	edge.gycpi.b.yahoodns.net		87.248.118.22	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:19.060277939 CEST	8.8.8.8	192.168.2.6	0xf643	No error (0)	munchkin.marketo.net	wildcard.marketo.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:19.061419010 CEST	8.8.8.8	192.168.2.6	0x302f	No error (0)	extend.vimeocdn.com	vimeo-video.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:19.061419010 CEST	8.8.8.8	192.168.2.6	0x302f	No error (0)	vimeo-video.map.fastly.net		151.101.114.109	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:19.062385082 CEST	8.8.8.8	192.168.2.6	0x8acf	No error (0)	10784251.fls.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:19.062385082 CEST	8.8.8.8	192.168.2.6	0x8acf	No error (0)	dart.l.doubleclick.net		216.58.215.230	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:19.064100981 CEST	8.8.8.8	192.168.2.6	0x740	No error (0)	intljs.rmtag.com		34.102.147.248	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:19.593832970 CEST	8.8.8.8	192.168.2.6	0x7996	No error (0)	j.6sc.co	j.6sc.co.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:19.603790045 CEST	8.8.8.8	192.168.2.6	0xac94	No error (0)	cdn.krxd.net	d.sni.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:19.605523109 CEST	8.8.8.8	192.168.2.6	0x6975	No error (0)	cdn.segment.com	d296je7bbdd650.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:19.605523109 CEST	8.8.8.8	192.168.2.6	0x6975	No error (0)	d296je7bbdd650.cloudfront.net		52.84.178.125	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:19.986383915 CEST	8.8.8.8	192.168.2.6	0x92d3	No error (0)	adservice.google.com		172.217.168.2	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.543541908 CEST	8.8.8.8	192.168.2.6	0xf87a	No error (0)	analytics.google.com	www3.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:20.543541908 CEST	8.8.8.8	192.168.2.6	0xf87a	No error (0)	www3.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.545592070 CEST	8.8.8.8	192.168.2.6	0xd161	No error (0)	www.google.de		172.217.168.3	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.554004908 CEST	8.8.8.8	192.168.2.6	0xa0fa	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:20.554004908 CEST	8.8.8.8	192.168.2.6	0xa0fa	No error (0)	stats.l.doubleclick.net		108.177.126.155	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.554004908 CEST	8.8.8.8	192.168.2.6	0xa0fa	No error (0)	stats.l.doubleclick.net		108.177.126.156	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.554004908 CEST	8.8.8.8	192.168.2.6	0xa0fa	No error (0)	stats.l.doubleclick.net		108.177.126.154	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.554004908 CEST	8.8.8.8	192.168.2.6	0xa0fa	No error (0)	stats.l.doubleclick.net		108.177.126.157	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.563288927 CEST	8.8.8.8	192.168.2.6	0xfcb	No error (0)	px.ads.linkedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:20.563288927 CEST	8.8.8.8	192.168.2.6	0xfcb	No error (0)	mix.linkedin.com	glb-na.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:20.563288927 CEST	8.8.8.8	192.168.2.6	0xfcb	No error (0)	glb-na.mix.linkedin.com	pop-esv5.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:20.563288927 CEST	8.8.8.8	192.168.2.6	0xfcb	No error (0)	pop-esv5.mix.linkedin.com		108.174.11.37	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.567282915 CEST	8.8.8.8	192.168.2.6	0x82dd	No error (0)	script.hotjar.com		52.84.174.19	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:20.567282915 CEST	8.8.8.8	192.168.2.6	0x82dd	No error (0)	script.hotjar.com		52.84.174.14	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.567282915 CEST	8.8.8.8	192.168.2.6	0x82dd	No error (0)	script.hotjar.com		52.84.174.78	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.567282915 CEST	8.8.8.8	192.168.2.6	0x82dd	No error (0)	script.hotjar.com		52.84.174.89	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.602514982 CEST	8.8.8.8	192.168.2.6	0x17be	No error (0)	googleads.g.doubleclick.net		172.217.168.66	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.692521095 CEST	8.8.8.8	192.168.2.6	0x595e	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:20.692521095 CEST	8.8.8.8	192.168.2.6	0x595e	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.809680939 CEST	8.8.8.8	192.168.2.6	0xa19e	No error (0)	c.6sc.co	c.6sc.co.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:20.813338995 CEST	8.8.8.8	192.168.2.6	0xa350	No error (0)	vars.hotjar.com		52.84.174.22	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.813338995 CEST	8.8.8.8	192.168.2.6	0xa350	No error (0)	vars.hotjar.com		52.84.174.96	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.813338995 CEST	8.8.8.8	192.168.2.6	0xa350	No error (0)	vars.hotjar.com		52.84.174.118	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.813338995 CEST	8.8.8.8	192.168.2.6	0xa350	No error (0)	vars.hotjar.com		52.84.174.120	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.932269096 CEST	8.8.8.8	192.168.2.6	0xc54f	No error (0)	sp.analytics.yahoo.com	spdc-global.pbp.gysm.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:20.932269096 CEST	8.8.8.8	192.168.2.6	0xc54f	No error (0)	spdc-global.pbp.gysm.yahoodns.net		212.82.100.181	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.938761950 CEST	8.8.8.8	192.168.2.6	0x6f5a	No error (0)	ut.ra.linksynergy.com		35.241.23.116	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.939064026 CEST	8.8.8.8	192.168.2.6	0x97c9	No error (0)	consent.linksynergy.com		35.241.23.116	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:20.941723108 CEST	8.8.8.8	192.168.2.6	0xe3fc	No error (0)	b.6sc.co	b.6sc.co.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:21.153446913 CEST	8.8.8.8	192.168.2.6	0xd299	No error (0)	epsilon.6sense.com		3.65.155.204	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:21.153446913 CEST	8.8.8.8	192.168.2.6	0xd299	No error (0)	epsilon.6sense.com		54.93.136.75	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:21.249583006 CEST	8.8.8.8	192.168.2.6	0xab32	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:21.254060984 CEST	8.8.8.8	192.168.2.6	0xd15c	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:21.254060984 CEST	8.8.8.8	192.168.2.6	0xd15c	No error (0)	star-mini.c10r.facebook.com		157.240.17.35	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:21.372519016 CEST	8.8.8.8	192.168.2.6	0x2c55	No error (0)	542-fmf-412.mktoresp.com		192.28.147.68	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:21.494368076 CEST	8.8.8.8	192.168.2.6	0xae68	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:22.460298061 CEST	8.8.8.8	192.168.2.6	0x27b8	No error (0)	consumer.krxd.net	d.sni.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:22.610194921 CEST	8.8.8.8	192.168.2.6	0x8586	No error (0)	idsync.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:22.958729982 CEST	8.8.8.8	192.168.2.6	0x7bb1	No error (0)	api.segment.io		52.38.120.169	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:22.958729982 CEST	8.8.8.8	192.168.2.6	0x7bb1	No error (0)	api.segment.io		44.225.192.231	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:22.958729982 CEST	8.8.8.8	192.168.2.6	0x7bb1	No error (0)	api.segment.io		52.88.208.102	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:22.958729982 CEST	8.8.8.8	192.168.2.6	0x7bb1	No error (0)	api.segment.io		52.89.95.104	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:22.958729982 CEST	8.8.8.8	192.168.2.6	0x7bb1	No error (0)	api.segment.io		52.38.215.191	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:22.958729982 CEST	8.8.8.8	192.168.2.6	0x7bb1	No error (0)	api.segment.io		52.39.24.11	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:22.958729982 CEST	8.8.8.8	192.168.2.6	0x7bb1	No error (0)	api.segment.io		54.69.177.146	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:22.958729982 CEST	8.8.8.8	192.168.2.6	0x7bb1	No error (0)	api.segment.io		52.43.10.86	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:23.390820026 CEST	8.8.8.8	192.168.2.6	0x27fc	No error (0)	adservice.google.de	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:23.390820026 CEST	8.8.8.8	192.168.2.6	0x27fc	No error (0)	pagead46.l.doubleclick.net		142.250.203.98	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:23.690254927 CEST	8.8.8.8	192.168.2.6	0xcbb5	No error (0)	www.qualtrics.com	cloudenhanced.qualtrics.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:23.701280117 CEST	8.8.8.8	192.168.2.6	0xd369	No error (0)	sp.analytics.yahoo.com	spdc-global.pbp.gysm.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:23.701280117 CEST	8.8.8.8	192.168.2.6	0xd369	No error (0)	spdc-global.pbp.gysm.yahoodns.net		212.82.100.181	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.207596064 CEST	8.8.8.8	192.168.2.6	0x70ce	No error (0)	beacon.krxd.net	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:25.207596064 CEST	8.8.8.8	192.168.2.6	0x70ce	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		34.246.41.247	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.207596064 CEST	8.8.8.8	192.168.2.6	0x70ce	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		54.72.233.167	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.207596064 CEST	8.8.8.8	192.168.2.6	0x70ce	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		54.154.117.125	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.207596064 CEST	8.8.8.8	192.168.2.6	0x70ce	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		34.243.105.17	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.207596064 CEST	8.8.8.8	192.168.2.6	0x70ce	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		52.50.226.72	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.207596064 CEST	8.8.8.8	192.168.2.6	0x70ce	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		52.215.215.228	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.207596064 CEST	8.8.8.8	192.168.2.6	0x70ce	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		52.48.45.204	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:25.207596064 CEST	8.8.8.8	192.168.2.6	0x70ce	No error (0)	prod-dub-beacon-1484770602.eu-west-1.elb.amazonaws.com		54.72.232.11	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.212475061 CEST	8.8.8.8	192.168.2.6	0x259f	No error (0)	usermatch.krxd.net	prod-ash-usermatch-1919559762.