ID: 449115
Cookbook: browseurl.jbs
Time: 09:19:53
Date: 15/07/2021
Version: 33.0.0 White Diamond

Table of Contents

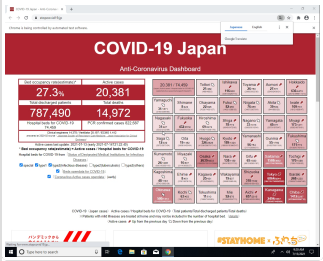
Windows Analysis Report https://www.stopcovid19.jp/

Overview

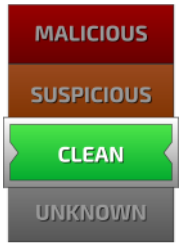
General Information

Sample URL:	http://https://www.stopcovid19.jp/
Analysis ID:	449115
Infos:	

Most interesting Screenshot:



Detection

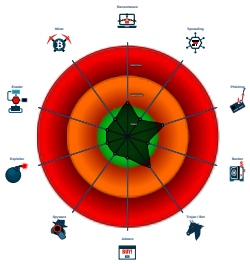


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Connects to several IPs in different ...
- Suspicious form URL found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 2936 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://www.stopcovid19.jp/' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5976 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1532,11141525606934232942,4789934611024801501,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1756 /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

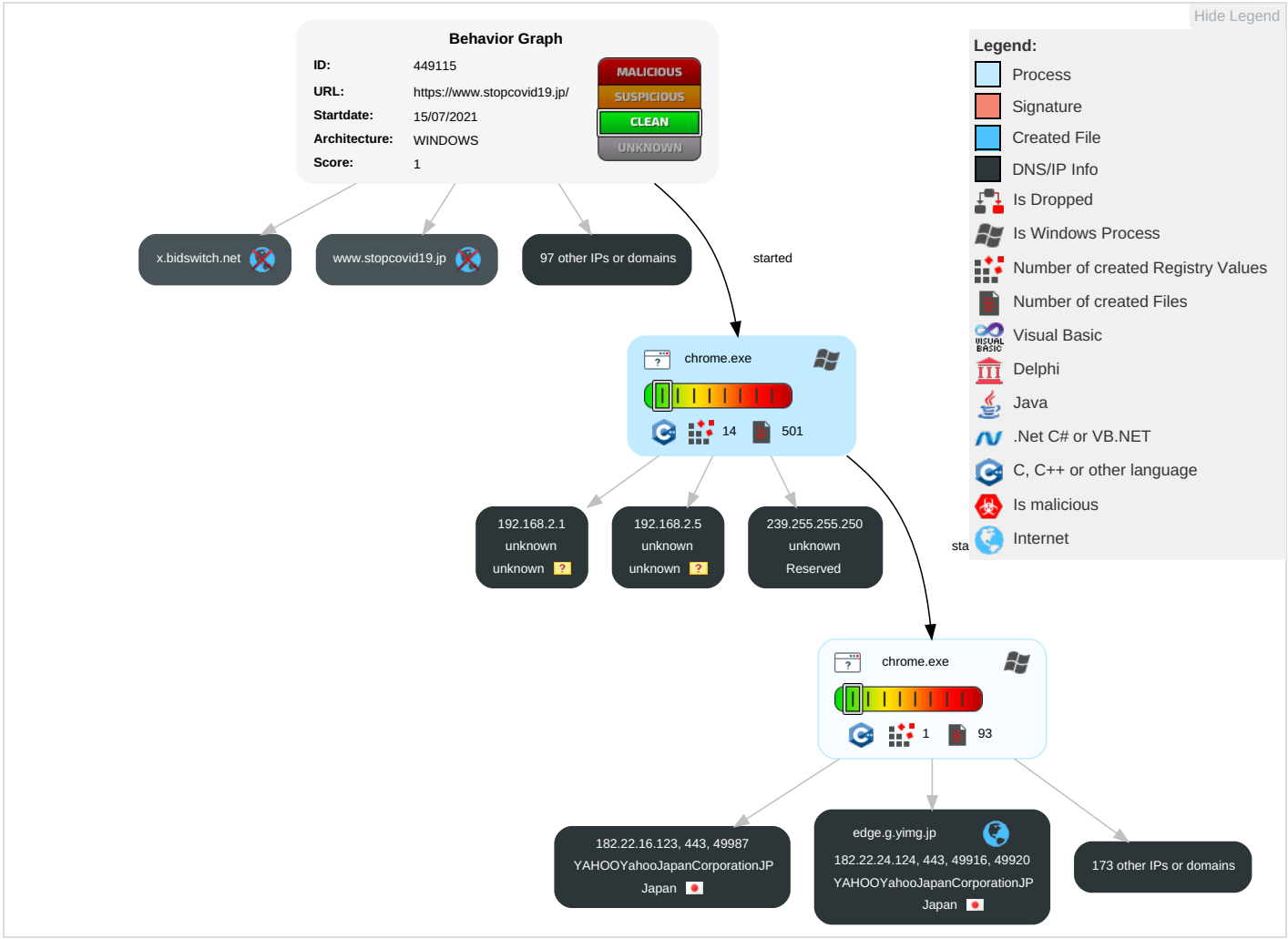
Click to jump to signature section

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	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	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	Modif Syste Partit
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 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carri Billin Fraud