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:25.212475061 CEST	8.8.8.8	192.168.2.6	0x259f	No error (0)	prod-ash-usermatch-1919559762.us-east-1.elb.amazonaws.com		34.236.226.59	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.212475061 CEST	8.8.8.8	192.168.2.6	0x259f	No error (0)	prod-ash-usermatch-1919559762.us-east-1.elb.amazonaws.com		52.0.135.151	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.212475061 CEST	8.8.8.8	192.168.2.6	0x259f	No error (0)	prod-ash-usermatch-1919559762.us-east-1.elb.amazonaws.com		34.237.161.69	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.212475061 CEST	8.8.8.8	192.168.2.6	0x259f	No error (0)	prod-ash-usermatch-1919559762.us-east-1.elb.amazonaws.com		107.21.231.45	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.212475061 CEST	8.8.8.8	192.168.2.6	0x259f	No error (0)	prod-ash-usermatch-1919559762.us-east-1.elb.amazonaws.com		3.226.4.120	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.212475061 CEST	8.8.8.8	192.168.2.6	0x259f	No error (0)	prod-ash-usermatch-1919559762.us-east-1.elb.amazonaws.com		54.90.48.240	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.212475061 CEST	8.8.8.8	192.168.2.6	0x259f	No error (0)	prod-ash-usermatch-1919559762.us-east-1.elb.amazonaws.com		3.216.128.157	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.212475061 CEST	8.8.8.8	192.168.2.6	0x259f	No error (0)	prod-ash-usermatch-1919559762.us-east-1.elb.amazonaws.com		18.210.140.68	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.212928057 CEST	8.8.8.8	192.168.2.6	0x117e	No error (0)	cm.g.doubleclick.net		172.217.168.34	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.237875938 CEST	8.8.8.8	192.168.2.6	0x9c0	No error (0)	aa.agkn.com	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:25.237875938 CEST	8.8.8.8	192.168.2.6	0x9c0	No error (0)	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		3.10.35.49	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.237875938 CEST	8.8.8.8	192.168.2.6	0x9c0	No error (0)	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		3.8.243.222	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.237875938 CEST	8.8.8.8	192.168.2.6	0x9c0	No error (0)	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		3.11.29.5	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:25.237875938 CEST	8.8.8.8	192.168.2.6	0x9c0	No error (0)	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		18.169.236.234	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.241044044 CEST	8.8.8.8	192.168.2.6	0x3cf7	No error (0)	dpm.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:25.241044044 CEST	8.8.8.8	192.168.2.6	0x3cf7	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:25.241044044 CEST	8.8.8.8	192.168.2.6	0x3cf7	No error (0)	edge-irl1.demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:25.241044044 CEST	8.8.8.8	192.168.2.6	0x3cf7	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		63.32.159.255	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.241044044 CEST	8.8.8.8	192.168.2.6	0x3cf7	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.240.90.211	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.241044044 CEST	8.8.8.8	192.168.2.6	0x3cf7	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		3.250.252.43	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.241044044 CEST	8.8.8.8	192.168.2.6	0x3cf7	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.16.73.168	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.241044044 CEST	8.8.8.8	192.168.2.6	0x3cf7	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.30.200.197	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.241044044 CEST	8.8.8.8	192.168.2.6	0x3cf7	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.17.54.18	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.241044044 CEST	8.8.8.8	192.168.2.6	0x3cf7	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.214.168.199	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.241044044 CEST	8.8.8.8	192.168.2.6	0x3cf7	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.211.62.226	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.248738050 CEST	8.8.8.8	192.168.2.6	0x8940	No error (0)	up.pixel.ad	centro.vo.llnwd.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:25.248738050 CEST	8.8.8.8	192.168.2.6	0x8940	No error (0)	centro.vo.llnwd.net		178.79.242.16	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.248738050 CEST	8.8.8.8	192.168.2.6	0x8940	No error (0)	centro.vo.llnwd.net		178.79.242.181	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.249900103 CEST	8.8.8.8	192.168.2.6	0x6a89	No error (0)	fei.pro-market.net		107.178.240.89	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:25.580471039 CEST	8.8.8.8	192.168.2.6	0x8209	No error (0)	pixel.sitescout.com		66.155.71.149	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:26.119410992 CEST	8.8.8.8	192.168.2.6	0x9399	No error (0)	pixel-sync.sitescout.com	pixel-a.sitescout.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:26.119410992 CEST	8.8.8.8	192.168.2.6	0x9399	No error (0)	pixel-a.sitescout.com		66.155.71.25	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:26.319345951 CEST	8.8.8.8	192.168.2.6	0x982	No error (0)	loadm.exelator.com	loadus.tm.ssl.exelator.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:26.319345951 CEST	8.8.8.8	192.168.2.6	0x982	No error (0)	loadus.tm.ssl.exelator.com	eu-west.load.exelator.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:26.319345951 CEST	8.8.8.8	192.168.2.6	0x982	No error (0)	eu-west.load.exelator.com	load-euw1.exelator.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:26.319345951 CEST	8.8.8.8	192.168.2.6	0x982	No error (0)	load-euw1.exelator.com		54.78.254.47	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:26.319371939 CEST	8.8.8.8	192.168.2.6	0xb5f3	No error (0)	sync.teads.tv	sync.teads.tv.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:26.319390059 CEST	8.8.8.8	192.168.2.6	0xe281	No error (0)	pixel.tapad.com		35.227.248.159	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:26.325958014 CEST	8.8.8.8	192.168.2.6	0x7e98	No error (0)	bcp.crwdcntrl.net		34.251.130.56	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:26.325958014 CEST	8.8.8.8	192.168.2.6	0x7e98	No error (0)	bcp.crwdcntrl.net		52.48.248.240	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:26.325958014 CEST	8.8.8.8	192.168.2.6	0x7e98	No error (0)	bcp.crwdcntrl.net		52.208.103.128	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:26.325958014 CEST	8.8.8.8	192.168.2.6	0x7e98	No error (0)	bcp.crwdcntrl.net		52.48.137.92	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:26.325958014 CEST	8.8.8.8	192.168.2.6	0x7e98	No error (0)	bcp.crwdcntrl.net		34.253.111.115	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:26.325958014 CEST	8.8.8.8	192.168.2.6	0x7e98	No error (0)	bcp.crwdcntrl.net		54.194.226.253	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:26.325958014 CEST	8.8.8.8	192.168.2.6	0x7e98	No error (0)	bcp.crwdcntrl.net		52.30.140.199	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:26.325958014 CEST	8.8.8.8	192.168.2.6	0x7e98	No error (0)	bcp.crwdcntrl.net		52.30.14.23	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:26.799009085 CEST	8.8.8.8	192.168.2.6	0xe424	No error (0)	js-agent.newrelic.com	newrelic.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:26.799009085 CEST	8.8.8.8	192.168.2.6	0xe424	No error (0)	newrelic.map.fastly.net		151.101.1.27	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:26.799009085 CEST	8.8.8.8	192.168.2.6	0xe424	No error (0)	newrelic.map.fastly.net		151.101.65.27	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:26.799009085 CEST	8.8.8.8	192.168.2.6	0xe424	No error (0)	newrelic.map.fastly.net		151.101.129.27	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:26.799009085 CEST	8.8.8.8	192.168.2.6	0xe424	No error (0)	newrelic.map.fastly.net		151.101.193.27	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:26.799757004 CEST	8.8.8.8	192.168.2.6	0x6ff8	No error (0)	zn725dkxtvxq847sl-qxm.siteintercept.qualtrics.com	siteintercept.qprod2.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:26.799757004 CEST	8.8.8.8	192.168.2.6	0x6ff8	No error (0)	siteintercept.qprod2.net	prodlb.siteintercept.qualtrics.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:27.062695980 CEST	8.8.8.8	192.168.2.6	0xae4a	No error (0)	bam.nr-data.net		162.247.242.21	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:27.062695980 CEST	8.8.8.8	192.168.2.6	0xae4a	No error (0)	bam.nr-data.net		162.247.242.20	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:27.062695980 CEST	8.8.8.8	192.168.2.6	0xae4a	No error (0)	bam.nr-data.net		162.247.242.19	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:27.062695980 CEST	8.8.8.8	192.168.2.6	0xae4a	No error (0)	bam.nr-data.net		162.247.242.18	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:27.081767082 CEST	8.8.8.8	192.168.2.6	0xfae0	No error (0)	siteintercept.qualtrics.com	siteintercept.qprod2.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:27.081767082 CEST	8.8.8.8	192.168.2.6	0xfae0	No error (0)	siteintercept.qprod2.net	prodlb.siteintercept.qualtrics.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:27.949775934 CEST	8.8.8.8	192.168.2.6	0x60a4	No error (0)	dpm.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:27.949775934 CEST	8.8.8.8	192.168.2.6	0x60a4	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:27.949775934 CEST	8.8.8.8	192.168.2.6	0x60a4	No error (0)	edge-irl1.demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:27.949775934 CEST	8.8.8.8	192.168.2.6	0x60a4	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		63.32.159.255	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:27.949775934 CEST	8.8.8.8	192.168.2.6	0x60a4	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.240.90.211	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:27.949775934 CEST	8.8.8.8	192.168.2.6	0x60a4	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		3.250.252.43	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:27.949775934 CEST	8.8.8.8	192.168.2.6	0x60a4	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.16.73.168	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:27.949775934 CEST	8.8.8.8	192.168.2.6	0x60a4	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.30.200.197	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:27.949775934 CEST	8.8.8.8	192.168.2.6	0x60a4	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.17.54.18	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:27.949775934 CEST	8.8.8.8	192.168.2.6	0x60a4	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.214.168.199	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:27.949775934 CEST	8.8.8.8	192.168.2.6	0x60a4	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.211.62.226	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:27.956231117 CEST	8.8.8.8	192.168.2.6	0x46e	No error (0)	pixel.tapad.com		35.227.248.159	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:27.970688105 CEST	8.8.8.8	192.168.2.6	0x5618	No error (0)	loadm.exelator.com	loadus.tm.ssl.exelator.