Behavior Graph

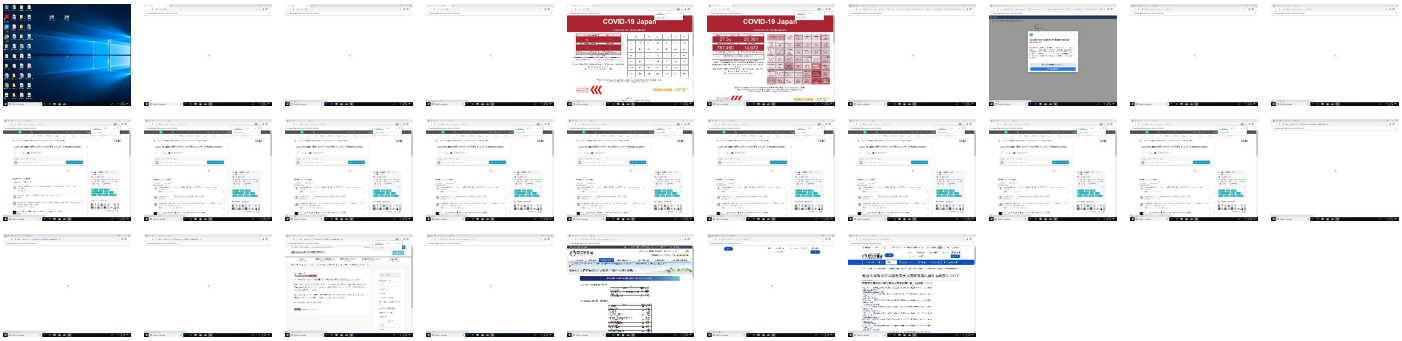


Screenshots

Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://www.stopcovid19.jp/	0%	Virustotal		Browse
http://https://www.stopcovid19.jp/	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.mhlw.go.jp/common/scripts/jquery.mk_smoothScroll.js	0%	Virustotal		Browse
http://https://www.mhlw.go.jp/common/scripts/jquery.mk_smoothScroll.js	0%	Avira URL Cloud	safe	
http://https://rubiconcm.digitaleast.mobi/usersync/rubicon.gif	0%	Virustotal		Browse
http://https://rubiconcm.digitaleast.mobi/usersync/rubicon.gif	0%	Avira URL Cloud	safe	
http://https://sync.intentiq.com/profiles_engine/ProfilesEngineServlet?at=20&mi=10&dpi=54	0%	Virustotal		Browse
http://https://sync.intentiq.com/profiles_engine/ProfilesEngineServlet?at=20&mi=10&dpi=54	0%	Avira URL Cloud	safe	
http://https://match.prod.bidr.io/cookie-sync/rp?bee_sync_partners=rp	0%	Virustotal		Browse
http://https://match.prod.bidr.io/cookie-sync/rp?bee_sync_partners=rp	0%	Avira URL Cloud	safe	
http://https://api.primecaster.net/adlogue/api/sync/rubicon	0%	Avira URL Cloud	safe	
http://https://yads.yjtag.yahoo.co.jp/tag?s=67018_295415&fr_id=yads_564321-0&sb_support=1&enc=UTF-8&u=https	0%	Avira URL Cloud	safe	
http://https://www.ja-ces.or.jp/wordpress/wp-includes/js/jquery/jquery.form.min.js?ver=4.2.1	0%	Avira URL Cloud	safe	
http://match.prod.bidr.io/cookie-sync/rp?bee_sync_partners=rp	0%	Avira URL Cloud	safe	
http://https://gu.dyntrk.com/adx/rbcn/us.php?dynk=r1b32c0n	0%	Avira URL Cloud	safe	
http://https://tr.blismedia.com/v1/api/sync/rubicon	0%	Avira URL Cloud	safe	
http://https://www.stopcovid19.jp/COVID-19	0%	Avira URL Cloud	safe	
http://https://mhlw.go.jp/A.B	0%	Avira URL Cloud	safe	
http://https://taisukef.github.io	0%	Avira URL Cloud	safe	
http://https://hatena.ne.jp/	0%	Avira URL Cloud	safe	
http://https://www.mhlw.go.jp/common/scripts/jquery.mk_inputFucus.js	0%	Avira URL Cloud	safe	
http://https://www.ja-ces.or.jp/wordpress/wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=5.1.	0%	Avira URL Cloud	safe	
http://https://b.hatena.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://https://mhlw.go.jp/H9	0%	Avira URL Cloud	safe	
http://https://www.mhlw.go.jp/common/scripts/jquery.mk_megaDropdown.js	0%	Avira URL Cloud	safe	
http://https://stopcovid19.jp/y3	0%	Avira URL Cloud	safe	
http://https://www.ja-ces.or.jp/wordpress/wp-content/plugins/svg-support/js/min/svgs-inline-min.js?ver=1.0.	0%	Avira URL Cloud	safe	
http://https://www.ja-ces.or.jp/wordpress/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp	0%	Avira URL Cloud	safe	
http://https://hatena.ne.jp/#	0%	Avira URL Cloud	safe	
http://https://match.deepintent.com/usersync/141?redir=https%3A%2F%2Fimage2.pubmatic.com%2FAdServer%2FPug%3	0%	Avira URL Cloud	safe	
http://https://www.ja-ces.or.jp/wordpress/wp-includes/js/wp-embed.min.js?ver=5.2.11	0%	Avira URL Cloud	safe	
http://https://www.mhlw.go.jp/common/scripts/newDate.js	0%	Avira URL Cloud	safe	
http://https://www.mhlw.go.jp/common/scripts/jquery.mk_location.js	0%	Avira URL Cloud	safe	
http://https://id5-sync.com/i/175/9.gif	0%	Avira URL Cloud	safe	
http://https://www.stopcovid19.jp/#	0%	Avira URL Cloud	safe	
http://https://b.hatena.ne.jp	0%	Avira URL Cloud	safe	
http://https://b.hatena.ne.jph	0%	Avira URL Cloud	safe	
http://https://www.stopcovid19.jp/:COVID-19	0%	Avira URL Cloud	safe	
http://https://b.hatena.ne.jp/favicon.ico=	0%	Avira URL Cloud	safe	
http://https://code4sabae.github.io/kafumon/lib/Chart.mjs	0%	Avira URL Cloud	safe	
http://https://hatena.ne.jp/A	0%	Avira URL Cloud	safe	
http://https://id.sharedid.org/usync?redir=https%3A%2F%2Fpixel.rubiconproject.com%2Ftap.php%3Fv%3D624210%26	0%	Avira URL Cloud	safe	
http://https://hatena.ne.jp/:xY	0%	Avira URL Cloud	safe	
http://https://hatena.ne.jp/H	0%	Avira URL Cloud	safe	
http://https://hatena.ne.jp/Zh=	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
taisukef.github.io	185.199.109.153	true	false		unknown
um.simpli.fi	169.50.137.190	true	false		high
lga-bh-bgp.contextweb.com	198.148.27.140	true	false		high
tls13.taboola.map.fastly.net	151.101.1.44	true	false		unknown
cnt.fout.jp	202.232.238.39	true	false		high
global.px.quantserve.com	91.228.74.134	true	false		high
cm119.appier.org	172.105.220.23	true	false		high
pixel-a.sitescout.com	66.155.71.25	true	false		high
platform.twitter.map.fastly.net	199.232.136.157	true	false		unknown
generic-2.lb.lm5v.com	162.55.6.212	true	false		unknown
t.co	104.244.42.5	true	false		high
mwzeom.zeotap.com	104.22.24.87	true	false		high
dualstack.tls13.taboola.map.fastly.net	151.101.1.44	true	false		unknown
repository.secomtrust.net	61.114.177.151	true	false		unknown
rtb-csync-itx4.smartadserver.com	185.86.139.89	true	false		high
adc.auone.jp	54.95.129.54	true	false		high
id.rlcdn.com	35.244.174.68	true	false		high
match.prod.bidr.io	52.16.214.249	true	false		unknown
static.am5.vip.prod.criteo.net	178.250.2.130	true	false		high
s.twitter.com	104.244.42.195	true	false		high
pixel.onaudience.com	146.59.148.16	true	false		unknown
inv-nets-eu-s2.admixer.net	146.0.227.109	true	false		high
d1ykf07e75w7ss.cloudfront.net	143.204.95.188	true	false		high
code4sabae.github.io	185.199.109.153	true	false		unknown
cdn.bigmining.com	143.204.98.58	true	false		high
ifccloud6.infocreate.co.jp	169.56.3.74	true	false		unknown
googlehosted.l.googleusercontent.com	172.217.168.33	true	false		high
aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com	3.10.35.49	true	false		high
s.w.org	192.0.77.48	true	false		high
cr-pall.ladsp.com	143.204.98.24	true	false		high
ssp-pc-layer7-lb-1418692822.ap-northeast-1.elb.amazonaws.com	13.230.7.5	true	false		high
mail.ja-ces.or.jp	164.46.34.110	true	false		unknown
edge.g.yimg.jp	182.22.24.124	true	false		high
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
idsync.rlcdn.com	35.244.174.68	true	false		high
rtb-csync-eqx.smartadserver.com	185.86.137.131	true	false		high
rtb.adentifi.com	54.236.227.29	true	false		unknown
sync.srv.stackadapt.com	54.81.207.173	true	false		high
b.hatena.ne.jp	143.204.98.109	true	false		unknown
tk3-805-12365.vw.sakura.ne.jp	27.134.249.119	true	false		unknown
osscdn.netdnasa9.netdna-cdn.com	23.111.8.154	true	false		high
pixel.tapad.com	35.227.248.159	true	false		high
twitter.com	104.244.42.1	true	false		high
sync.ipredictive.com	34.232.92.67	true	false		unknown
aax-eu.amazon-adsystem.com	52.95.124.170	true	false		high
cs41.wac.edgecastcdn.net	93.184.220.66	true	false		high
dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com	3.124.143.99	true	false		high
syndication.twitter.com	104.244.42.200	true	false		high
d.socdm.com	202.241.208.56	true	false		high
gum.am5.vip.prod.criteo.com	178.250.2.146	true	false		high
www.google.ch	172.217.168.3	true	false		high
ib.anycast.adnxs.com	37.252.172.249	true	false		high
prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud	18.156.0.31	true	false		unknown
edge.gycpi.b.yahoodns.net	87.248.118.22	true	false		unknown
optomaton.geo.iponweb.net	35.210.178.101	true	false		unknown
pug-lhr.pubmatic.com	185.64.190.80	true	false		high
eu-u.openx.net	35.244.159.8	true	false		high
spl.zeotap.com	104.22.25.87	true	false		high
elb-aws-fr-clickdistrict-1651093077.eu-central-1.elb.amazonaws.com	3.127.51.194	true	false		high
hbopenbid22000nf.pubmatic.com	185.64.189.112	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
penta.a.one.impact-ad.jp	107.178.248.96	true	false		high
widget.par.vip.prod.criteo.com	178.250.0.163	true	false		high
sync.crwdcntrl.net	52.48.248.240	true	false		high
cm.g.doubleclick.net	216.58.215.226	true	false		high
ds-pr-bh.ybp.gysm.yahoodns.net	212.82.100.176	true	false		unknown
sync.1rx.io	213.19.147.44	true	false		high
ads.playground.xyz	34.98.107.212	true	false		unknown
bidder.am5.vip.prod.criteo.com	178.250.2.131	true	false		high
star-mini.c10r.facebook.com	157.240.195.35	true	false		high
d1o24znjkq68c8.cloudfront.net	143.204.98.37	true	false		high
pugm22000nf.pubmatic.com	185.64.189.115	true	false		high
us-u.openx.net	34.98.64.218	true	false		high
stats.l.doubleclick.net	74.125.128.155	true	false		high
s.hatena.ne.jp	18.182.163.232	true	false		unknown
g.deepintent.com	169.197.150.8	true	false		unknown
a.tribalfusion.com	104.18.12.5	true	false		high
cr-p31.ladsp.jp	143.204.98.44	true	false		unknown
io.narrative.io	52.212.225.58	true	false		high
aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com	52.29.225.117	true	false		high
pixel-origin.mathtag.com	185.29.132.144	true	false		high
s.tribalfusion.com	104.18.12.5	true	false		high
alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com	54.93.69.146	true	false		high
a97adde81b00f2ca4.awsglobalaccelerator.com	13.248.242.197	true	false		unknown
hatena-d.openx.net	34.98.64.218	true	false		high
dac-yieldone-gce.pool.iponweb.net	35.213.109.249	true	false		unknown
elb-aws-ie-rockabox-scoota-2052063539.eu-west-1.elb.amazonaws.com	52.17.35.107	true	false		high
avi-aud-k8s-ams.pubmatic.com	185.64.189.249	true	false		high
rtb.gumgum.com	52.18.52.16	true	false		high
pb.ladsp.com	54.95.166.26	true	false		high
match.bnmla.com	38.27.122.158	true	false		unknown
ad.as.amanad.adtdp.com	143.204.98.55	true	false		high
tg.dr.socdm.com	124.146.215.52	true	false		high
sync.resetdigital.co	45.35.192.162	true	false		unknown
alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com	52.58.102.227	true	false		high
ums.acuityplatform.com	154.59.122.79	true	false		unknown
pug22000nf.pubmatic.com	185.64.189.110	true	false		high
spug22000nf.pubmatic.com	185.64.189.114	true	false		high
pmp.mxptint.net	204.2.255.233	true	false		unknown
visitor.fiftyt.com	35.201.96.126	true	false		unknown
b.st-hatena.com	143.204.98.89	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://i.socdm.com/sdk/html/adg-azs-container.html	false		high
http://https://s.tribalfusion.com/z/i.match?p=b11&redirect=https%3A//simage2.pubmatic.com/AdServer/Pug%3Fvcode%3Dbz0yJnR5cGU9MSZjb2RlPTMzMjYmdGw9MTI5NjAw%26piggybackCookie%3D%24TF_USER_ID_ENC%24&u=${PUBMATIC_UID}	false		high
http://https://dis.criteo.com/dis/usersync.aspx?r=3&p=4&cp=pubmaticUS&cu=1&&gdpr=0&gdpr_consent=&url=https://simage2.pubmatic.com/AdServer/Pug?vcode=bz0yJnR5cGU9MSZjb2RlPTE5MjgmdGw9NDMyMDA=&piggybackCookie=uid:@@CRITEO_USERID@@	false		high
http://https://www.stopcovid19.jp/	false		unknown
http://https://acdn.adnxs.com/dmp/async_usersync.html	false		high
http://https://adc.auone.jp/api/v1/sync/web?u=YO-h4MCo5sEAALQoIuEAAAAA&ut=1&st=2&ref=https%3A%2F%2Fb.hatena.ne.jp%2Fentry%2Fs%2Fwww.stopcovid19.jp%2F	false		high
http://https://image2.pubmatic.com/AdServer/Pug?vcode=bz0yJnR5cGU9MSZjb2RlPTMyMDImdGw9MTI5NjAw&piggybackCookie=8Qiqtu4fCnqXvBNLMuLvYA	false		high
http://https://simage2.pubmatic.com/AdServer/Pug?vcode=bz0yJnR5cGU9MSZjb2RlPTMyMDMmdGw9NDMyMDA=&piggybackCookie=RX-045ac90d-7f34-449f-bcd3-a948b166aa59-003	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
124.146.215.52	tg.dr.socdm.com	Japan		2514	INFOSPHERENTTPCCommunicationsIncJP	false
93.184.220.66	cs41.wac.edgecastcdn.net	European Union		15133	EDGECASTUS	false
104.244.42.200	syndication.twitter.com	United States		13414	TWITTERUS	false
27.134.249.119	tk3-805-12365.vw.sakura.ne.jp	Japan		9370	SAKURA-BSAKURAInternetIncJP	false
185.64.190.80	pug-lhr.pubmatic.com	United Kingdom		62713	AS-PUBMATICUS	false
54.236.227.29	rtb.adentifi.com	United States		14618	AMAZON-AESUS	false
202.241.208.56	d.socdm.com	Japan		4694	IDCFIDCFrontierIncJP	false
38.27.122.158	match.bnmla.com	United States		14277	GIGSTREEMUS	false
182.22.16.123	unknown	Japan		23816	YAHOOYahooJapanCorporationJP	false
216.58.215.226	cm.g.doubleclick.net	United States		15169	GOOGLEUS	false
185.199.109.153	taisukef.github.io	Netherlands		54113	FASTLYUS	false
178.250.0.163	widget.par.vip.prod.criteo.com	France		44788	ASN-CRITEO-EUROPEFR	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
18.156.0.31	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud	United States		16509	AMAZON-02US	false
52.18.52.16	rtb.gumgum.com	United States		16509	AMAZON-02US	false
143.204.98.24	cr-pall.ladsp.com	United States		16509	AMAZON-02US	false
35.244.174.68	id.rlcdn.com	United States		15169	GOOGLEUS	false
104.18.12.5	a.tribalfusion.com	United States		13335	CLOUDFLARENETUS	false
183.79.248.124	unknown	Japan		24572	YAHOO-JP-AS-APYahooJapanJP	false
18.182.163.232	s.hatena.ne.jp	United States		16509	AMAZON-02US	false
52.212.225.58	io.narrative.io	United States		16509	AMAZON-02US	false
204.2.255.233	pmp.mxptint.net	United States		20940	AKAMAI-ASN1EU	false
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
185.64.189.110	pug22000nf.pubmatic.com	United Kingdom		62713	AS-PUBMATICUS	false
169.197.150.8	g.deepintent.com	United States		19381	SIMPLY-BITS-LLCUS	false
185.64.189.112	hbopenbid22000nf.pubmatic.com	United Kingdom		62713	AS-PUBMATICUS	false
185.64.189.114	spug22000nf.pubmatic.com	United Kingdom		62713	AS-PUBMATICUS	false
185.64.189.115	pugm22000nf.pubmatic.com	United Kingdom		62713	AS-PUBMATICUS	false
37.252.172.249	ib.anycast.adnxs.com	European Union		29990	ASN-APPNEXUS	false
157.240.195.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false
143.204.98.37	d1o24znjkq68c8.cloudfront.net	United States		16509	AMAZON-02US	false
178.250.2.130	static.am5.vip.prod.criteo.net	France		44788	ASN-CRITEO-EUROPEFR	false
61.114.177.151	repository.secomtrust.net	Japan		10006	SECOMTRUSTSECOMTrustSystemsCoLtdJP	false
185.86.137.131	rtb-csync-eqx.smartadserver.com	France		201081	SMARTADSERVERFR	false
178.250.2.131	bidder.am5.vip.prod.criteo.com	France		44788	ASN-CRITEO-EUROPEFR	false
143.204.98.109	b.hatena.ne.jp	United States		16509	AMAZON-02US	false
91.228.74.134	global.px.quantserve.com	United Kingdom		27281	QUANTCASTUS	false
169.50.137.190	um.simpli.fi	United States		36351	SOFTLAYERUS	false
66.155.71.25	pixel-a.sitescout.com	Canada		13768	COGECO-PEER1CA	false
74.125.128.155	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
54.95.166.26	pb.ladsp.com	United States		16509	AMAZON-02US	false
157.240.196.15	unknown	United States		32934	FACEBOOKUS	false
35.201.96.126	visitor.fiftyt.com	United States		15169	GOOGLEUS	false
182.22.24.124	edge.g.yimg.jp	Japan		23816	YAHOOYahooJapanCorporationJP	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
143.204.98.44	cr-p31.ladsp.jp	United States		16509	AMAZON-02US	false
199.232.136.157	platform.twitter.map.fastly.net	United States		54113	FASTLYUS	false
3.124.143.99	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
143.204.95.188	d1ykf07e75w7ss.cloudfront.net	United States		16509	AMAZON-02US	false
52.95.124.170	aax-eu.amazon-adsystem.com	United States		16509	AMAZON-02US	false
212.82.100.176	ds-pr-bh.ybp.gysm.yahoodns.net	United Kingdom		34010	YAHOO-IRDGB	false
143.204.98.55	ad.as.amanad.adtdp.com	United States		16509	AMAZON-02US	false
143.204.98.58	cdn.bigmining.com	United States		16509	AMAZON-02US	false
52.16.214.249	match.prod.bidr.io	United States		16509	AMAZON-02US	false
35.213.109.249	dac-yieldone-gce.pool.iponweb.net	United States		19527	GOOGLE-2US	false
52.17.35.107	elb-aws-ie-rockabox-scoota-2052063539.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
52.29.225.117	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
213.19.147.44	sync.1rx.io	United Kingdom		26120	RHYTHMONEUS	false
202.232.238.39	cnt.fout.jp	Japan		2497	IIJInternetInitiativeJapanIncJP	false
34.232.92.67	sync.ipredictive.com	United States		14618	AMAZON-AESUS	false
185.199.108.153	unknown	Netherlands		54113	FASTLYUS	false
182.22.31.252	unknown	Japan		23816	YAHOOYahooJapanCorporationJP	false
13.248.242.197	a97adde81b00f2ca4.awsglobalaccelerator.com	United States		16509	AMAZON-02US	false
13.230.7.5	ssp-pc-layer7-lb-1418692822.ap-northeast-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
54.93.69.146	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
143.204.98.70	d1g3u69q0yy58t.cloudfront.net	United States		16509	AMAZON-02US	false
107.178.248.96	penta.a.one.impact-ad.jp	United States		15169	GOOGLEUS	false
146.59.148.16	pixel.onaudience.com	Norway		16276	OVHFR	false
185.29.132.144	pixel-origin.mathtag.com	United Kingdom		30419	MEDIAMATH-INCUS	false
198.148.27.140	lga-bh-bgp.contextweb.com	United States		19189	PULSEPOINTUS	false
87.248.118.22	edge.gycpi.b.yahoodns.net	United Kingdom		203220	YAHOO-DEBDE	false
3.127.51.194	elb-aws-fr-clickdistrict-1651093077.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
104.244.42.5	t.co	United States		13414	TWITTERUS	false
34.98.64.218	us-u.openx.net	United States		15169	GOOGLEUS	false
172.217.168.33	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
143.204.98.89	b.st-hatena.com	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1
192.168.2.5
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond

Analysis ID:	449115
Start date:	15.07.2021
Start time:	09:19:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://www.stopcovid19.jp/
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:	12
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.win@67/299@181/78
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://www.facebook.com/sharer/sharer.php?kid_directed_site=0&sdk=joey&u=https%3A%2F%2Fwww.stopcovid19.jp%2F&display=popup&ref=plugin&src=share_button • Browse: https://b.hatena.ne.jp/entry/s/www.stopcovid19.jp/ • Browse: https://www.ja-ces.or.jp/info-ce/%e4%ba%ba%e5%b7%a5%e5%91%bc%e5%90%b8%e5%99%a8%e3%81%8a%e3%82%88%e3%81%b3ecmo%e8%a3%85%e7%bd%ae%e3%81%ae%e5%8f%96%e6%89%b1%e5%8f%b0%e6%95%b0%e7%ad%89%e3%81%ab%e9%96%a2%e3%81%99%e3%82%8b%e7%b7%8a/ • Browse: https://www.mhlw.go.jp/bunya/kenkou/kekkaku-kansenshou15/02-02.html • Browse: https://www.mhlw.go.jp/stf/seisakunitsuite/newpage_00023.html
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
09:20:48	API Interceptor	4x 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:\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):	244080
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	6144:0rec7VDBGbrec7VDBGbrec7VDBGbrec7VDBGm:0reGZ8breGZ8breGZ8breGZ8m
MD5:	297B8B6156FC978E98086708BE851002
SHA1:	B0D749B7C1CECCF6F588F194607A76F81F73C5D2
SHA-256:	C0D6629F1B36C27A5B0F9E23FB3739219FBC20E1BC2974D84B1C6F929358EA8B
SHA-512:	251146031870BC5086D07D5AF6FAD5E901FFAE35F9A86708EE21CB1193F31673D83B57343BD5AD676D7E31B0C15E35715F19BF83F4C508F276766F267ABD5716
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...l.....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\9096A354A7A3E42F3F619F51DB75C6B9	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	891
Entropy (8bit):	7.448995063038933
Encrypted:	false
SSDEEP:	24:KEoum2gXtoum2h73IdYFp7pli5e5dk6Zp9fmje+7jOOS:KHum2Jum2R3Ide2wdxKL7jOOS
MD5:	6C397DA40E5559B23FD641B11250DE43
SHA1:	5F3B8CF2F810B37D78B4CEEC1919C37334B9C774
SHA-256:	513B2CECB810D4CDE5DD85391ADFC6C2DD60D87BB736D2B521484AA47A0EBEF6
SHA-512:	0F0369B90EF4930F59BD5C0091067200828BDE84EA703C1029EC5603CF4BD1084F0E7E15F370DD5554A9E310D60BD01BA54492E2E6D6301E44609033EA9EDBC3
Malicious:	false
Reputation:	low
Preview:	0..w0..._.....0...*.H.....0]1.0...U....JP1%0#..U....SECOM Trust Systems CO.,LTD.1'0%..U....Security Communication RootCA20...0905290500039Z..29052905003 9Z0] 1.0...U....JP1%0#..U....SECOM Trust Systems CO.,LTD.1'0%..U....Security Communication RootCA20.."0...*.H.....0.....9R.R...Y..]R.:Ce.K...6..d..^.....=K..].!. A..~v...>64.;..1.Et.=W.....j..A.....B...8..LT..6.E.{.e...M..~..;...:V.ZoviR.z...j.]R.-.k5.....j.:..7G.~WO?..g....SU...}.....x..a....J.....9..p.(?..@^c.<.*..k..Yj;.o....J..N..:.'.S..\$.k.P.- <..D4'.u.....B0@0...U.....we..|@....,8...<.0...U.....0...U.....0....0...*.H.....L:.D..E..~...B.d...Yl..._j.J..z....Er.q.:..o...#..\$.....q..).l]3_d.e;.o.vx..H..?.....N...U.....>. |..^...Oh:....C..W\bh|.....b.+..4.j...)V<..7.#l.N..tF.l..4...D..1r.I.....|.U.....G.5Z....[.q)....z....W#..!.?J9..I...7..]..3^.(|.}'....7

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\C8408FE5CA4467EE4DA84A76EF238FE3	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1129
Entropy (8bit):	7.296884447669073
Encrypted:	false
SSDEEP:	24:lvKUB888i7ZDlwjwN9CMDybfzHZib7H9JgPTPdvaI:l5m8nZZVmVTZc7H9JgPTPBaI
MD5:	312128F5A0ED7BA54B6582928756BA83
SHA1:	48504E974C0DAC5B5CD476C8202274B24C8C7172
SHA-256:	730C1BDCD85F57CE5DC0BBA733E5F1BA5A925B2A771D640A26F7A454224DAD3B
SHA-512:	DD35F36F0DB81B56A1CC9F734E4258D66125530FA8CFAF6B5EFE79D5173183024EBC78543B69BDD89FDE3724816A035A20CBDCEDB5E44DD2B746AB9B0B304C CD
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\C8408FE5CA4467EE4DA84A76EF238FE3	
Preview:	0..e0..M.....@.u.....!.....0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...201007192140Z..210929192140Z021.0...U....US1.0...U....Let's Encrypt1.0...U....R30.."0...*.H.....0.....(.....U.....zB..]&..+..L...k.u...G..U5W....9...<B.Nn.;.....\.Y8...i.Z.....$%..7q.....;ERE...S.4.R...`p.T..m...@4k+.f.f4|.k..W)..0.]. ro....X=.....+.....q].F..%...`guf.....\.S.:..G.....w?.S.....p...c.....S...H...i.%u...R...Q.....h0..d0...U.....0.....0...U.....0K..+.....?0=0;..+.....0../http://apps.identrust.com/roots/dstrootcax3.p7c0...U.#..0.....{,q...K.u...`...0T..U. .M0K0...g.....0?..+.....000...+....."http://cps.root-x1.letsencrypt.org0<..U...50301./.-.+http://crl.identrust.com/DSTROOTCAX3CRL.crl0...U.....XV.P.@.....0...U.%..0...+.....+.....0...*.H.....L.....71.....kb.lX.I~<....(a....s.I.z5....h...V./m.X.n56..s..m^..nr.*...Wd.[.i...|K ....rs...m.....a:.X}t6+U.=.c..C.9..kW.?

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):	1304
Entropy (8bit):	3.1576103530920845
Encrypted:	false
SSDEEP:	24:R+5kPcUQUfeD+5kPcUQUfee55kPcUQUfee55kPcUQUfet:n1Q91QeG1QeG1Qt
MD5:	1ED90EE46986A4D2419E54E48CCFCFF8
SHA1:	E729567781096785FF3698E53FBDF5B3E8D1FC42
SHA-256:	B1340939578630111E4DF321702E3B970F21DFC5758DC7C0C1EAF98687769A0AB
SHA-512:	D7C3A6BEB6B5D98A810B2D2E2A23D3DCEE75F4CF0BEC3FBBFECE6E99E71D03DF35246133B8D53EF86EA45258F2643E74E76B4114F749AD928F7D48BDE4904AB6
Malicious:	false
Reputation:	low
Preview:	p..... .....Jy..(..... .....T'._.....$.....\...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...p..... .....Jy..(..... .....T'._.....$.....\...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.".. .p..... .....S...Jy..(..... .....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."...p..... .....S...Jy

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\9096A354A7A3E42F3F619F51DB75C6B9	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	282
Entropy (8bit):	3.0522897993352873
Encrypted:	false
SSDEEP:	3:kkFklwZkNl1fllXlE/hLo3BRlRCd+iYl+XrJ91DAfjVvLlwvLlXPl1PclGlSdWng:kKJGlQij+dlJ9ufj76XPcGIRc21
MD5:	24AEF37955CB47D66506F150DD60D04C
SHA1:	F7472D27647154CA834F84501BCAE34707357D9E
SHA-256:	ABD95346037AFF68E28560B51949D41B720F8FDDA4A0287117229D7F35039EDB
SHA-512:	5C46DA03257E06FC2425AAD0AE278CD8E41ED6CA4DB88F151298EE59C45FD0BE6AC869254B202A074DD5CFB805CEAF5DCAE23E74971DC4520028D9D5F79439F
Malicious:	false
Reputation:	low
Preview:	p..... ....p....g./Jy..(..... .....D.....6.....{...h.t.t.p.:././.r.e.p.o.s.i.t.o.r.y...s.e.c.o.m.t.r.u.s.t...n.e.t./.S.C.-.R.o.o.t.2./.S.C.R.o.o.t.2.c.a...c.e.r...".3.0.0.0.1.d.-.3.7.b.-.4.6.b.8.1.c.6.c.b.2.d.4.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\C8408FE5CA4467EE4DA84A76EF238FE3	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	192
Entropy (8bit):	2.756882412434545
Encrypted:	false
SSDEEP:	3:kkFklRPNTE/XfllXlE/7Hk5jORDU+lJuRdxPlIXlflYD2Ht:kKGEsHOaOa8RdE1fW6N
MD5:	53E49B5C89C29C0CBEF6C2D2049B5A39
SHA1:	007D05E96C7BD12807572C55A1892B0E986E52AA
SHA-256:	651F32596F65152D504DA46A850CFCE0C73F9EDA3DA74225FEB81F56C36A0377
SHA-512:	86FC11C65EB70EFCF25A45525856B5BB9E3CDFB19725841C18DE5CE1047F85F366C8A76EC65ED2B644F5B8828314562D2D53448D3DC553A6F93FE4505ABB505
Malicious:	false
Reputation:	low
Preview:	p..... .....".(.Iy..(..... .....]..... .....i...h.t.t.p.:././.r.3...i...l.e.n.c.r...o.r.g./...".6.0.2.7.2.6.5.1.-.4.6.9."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\07f5191b-c2ea-4d7b-a268-9f1ccca25e8f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\07f5191b-c2ea-4d7b-a268-9f1ccca25e8f.tmp	
Category:	dropped
Size (bytes):	173641
Entropy (8bit):	6.079563455918964
Encrypted:	false
SSDEEP:	3072:r7Yu/l7/Xt8fQNi4F2lXqZnERTOFuTFcbXafIB0u1GOJmA3iuRS:nYN798YNjwlXqZnE1BaqfIlUOoSiuRS
MD5:	2C124987F416F04F41DC8FEB77BBE68F
SHA1:	917F797C76C1F323E32C418CE636BB462E99E7A0
SHA-256:	B18BDC2D51A461214D7D2DDEE4A8B8FD9D6F4CF930E6ACA06810444916C02E4A
SHA-512:	D71E1B58D2DF88FFB10BEF2F237C6BD41FC3F0034F98CE0BD4E71C6CAE34AA6834562D0A164201E61864AB5F0EEAC664EF8C4F5EBBB7BD0943ECDA6DB1109C7C
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.62633364150577e+12,"network":1.626333643e+12,"ticks":4026307162.0,"uncertainty":5383642.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715824031"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\13361eca-bb5c-4842-980a-caf29adaab87.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	95428
Entropy (8bit):	3.7516688550743917
Encrypted:	false
SSDEEP:	384:9vGN5Hw+nILzV8ixwNxrKvVf3+RraH7SGylrgDZRxWDzX7mrUVrmEQyA/hh5eOP/:teWhNG3MGUeXZTz4/jSfKZPlFv
MD5:	856C6B86E60CFC8CB85AC1CFC19A6A1A
SHA1:	60F1B8CF1C1CF17DE30E493BA0CBFD9326D5244E
SHA-256:	8BF3FFF47F587BBE9FFA4EC9FDD3480EFFAF3BB052166E8C4CBA5135BAA75AEA
SHA-512:	247D331B5E0BD5AA0F04D90F83829178A5ABBB698BA1E6A3A84E57D7774170B9A7BC621FA7D0CE42EC57BC15CAF4CDE6016673342AD2250F353B37E84A145A4C
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\17bbf285-ef36-4d74-b191-6b129e999017.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):	173641
Entropy (8bit):	6.079563611530981
Encrypted:	false
SSDEEP:	3072:b7Uu/l7/Xt8fQNi4F2lXqZnERTOFuTFcbXafIB0u1GOJmA3iuRS:3UN798YNjwlXqZnE1BaqfIlUOoSiuRS
MD5:	DDCCB07600DB2F6588E31C605AC4206E
SHA1:	6D713F48EF272056DEA2C0DBB1A70D178F409E35
SHA-256:	E5AF6E4FB497C9812D5DD0733276A6C67C33E318351B4F84AC34AD95D5BC8DF8
SHA-512:	BE9C42590F2C571654F3276D2268AAB59429A3BC43929E194B3B1F9F4E05ADF2857B36C4FEDB0C2FA5E6E8A5E4D44F31D23767525C95C6A33F8AA8F6A3816A6
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-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.626333643e+12,"network":1.626333643e+12,"ticks":4026307162.0,"uncertainty":5383642.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\5309e44f-d887-4a85-bdfc-f4027bbc3263.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\5309e44f-d887-4a85-bdfc-f4027bbc3263.tmp