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:27.970688105 CEST	8.8.8.8	192.168.2.6	0x5618	No error (0)	loadus.tm.ssl.exelator.com	eu-west.load.exelator.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:27.970688105 CEST	8.8.8.8	192.168.2.6	0x5618	No error (0)	eu-west.load.exelator.com	load-euw1.exelator.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:27.970688105 CEST	8.8.8.8	192.168.2.6	0x5618	No error (0)	load-euw1.exelator.com		54.78.254.47	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:27.991636992 CEST	8.8.8.8	192.168.2.6	0x6df3	No error (0)	sync.teads.tv	sync.teads.tv.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:28.000842094 CEST	8.8.8.8	192.168.2.6	0x2d42	No error (0)	bcp.crwdcntrl.net		34.251.130.56	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:28.000842094 CEST	8.8.8.8	192.168.2.6	0x2d42	No error (0)	bcp.crwdcntrl.net		52.48.248.240	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:28.000842094 CEST	8.8.8.8	192.168.2.6	0x2d42	No error (0)	bcp.crwdcntrl.net		52.208.103.128	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:28.000842094 CEST	8.8.8.8	192.168.2.6	0x2d42	No error (0)	bcp.crwdcntrl.net		52.48.137.92	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:28.000842094 CEST	8.8.8.8	192.168.2.6	0x2d42	No error (0)	bcp.crwdcntrl.net		34.253.109.165	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:28.000842094 CEST	8.8.8.8	192.168.2.6	0x2d42	No error (0)	bcp.crwdcntrl.net		52.30.140.199	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:28.000842094 CEST	8.8.8.8	192.168.2.6	0x2d42	No error (0)	bcp.crwdcntrl.net		34.253.111.115	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:28.000842094 CEST	8.8.8.8	192.168.2.6	0x2d42	No error (0)	bcp.crwdcntrl.net		54.194.226.253	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:36.057650089 CEST	8.8.8.8	192.168.2.6	0xb0a0	No error (0)	login.qualtrics.com	cloudenhanced.qualtrics.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:36.677629948 CEST	8.8.8.8	192.168.2.6	0xd8a4	No error (0)	use.typekit.net	use-stls.adobe.com.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:36.865190983 CEST	8.8.8.8	192.168.2.6	0x6c41	No error (0)	p.typekit.net	p.typekit.net-v3.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:36.901377916 CEST	8.8.8.8	192.168.2.6	0xfa06	No error (0)	unpkg.com		104.16.126.175	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:36.901377916 CEST	8.8.8.8	192.168.2.6	0xfa06	No error (0)	unpkg.com		104.16.125.175	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:36.901377916 CEST	8.8.8.8	192.168.2.6	0xfa06	No error (0)	unpkg.com		104.16.122.175	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:36.901377916 CEST	8.8.8.8	192.168.2.6	0xfa06	No error (0)	unpkg.com		104.16.124.175	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:36.901377916 CEST	8.8.8.8	192.168.2.6	0xfa06	No error (0)	unpkg.com		104.16.123.175	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:36.904903889 CEST	8.8.8.8	192.168.2.6	0xf818	No error (0)	s.qualtrics.com	cloudenhanced.qualtrics.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:39.049036980 CEST	8.8.8.8	192.168.2.6	0xf634	No error (0)	login.qualtrics.com	cloudenhanced.qualtrics.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:39.095841885 CEST	8.8.8.8	192.168.2.6	0xa254	No error (0)	image2.pubmatic.com	pug-lhrc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:39.095841885 CEST	8.8.8.8	192.168.2.6	0xa254	No error (0)	pug-lhrc.pubmatic.com	pug-lhr.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:39.095841885 CEST	8.8.8.8	192.168.2.6	0xa254	No error (0)	pug-lhr.pubmatic.com		185.64.190.80	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:39.096122026 CEST	8.8.8.8	192.168.2.6	0xa52c	No error (0)	sync.search.spotxchange.com	sync.search-gtm.spotxchange.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:39.096122026 CEST	8.8.8.8	192.168.2.6	0xa52c	No error (0)	ams01.sync.search.spotxchange.com		185.94.180.126	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:39.096122026 CEST	8.8.8.8	192.168.2.6	0xa52c	No error (0)	ams01.sync.search.spotxchange.com		185.94.180.125	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:39.100379944 CEST	8.8.8.8	192.168.2.6	0x52d	No error (0)	us-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:39.100379944 CEST	8.8.8.8	192.168.2.6	0x52d	No error (0)	us-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:39.105604887 CEST	8.8.8.8	192.168.2.6	0x909d	No error (0)	tags.bluekai.com	tags.bluekai.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:39.515980959 CEST	8.8.8.8	192.168.2.6	0xa594	No error (0)	zncydxfem8jrupnsj-qwebsite.siteintercept.qualtrics.com	siteintercept.qprod2.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:39.515980959 CEST	8.8.8.8	192.168.2.6	0xa594	No error (0)	siteintercept.qprod2.net	prodlb.siteintercept.qualtrics.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:42.494949102 CEST	8.8.8.8	192.168.2.6	0x57f7	No error (0)	client-registry.mutinycdn.com	c3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:42.644229889 CEST	8.8.8.8	192.168.2.6	0x697f	No error (0)	solve-widget.forethought.ai		104.17.177.49	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:42.644229889 CEST	8.8.8.8	192.168.2.6	0x697f	No error (0)	solve-widget.forethought.ai		104.18.223.46	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:42.717977047 CEST	8.8.8.8	192.168.2.6	0xd058	No error (0)	user-data.mutinycdn.com	c3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:42.840327978 CEST	8.8.8.8	192.168.2.6	0xea96	No error (0)	cse.google.com		142.250.203.110	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:43.472343922 CEST	8.8.8.8	192.168.2.6	0xbd85	No error (0)	pixel.advertising.com	prod.ups-adcom.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:43.472343922 CEST	8.8.8.8	192.168.2.6	0xbd85	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)
Jul 23, 2021 17:24:43.472343922 CEST	8.8.8.8	192.168.2.6	0xbd85	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.184.153.186	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.472343922 CEST	8.8.8.8	192.168.2.6	0xbd85	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.159.140.98	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.472343922 CEST	8.8.8.8	192.168.2.6	0xbd85	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		52.59.28.101	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.472343922 CEST	8.8.8.8	192.168.2.6	0xbd85	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		52.57.10.248	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.472343922 CEST	8.8.8.8	192.168.2.6	0xbd85	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		35.156.153.71	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.472343922 CEST	8.8.8.8	192.168.2.6	0xbd85	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		52.59.102.119	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.472343922 CEST	8.8.8.8	192.168.2.6	0xbd85	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		18.185.160.211	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.472343922 CEST	8.8.8.8	192.168.2.6	0xbd85	No error (0)	prod.ups-eu-central-1.aolp-ds-prd.aws.oath.cloud		52.28.254.214	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.474656105 CEST	8.8.8.8	192.168.2.6	0xc977	No error (0)	ce.lijit.com	vap.lijit.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:43.474656105 CEST	8.8.8.8	192.168.2.6	0xc977	No error (0)	vap.lijit.com	emeas.vap.lijit.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:43.474656105 CEST	8.8.8.8	192.168.2.6	0xc977	No error (0)	emeas.vap.lijit.com	oeu.vap.lijit.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:43.474656105 CEST	8.8.8.8	192.168.2.6	0xc977	No error (0)	oeu.vap.lijit.com		72.251.249.14	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.474656105 CEST	8.8.8.8	192.168.2.6	0xc977	No error (0)	oeu.vap.lijit.com		216.52.2.30	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.474656105 CEST	8.8.8.8	192.168.2.6	0xc977	No error (0)	oeu.vap.lijit.com		216.52.2.19	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.474656105 CEST	8.8.8.8	192.168.2.6	0xc977	No error (0)	oeu.vap.lijit.com		216.52.2.39	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.474656105 CEST	8.8.8.8	192.168.2.6	0xc977	No error (0)	oeu.vap.lijit.com		216.52.2.48	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.474656105 CEST	8.8.8.8	192.168.2.6	0xc977	No error (0)	oeu.vap.lijit.com		72.251.249.9	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.474656105 CEST	8.8.8.8	192.168.2.6	0xc977	No error (0)	oeu.vap.lijit.com		72.251.249.13	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.474684954 CEST	8.8.8.8	192.168.2.6	0x53f5	No error (0)	ib.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:43.474684954 CEST	8.8.8.8	192.168.2.6	0x53f5	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:43.474684954 CEST	8.8.8.8	192.168.2.6	0x53f5	No error (0)	ib.anycast.adnxs.com		37.252.173.62	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:43.474684954 CEST	8.8.8.8	192.168.2.6	0x53f5	No error (0)	ib.anycast.adnxs.com		37.252.172.250	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.474684954 CEST	8.8.8.8	192.168.2.6	0x53f5	No error (0)	ib.anycast.adnxs.com		37.252.172.249	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.474684954 CEST	8.8.8.8	192.168.2.6	0x53f5	No error (0)	ib.anycast.adnxs.com		37.252.172.45	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.474684954 CEST	8.8.8.8	192.168.2.6	0x53f5	No error (0)	ib.anycast.adnxs.com		37.252.172.38	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.474684954 CEST	8.8.8.8	192.168.2.6	0x53f5	No error (0)	ib.anycast.adnxs.com		37.252.172.36	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.474684954 CEST	8.8.8.8	192.168.2.6	0x53f5	No error (0)	ib.anycast.adnxs.com		37.252.173.22	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.474684954 CEST	8.8.8.8	192.168.2.6	0x53f5	No error (0)	ib.anycast.adnxs.com		37.252.172.37	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.481956959 CEST	8.8.8.8	192.168.2.6	0x7ff6	No error (0)	su.addthis.com	m.addthisedge.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:43.481956959 CEST	8.8.8.8	192.168.2.6	0x7ff6	No error (0)	m.addthisedge.com	ds-m.addthisedge.