Size (bytes):	173641
Entropy (8bit):	6.079566075568657
Encrypted:	false
SSDEEP:	3072:bolu/I7/Xt8fQNi4F2lXqZnERTOFuTFcbXafIB0u1GOJmA3iuRS:8lN798YNjwlXqZnE1BaqfIlUOoSiuRS
MD5:	6EC1EEC8697EAA01B6F6AA2D796813DA
SHA1:	24536DADB1B42E2E08BCCA4F1A6608085A529A53
SHA-256:	BB73F152959B8A7959FED19BA31550AFFA3C325B29E88909187FEC918B996385
SHA-512:	01B57BBAFF705D9A758F2A19CBFF2A27CEA7A3274806E4FC1FD9F819D7407FEF21906FA594DCDC5E77908AAE3709A994B309EDC599A22E499B7FA13E7682FB8 6
Malicious:	false
Reputation:	low
Preview:	 {"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"use r":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_t ime":{"network_time_mapping":{"local":1.62633364150577e+12,"network":1.626333643e+12,"ticks":4026307162.0,"uncertainty":5383642.0}},"os_crypt":{"encrypted_key": "RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiL GeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwR gUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_ manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"d

C:\Users\user\AppData\Local\Google\Chrome\User Data\6e75c698-35a5-4636-ad04-2f20ab382cbe.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.751312042912003
Encrypted:	false
SSDEEP:	384:zvGN5Hw+DLExwNxrKvVf3+RraH7SGylrgDZRxWDzX7mrUVrmEHA/hh5eOP3BNP8P:OWhNG3uGUeXZTz4/jSfKZPlFU
MD5:	81FB3699A689023E5192AD9117762252
SHA1:	39E6B8A74B4FDC941D5B284C51CF86AA46E6D63A
SHA-256:	E8F9E6D60209CB63061679ED4C94A684BA0B401939669A82EB4F54CE64CE389B
SHA-512:	B0B1DA63D5F65B6F4D0F0958C332ED6BC300ABB75026C5223DF830AB6471F8A7D95D92542FE6ED3E30759AB6195E26315C8E56B8E239C598E21DD43C6A8A411
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\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:FkXwgs0oRL6twgs0oRL6twgs0oRLn:+taRL+taRL+taRLn
MD5:	E6C1693D9F0F6B6E878D098FBFD4C92A
SHA1:	D9D2708143B4A3BA5D14DFED59DCB6B88DF172D9
SHA-256:	E9DA6B8F6549D084D8740EB4C25755989B057EBF4F36B5E526F34DFFAB7500CF
SHA-512:	19B28BFE66708B294AB033C2F87D219E1C29D4F9363AC92E89B9406F6E2ACB13AD5DF73DD7E163D1ADEC0AF89C42DA112AE153EB23378EC29302F91192B7C5 9
Malicious:	false
Reputation:	low
Preview:	 sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....sdPC.....UO..E.D.Q.o....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1257eab8-61d5-486e-a5fb-d5c82d2aff9c.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):	2546
Entropy (8bit):	5.603838340355171
Encrypted:	false
SSDEEP:	48:YreUOiieUQ6UUhvEUGijUpvUbSKUyB7zUsLqPeUekUeH+U3lqwUHUerUz1Uo:EeUOiieUZUUaUhjUxUbSKUyB7zUsePe2

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1257eab8-61d5-486e-a5fb-d5c82d2aff9c.tmp	
MD5:	5097E9B13A6E8D2F4A5E60EAEA6B51A7
SHA1:	4946E1109741CCE88D98D6D7A004EBA0C9E5EBD0
SHA-256:	A77884E0DF33618E29455A2202184F314ED612327FB62156DBA0AC39F934E87E
SHA-512:	860BAC59669A3390EACD677A8442A86181D09918072D61AD7CC299576F7C984E38157B2E6700BD50BABD30AFDE872D4B84F191961D211A95DFFF03B1C03BBDEC
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1637220045.607956,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626333645.607962},{"expiry":1657869644.584109,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626333644.584114},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1641885682.420145,"host":"TZmujbl93Yt3JI8wZ4X/zjkA0WFNGNW44A+o7h4YyHw=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626333682.420149},{"expiry":1657869647.205209,"host":"XOQLzqdQxNgMj/4MVc4Rpg9bCVZob5H6tbzVJkKXVZA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626333647.205214},{"expiry":1637220045.131765,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1bbb7ac5-a5d1-41aa-a307-d7baa5c040dd.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):	5197
Entropy (8bit):	4.967940352527838
Encrypted:	false
SSDEEP:	96:nuLqAtMpIKIs5k0JCKL8kkI18bOTlVuHn:nuLHMpIuh4KfkIK
MD5:	AF98323F225AA230A9CF3993A9434299
SHA1:	29FC11330D4C8138BFC2CA0CD08F6484B936244D
SHA-256:	8B748FEF102C2628CC561CA0DAB4240F34C6BB1BF1C31D6BDE115D4DAE7725C1
SHA-512:	26CB56FF4D11EAA6F443A21A647B4616A3F53D6EC01A1AFE89A7BF77094CBD742711EAB63ED6079038A2E61AD48D8B2CE365D1D4910AC631A550D1D1E1736EB
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13270807238076514","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","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","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1fc45c48-6085-4afb-a115-60203fe8089c.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):	2714
Entropy (8bit):	5.604189856264938
Encrypted:	false
SSDEEP:	48:YueU8ieUp6UUhIEUBijUpbUj3SKU/UU0zUEbqPeUekUeH+U3lqwUHUerU/Uc:1eU8ieUwUU7UcjUtUj3SKUcU0zUhPeUv
MD5:	051DEE88AD00CCB260928FE41AF944E8
SHA1:	C998B3FB4C18B21B7B778E31871676343A5FF9D3
SHA-256:	C2DB149CA09D86B1898A3EAC588D60AC679226F70145238809C8F833C66E9C4A
SHA-512:	695D5009701F6A4A464A731C7D875992921EC507486E19F7CAADE22AA9D24C45C8D4986F60679EFD96AB14EFF56ED25CB52BC7A695F7B7A9B4F6E03480D4E69
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1637220093.901481,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626333693.901487},{"expiry":1657869694.200656,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626333694.200661},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1641885690.370332,"host":"TZmujbl93Yt3JI8wZ4X/zjkA0WFNGNW44A+o7h4YyHw=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626333690.370336},{"expiry":1657869647.205209,"host":"XOQLzqdQxNgMj/4MVc4Rpg9bCVZob5H6tbzVJkKXVZA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626333647.205214},{"expiry":1657869693.225699,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\392c3e29-f64a-40b8-a373-0015566343ae.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):	5861
Entropy (8bit):	5.169397469229062
Encrypted:	false
SSDEEP:	96:nuLOHyMkeeekWIKIz5k0JCKL8kkI18bOTz7VuHn:nuLJMTedWIBh4KfkI9i
MD5:	7A73F2C9E608347F95E2D1A8F743CCA4

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\392c3e29-f64a-40b8-a373-0015566343ae.tmp	
SHA1:	1586D1F52732153001A854EE49E8E3C7B2A22E55
SHA-256:	07DE489DDBFAE589964D6A900A58978DB90DCC0B3113056CA97180CECFEDB5C1
SHA-512:	9471824DA573FC9AC666285484ED3DCEDF3D964D0FE514BC13A48DCA0C9132E22A1E434D23355C7C2855E04C11EDD89DE9F5BEFC77D86C12BB8C9B494F3EC9E
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13270807238076514","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","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","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3d35275f-adda-489f-bd74-6e45d6c7ac62.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):	5887
Entropy (8bit):	5.172322276857838
Encrypted:	false
SSDEEP:	96:nuL+jyMkeeekWIKIW5k0JCKL8kkI1+tbOTzBVuHn:nuLtMTedWIEh4KfkIsm4
MD5:	5EB88129F7919B4436818BFAF773866D
SHA1:	6F76DA27831DF1998BF2C9F49AE922B14D2F37D5
SHA-256:	FDB45CBC1F7065B83FDCCBA1B17EDF616B4044EE84B4D6CBA7A3BE6EACAEE07C
SHA-512:	D13108EDE6C91CA7BE634D4DF9B9902332DEED588BDDF8183FEF4A923A0AA915C70DDEB16353E9B38193F1DFCA3EAAC4BBACA0DDF1D6AB6AD73BAD630C4D9E4
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13270807238076514","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","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","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\45bbe0ee-f342-4060-b567-48c1d93cd8fc.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):	5897
Entropy (8bit):	5.17461140604495
Encrypted:	false
SSDEEP:	96:nuLsjyMkeeekWIKIbe5k0JCKL8kkI1+tbOTzBVuHn:nuLvMTedWIdeh4KfkIsm4
MD5:	AC37B96E91EA718E2B588FF087AA73FA
SHA1:	0EFBCF088B15EC84CD78706D8B4D5720F9F750FE
SHA-256:	4F94DE14BDD0F6589BF8CF5D94F011336555850D80100B8F529EFFF2405FC413
SHA-512:	3DE8D4CCAB43712E3BB70DF07E8BC1E5BAF410FC09C3E5F56DDEC6FBA0D57567E227D3CFD51EDD915BB293F8A97F2621D074D5FF7F78036DB56976D217C2EF5
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13270807238076514","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_all_tabs":false},"browser":{"default_browser_infobar_last_declined":"13245924607060180","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","2042016"],"daily_recei

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\62d29eba-b592-409f-9efa-bab7873c3b4a.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):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIIyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\62d29eba-b592-409f-9efa-bab7873c3b4a.tmp	
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607497410","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":27387},"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607334226","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34287},"server":"https://ssl.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607463627","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31787},"server":"https://fonts.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248516607318875","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":23359},"server":"https://apis.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\80f55b8d-8fd2-440a-a15e-19001067ad39.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):	22602
Entropy (8bit):	5.536310244323537
Encrypted:	false
SSDEEP:	384:QOEt0LlaaXV1kXqKf/pUZNCgVLH2HfDkrUHHGEnZi0ZY4w:jLI7V1kXqKf/pUZNCgVLH2HfQrUnGEny
MD5:	DA911691D4C764BA78E6FAAAD6ECD9F3
SHA1:	0910ED626FD6A972BD4D11C9E1CA030CC7599BBA
SHA-256:	123FFF6A7853C6D8C6783BCD2447A92CD173277900D5A614020466F6EE90DA44
SHA-512:	585DFD9E0E8FE7767C9E19308CE63342B66E3C5F39EF7A8DD2EA56D8F9FE37CC87CA3F10D4277AF624EFDCD5AAF1D33052B254DA8C32E83EDCC28AC4170B4A05
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":"13270807237732744","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\82c086a3-9b05-4929-971a-eb41cb71f415.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):	4829
Entropy (8bit):	4.83639871285926
Encrypted:	false
SSDEEP:	96:JzMKDHGXOrUxCt0mq3rC6qObaU61H686icH31IoSxZMRfo0MG3GKVWGmGXehM:JzMKDHGXOrUxCt0mq3rC6qObaU61H68y
MD5:	115D814BF1E54192A1850A10B3B0F051
SHA1:	1472301DFB0A843115EE64228C86BA781649980B
SHA-256:	27286C1D11CB899259DEC3BE825247FBD88441310A2D2CC9E54B9FE1B712168C
SHA-512:	178ADA8978965F94FB560FB5ADF9FF3CCDC567BE5DB3F767A0BB0C9EFFE43AA46AC5C59A4128C560A580BA0C974026D6C8D9B01E4865B8D1763B03247C06044
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://play.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13273399243603995","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13273399243927051","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://fonts.gstatic.com",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9204a067-40ec-484e-856b-7ae04dc0f8b0.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):	2882
Entropy (8bit):	5.603414068495031
Encrypted:	false
SSDEEP:	48:YueU8ieUp6UUhlEUBijUpbUj3SKU/UU0zUEOCAUr/qPeUekUeH+U3lqwUHUerULT:1eU8ieUwUU7UcjUtUj3SKUcU0zUPRUrE
MD5:	54D421259410EE619E756202F7EAAF6B
SHA1:	5EBA9A51328A8F305D1695B592DC9D05DA486612

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9204a067-40ec-484e-856b-7ae04dc0f8b0.tmp	
SHA-256:	3FA3CA2AAA270C8CB1F0DA6C997E20E3DE133EB9F1A5D5DC8BC4D24728A5E16C
SHA-512:	69E0F6DA4FD892184D6CB6160E63166CE21B0D93009002474E381A6D44590F0B3953502C8A48943BFF87B5A1632D948C6027D05A8F760E03BA8EE85BC1B790AB
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1637220093.901481,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626333693.901487},{"expiry":1657869694.200656,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626333694.200661},{"expiry":1632986995.029294,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601450995.029298},{"expiry":1641885690.370332,"host":"TZmujbl93Yt3JI8wZ4X/zjkA0WFNGNW44A+o7h4YyHw=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626333690.370336},{"expiry":1657869647.205209,"host":"XOQLzqdQxNgMj/4MVc4Rpg9bCVZob5H6tbzVJkKXVZA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626333647.205214},{"expiry":1657869693.225699,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\96e1c5a1-569a-4ceb-b126-2a12afd1c45e.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):	22601
Entropy (8bit):	5.536233374995903
Encrypted:	false
SSDEEP:	384:QOEt0LlaaXV1kXqKf/pUZNCgVLH2HfDkrUHHGnnZifZY4jx:jLl7V1kXqKf/pUZNCgVLH2HfQrUnGnni
MD5:	ECEF70892C5B4D7731E6656C66706609
SHA1:	360FE9D6D806BA9CFABCF1E55F0C86C34157B6A1
SHA-256:	182E90BE3D76C6EE68FB5798A5A28F860293E322669ADCD7842F6959234944A5
SHA-512:	83709AD517C86030933D6FB72E4310F8756BED86E70E81DDD78D5C4F4900C64969B248B1BD582CB7233D71C3C13B13978788E0A2D2B778D7B8BF4D2486789958
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":"13270807237732744","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.25093489283942
Encrypted:	false
SSDEEP:	6:mFcgOKM+q2Pwkn23iKKdK9RXXTZIFUtpEcgOQ1ZmwPEcgOypMVkwOwkn23iKKdKT:UcmM+vYf5Kk7XT2FUtpEcO/PEcwMV5J3
MD5:	215A89614F27806F1D5710DACB8E4E3F
SHA1:	869FF097782ED9C644895338C69C1549CB60654C
SHA-256:	825355881C3B5C7B19B192605F7E4409B9C6CB386277DDB1C29A4B5AB360D8A0
SHA-512:	36A136761DAA5CA3E8F39954E198FAE0BD8CDE45BF41B9C3680A7E6D265BA27F0D6ACF7193BBA07E08BD685804792A6AB25886A6F8A2B987A0551F8ECF027E57
Malicious:	false
Reputation:	low
Preview:	2021/07/15-09:20:56.414 7fc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/07/15-09:20:56.415 7fc Recovering log #3.2021/07/15-09:20:56.416 7fc 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):	318
Entropy (8bit):	5.239572827328485
Encrypted:	false
SSDEEP:	6:mFcgiTN4q2Pwkn23iKKdKyDZIFUtpEcgsVTNJZmwPEcgEDkwOwkn23iKKdKyJLJ:UcDavYf5Kk02FUtpEc3VT/PEcR5Jf5K1
MD5:	8030B525271F8DEA80C2A731349ACCD7
SHA1:	30034A90E8871080E9FA5A164D813E96006EE3AE
SHA-256:	CB1F478410FC9F110EED7986CFD0FB3A059C789B8E9D37C041CC4692299A513B
SHA-512:	2D46661E486915E5AE68FA41E4B7A7E043ED6C7C5CFC353498F3A28D0ED896C96013DEB6AC3C205F0995F7468BE6B6720E9E9EAC0FFBA1DFB6DCC62AA2B4A4D
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Reputation:	low
Preview:	2021/07/15-09:20:56.464 1084 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/07/15-09:20:56.480 1084 Recovering log #3.2021/07/15-09:20:56.482 1084 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\025f1edcacd2ee39_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.422152174016108
Encrypted:	false
SSDEEP:	6:mcggXYGL8YLEJIGYPgKv/S0glAxriJh1Yi5tlhK6t:bcYqI34Kv/ZFxrKzN
MD5:	114BF5142ED4191CD28D65A6730A35A7
SHA1:	18886EDE3E3C6869866F927A2DBDDCE6AD647B24
SHA-256:	F656DEEE6A81420B2573E3E6E2D0C73F9236749F479B3835103D57BC92A9B1F3
SHA-512:	507967E8621BC8F320251DA098B3BC2E07E2CB4095E2793543545E78854EF8D6E5AE662EEF43D8F1E36F20AB5D14C033F670D8F891556A7B08B29C79E498C7F9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T....._keyhttps://www.mhlw.go.jp/common/scripts/jquery.mk_location.js .https://mhlw.go.jp/g.=..%/.....h.....y..P...R....U|O..2...Gk...Y^D...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\02889551788d14d1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	239
Entropy (8bit):	5.738788684896844
Encrypted:	false
SSDEEP:	6:mUkVYGL+MORm/ITCm8EI7x6lSsFdyWjvAeK6t:pkNpgTCmVI7xO/br3
MD5:	65E67EED04485D0E2774525AED4269FB
SHA1:	5ABBA0F9ADD8CC3BD0B3861F7736EE6CCE6E757F
SHA-256:	FD14BF67F4FF3485CF4D4543F6989AF943E9D01D85BB980ED8FDC3734D1099E2
SHA-512:	2A4320E77DB3FA0C6150E00A564847305A4EED1FB715329A14406BD635674658151B4F3FB90EE27B990E186A02BD617D58CED73E9E32F53509C7EBA338F05FC0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k.....00...._keyhttps://www.google-analytics.com/gtm/js?id=GTM-57M9G3G&cid=1860853571.1626333663 .https://hatena.ne.jp/.g...%/.....l.....W.....`@.l0....D...!....A..Eo.....Dd.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\04b54609843d02e7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	200
Entropy (8bit):	5.456349299588844
Encrypted:	false
SSDEEP:	3:m+lMS/08RzYP2FycyGYIKSFvDzY4mV1/tlHCo/gt/S42kdl9cq9eG9UmjllpK5kt:mA/VYe1K2YF1/SigS4l9l9n9/1K6t
MD5:	C4A82D2A5E68AC7BEF260A32E5322102
SHA1:	FF00C3B758ED1DE07937129117CFA36125224CD3
SHA-256:	64E572A4D63C44F6C3CEE0FF4B8785DAF88E6B81E1E016EB9E1B2CF1F5FF3E0E
SHA-512:	30F13B09E8C2128387811A33BC4CCFBF60C7EA09ECAE9F8DCE2680502DCD556CD5807107153A2F14ED7FEA9088DFDBCC8B70E353B503687671350CAE83E8AA1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....D....7....._keyhttps://code.jquery.com/jquery-3.2.1.min.js .https://mhlw.go.jp/H9...%/.....S..i...B../8._t.iI...NoH../...A..Eo.....y.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0b91c0c5c27d6e45_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	197
Entropy (8bit):	5.4379146522837605
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0b91c0c5c27d6e45_0	
SSDEEP:	6:myE/yEYGLHje1dOAlS0kiPxOg/B5RK6t:oPjmb/kihr
MD5:	F1A0704F464E63FE84DF37B1D59F992D
SHA1:	1F709B7F362A0B415995F13FA9261CA2C59FA241
SHA-256:	D5E01C69D3E0C81114BCF145D6AE524B5ABFC9E41AB14ECFF55B1D426088FBA0
SHA-512:	36C72FF7FC1A217F75820FE0B75195903A7E5BAE7EA838E9BFA173D68B6C7D50EFD57B00BF638B11C1117F40B447EC1CE039489D753E39E222934FACC5D8D7F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....A.....,...._keyhttps://www.stopcovid19.jp/fukuno.js .https://stopcovid19.jp/Y...%/.....W-..p.P....C...2S.u..u./.?0.]...A..Eo.....K.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0da2f868400f82ef_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.763848423430045
Encrypted:	false
SSDEEP:	6:mqYk+f2pomBMiQfzhmJ2W5aSjlKBVTehjoNbK6t:z++amBbAkJHEGKDTelwN
MD5:	D49FA88813D79244A8A4F1C2423D9E5D
SHA1:	6AF837F224AB5849E3690B1042D1D3E95C61D8E0
SHA-256:	257CBA1D61D2229CE8257C9F11A3B273CBEDD22E0BCD2520F7CC72B76A4FCA43
SHA-512:	2B56BE12DC1342DF779C4A63F9D2483845A66B788939C39B275B67C70AA86C61C2963E11959EF3B1E354B717964BA48B67BE57CBDCE38300CE148229E2CEA8A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....J...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yj/r/IUy0P1uEqH3.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/VY..%/.....i.....T..Db.rqY'.....;..|.x.g .....A..Eo....."..........A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0de576a9af9c678f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	198
Entropy (8bit):	5.380291669082768
Encrypted:	false
SSDEEP:	6:m7PYKxDCiGzWwoUo+9SlpXkTyfwXsdh40lhK6t:KH7GJs+9W6PsL
MD5:	EF2F3AE4F33F9D45219F18B2DD26F0C0
SHA1:	C4D6A0FDF3DE86458C7885FB3E5C0169FD4FB071
SHA-256:	ABC4CC84453D453B7AA844AD614600A6BC52D43D29E0A163D76C757A004FDCD2
SHA-512:	D8A49003428906B0DF7331F3A2D2B475865236DC330F7CCA4AD5BC076B3121AF4186F5B83FC1C0F061AE4E2773206C89CF6A6A6692A93DACE2F2A1D763D49F5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....B.....a...._keyhttps://platform.twitter.com/widgets.js .https://ja-ces.or.jp/X....%/.....w.....W{.T.....FY....P-B.K.8.:..sb..A..Eo.....)9.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\135a9e73b7a29232_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	43888
Entropy (8bit):	6.146029008603494
Encrypted:	false
SSDEEP:	768:zjEtYm6X9bQ3pxFHPIcv4+EP00tgKsoGVu98dJMUkONp+1nhsFsb95fQbl5S2p:PEam6W3p3vIcv4b0JQbibS2p
MD5:	68E12404605CC63293B7B8C800041E32
SHA1:	83BD78B2C27F3F223C0BCDF263AAE232F9590C28
SHA-256:	AC778CFD76EF8B8BAB49C704F19E97CA95B9F7D317642A87BF5238EB463D5252
SHA-512:	C8953B1B542BF15D534E58E3DEF75F87298D0D3C80690468D21BAECE0367AC791622ACA2F37A1B5ADFACDE08615D67840C367BCCEE7419CC9A15C71D8691DA 6B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H...Nj...._keyhttps://eus.rubiconproject.com/usync.js .https://rubiconproject.com/..E..%/.....d.....K.L.....\....)....M\.,%..fG.A..Eo..... .@.....A..Eo..... .....'..|....O.....G.....(S....`<....hL`0.....L`.....Qc"^.....comments..QcV.....rtb_sync.(S.4.`".....L`..... Qf.0[.....retrieveQ ueryParams...Qb..).....p.....K`....Dg.....&.\..&.(...PQ...(Rc.....Qd.u.....isSellerSync`....Da.....b.....P..@.-....4P.....'...https://eus.rubiconproject.com/usync. js.a.....D`....D`....D`.....%....`....&...&....&.(S...`.....4L`.....Qe..nH....skipBuyerSync.....Qbz@.....Math..Qc...v....floor.....Qc.....random.....1...QcR/J.....sample....Qe>O.... ..alreadyRanOnPage..Qb...:....log..4Qk....%...skipping buyer sync cause already ran....0Qj>_..#...skipping buyer sync due to sampling...K`....D.a. .....&....h.....u.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\185f65919f8657a6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.738847853388139
Encrypted:	false
SSDEEP:	6:mjtgEYk+f2pomJ2iGyhmJ2yfvSwl8C8JwfrHrfRK6t:eD++amJ2ivkJ3PlJ8GzHTr
MD5:	926A51005B0EF89133A80E43F3B3CDAC
SHA1:	5E7F1F293A788C847D896E105757963428AE4976
SHA-256:	7BE4422708E1D5C4231799F421D03501D6E31BB2E8A713B994CE1FD948B96FF0
SHA-512:	ED2519F2AD0E252C4133C369211FCAC22E82E1BBF0B1938AE11FF8306E2E648ECB9D5FEBF541BDAFAA30908451B3392410CCF0BA9118C287632EBE38407B82F D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y9/r/ugD21mPGNBo.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.C..%/.....S.....#...._.l.....).....~.. .._...b.A..Eo.....C.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1ada5ae8963a52d7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.729840662629358
Encrypted:	false
SSDEEP:	6:mhl/lXYk+f2pomdMCWXewhmJ2eSmahQ1nAmbK6t:IXz++amdzwkJNShQ9N
MD5:	52AF597BBE68C377B1087F583658DDEA
SHA1:	D0578D71F1BBFC870F5B2618DBA165EE8BED047E
SHA-256:	1811A40F36D04A2BC71ACB5AFA696F4A05B23AA7C241E8CCDE9DF8BC94269EA4
SHA-512:	D0E63E11A3EF357AA789A031A14BC2B436F53624C3E3BE3DA6270D34E84A91BD95698A5367875B9139979C9B1F75A9B70686BCAA86AB1D4A6D704E979F48CAF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...J..V...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yv/r/GG1Y0sYc7My.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/^Z..%/.....j.....i...c..<.%...7.....T....#.!..- .A..Eo.....D.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1ceb78fd7b4f42b9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.500700939512458
Encrypted:	false
SSDEEP:	6:maPiYGL8YLEJlkcWIfYCX/SF1tlU5KfGTa/hK6t:/PvYqIUnCX/2u5EG2/7
MD5:	98E8269B621B14E866C4191371B246B4
SHA1:	6E9D9872363F4056D5451F8951CFC3374D042881
SHA-256:	28B4012E0FF50BB610E8DFCFEFB699EDA74025BC5906174AB478F71287092B06
SHA-512:	447FCAF8F5E7532BCFFCDC1F848A7C0024E3FCC82D6BD5453BFD3464E56DA7895596E5BCB566DE316F0EE2428C9C5D614EC7E783866D1111EFCAEDB4B1C1D DEB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....[....._keyhttps://www.mhlw.go.jp/common/scripts/jquery.mk_inputFucus.js .https://mhlw.go.jp/..?..%/.....}.8.E.....:.!.3...u...A..Eo.....Z.A..... A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1ed688489afa22d3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	243
Entropy (8bit):	5.496033682202563
Encrypted:	false
SSDEEP:	6:mfPYGL8IGKXVUf4adTSNFVgGzWfSQeUnnp6BTom4KthK6t:sKf4YTUFiGGJzwFomjt7
MD5:	36949F377FB86B3AF68E490C16890D5D
SHA1:	FF2253D3720626DB53E4F5EFC5E13436A7D70AF1
SHA-256:	DE0916C9B317AA8EEC196E2647973C850EE1D0657360CD42307ADEB3B814EC87