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:43.483072042 CEST	8.8.8.8	192.168.2.6	0xd848	No error (0)	match.sharethrough.com	match-eu-central-1-ecs.sharethrough.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:43.483072042 CEST	8.8.8.8	192.168.2.6	0xd848	No error (0)	match-eu-central-1-ecs.sharethrough.com		35.158.176.66	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.483072042 CEST	8.8.8.8	192.168.2.6	0xd848	No error (0)	match-eu-central-1-ecs.sharethrough.com		18.158.174.89	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.483072042 CEST	8.8.8.8	192.168.2.6	0xd848	No error (0)	match-eu-central-1-ecs.sharethrough.com		35.158.223.21	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.483072042 CEST	8.8.8.8	192.168.2.6	0xd848	No error (0)	match-eu-central-1-ecs.sharethrough.com		3.125.134.133	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.899462938 CEST	8.8.8.8	192.168.2.6	0xb519	No error (0)	client.mutinycdn.com		52.84.174.89	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.899462938 CEST	8.8.8.8	192.168.2.6	0xb519	No error (0)	client.mutinycdn.com		52.84.174.8	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.899462938 CEST	8.8.8.8	192.168.2.6	0xb519	No error (0)	client.mutinycdn.com		52.84.174.116	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:43.899462938 CEST	8.8.8.8	192.168.2.6	0xb519	No error (0)	client.mutinycdn.com		52.84.174.80	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:44.662621975 CEST	8.8.8.8	192.168.2.6	0x3ad	No error (0)	clients1.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:44.662621975 CEST	8.8.8.8	192.168.2.6	0x3ad	No error (0)	clients.l.google.com		142.250.186.46	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:44.970489979 CEST	8.8.8.8	192.168.2.6	0xa328	No error (0)	cdn.lr-ingest.io		104.21.50.127	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:44.970489979 CEST	8.8.8.8	192.168.2.6	0xa328	No error (0)	cdn.lr-ingest.io		172.67.163.57	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:45.054300070 CEST	8.8.8.8	192.168.2.6	0x7d8c	No error (0)	o185886.ingest.sentry.io		34.120.195.249	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:45.450340986 CEST	8.8.8.8	192.168.2.6	0x1078	No error (0)	api-v2.mutinyhq.io	gentle-meadow-3800.shrouded-lake-4691.herokuspace.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:45.450340986 CEST	8.8.8.8	192.168.2.6	0x1078	No error (0)	gentle-meadow-3800.shrouded-lake-4691.herokuspace.com		34.210.130.159	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:45.450340986 CEST	8.8.8.8	192.168.2.6	0x1078	No error (0)	gentle-meadow-3800.shrouded-lake-4691.herokuspace.com		50.112.148.251	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:45.508327007 CEST	8.8.8.8	192.168.2.6	0x913b	No error (0)	api.foreth ought.ai		104.18.223.46	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:45.508327007 CEST	8.8.8.8	192.168.2.6	0x913b	No error (0)	api.foreth ought.ai		104.17.177.49	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:45.740772963 CEST	8.8.8.8	192.168.2.6	0xb2a7	No error (0)	ups.analyt ics.yahoo.com	prod.ups-ats.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:45.740772963 CEST	8.8.8.8	192.168.2.6	0xb2a7	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)
Jul 23, 2021 17:24:45.740772963 CEST	8.8.8.8	192.168.2.6	0xb2a7	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		3.126.56.137	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:45.740772963 CEST	8.8.8.8	192.168.2.6	0xb2a7	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		18.156.0.31	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:46.385481119 CEST	8.8.8.8	192.168.2.6	0x59c0	No error (0)	solve-widget.forethought.ai		104.17.177.49	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:46.385481119 CEST	8.8.8.8	192.168.2.6	0x59c0	No error (0)	solve-widget.forethought.ai		104.18.223.46	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:46.465472937 CEST	8.8.8.8	192.168.2.6	0xa839	No error (0)	zn85jou57xphaxsod-qxm.siteintercept.qualtrics.com	siteintercept.qprod2.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:46.465472937 CEST	8.8.8.8	192.168.2.6	0xa839	No error (0)	siteintercept.qprod2.net	prodlb.siteintercept.qualtrics.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:46.466682911 CEST	8.8.8.8	192.168.2.6	0x6847	No error (0)	zn5bvpdtma7urhqyn-qdigitalsupport.siteintercept.qualtrics.com	siteintercept.qprod2.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:46.466682911 CEST	8.8.8.8	192.168.2.6	0x6847	No error (0)	siteintercept.qprod2.net	prodlb.siteintercept.qualtrics.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:46.766701937 CEST	8.8.8.8	192.168.2.6	0x3d62	No error (0)	d3tnn7lar6ozas.cloudfront.net		52.222.196.201	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:46.766701937 CEST	8.8.8.8	192.168.2.6	0x3d62	No error (0)	d3tnn7lar6ozas.cloudfront.net		52.222.196.173	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:46.766701937 CEST	8.8.8.8	192.168.2.6	0x3d62	No error (0)	d3tnn7lar6ozas.cloudfront.net		52.222.196.115	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:46.766701937 CEST	8.8.8.8	192.168.2.6	0x3d62	No error (0)	d3tnn7lar6ozas.cloudfront.net		52.222.196.73	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:47.636154890 CEST	8.8.8.8	192.168.2.6	0x8691	No error (0)	siteintercept.qualtrics.com	siteintercept.qprod2.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:47.636154890 CEST	8.8.8.8	192.168.2.6	0x8691	No error (0)	siteintercept.qprod2.net	prodlb.siteintercept.qualtrics.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:47.994788885 CEST	8.8.8.8	192.168.2.6	0x3662	No error (0)	www.qualtrics.com	cloudenhanced.qualtrics.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:48.253144026 CEST	8.8.8.8	192.168.2.6	0x2d5f	No error (0)	gstaticadssl.l.google.com		172.217.168.3	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:48.738296986 CEST	8.8.8.8	192.168.2.6	0xc27a	No error (0)	s.w.org		192.0.77.48	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:49.871932983 CEST	8.8.8.8	192.168.2.6	0xb204	No error (0)	rtb-csync.smartadserver.com	rtb-csync.usersync-prod-sas.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:49.871932983 CEST	8.8.8.8	192.168.2.6	0xb204	No error (0)	rtb-csync-eqx.smartadserver.com		185.86.137.131	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:49.871932983 CEST	8.8.8.8	192.168.2.6	0xb204	No error (0)	rtb-csync-eqx.smartadserver.com		185.86.137.133	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:49.871932983 CEST	8.8.8.8	192.168.2.6	0xb204	No error (0)	rtb-csync-eqx.smartadserver.com		185.86.137.110	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:49.871932983 CEST	8.8.8.8	192.168.2.6	0xb204	No error (0)	rtb-csync-eqx.smartadserver.com		185.86.137.132	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:49.872279882 CEST	8.8.8.8	192.168.2.6	0xe5c0	No error (0)	eb2.3lift.com	eu-eb2.3lift.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:49.872279882 CEST	8.8.8.8	192.168.2.6	0xe5c0	No error (0)	eu-eb2.3lift.com		76.223.111.18	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:49.872279882 CEST	8.8.8.8	192.168.2.6	0xe5c0	No error (0)	eu-eb2.3lift.com		13.248.245.213	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:49.878781080 CEST	8.8.8.8	192.168.2.6	0xf16	No error (0)	bh.contextweb.com	lga-bh.contextweb.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:49.878781080 CEST	8.8.8.8	192.168.2.6	0xf16	No error (0)	lga-bh.contextweb.com	lga-bh-bgp.contextweb.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:49.878781080 CEST	8.8.8.8	192.168.2.6	0xf16	No error (0)	lga-bh-bgp.contextweb.com		198.148.27.140	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:49.878781080 CEST	8.8.8.8	192.168.2.6	0xf16	No error (0)	lga-bh-bgp.contextweb.com		198.148.27.139	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:49.879296064 CEST	8.8.8.8	192.168.2.6	0xac19	No error (0)	r.casalemedia.com	r.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:49.880729914 CEST	8.8.8.8	192.168.2.6	0x91a5	No error (0)	partners.tremorhub.com	partners-alb-1113315349.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:49.880729914 CEST	8.8.8.8	192.168.2.6	0x91a5	No error (0)	partners-alb-1113315349.us-east-1.elb.amazonaws.com		34.199.218.203	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:49.880729914 CEST	8.8.8.8	192.168.2.6	0x91a5	No error (0)	partners-alb-1113315349.us-east-1.elb.amazonaws.com		3.213.87.232	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:49.880729914 CEST	8.8.8.8	192.168.2.6	0x91a5	No error (0)	partners-alb-1113315349.us-east-1.elb.amazonaws.com		34.195.162.159	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:49.880729914 CEST	8.8.8.8	192.168.2.6	0x91a5	No error (0)	partners-alb-1113315349.us-east-1.elb.amazonaws.com		3.94.140.254	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:49.880729914 CEST	8.8.8.8	192.168.2.6	0x91a5	No error (0)	partners-alb-1113315349.us-east-1.elb.amazonaws.com		52.5.168.148	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:49.880729914 CEST	8.8.8.8	192.168.2.6	0x91a5	No error (0)	partners-alb-1113315349.us-east-1.elb.amazonaws.com		54.85.113.217	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:49.880729914 CEST	8.8.8.8	192.168.2.6	0x91a5	No error (0)	partners-alb-1113315349.us-east-1.elb.amazonaws.com		52.206.168.194	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:49.880729914 CEST	8.8.8.8	192.168.2.6	0x91a5	No error (0)	partners-alb-1113315349.us-east-1.elb.amazonaws.com		3.222.67.143	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:50.385664940 CEST	8.8.8.8	192.168.2.6	0xd520	No error (0)	cdn.krxd.net	d.sni.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:54.248289108 CEST	8.8.8.8	192.168.2.6	0x4fd4	No error (0)	tags.rd.linksynergy.com	tags-cluster.rd.linksynergy.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:54.248289108 CEST	8.8.8.8	192.168.2.6	0x4fd4	No error (0)	tags-cluster.rd.linksynergy.com		34.98.67.3	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:54.337399006 CEST	8.8.8.8	192.168.2.6	0x57c2	No error (0)	cm.t.tailtarget.com		34.102.185.99	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:54.338742971 CEST	8.8.8.8	192.168.2.6	0xd962	No error (0)	c.deployads.com		52.51.116.157	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:54.338742971 CEST	8.8.8.8	192.168.2.6	0xd962	No error (0)	c.deployads.com		34.242.67.247	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:54.338860035 CEST	8.8.8.8	192.168.2.6	0x62df	No error (0)	i.liadm.com	idaas-ext.cph.liveintent.