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1ed688489afa22d3_0	
SHA-512:	2FC7B7F737D393AE41F38FEE2C267F8D58B2DA5B45F2A9D30BDDB30E67CC5D8815DD4C55FC44EAC1AFB9D9F2A4C11BEEE0C315E986BB19F080B99CDA9C9BA4D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o....._keyhttps://www.ja-ces.or.jp/wordpress/wp-includes/js/wp-emoji-release.min.js?ver=5.2.11 .https://ja-ces.or.jp/.s...%/.....Px.....<W.Y(T%.{..r.g.....H.(wC..\..A..Eo.....|wY.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1eec102889a7d5de_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.4646786343408165
Encrypted:	false
SSDEEP:	6:mgqEYGL8YLEJImJ2HY/aS3wLCTq6M3At+5/ZK6t:CYqICnSM6COv1hT
MD5:	55DEE79F96539F70D6033C48D33E50C7
SHA1:	198058813D251DC7C32100D2A949A30C56A02F2F
SHA-256:	15FBA0D44B64C36E2D2F12AE51E069A3597ED03CE75830E8DAC9187548B91C4D
SHA-512:	A51302DC3E45B4D498FA0EA15F3E9E4B34A082046D23628FF385BD28CFE1C1ACDCB308863BEFC281878CD4C10583E47A211A1937430650493755241C5303C0D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O....._keyhttps://www.mhlw.go.jp/common/scripts/DD_belatedPNG.js .https://mhlw.go.jp/..B..%/.....:.k!...W5.K6Q...8.>.De...._..A..Eo.....Z.01.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1fe1ce509956500f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	196
Entropy (8bit):	5.414366090291771
Encrypted:	false
SSDEEP:	3:m+lD9dA8RzYkwLLIK7CVRv8EI7K/tltlHCtLlll/pppPBzKIvgsXtqZm2hlltlpD:mk9PYk+O58EI7ktlStL/rxxXhaDK6t
MD5:	BFC77A751AD823EF9794E8D5E36FF0A3
SHA1:	E4817FDBB58933CE633601B5D2099611D6A8A468
SHA-256:	1C82D88ACB12938D8C5CF42AE5523C43A340C7B8AE7AB6E24D2CBDE8BCDCB2FC
SHA-512:	886A57DF81E6C38741CD53F4D90320191B3FDF974C37DD7DA1AE8A97FF20A947B6753515713E24CDAE17D88CD6F6681EB75ECAA6A20E861FE468E3E9E820A01B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....^....._keyhttps://static.ads-twitter.com/uwt.js .https://hatena.ne.jp/U....%/.....L.LQ...$..4....-V..'....u..o...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2010a3486f72e241_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	224
Entropy (8bit):	5.41559930993283
Encrypted:	false
SSDEEP:	3:m+lUV6v8RzYrSL8Y4GK1JlWxIE2F7zY4p/vtlHCo/gQ9hCoE9p4mZ7/tpK5kt:m/6EYGL8YLEJlJYY3SoIQ29prZnK6t
MD5:	31D4101FCB15EF7F1E5A92A0883E3D7E
SHA1:	89BC280A08BE7EE6A1CC3C988C3CB80B45B2F944
SHA-256:	463F6461E9EDA1064795239937C69A9EE7AA9802A97DA9B1127FFACA9453A90E
SHA-512:	168BB311FEF5CC282FEC3D26F5B888ED9BAAE826612F7503F8360C4952751A52AF8475691C984B28703ECA7FAC9887E4FEE60E186444D5187E6E87BF1795B636
Malicious:	false
Reputation:	low
Preview:	0\r..m.....\.....n...._keyhttps://www.mhlw.go.jp/common/scripts/jquery.mk_styleAdjust_icon.js .https://mhlw.go.jp/..A..%/.....l.....~.E....6.i.A.'F.J...CH....f.\.A..Eo.....D.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\22af22b9e46fc343_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\22af22b9e46fc343_0	
Entropy (8bit):	5.556273964854746
Encrypted:	false
SSDEEP:	6:mQ2VYGL8IGKXVYAscDXxajbMCXxdLpTcwGzWJ9SaX0CGbX/niDK6t:2v5iM0HLpTcwG2Mji1
MD5:	770192B6B242594A0E6B487536F0F1A9
SHA1:	01063373C3582222B5042BB64642AA354AB53B19
SHA-256:	B261AD5D60C3BAE8EF831739C2FCCB749E5FE2B8596274158C85422EF9BF829C
SHA-512:	8220E21FF5BFC7559EFB30B6B8D06A14F6DA8DADA82AF1736B6ABD89B0E64695D0C2F789824935CB363E1D5AEB8606641AA08BB125D1C79C0D733B00F6A8DF1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V...._keyhttps://www.ja-ces.or.jp/wordpress/wp-content/plugins/lightning-advanced-unit/js/lightning-adv.min.js?ver=3.3.3 .https://ja-ces.or.jp/.....%/..... ..Au.....p/...h.xIl....T...'!.....A..Eo.....[.J".....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\254c5407071bb61d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	308
Entropy (8bit):	5.579857485086237
Encrypted:	false
SSDEEP:	6:mN/lXYKE12xY52s2JdQG+/K6tQ3SIGJdQG+75l:+/ldEUK52sKqW2a7
MD5:	DEFFE38916D2A3761B04C633F61B62F8
SHA1:	89632F574351E6E08D30494F965D8DE56EF12705
SHA-256:	A7795D6301A61305E4D95F51253CEAD461185139F69C04BB7846C55FEA9E9A71
SHA-512:	118C34B81CE8456CDF0628DBD0425E00C5825ADFF6995BA61CBD810AB5D0B61FC136C32E4C3E83CBC4AAB40518F509704C48A77DC11EB50FF0B129775A96A82
Malicious:	false
Reputation:	low
Preview:	0\r..m.....\.....\....._keyhttps://ewb-c.infocreate.co.jp/ewbc/ptspk_loader.js?siteId=031_mhlw .https://mhlw.go.jp/(.H..%/.....n.....U...s.MK.l.8..l..o.....`M..A..Eo..... .....A..Eo.....(.H..%/.....k.....U...s.MK.l.8..l..o.....`M..A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2d25afbbb58fae73_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	244
Entropy (8bit):	5.785927206583515
Encrypted:	false
SSDEEP:	6:mqnXYGLYX2UjUbH7yhmJ2ZaSZ69X5oAI/m4d5lDK6t:RdbGkJQadpOX
MD5:	B150F01354DE8CEEA1BB862EA88B3D60
SHA1:	3163E76707E325D63E9051581B7620CA8C01BA26
SHA-256:	0157C3F06C2901A72D2A3CC589129087A6C7B56872DECC52E9570E0354A664F7
SHA-512:	0940FBE28037B4A52F134C003F5D9D5609A6BDBDED9E21C9B472483BE6C19FCD35CC0FABE05C94817C036AC6E75F9A9AC925066447D99104E38C26EC5426E60
Malicious:	false
Reputation:	low
Preview:	0\r..m.....p....}....._keyhttps://www.facebook.com/rsrc.php/v3irB34/y7/l/ja_JP/bIuqT9-AQr-.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.0..%/.....x.....xVc.+;...)..... ...z...p.....A..Eo.....vgS.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2e945b9f3fee2c50_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	411
Entropy (8bit):	5.770156200016439
Encrypted:	false
SSDEEP:	12:EMGKjqoTCIHBDaTYq/aYjWXiSVI7l7Xu:EXUtCCkdTyXiSVI7Fu
MD5:	AE98E80E894EBC5BCBB96EFC68A3AED7
SHA1:	68DA62B7DA52A4B38F4EF2EEF7FDF2DCE734FBBA
SHA-256:	6F3D487EA4F398C8864B601ADEC3C1DE2987F27CD20F0D8F4FB7483E6FC5CA90
SHA-512:	04388CA483E5BF1EA2E7B66F84F9F7C0A6A2911162CB2A9CF870E6F9C7DA77507A6D7B7CC883CB7881BAB53D5D741CF4ECD83C215FDAEABE9019FBACF520AD88
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2e945b9f3fee2c50_0	
Preview:	0\r..m....._keyhttps://i.socdm.com/sdk/js/adg-script-loader.js?displayid=1&async=true&flexibleOL=true&autoPadding=true&tagver=2.0.0&id=92278&targetID=adg-slot-wrapper-entry-double-rectangle-left&adType=RECT&width=300&height=250&apsamznbid=2&apsamzniid=&label_random=6 .https://hatena.ne.jp/u.L..%/.....R.....'..=.....4.....H.....8g.~...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3478c12dca436e2d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.722952302860543
Encrypted:	false
SSDEEP:	3:m+lYm8RzYkwLf3G9LomYI207G3V2QufRJ2EtlHC7l/tCeprlzt46XG8E6RmUpspD:mdYk+f2pomTyhmJ2ES7tfztBmwOK6t
MD5:	41E7825D02E1257B5886DFD9239A15E5
SHA1:	10BEC8ED22ED0AC647DB0E3ACA2F01B42A7E3D31
SHA-256:	A15546220185BFCCA2ED7D707B31FB6DA97BB9BB40876EEB3FD4261F428F3933
SHA-512:	BF67B4FACBA3453F5C171297FFA1A03F60ADCB5DCC51B22069E895CBB665492A5418B58A84FD2DA626633E43DF3C2E35E8C105601ADA1E54931A899648BB426 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....z....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/ys/r/YL6q3hajciu.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....%/.....K...{..B..:&MM..FV..O%...r.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\374f2986eab128df_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	199
Entropy (8bit):	5.410437921842627
Encrypted:	false
SSDEEP:	6:mFvPYGL8YLE6c2vfYQSAXeB89kP4v/hK6t:IUYe24QbO2kPg
MD5:	29F21BDDAD06C095BB2DFE056933F010
SHA1:	FFB6DD555ACDDA5954080F7950F1C848D5295D04
SHA-256:	3DB3343D501D13654DDB4E7F1E96663CBE5E07CCA0DDD4E609B2191FCE9095E5
SHA-512:	B92DC472C268697578B1C79CFE0F2FB904098040B8DB3D6ADE3B0FE55DACC8F69B6F20679D9506A600E2E1A5A72EEAB734E71FB6BA344DB1B42D5DBA251854 83
Malicious:	false
Reputation:	low
Preview:	0\r..m.....C....._keyhttps://www.mhlw.go.jp/common/js/bundle.js .https://mhlw.go.jp/J....%/.....0..+...w!..+..9.5..+.#?..A..Eo.....x.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3a2bde8044c36811_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	458
Entropy (8bit):	5.440355006039192
Encrypted:	false
SSDEEP:	6:mSYk+8my48EI7PSUdevg9Ck9FZK6tWS3KlQevg9Ck8SgqevgCkdQSQIevg9CkE:z+854VI7P9dei9FTwJqei8TqeimRIei
MD5:	DD64B2C0F8490DE5CFA67892696CD8A8
SHA1:	95B67719493B1622A497BE943ECAC1B250C44227
SHA-256:	EC171ACD1B63717C43BD565C6F962522EEE325658412CEB52EE500275B1C60F9
SHA-512:	7064B701712B8809CAEC06DC543095E4D4B7F4754BFA3D053EB7733C8250F621C64C21499E006C05F818BF6ED4985D17EEA94D8462089164BAF4A4C7D781176A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J.....(....._keyhttps://static.criteo.net/js/ld/publishertag.js .https://hatena.ne.jp/.h=..%/.....y.....k.J9D.o}...)TV....._..C.g..v..A..Eo.....C.....A..Eo..... .....h=..%/.....k.J9D.o}...)TV....._..C.g..v..A..Eo.....z6.....h=..%/.....k.J9D.o}...)TV....._..C.g..v..A..Eo.....4..F.....h=..%/.....k.J9D.o}...)TV. ...._..C.g..v..A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3bb10d6b1efce9fd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.7485702701711565
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3bb10d6b1efce9fd_0	
SSDEEP:	6:mkUYk+f2pomWuAO7PchmJ21S86j4a/jgPk+RK6t:i++am77EkJOZbmby
MD5:	17B53D1E737D8CA613BCE3CC166850DB
SHA1:	9FF5C299927B21E1CB23F97C312B67F3220B509B
SHA-256:	9AD9DD3CE8D013C00D93B20C4CFBD285E1C832A45C934477E83BAACE94588F98
SHA-512:	35A5EAAA8672410AABF562D1E680BAAF1FE7D02CC57A33CEBBE85F44C835DB71105060DCD0667E36F605C2854C59A7CC84C9935A1B2D310F1C301558ECF30FC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...^*~....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3i2UN4/yt/l/de_DE/tpIQPRjSdgv.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/dB..%/.....?.....w.@N...vpC....p..7.P.....t..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3e325b24ae8e7fc3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	244
Entropy (8bit):	5.552706891769479
Encrypted:	false
SSDEEP:	6:mI0+YGL8IGKXVUfIQKvKXvYTrGzWX3SjuLP/bKAv3K6t:fxKfIQKSATrGa3iOX75
MD5:	3AB29FB004FE0CD994144659FD7E4855
SHA1:	0A409FE54E68ACB89031DF4548D1664E360C6268
SHA-256:	33728A28E6E840592FC3EEDEF6AA74CFDF6AFA602CAAF46D150A1604DCB7DC01
SHA-512:	3322BBD0EAF3854D1A81C43AFCAAAA3A8BBCE9B2D52E8068ABC4AD075D4C3E5D234B54F11D1D1EAB81C45380B73793038E9965737220433CA7F7DDC21D5D291
Malicious:	false
Reputation:	low
Preview:	0\r..m.....p..._. ....._keyhttps://www.ja-ces.or.jp/wordpress/wp-includes/js/jquery/jquery.form.min.js?ver=4.2.1 .https://ja-ces.or.jp/.....%/.....;v.....V..j.9V.....P.....D+I..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3f06794e593404b1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.770668933914948
Encrypted:	false
SSDEEP:	6:mSfYk+f2pomoTLhmJ2afvS7JNo+VYxaK6t:3r++amoTLkJL4NIs
MD5:	10CCEB295D58568CB81143D075592309
SHA1:	7D9DA31CABE1904E967207B3BB8B31B0006E1FF5
SHA-256:	0BCB5866FD84584B1FCBAB0962098778ED6D3493580658D854E68FEF980982B9
SHA-512:	EBCB9FA8F6C9A459CE7B20986A0A813155865A60F54D8AE77377C4FFDDC42A5644646368440FDCF9DB11357DB5772FDA59D3575F6BDB471F0740C35742B348A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....F.;...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y5/r/MDvm8UUNBBw.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/!...%/.....g..z..N...G.;@.$...z{.P.....A..Eo.....^.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\417d44c966162bbf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	333
Entropy (8bit):	5.639801259950797
Encrypted:	false
SSDEEP:	6:mFlXYBZsmzRqpV5Ko1r/WvHZS+HSklquPbUqNDxnK6t:/a+RqPXr/WfJHTltp
MD5:	7C22297F1CC0E37F3997CD2A0B8405A0
SHA1:	CE3683176972E6350F3D6BE3C892A826000EE6B3
SHA-256:	4D7BB3F4872F0FC53FBA39C6040032814475D084F4AB3AA6ADDB0F639111A526
SHA-512:	56D6415390C0FF2526B59E413C970D69205937236592EDFCDF3FE9ECCF5C1B2FEABD7D12338A1D0D72F706164319348701742EE806E57EDC6D1FD9A8DA301E0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....?....._keyhttps://image6.pubmatic.com/AdServer/PugMaster?sec=1&async=1&kdntuid=1&rnd=25560792&p=157377&s=0&a=0&ptask=ALL&np=0&fp=0&mpc=0&spug=1&coppa=0&gdpr=0&gdpr_consent=&us_privacy= .https://pubmatic.com/.....%/.....#.....23.....*..F~_P../.....hk.ng&7.A..Eo.....9.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\41e713294820c411_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	412
Entropy (8bit):	5.7091343667192325
Encrypted:	false
SSDEEP:	12:kkGKjqogIHae/aYjWXiSVI7e5k8Z8VJ7:4U+CaOTyXiSVI7e5kF7
MD5:	69E53E3B2084CE41CB09A973E3E7F24D
SHA1:	E6D51320EB286804B3151C6903096C5482DB8AB8
SHA-256:	94257872F94C358070BCBD6C16E7EA32019F1A485E50AA9F0B06A0B94E16A914
SHA-512:	21A363D29CB6ACE5CBE21CC658079237475 23C25455E5ECC5319BEF4CC905ED4AA8E51BDCBC31A8CC295A282C92EDB4F9E647502AB0C5EAB510B251EB31F6FAE
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://i.socdm.com/sdk/js/adg-script-loader.js?displayid=1&async=true&flexibleOL=true&autoPadding=true&tagver=2.0.0&id=92328&targetID=adg-slot-wrapper-entry-rectangle-bottom-right&adType=RECT&width=300&height=250&apsamznbid=2&apsamzniid=&label_random=6 .https://hatena.ne.jp/..L..%/.....n.)..C&..nN.P#.fs.i....6.....A..Eo.....5.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\42fa32866eba36b2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.78674367505801
Encrypted:	false
SSDEEP:	6:mDYk+f2pomW0xOu8whmJ2y1fvSxYMT512UDNY7H4o5RK6t:S++amPgu/kJNxCh2q2j
MD5:	C533FC8D56E1734302482AFD4319E0B5
SHA1:	91370831C67B4F6A7F73C50AEF6425DC3C531AC1
SHA-256:	067E1D48A4C5D02BC080454CB1662E08478B4C5E935429068E17F26F52238D0B
SHA-512:	93BF06A9AB200C2FCBA11342314A25001AD8F881C9CCF79276DFB903DDCDC2D29D59BF83DAF72B1822AEC68105FA7EAFF879C21565955456AF248185A4D428EA
Malicious:	false
Reputation:	low
Preview:	0\r..m......s....._....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iMoJ4/yX/l/de_DE/a-2ellqyU3L.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.q..%/.....v.....T...[.-..HD.....(G.A..Eo.....\.R.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\446f107d2b69240e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.72756990171896
Encrypted:	false
SSDEEP:	6:mH3Yk+f2pomWdO7REwhmJ2SSLQ0GAxAqRK6t:QT++amZ7NkJJ437
MD5:	BE55D5EAE60AF055E86B6DC03656A62C
SHA1:	B7677FD135F4EB9774C87C76EEC2DD4A44751EAD
SHA-256:	8162FA565E432D2F02785441E5048479083C867885176260100C39F11F4B55B8
SHA-512:	2AE1EEC2E53077AB7092C9246623795A71EC28A966E7E73618449083D8F92043D343FFC68A1E17606FCC3A1E1723C3AE7FEF2997F0C64E5F93FDC3BFE7B22346
Malicious:	false
Reputation:	low
Preview:	0\r..m......s...cZF....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3ibyi4/y1/l/de_DE/bt7u4jh_X13.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/r...%/.....n.[..{...xd..I.o.T?..|...0)...A..Eo.....-.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4f99f75766b6b7fe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	398
Entropy (8bit):	5.76124899681435
Encrypted:	false
SSDEEP:	6:mhWPYX20EKH/bbLCosbnKYKPHnRcIe4AXUYKl3bXELml8EI76XSdvK7ZFbhK6t:CGKjqoEnhIHR5e4AXUYKlXiSVI7ESkH
MD5:	D39F5A227E577DC982C27B9133205A03
SHA1:	84A53CEB88A83E9938CAF4FB14A414558C6378B0
SHA-256:	114C162727132FB8E26CD73239E1BF9459504D086B0A72A7513E7D74E96E01BE