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:54.338860035 CEST	8.8.8.8	192.168.2.6	0x62df	No error (0)	idaas-ext.cph.liveintent.com		54.85.213.120	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:54.338860035 CEST	8.8.8.8	192.168.2.6	0x62df	No error (0)	idaas-ext.cph.liveintent.com		52.205.241.172	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:54.338860035 CEST	8.8.8.8	192.168.2.6	0x62df	No error (0)	idaas-ext.cph.liveintent.com		54.84.63.116	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:54.338860035 CEST	8.8.8.8	192.168.2.6	0x62df	No error (0)	idaas-ext.cph.liveintent.com		35.174.152.180	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:54.338860035 CEST	8.8.8.8	192.168.2.6	0x62df	No error (0)	idaas-ext.cph.liveintent.com		54.172.13.178	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:54.338860035 CEST	8.8.8.8	192.168.2.6	0x62df	No error (0)	idaas-ext.cph.liveintent.com		52.207.136.156	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:54.338860035 CEST	8.8.8.8	192.168.2.6	0x62df	No error (0)	idaas-ext.cph.liveintent.com		54.205.238.80	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:54.338860035 CEST	8.8.8.8	192.168.2.6	0x62df	No error (0)	idaas-ext.cph.liveintent.com		52.55.124.30	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:54.355534077 CEST	8.8.8.8	192.168.2.6	0x8a47	No error (0)	pixel.rubiconproject.com	pixel.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:55.077296019 CEST	8.8.8.8	192.168.2.6	0x3704	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:55.077296019 CEST	8.8.8.8	192.168.2.6	0x3704	No error (0)	stats.l.doubleclick.net		108.177.126.154	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.077296019 CEST	8.8.8.8	192.168.2.6	0x3704	No error (0)	stats.l.doubleclick.net		108.177.126.156	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.077296019 CEST	8.8.8.8	192.168.2.6	0x3704	No error (0)	stats.l.doubleclick.net		108.177.126.157	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.077296019 CEST	8.8.8.8	192.168.2.6	0x3704	No error (0)	stats.l.doubleclick.net		108.177.126.155	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.107554913 CEST	8.8.8.8	192.168.2.6	0x5272	No error (0)	d.agkn.com	data.agkn.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:55.107554913 CEST	8.8.8.8	192.168.2.6	0x5272	No error (0)	data.agkn.com	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:55.107554913 CEST	8.8.8.8	192.168.2.6	0x5272	No error (0)	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com		18.194.175.178	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.107554913 CEST	8.8.8.8	192.168.2.6	0x5272	No error (0)	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com		52.59.79.213	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:55.107554913 CEST	8.8.8.8	192.168.2.6	0x5272	No error (0)	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com		35.157.140.213	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.107554913 CEST	8.8.8.8	192.168.2.6	0x5272	No error (0)	tag-terraform-elb-1705565586.eu-central-1.elb.amazonaws.com		18.195.172.136	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.389276981 CEST	8.8.8.8	192.168.2.6	0x45ea	No error (0)	insight.adsrvr.org	insight-566961044.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:55.389276981 CEST	8.8.8.8	192.168.2.6	0x45ea	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		52.30.148.233	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.389276981 CEST	8.8.8.8	192.168.2.6	0x45ea	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		34.254.127.126	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.389276981 CEST	8.8.8.8	192.168.2.6	0x45ea	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		99.80.189.193	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.389276981 CEST	8.8.8.8	192.168.2.6	0x45ea	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		52.50.64.214	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.389276981 CEST	8.8.8.8	192.168.2.6	0x45ea	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		52.31.175.99	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.389276981 CEST	8.8.8.8	192.168.2.6	0x45ea	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		54.77.48.133	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.389276981 CEST	8.8.8.8	192.168.2.6	0x45ea	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		34.255.138.57	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.389276981 CEST	8.8.8.8	192.168.2.6	0x45ea	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		34.254.108.170	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.393924952 CEST	8.8.8.8	192.168.2.6	0xee9a	No error (0)	match.adsrvr.org	match-aga.adsrvr.org		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:55.393924952 CEST	8.8.8.8	192.168.2.6	0xee9a	No error (0)	match-aga.adsrvr.org	a97adde81b00f2ca4.awsglobalaccelerator.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:55.393924952 CEST	8.8.8.8	192.168.2.6	0xee9a	No error (0)	a97adde81b00f2ca4.awsglobalaccelerator.com		76.223.111.131	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.393924952 CEST	8.8.8.8	192.168.2.6	0xee9a	No error (0)	a97adde81b00f2ca4.awsglobalaccelerator.com		13.248.242.197	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:55.434775114 CEST	8.8.8.8	192.168.2.6	0xd909	No error (0)	9876505.fls.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:55.434775114 CEST	8.8.8.8	192.168.2.6	0xd909	No error (0)	dart.l.doubleclick.net		216.58.215.230	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:56.291872978 CEST	8.8.8.8	192.168.2.6	0xef7a	No error (0)	i6.liadm.com	idaas6.cph.liveintent.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:56.291872978 CEST	8.8.8.8	192.168.2.6	0xef7a	No error (0)	idaas6.cph.liveintent.com		3.209.93.152	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:56.291872978 CEST	8.8.8.8	192.168.2.6	0xef7a	No error (0)	idaas6.cph.liveintent.com		34.196.0.51	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:56.291872978 CEST	8.8.8.8	192.168.2.6	0xef7a	No error (0)	idaas6.cph.liveintent.com		34.198.52.7	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:56.291872978 CEST	8.8.8.8	192.168.2.6	0xef7a	No error (0)	idaas6.cph.liveintent.com		52.20.143.54	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:56.291872978 CEST	8.8.8.8	192.168.2.6	0xef7a	No error (0)	idaas6.cph.liveintent.com		34.202.24.13	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:56.291872978 CEST	8.8.8.8	192.168.2.6	0xef7a	No error (0)	idaas6.cph.liveintent.com		52.73.168.142	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:56.291872978 CEST	8.8.8.8	192.168.2.6	0xef7a	No error (0)	idaas6.cph.liveintent.com		34.202.20.24	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:56.291872978 CEST	8.8.8.8	192.168.2.6	0xef7a	No error (0)	idaas6.cph.liveintent.com		52.70.165.207	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:58.021573067 CEST	8.8.8.8	192.168.2.6	0x90c2	No error (0)	match.adsrvr.org	match-aga.adsrvr.org		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:58.021573067 CEST	8.8.8.8	192.168.2.6	0x90c2	No error (0)	match-aga.adsrvr.org	a97adde81b00f2ca4.awsglobalaccelerator.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:58.021573067 CEST	8.8.8.8	192.168.2.6	0x90c2	No error (0)	a97adde81b00f2ca4.awsglobalaccelerator.com		76.223.111.131	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:58.021573067 CEST	8.8.8.8	192.168.2.6	0x90c2	No error (0)	a97adde81b00f2ca4.awsglobalaccelerator.com		13.248.242.197	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:58.033674955 CEST	8.8.8.8	192.168.2.6	0x95fb	No error (0)	insight.adsrvr.org	insight-566961044.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:58.033674955 CEST	8.8.8.8	192.168.2.6	0x95fb	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		52.30.148.233	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:58.033674955 CEST	8.8.8.8	192.168.2.6	0x95fb	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		34.254.127.126	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:58.033674955 CEST	8.8.8.8	192.168.2.6	0x95fb	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		99.80.189.193	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:58.033674955 CEST	8.8.8.8	192.168.2.6	0x95fb	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		52.50.64.214	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:58.033674955 CEST	8.8.8.8	192.168.2.6	0x95fb	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		52.31.175.99	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:58.033674955 CEST	8.8.8.8	192.168.2.6	0x95fb	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		54.77.48.133	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:58.033674955 CEST	8.8.8.8	192.168.2.6	0x95fb	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		34.255.138.57	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:58.033674955 CEST	8.8.8.8	192.168.2.6	0x95fb	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		34.254.108.170	A (IP address)	IN (0x0001)