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4f99f75766b6b7fe_0	
SHA-512:	4D6882CF9E3DFD4E1B6ADA2BC276EAFBA9788C715C7318140D150E94C44DA3B40A95FADDC1A51CB6C33D71F1A5A010F6B379608BE4FFD907145247E500E7E1B0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....#>....._keyhttps://i.socdm.com/sdk/js/adg-script-loader.js?displayid=1&async=true&flexibleOL=true&autoPadding=true&tagver=2.0.0&id=92625&targetID=adg-slot-wrapper-entry-text-ad&adType=TABLET&width=728&height=90&apsamznbid=2&apsamzniid=&label_random=6 .https://hatena.ne.jp/y.L..%/.....J.....zq(.....%..[.....) A?T..R..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\501b480118794d26_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.87775080991336
Encrypted:	false
SSDEEP:	6:mIYGL+MlwJJS8EI7LHSeWEXXjhgNNl/hK6tYcMAK/5TysSbp+EXjhgNbk/:FIwvSVI7LHVWEX9ghWc8/299gJk/
MD5:	507ABF03F186289696FB9338EBD6A4BF
SHA1:	AAD0DE88DAA5B00E5DA853002025F43ED8C2749A
SHA-256:	DF4D73C39F1ADBC70BDB494C9167880774E08F8FEB67D20371C64DAA981ECBE6
SHA-512:	8008014A7DC6FD350CA6DCD1340A63AA80B5950815BC52D8BAF81D5EF6327C271759A359180EB30FC4C070E539DEA5A85312A151C9139A592877A4965CC359A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H....._keyhttps://www.google-analytics.com/analytics.js .https://hatena.ne.jp/q....%/.....h.....C.Y/!Y..F..$..Dz&.I...f...#.r...A..Eo.....0.....A..Eo.....q....%/.0!..B9385DB78262768CB4ED9051FA35C2468E7FB8AB2C778CD77886AEB23D9DDC3AC.Y/!Y..F..$..Dz&.I...f...#.r...A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\509232bb9ca12ba0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.578598281508151
Encrypted:	false
SSDEEP:	6:mPVYGLSmXZCLRpj8EI75tlSgiuObFhygK4P/K6t:aUjVI75XUBBhz7h
MD5:	F375D17E33E586CFA6EDE77B9C8D740C
SHA1:	091AF8AD30660B8C6783FD6C368520F774FDC285
SHA-256:	6E3B593F8B109878E7EB695930B8A8994A143EC869A135DAAA8288ED5965B536
SHA-512:	F215335CF4EB254CC91085309BE6D2259F519EF66062919341D265719BE7CB37BB9CF74EC978F6719FDE49157351B822D9BA2247C67155EC7DE0452E80EFE870
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....H....._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-5TDHQX .https://hatena.ne.jp/...%/.....j..>.L...I.q..q..u.x. Jk>"....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\51196661b8f777b5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	192
Entropy (8bit):	5.298784263870987
Encrypted:	false
SSDEEP:	3:m+l8rHC8RzYzTgukTVDv8EI7lVFXtlHCfdAEgigDmWj2Wcx2h44mM8XlpK5kt:mPPYtWVj8EI7YXSfCZmWjxEFM8DK6t
MD5:	FFEC0EEC6D052062B35EB6040F5AC492
SHA1:	3361876F5E773854C4AB640871E9EB979B7EEC24
SHA-256:	82A3E28F324F16CA1FF06D2245FE3895D1FE9CD80E25A9F9608D100AE9A656E8
SHA-512:	5E2F8D5E928A56D6BFE07F84B1F980A30DCF9F6F7D5A33372545E234D5D19124C70D7E0CFAE3AC22AD3C16FF7FC827560EFD7C00F996CD0AFEBE932AEDAF177
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<....._....._keyhttps://yads.c.yimg.jp/js/yads.js .https://hatena.ne.jp/.Q0..%/.....%a...E.+U..SK.....3.4Q@..i....A..Eo.....Zp.=.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5d9be227865dff27_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\5d9be227865dff27_0	
Size (bytes):	193
Entropy (8bit):	5.3568182266417885
Encrypted:	false
SSDEEP:	3:m+lE1/llA8RzYzTgukXPCVRYsspFfAK/tlHCqll/b0egQ9p8pbVRmM7tllpK5kt:mj1/lXYtmPCVa0K/SqXdp4C0K6t
MD5:	9F4C11A89EE7AA8B7BECA5F16CC895E7
SHA1:	BC6260C3FFB8B87A720658E232D4A0D898D833E2
SHA-256:	C42AE1BEC364BD4F2AC26C363D9D287F9ABC431818430D3C94C56CF7A50EDA4C
SHA-512:	50F38FA427E5A642C685E51321D661D7E1A038865BF3A5F5E8B401174EC0BD212FD0D34A189FBA3DE41345AC34A9258069FD1A8D32CAF9D4B74B63135EB4035
Malicious:	false
Reputation:	low
Preview:	0\r..m.....=.....{....._keyhttps://yads.c.yimg.jp/js/yads-async.js .https://yimg.jp/..L..%/.....M.....$K.<....2I.mN.u...I...L.Yft5.A..Eo.....c.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6115739dd1388ec4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.427621714839514
Encrypted:	false
SSDEEP:	6:m3PYGL8YLEJlzWFVhY3aSNg/WEW4YIK6t:jYqI6F43a+g/s4J
MD5:	B7698F6FB17873311A73884D36249B7B
SHA1:	0CEA101B5C4F00BA7A78924AA1323DA91069CCCC
SHA-256:	D21900A200FAA290D27B5B7D48CF0ECCE1DEFB0A2C94BE3734106B620350C9AA
SHA-512:	7E1FF522D6539DAA31FF73087297BDA53D1A7B477EEC13FAD2C0CCD534C619D480200D5D02C5B0F41BC15BC06904C7B7B15B50D4E02814DBE400747D4CBB1 D3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H....mxb...._keyhttps://www.mhlw.go.jp/common/scripts/jquery.js .https://mhlw.go.jp/l`;..%/.....3@...%UXvO...{}.h_...}.....]....A..Eo.....k.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6198a102811c2f6d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	251
Entropy (8bit):	5.528080576688287
Encrypted:	false
SSDEEP:	6:mgvXYGL8IGKXVYAkF/0MBXPdTzgGzW+ZSxq5PgUvhOf+45TK6t:NvdvG/0MhVTzgG5Oa6hF
MD5:	E3CBB84E44AA20E005E381D3BF8FFAC7
SHA1:	4F2D669720979191CE866308F7CCFC8F4D632D8E
SHA-256:	8EC5D35747F81E3A9BAAF618F40D10B36FA5328F01F7A0D89C6D9493E196117C
SHA-512:	2A91769C06CD17586BF12A0BDE66E5E8E644CE0691C72C33649D704433FF722B1037200E686B1322D47E4D73135B66751380D56E6198710F4229DA8801E1B505
Malicious:	false
Reputation:	low
Preview:	0\r..m.....w....._keyhttps://www.ja-ces.or.jp/wordpress/wp-content/themes/lightning/js/lightning.min.js?ver=5.1.2 .https://ja-ces.or.jp/VO...%/.....@u.....K..... Hx.....".13....VM$.A..Eo..... w.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6214889f7c2e82fe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.696377377462819
Encrypted:	false
SSDEEP:	6:mMEYk+f2pomPMvmhmJ2EOCSN51HRdqK6t:Q++amAmkJHQH0
MD5:	CCCF38894E770989B5DFDE454E3B93AA
SHA1:	D2500C8AF8D1428A6C8EDF1C624EA10940BC02F4
SHA-256:	075B31B389FC12BE0487D8204E46540514713526323A1185FAA8EC802E983A7F
SHA-512:	D0412164A2C775857769FAC88270318F8E67C6F1994CD75468D19300DF7FB8FED298B0161FC59EC2C091AC08C395AC5F81937AAD8E8CF30EFE79349B39E8302F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....>.B...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yd/r/Nk-rM4iWJZl.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/G[..%/.....I.....H}.Q..U3.1g\..=..6..n..xv T....?.A..Eo.....6.s.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6386862eb4b2bb21_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.677969582459076
Encrypted:	false
SSDEEP:	6:m+/VYk+f2pom70XzhmJ2lShiNTs+xin0zbK6t:FN++am70XzkJeOKTj
MD5:	6E60407A6FD883A030050A847E8EB191
SHA1:	04C953261DA3250CFA5E4F48204340F677D3E301
SHA-256:	AA00860C81D98697010F89401B2FA937D54DD5B665520C90D83E5080B9A2FF19
SHA-512:	C904641C53AC3BE2BE7C0C3C7388AC81188F8F0DE059AB072D82ADE86B6C307D477EB454763E19BD50E72F08C9B40EC2D1778BC0A948A7312D806944B61DD4 4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y_/r/JopZtdti8dq.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/?C..%/.....F.....;...L.tUq9..,F....x..H. ....).A..Eo.....Lc*.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\665a8aa81f8330ba_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	74200
Entropy (8bit):	6.106038115358412
Encrypted:	false
SSDEEP:	1536:YtrghDqJ1wDb9LZ5PlhNaZ2VE58ML/pEqTII9d6aTniF9dzf:Irg8PwjbhK2V28MtN8IX6ariF9p
MD5:	4B8E6E4A8A551E4FF55A28AE0DCDD1DD
SHA1:	5BE5DB6FE1EB61948553310699E6BA675BE3D1CF
SHA-256:	F10266AFE7ED6F25C194A7F8419A866BA9081B905AE5FCD29F129009A38D34FC
SHA-512:	BD62B7E1D457D8A8681363A79B50EDC1821B985C05A6B5D7635DD07AF867CFCD308107C243047F4117E0BF130599A1D2371976AC1EDAE63EE72DEEE684720E3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....K.....B9385DB78262768CB4ED9051FA35C2468E7FB8AB2C778CD77886AEB23D9DDC3A.....'.....O..... ...d.....8.....`.....D..... .....\...x.....(S.D..`B.....L`.....(S.]..`p.....L``....u.Rc.....R.....Qb.....n.....Qb6g.....q.....Qb.C%.....r.....Qb..r.....t.....Qb.e.....v.....Qb.B.....x.....Qb.....y .....Qbj.TC....z.....Qb.....A.....Qbj.N....B.....Qbz";v....C.....Qb.....F.....QbN].....E.....Qb..y.....D.....Qb^..3....G.....Qb.+.z....H.....Qb.E.....J.....Qb.....I.....Qb...N....K.....Qb".. M....aa....Qb.a.....L.....Qb.1x.....N.....Qb>..4....O.....Qbn-.{....P.....Qb.....M.....Qb~..&....da....Qb.....ea....QbN.....Q.....Qb...L....S.....Qb.}x#....R.....Qb.H.u....ia....Qb.. .m....U.....Qb...8....ha....Qb..t%....T.....Qb.....V.....Qb".....W.....QbF.....Z.....Qb.6q.....Y.....QbR..7....X.....QbB..f....ba....Qb.y.....ca.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\693b0dfadae079cc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.4592469285776275
Encrypted:	false
SSDEEP:	6:mxV/XYGL8lGKXVUfJCPTSNFVgGzWIX/SElGkzC5fTVhdK6t:OddKfJCPTUFiGV/TV+B1
MD5:	5370C8DD5177452B1D571B3696327AFE
SHA1:	2172FBBAC12CCDB7EBEC25CB14562402C25B3489
SHA-256:	60722579D15DADD1F0AE0FADBEBD3E07A467C6B904E54548205ACD376D2C5033
SHA-512:	F19A587D744167F79F505BA4C4CD0D6931BDC881D047B814D865A652F25F451A45DA6630B73A0934E211C7C2A5AB1A006491BBD1C909B30F5F6C382527E2E432
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g...D.Q....._keyhttps://www.ja-ces.or.jp/wordpress/wp-includes/js/wp-embed.min.js?ver=5.2.11 .https://ja-ces.or.jp/.....%/.....Aw.....o.&./{...T|SQ.I.L.KtED_ .W.r....A..Eo.....h.@.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6be9779e925d9085_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.410592593935031
Encrypted:	false
SSDEEP:	6:mkPEYGL8lGKXVUfIQKddTlgGzWnfaS21uzy3Gr4K6t:AKfIQKDTlgG4fadzv
MD5:	5D79384FF4E621D089DA2A37C1687A8D
SHA1:	E831C1A1C69A166822B558660FDDB4D3EB273CA9