Jul 23, 2021 17:24:58.035569906 CEST	8.8.8.8	192.168.2.6	0xdff5	No error (0)	idsync.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:24:58.444832087 CEST	8.8.8.8	192.168.2.6	0x6092	No error (0)	tags.rd.linksynergy.com	tags-cluster.rd.linksynergy.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:24:58.444832087 CEST	8.8.8.8	192.168.2.6	0x6092	No error (0)	tags-cluster.rd.linksynergy.com		34.98.67.3	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:00.853984118 CEST	8.8.8.8	192.168.2.6	0x9cda	No error (0)	cdn.jsdelivr.net	jsdelivr.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:00.853984118 CEST	8.8.8.8	192.168.2.6	0x9cda	No error (0)	jsdelivr.map.fastly.net		151.101.1.229	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:00.853984118 CEST	8.8.8.8	192.168.2.6	0x9cda	No error (0)	jsdelivr.map.fastly.net		151.101.65.229	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:00.853984118 CEST	8.8.8.8	192.168.2.6	0x9cda	No error (0)	jsdelivr.map.fastly.net		151.101.129.229	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:00.853984118 CEST	8.8.8.8	192.168.2.6	0x9cda	No error (0)	jsdelivr.map.fastly.net		151.101.193.229	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:00.854577065 CEST	8.8.8.8	192.168.2.6	0xc1d7	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:02.939964056 CEST	8.8.8.8	192.168.2.6	0xf599	No error (0)	player.vimeo.com	vimeo.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:02.939964056 CEST	8.8.8.8	192.168.2.6	0xf599	No error (0)	vimeo.map.fastly.net		151.101.0.217	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:02.939964056 CEST	8.8.8.8	192.168.2.6	0xf599	No error (0)	vimeo.map.fastly.net		151.101.64.217	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:02.939964056 CEST	8.8.8.8	192.168.2.6	0xf599	No error (0)	vimeo.map.fastly.net		151.101.128.217	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:02.939964056 CEST	8.8.8.8	192.168.2.6	0xf599	No error (0)	vimeo.map.fastly.net		151.101.192.217	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:03.426377058 CEST	8.8.8.8	192.168.2.6	0x46c3	No error (0)	js.driftt.com	dl7g9llrghqi1.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:03.426377058 CEST	8.8.8.8	192.168.2.6	0x46c3	No error (0)	dl7g9llrghqi1.cloudfront.net		52.222.174.22	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:03.426377058 CEST	8.8.8.8	192.168.2.6	0x46c3	No error (0)	dl7g9llrghqi1.cloudfront.net		52.222.174.83	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:03.426377058 CEST	8.8.8.8	192.168.2.6	0x46c3	No error (0)	dl7g9llrghqi1.cloudfront.net		52.222.174.126	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:03.426377058 CEST	8.8.8.8	192.168.2.6	0x46c3	No error (0)	dl7g9llrghqi1.cloudfront.net		52.222.174.119	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:03.768981934 CEST	8.8.8.8	192.168.2.6	0x661c	No error (0)	consent.trustarc.com		52.222.174.42	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:03.768981934 CEST	8.8.8.8	192.168.2.6	0x661c	No error (0)	consent.trustarc.com		52.222.174.125	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:03.768981934 CEST	8.8.8.8	192.168.2.6	0x661c	No error (0)	consent.trustarc.com		52.222.174.74	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:03.768981934 CEST	8.8.8.8	192.168.2.6	0x661c	No error (0)	consent.trustarc.com		52.222.174.69	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.615904093 CEST	8.8.8.8	192.168.2.6	0xe11d	No error (0)	thrtle.com		52.86.201.23	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.615904093 CEST	8.8.8.8	192.168.2.6	0xe11d	No error (0)	thrtle.com		34.228.209.42	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.615904093 CEST	8.8.8.8	192.168.2.6	0xe11d	No error (0)	thrtle.com		34.194.106.172	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.615904093 CEST	8.8.8.8	192.168.2.6	0xe11d	No error (0)	thrtle.com		52.0.73.248	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:25:04.615904093 CEST	8.8.8.8	192.168.2.6	0xe11d	No error (0)	thrtle.com		3.215.242.19	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.615904093 CEST	8.8.8.8	192.168.2.6	0xe11d	No error (0)	thrtle.com		3.226.4.134	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.615904093 CEST	8.8.8.8	192.168.2.6	0xe11d	No error (0)	thrtle.com		3.212.71.107	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.615904093 CEST	8.8.8.8	192.168.2.6	0xe11d	No error (0)	thrtle.com		54.167.47.210	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.616869926 CEST	8.8.8.8	192.168.2.6	0xc933	No error (0)	ssc-cms.33across.com	pixel.33across.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:04.616869926 CEST	8.8.8.8	192.168.2.6	0xc933	No error (0)	pixel.33across.com		208.100.17.176	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.622808933 CEST	8.8.8.8	192.168.2.6	0x3d6e	No error (0)	ads.stickyadstv.com	ip1.ads.stickyadstv.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:04.624314070 CEST	8.8.8.8	192.168.2.6	0x399c	No error (0)	api.retargetly.com		104.22.17.141	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.624314070 CEST	8.8.8.8	192.168.2.6	0x399c	No error (0)	api.retargetly.com		104.22.16.141	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.624314070 CEST	8.8.8.8	192.168.2.6	0x399c	No error (0)	api.retargetly.com		172.67.8.244	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.629225016 CEST	8.8.8.8	192.168.2.6	0xe011	No error (0)	i.vimeocdn.com	vimeo-video.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:04.629225016 CEST	8.8.8.8	192.168.2.6	0xe011	No error (0)	vimeo-video.map.fastly.net		151.101.114.109	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.644929886 CEST	8.8.8.8	192.168.2.6	0x12b2	No error (0)	fresnel.vimeocdn.com		34.120.202.204	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.656219959 CEST	8.8.8.8	192.168.2.6	0xe0ed	No error (0)	f.vimeocdn.com	vimeo-video.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:04.656219959 CEST	8.8.8.8	192.168.2.6	0xe0ed	No error (0)	vimeo-video.map.fastly.net		151.101.114.109	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.785098076 CEST	8.8.8.8	192.168.2.6	0xbefc	No error (0)	vimeo.com		151.101.64.217	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.785098076 CEST	8.8.8.8	192.168.2.6	0xbefc	No error (0)	vimeo.com		151.101.128.217	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.785098076 CEST	8.8.8.8	192.168.2.6	0xbefc	No error (0)	vimeo.com		151.101.0.217	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:04.785098076 CEST	8.8.8.8	192.168.2.6	0xbefc	No error (0)	vimeo.com		151.101.192.217	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:05.092921019 CEST	8.8.8.8	192.168.2.6	0x9f25	No error (0)	player-telemetry.vimeo.com		34.120.202.204	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:05.546266079 CEST	8.8.8.8	192.168.2.6	0xd711	No error (0)	j.6sc.co	j.6sc.co.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:07.375690937 CEST	8.8.8.8	192.168.2.6	0xa6e	No error (0)	b.6sc.co	b.6sc.co.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:07.744918108 CEST	8.8.8.8	192.168.2.6	0x658f	No error (0)	customer.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:07.744918108 CEST	8.8.8.8	192.168.2.6	0x658f	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
Jul 23, 2021 17:25:07.744918108 CEST	8.8.8.8	192.168.2.6	0x658f	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:07.744918108 CEST	8.8.8.8	192.168.2.6	0x658f	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:07.744918108 CEST	8.8.8.8	192.168.2.6	0x658f	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		54.147.21.139	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:07.745249033 CEST	8.8.8.8	192.168.2.6	0x4deb	No error (0)	conversation.api.drift.com	istio.api.drift.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:07.745249033 CEST	8.8.8.8	192.168.2.6	0x4deb	No error (0)	istio.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:07.745249033 CEST	8.8.8.8	192.168.2.6	0x4deb	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		50.16.7.188	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:07.745249033 CEST	8.8.8.8	192.168.2.6	0x4deb	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:07.745249033 CEST	8.8.8.8	192.168.2.6	0x4deb	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:07.745249033 CEST	8.8.8.8	192.168.2.6	0x4deb	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		54.147.21.139	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:07.745353937 CEST	8.8.8.8	192.168.2.6	0x5686	No error (0)	metrics.api.drift.com	istio.api.drift.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:07.745353937 CEST	8.8.8.8	192.168.2.6	0x5686	No error (0)	istio.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:07.745353937 CEST	8.8.8.8	192.168.2.6	0x5686	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
Jul 23, 2021 17:25:07.745353937 CEST	8.8.8.8	192.168.2.6	0x5686	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:07.745353937 CEST	8.8.8.8	192.168.2.6	0x5686	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:07.745353937 CEST	8.8.8.8	192.168.2.6	0x5686	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		54.147.21.139	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:07.783566952 CEST	8.8.8.8	192.168.2.6	0x9f81	No error (0)	targeting.api.drift.com	istio.api.drift.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:07.783566952 CEST	8.8.8.8	192.168.2.6	0x9f81	No error (0)	istio.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:07.783566952 CEST	8.8.8.8	192.168.2.6	0x9f81	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		54.147.21.139	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:07.783566952 CEST	8.8.8.8	192.168.2.6	0x9f81	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		50.16.7.188	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:07.783566952 CEST	8.8.8.8	192.168.2.6	0x9f81	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:07.783566952 CEST	8.8.8.8	192.168.2.6	0x9f81	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:08.515376091 CEST	8.8.8.8	192.168.2.6	0x66c5	No error (0)	sentry.io		35.188.42.15	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:13.264394045 CEST	8.8.8.8	192.168.2.6	0xe079	No error (0)	bootstrap.api.drift.com	istio.api.drift.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:13.264394045 CEST	8.8.8.8	192.168.2.6	0xe079	No error (0)	istio.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:13.264394045 CEST	8.8.8.8	192.168.2.6	0xe079	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
Jul 23, 2021 17:25:13.264394045 CEST	8.8.8.8	192.168.2.6	0xe079	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		50.16.7.188	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:13.264394045 CEST	8.8.8.8	192.168.2.6	0xe079	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:13.264394045 CEST	8.8.8.8	192.168.2.6	0xe079	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:13.924267054 CEST	8.8.8.8	192.168.2.6	0x9ace	No error (0)	embeds.driftcdn.com		52.222.174.56	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:13.924267054 CEST	8.8.8.8	192.168.2.6	0x9ace	No error (0)	embeds.driftcdn.com		52.222.174.73	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:13.924267054 CEST	8.8.8.8	192.168.2.6	0x9ace	No error (0)	embeds.driftcdn.com		52.222.174.107	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:13.924267054 CEST	8.8.8.8	192.168.2.6	0x9ace	No error (0)	embeds.driftcdn.com		52.222.174.45	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:14.155092001 CEST	8.8.8.8	192.168.2.6	0xcc2e	No error (0)	jadserve.postrelease.com	jadserve.postrelease.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:14.157181025 CEST	8.8.8.8	192.168.2.6	0x67f6	No error (0)	sync.1rx.io		213.19.147.45	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:14.157778025 CEST	8.8.8.8	192.168.2.6	0x6155	No error (0)	public-prod-dspcookiematching.dmxleo.com		34.120.25.144	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:14.159352064 CEST	8.8.8.8	192.168.2.6	0x76ff	No error (0)	sync.navdmp.com		104.16.14.243	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:14.159352064 CEST	8.8.8.8	192.168.2.6	0x76ff	No error (0)	sync.navdmp.com		104.16.15.243	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:14.159352064 CEST	8.8.8.8	192.168.2.6	0x76ff	No error (0)	sync.navdmp.com		104.16.12.243	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:14.159352064 CEST	8.8.8.8	192.168.2.6	0x76ff	No error (0)	sync.navdmp.com		104.16.11.243	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:14.159352064 CEST	8.8.8.8	192.168.2.6	0x76ff	No error (0)	sync.navdmp.com		104.16.13.243	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:14.160161018 CEST	8.8.8.8	192.168.2.6	0xaf8d	No error (0)	e1.emxdgt.com		18.195.155.181	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:14.314332962 CEST	8.8.8.8	192.168.2.6	0x8e65	No error (0)	certificates.godaddy.com	gdcrl.godaddy.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:14.371264935 CEST	8.8.8.8	192.168.2.6	0x9abb	No error (0)	sync.targeting.unrulymedia.com	sync.1rx.io		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:14.371264935 CEST	8.8.8.8	192.168.2.6	0x9abb	No error (0)	sync.1rx.io		213.19.147.45	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:14.891082048 CEST	8.8.8.8	192.168.2.6	0x3b44	No error (0)	www-google-analytics.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:15.121653080 CEST	8.8.8.8	192.168.2.6	0x1df0	No error (0)	googleads.g.doubleclick.net		172.217.168.2	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:25:16.706187963 CEST	8.8.8.8	192.168.2.6	0xf13f	No error (0)	presence.api.drift.com	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:16.706187963 CEST	8.8.8.8	192.168.2.6	0xf13f	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		35.174.210.7	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:16.706187963 CEST	8.8.8.8	192.168.2.6	0xf13f	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		54.85.240.191	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:16.706187963 CEST	8.8.8.8	192.168.2.6	0xf13f	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		54.173.95.250	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:16.706187963 CEST	8.8.8.8	192.168.2.6	0xf13f	No error (0)	a2f905133e04e4d35ade9cd4751dd35b-4fd69d4b6621dbbd.elb.us-east-1.amazonaws.com		52.0.218.127	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:16.707612038 CEST	8.8.8.8	192.168.2.6	0xfc17	No error (0)	79332-32.chat.api.drift.com	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:16.707612038 CEST	8.8.8.8	192.168.2.6	0xfc17	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		54.164.185.154	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:16.707612038 CEST	8.8.8.8	192.168.2.6	0xfc17	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		54.145.12.192	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:16.707612038 CEST	8.8.8.8	192.168.2.6	0xfc17	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		52.203.176.110	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:16.707612038 CEST	8.8.8.8	192.168.2.6	0xfc17	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		52.7.163.75	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:16.707612038 CEST	8.8.8.8	192.168.2.6	0xfc17	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		54.209.43.145	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:16.707612038 CEST	8.8.8.8	192.168.2.6	0xfc17	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		52.72.43.177	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:16.707612038 CEST	8.8.8.8	192.168.2.6	0xfc17	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		34.206.108.81	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 23, 2021 17:25:16.707612038 CEST	8.8.8.8	192.168.2.6	0xfc17	No error (0)	ee15ba61-wschat-wschatalb-6fcf-2062696737.us-east-1.elb.amazonaws.com		3.219.62.124	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:16.891526937 CEST	8.8.8.8	192.168.2.6	0xa22c	No error (0)	event.api.drift.com	alb-event-1454785217.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:16.891526937 CEST	8.8.8.8	192.168.2.6	0xa22c	No error (0)	alb-event-1454785217.us-east-1.elb.amazonaws.com		34.234.150.139	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:16.891526937 CEST	8.8.8.8	192.168.2.6	0xa22c	No error (0)	alb-event-1454785217.us-east-1.elb.amazonaws.com		54.172.114.57	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:17.399919987 CEST	8.8.8.8	192.168.2.6	0x5aff	No error (0)	flow.api.drift.com	istio.api.drift.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:17.399919987 CEST	8.8.8.8	192.168.2.6	0x5aff	No error (0)	istio.api.drift.com	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 23, 2021 17:25:17.399919987 CEST	8.8.8.8	192.168.2.6	0x5aff	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		50.16.7.188	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:17.399919987 CEST	8.8.8.8	192.168.2.6	0x5aff	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		34.193.113.164	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:17.399919987 CEST	8.8.8.8	192.168.2.6	0x5aff	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		3.94.218.138	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:17.399919987 CEST	8.8.8.8	192.168.2.6	0x5aff	No error (0)	afe79c04fd8464db69f453355c110684-6aa967fe209738b1.elb.us-east-1.amazonaws.com		54.147.21.139	A (IP address)	IN (0x0001)
Jul 23, 2021 17:25:19.349761963 CEST	8.8.8.8	192.168.2.6	0x342d	No error (0)	www-google tagmanager.l.google.com		172.217.168.8	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 23, 2021 17:24:15.051064014 CEST	104.17.70.206	443	192.168.2.6	49747	CN=success.qualtrics.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jun 07 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Tue Jun 07 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 23, 2021 17:24:15.052525997 CEST	104.17.70.206	443	192.168.2.6	49746	CN=success.qualtrics.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jun 07 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Tue Jun 07 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jul 23, 2021 17:24:15.053000927 CEST	104.17.70.206	443	192.168.2.6	49748	CN=success.qualtrics.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jun 07 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Tue Jun 07 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jul 23, 2021 17:24:15.501223087 CEST	52.217.64.246	443	192.168.2.6	49753	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Jun 23 02:00:00 CEST 2021 Tue Dec 08 13:05:07 CET 2015	Mon Jul 25 01:59:59 CEST 2022 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Jul 23, 2021 17:24:15.619477987 CEST	52.217.64.246	443	192.168.2.6	49754	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Wed Jun 23 02:00:00 CEST 2021 Tue Dec 08 13:05:07 CET 2015	Mon Jul 25 01:59:59 CEST 2022 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Jul 23, 2021 17:24:16.647226095 CEST	52.217.18.236	443	192.168.2.6	49755	CN=*.s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 11 01:00:00 CET 2021 Tue Dec 08 13:05:07 CET 2015	Sat Feb 12 00:59:59 CET 2022 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 23, 2021 17:24:16.656866074 CEST	52.217.18.236	443	192.168.2.6	49756	CN=*.s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 11 01:00:00 CET 2021 Tue Dec 08 13:05:07 CET 2015	Sat Feb 12 00:59:59 CET 2022 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Jul 23, 2021 17:24:19.397527933 CEST	151.101.114.109	443	192.168.2.6	49779	CN=*.vimeocdn.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue May 18 20:45:52 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Sun Jun 19 20:45:51 CEST 2022 Sun Mar 18 01:00:00 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jul 23, 2021 17:24:20.925152063 CEST	108.174.11.37	443	192.168.2.6	49788	CN=px.ads.linkedin.com, O=LinkedIn Corporation, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Apr 15 02:00:00 CEST 2021 Wed Sep 23 02:00:00 CEST 2020	Sat Oct 16 01:59:59 CEST 2021 Mon Sep 23 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
Jul 23, 2021 17:24:21.113197088 CEST	212.82.100.181	443	192.168.2.6	49796	CN=*.analytics.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=*.analytics.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon May 24 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013 Mon May 24 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Thu Nov 18 00:59:59 CET 2021 Sun Oct 22 14:00:00 CEST 2028 Thu Nov 18 00:59:59 CET 2021 Sun Oct 22 14:00:00 CEST 2028	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
					CN=*.analytics.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon May 24 02:00:00 CEST 2021	Thu Nov 18 00:59:59 CET 2021		
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 23, 2021 17:24:21.255850077 CEST	3.65.155.204	443	192.168.2.6	49800	CN=*.6sense.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Jun 30 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Jul 30 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Jul 23, 2021 17:24:21.478125095 CEST	3.65.155.204	443	192.168.2.6	49804	CN=*.6sense.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Jun 30 02:00:00 CEST 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Jul 30 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 23, 2021 17:24:21.765294075 CEST	192.28.147.68	443	192.168.2.6	49803	CN=*.mktoresp.com, OU=IT, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jan 17 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jan 21 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jul 23, 2021 17:24:21.841064930 CEST	192.28.147.68	443	192.168.2.6	49805	CN=*.mktoresp.com, OU=IT, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jan 17 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jan 21 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jul 23, 2021 17:24:23.346168995 CEST	52.38.120.169	443	192.168.2.6	49816	CN=*.segment.com, O="Segment.io, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jul 19 02:00:00 CEST 2021 Wed Apr 14 02:00:00 CEST 2021	Wed Aug 10 01:59:59 CEST 2022 Mon Apr 14 01:59:59 CEST 2031	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Apr 14 02:00:00 CEST 2021	Mon Apr 14 01:59:59 CEST 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 23, 2021 17:24:23.824590921 CEST	212.82.100.181	443	192.168.2.6	49824	CN=*.analytics.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=*.analytics.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon May 24 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013 Mon May 24 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Thu Nov 18 00:59:59 CET 2021 Sun Oct 22 14:00:00 CEST 2028 Thu Nov 18 00:59:59 CET 2021 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
					CN=*.analytics.yahoo.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon May 24 02:00:00 CEST 2021	Thu Nov 18 00:59:59 CET 2021		
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jul 23, 2021 17:24:25.301198959 CEST	34.246.41.247	443	192.168.2.6	49831	CN=beacon.krxd.net, O="salesforce.com, inc.", L=San Francisco, ST=California, C=US CN=beacon.krxd.net, O="salesforce.com, inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jan 13 01:00:00 CET 2021 Wed Jan 13 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Jan 08 00:59:59 CET 2022 Sat Jan 08 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=beacon.krxd.net, O="salesforce.com, inc.", L=San Francisco, ST=California, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	Wed Jan 13 01:00:00 CET 2021	Sat Jan 08 00:59:59 CET 2022		
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jul 23, 2021 17:24:25.305349112 CEST	3.10.35.49	443	192.168.2.6	49835	CN=*.agkn.com CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Jul 25 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006 Mon Nov 06 13:23:33 CET 2017	Sun Sep 18 14:00:00 CEST 2022 Mon Nov 10 01:00:00 CET 2031 Sat Nov 06 13:23:33 CET 2027	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Jul 23, 2021 17:24:25.340262890 CEST	63.32.159.255	443	192.168.2.6	49837	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Dec 02 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Mon Jan 03 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jul 23, 2021 17:24:25.483038902 CEST	34.236.226.59	443	192.168.2.6	49832	CN=usermatch.krxd.net, O="salesforce.com, inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jul 13 02:00:00 CEST 2021 Thu Sep 24 02:00:00 CEST 2020	Wed Jul 13 01:59:59 CEST 2022 Tue Sep 24 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jul 23, 2021 17:24:25.483086109 CEST	34.236.226.59	443	192.168.2.6	49833	CN=usermatch.krxd.net, O="salesforce.com, inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Jul 13 02:00:00 CEST 2021 Thu Sep 24 02:00:00 CEST 2020	Wed Jul 13 01:59:59 CEST 2022 Tue Sep 24 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jul 23, 2021 17:24:25.650502920 CEST	66.155.71.149	443	192.168.2.6	49842	CN=*.sitescout.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jan 15 01:00:00 CET 2020 Mon Nov 06 13:23:33 CET 2017	Wed Feb 02 13:00:00 CET 2022 Sat Nov 06 13:23:33 CET 2027	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 23, 2021 17:24:26.221970081 CEST	66.155.71.25	443	192.168.2.6	49845	CN=*.sitescout.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jan 15 01:00:00 CET 2020 Mon Nov 06 13:23:33 CET 2017	Wed Feb 02 13:00:00 CET 2022 Sat Nov 06 13:23:33 CET 2027	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Jul 23, 2021 17:24:26.365606070 CEST	63.32.159.255	443	192.168.2.6	49846	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Dec 02 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Mon Jan 03 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Jul 23, 2021 17:24:26.418000937 CEST	54.78.254.47	443	192.168.2.6	49847	CN=*.exelator.com, O="THE NIELSEN COMPANY (US), LLC", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jun 02 02:00:00 CEST 2021 Thu Sep 24 02:00:00 CEST 2020	Wed Jun 08 01:59:59 CEST 2022 Tue Sep 24 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jul 23, 2021 17:24:26.449398994 CEST	34.251.130.56	443	192.168.2.6	49850	CN=*.crwdcntrl.net, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu Apr 29 15:37:41 CEST 2021 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Tue May 31 15:37:41 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Jul 23, 2021 17:24:26.848334074 CEST	151.101.1.27	443	192.168.2.6	49852	CN=*.newrelic.com CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed May 05 23:39:18 CEST 2021 Tue Jul 28 02:00:00 CEST 2020	Mon Jun 06 23:39:17 CEST 2022 Sun Mar 18 01:00:00 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GlobalSign Atlas R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
Jul 23, 2021 17:24:27.350322962 CEST	162.247.242.21	443	192.168.2.6	49857	CN=*.nr-data.net, O="New Relic, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 05 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Tue Feb 08 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jul 23, 2021 17:24:28.023015022 CEST	35.227.248.159	443	192.168.2.6	49865	CN=*.tapad.com, O="Tapad, Inc.", L=New York, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Oct 05 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Sat Nov 06 01:00:00 CET 2021 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
Jul 23, 2021 17:24:28.047635078 CEST	63.32.159.255	443	192.168.2.6	49864	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Dec 02 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Mon Jan 03 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 23, 2021 17:24:28.061144114 CEST	54.78.254.47	443	192.168.2.6	49866	CN=*.exelator.com, O="THE NIELSEN COMPANY (US), LLC", L=New York, ST=New York, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jun 02 02:00:00 CEST 2021 Thu Sep 24 02:00:00 CEST 2020	Wed Jun 08 01:59:59 CEST 2022 Tue Sep 24 01:59:59 CEST 2030	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
Jul 23, 2021 17:24:28.109925985 CEST	34.251.130.56	443	192.168.2.6	49868	CN=*.crwdcntrl.net, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu Apr 29 15:37:41 CEST 2021 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Tue May 31 15:37:41 CEST 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Jul 23, 2021 17:24:37.573936939 CEST	66.155.71.149	443	192.168.2.6	49888	CN=*.sitescout.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jan 15 01:00:00 CET 2020 Mon Nov 06 13:23:33 CET 2017	Wed Feb 02 13:00:00 CET 2022 Sat Nov 06 13:23:33 CET 2027	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
Jul 23, 2021 17:24:38.728564024 CEST	66.155.71.25	443	192.168.2.6	49893	CN=*.sitescout.com CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jan 15 01:00:00 CET 2020 Mon Nov 06 13:23:33 CET 2017	Wed Feb 02 13:00:00 CET 2022 Sat Nov 06 13:23:33 CET 2027	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 23, 2021 17:24:39.153407097 CEST	185.94.180.126	443	192.168.2.6	49899	CN=*.search.spotxchange.com, O="SpotX, Inc", L=Broomfield, ST=Colorado, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Apr 08 02:00:00 CEST 2021 Mon Nov 06 13:23:45 CET 2017	Tue May 10 01:59:59 CEST 2022 Sat Nov 06 13:23:45 CET 2027	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 23, 2021 17:24:39.154150963 CEST	185.64.190.80	443	192.168.2.6	49898	CN=*.pubmatic.com, O="PubMatic, Inc.", L=Redwood City, ST=California, C=US CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Dec 07 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri May 12 20:46:00 CEST 2000	Wed Dec 15 00:59:59 CET 2021 Mon May 12 01:59:59 CEST 2025 Tue May 13 01:59:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Sep 24 02:00:00 CEST 2020	Mon May 12 01:59:59 CEST 2025		
					CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri May 12 20:46:00 CEST 2000	Tue May 13 01:59:00 CEST 2025		
Jul 23, 2021 17:24:39.299911976 CEST	185.94.180.126	443	192.168.2.6	49904	CN=*.search.spotxchange.com, O="SpotX, Inc", L=Broomfield, ST=Colorado, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Apr 08 02:00:00 CEST 2021 Mon Nov 06 13:23:45 CET 2017	Tue May 10 01:59:59 CEST 2022 Sat Nov 06 13:23:45 CET 2027	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 23, 2021 17:24:39.300167084 CEST	185.94.180.126	443	192.168.2.6	49903	CN=*.search.spotxchange.com, O="SpotX, Inc", L=Broomfield, ST=Colorado, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Apr 08 02:00:00 CEST 2021 Mon Nov 06 13:23:45 CET 2017	Tue May 10 01:59:59 CEST 2022 Sat Nov 06 13:23:45 CET 2027	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 23, 2021 17:24:39.351749897 CEST	185.94.180.126	443	192.168.2.6	49906	CN=*.search.spotxchange.com, O="SpotX, Inc", L=Broomfield, ST=Colorado, C=US CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Apr 08 02:00:00 CEST 2021 Mon Nov 06 13:23:45 CET 2017	Tue May 10 01:59:59 CEST 2022 Sat Nov 06 13:23:45 CET 2027	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=GeoTrust RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:45 CET 2017	Sat Nov 06 13:23:45 CET 2027		
Jul 23, 2021 17:24:43.520418882 CEST	18.184.153.186	443	192.168.2.6	49925	CN=pixel.advertising.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=pixel.advertising.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Mar 01 01:00:00 CET 2021 Mon Mar 01 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 25 01:59:59 CEST 2021 Wed Aug 25 01:59:59 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=pixel.advertising.com, O=Oath Inc, L=Sunnyvale, ST=California, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Mar 01 01:00:00 CET 2021	Wed Aug 25 01:59:59 CEST 2021		
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jul 23, 2021 17:24:43.529078007 CEST	37.252.173.62	443	192.168.2.6	49927	CN=*.adnxs.com, O=Xandr Inc., L=New York, ST=New York, C=US CN=GeoTrust ECC CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust ECC CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 05 01:00:00 CET 2021 Mon Nov 06 13:24:09 CET 2017	Sun Feb 20 00:59:59 CET 2022 Sat Nov 06 13:24:09 CET 2027	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GeoTrust ECC CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:24:09 CET 2017	Sat Nov 06 13:24:09 CET 2027		
Jul 23, 2021 17:24:43.651734114 CEST	35.158.176.66	443	192.168.2.6	49929	CN=*.sharethrough.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 09 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Oct 11 02:00:00 CEST 2021 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5336 Parent PID: 3888

General

Start time:	17:24:01
Start date:	23/07/2021
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://covid.census.gov/CP/Register.php?OptOut=true&RID=CGC_daprBTqzoTB4ekC&LID=UR_0ix3gy2rnDlg56J&DID=EMD_SqN0lR2ri39yTOI&BT=dXNjZW5zdXNidXJlYXVjb3ZpZA&_=1'
Imagebase:	0x7ff7c15e0000
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: 1724 Parent PID: 5336

General

Start time:	17:24:03
Start date:	23/07/2021
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=1640,2244722290038112252,7691160406664226266,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1960 /prefetch:8
Imagebase:	0x7ff7c15e0000
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

Disassembly