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6be9779e925d9085_0	
SHA-256:	17D329CA67695CE46771143185431E9D4DFCD90441AAA772C0EC084F81B0A6F5
SHA-512:	05A0459341C99C11AD4EF2ADB4EC12F54F3F9A581748357642FF4CD5968BE4D60D67E1051605EE5B67CFE611A23A230244B09FE6E75D4821E0DD13311B320BA(
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...(..4...._keyhttps://www.ja-ces.or.jp/wordpress/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1 .https://ja-ces.or.jp/.B...%/.....9u.....K.Wa....Q.5$ .X>=.szN..4a.....j..A..Eo.....y..P.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6c328409abe273f8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	260
Entropy (8bit):	5.547611701243024
Encrypted:	false
SSDEEP:	6:m4XYGL8lGKXVYAscOGAlACongGzWls3HSdE6esBoiXrnzK6t:3v0G0ACJGDHuErwoip
MD5:	F26A1FCB367495C7C52BAF4E77C812A2
SHA1:	5C5CADC7F5DE5EC5A3D43145ADEF5D5DEF28A6C9
SHA-256:	3CBEA22A9EE2F21A63236093AEDD4E1D51EE2E8D4CDD7DD8D1F2A79CB6D42559
SHA-512:	DEE2FE3865F693C6D47754C6AD26F3723961C508EFF17523831DBE4088498599FBB7D470665434724A2783BBDFB66145493F4CA555681A1DFFAA59FEC268BC7A
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://www.ja-ces.or.jp/wordpress/wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=5.1.4 .https://ja-ces.or.jp/.....%/.....8v..... .O.D.`].5..N.F.U...O...!54..... .A..Eo.....&.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7052c509a8f8b1f1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	200
Entropy (8bit):	5.460137733252597
Encrypted:	false
SSDEEP:	6:mfYL39j8EI7Ol91/S2VUHrSz/kYphK6t:RNjVI7O5/5gK/z7
MD5:	32141AC196AB7CB07A88E7888013D21B
SHA1:	9014E0B402D7DBAD5BCB05CC77B602FADE7695D5
SHA-256:	4A5A1F191AC2695E6CAB75DF5B8495A99F4BE93E108A210C55AA052160798731
SHA-512:	F15C043D68B4B88A2518BDEB96ADA891D50EAA12FD37AD8E77D765CB21125C6B6351AB3951BA6DB8C82CD7CED89FA56550B3C00AB47DFEC17A5F241CA3692 FA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....D.....3...._keyhttps://yads.c.yimg.jp/uadf/yads_vimps.js .https://hatena.ne.jp/.b4..%/.....5\.[..Vw.]!*...d...JP...Yo....A..Eo.....T.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\71ff639c7a25c6fb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.440568560702981
Encrypted:	false
SSDEEP:	6:mVYXYGL8YLEJIyXM7kEBPYd1/S9gIf7tjawh/ThK6t:UYqIl7kogPOgIf7tjNp/
MD5:	849C775AE1A2ED0F2715BBF448B50727
SHA1:	537AD0B8441B07BE4690A98F8FA95E63474441CF
SHA-256:	9FB708861B4005E593455FE275D24FB8B35CBBDF07D5BB2CA81B6131AB07D117
SHA-512:	62567D88D8F11E5988F6A3B87D4589444372BE8F56E6DF4FAA8A6C31BB2E3C8CABE5A47E97017BA17C092CC47F16461D7281EE0F1103683BBB9561B182C595A5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O....._keyhttps://www.mhlw.go.jp/common/scripts/_scriptLoader.js .https://mhlw.go.jp/fm:..%/.....lz...V.HP.ZE...+vF.7.....k..Z..A..Eo.....xB.....A..Eo .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\73ccb4559ad00796_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	220

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\73ccb4559ad00796_0	
Entropy (8bit):	5.476236845603668
Encrypted:	false
SSDEEP:	3:m+lJmmll08RzYrSL8Y4GK1JlWxjk0zY4kHXtlHCpg30UMRtpgXoz4mA+pK5kt:mO1/VYGL8YLEJIM9Y9HXSKiTrhK6t
MD5:	ADCCA35FA70018033148B627191FFEC7
SHA1:	BA92CF04A6A977650D84C134E20A6B09B2B37B90
SHA-256:	294B23F7463C2B2B91956DFA948EB37B75AD3405294BFB79D0C5A49C1BF20D96
SHA-512:	117AC319286DA67029585FF6971944A54600128F8F00DAA140B86FFAEB763E56BF54F7FD8DF6208FB29552C4F54893CA75E496FFFADB8B00874AC079E4889428
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X...1....._keyhttps://www.mhlw.go.jp/common/scripts/jquery.mk_megaDropdown.js .https://mhlw.go.jp/.n@..%/.....rq..E.<E._.....;...9.?..J..A..Eo.... ..f#m.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\76015e3a4b6224a2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.765403820617526
Encrypted:	false
SSDEEP:	6:mjEYk+f2pomWzVeAOZTLahmJ2YuvSTYFE4k4NwK6t:0U++amMOZTmkJidFzkD
MD5:	DF52D552C75F71BCE3F59CF7B1DE7444
SHA1:	E179197B89A2D2323667B422B67C3845A12ECEA0
SHA-256:	7637B64CF4F87A21AC61B68E69F2E033617E8410D57046C852F1B383DAA29E35
SHA-512:	46703D0F494F7755A5D7B6A8EF3761A4077188E87995D12A1ABB182AE4AF8338BAE1272EFF7712CB7E159B8AA0026BDF3485396FA5B651230E5856DFBA943213
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iVab4/y2/l/de_DE/RTkqPFbXKo8.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/[...%/.....gE. 2@h[.R.g].Sqx...:7.Pl.8.;,..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\777a7fe0d0f666fc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	249
Entropy (8bit):	5.720819239355275
Encrypted:	false
SSDEEP:	6:myYkmLf+kmXCUkAFuAEQK8EI7sllSdsxahKz34WZK6t:4+ktdLAE9VI7Misw0hT
MD5:	6784C0B751C9F7A9ED5B2CAA72CFDBA0
SHA1:	D66BA586AAF434E225A5B5594C2C6982D64B071D
SHA-256:	BE3A81EC4EA7F451C60CA604859E6D65BD56D0839EE70A6CD6441787437703DF
SHA-512:	11B390D6392617D78FD508DD9C48F9665D5CC46DE1778B0577422240CC2E8902A2BE59F9657FC7511A153D6BC1860E431FFCAD5347720A7509F60ED55792E062
Malicious:	false
Reputation:	low
Preview:	0\r..m.....u....n!....._keyhttps://b.st-hatena.com/js/v4/bookmark.js?version=b28e833a092c996f374596d23318dea9e3c5a9c8 .https://hatena.ne.jp/....%/..... .._u.....7....k..Vx.....A..Eo.....5(.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7aee37dd622a4e46_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.711296930256191
Encrypted:	false
SSDEEP:	6:mcc/YGLSmXZCep5ZQzpCGNFV3p8EI7slSJshgWuzum4ihK6t:r0Lp5IpD5VI7ERGJJ7
MD5:	C54BC5D8D2C8E57C35CD9BE4CFDBD5F9
SHA1:	3BD8375B04DC4AB472D8F30B4C900ED318995798
SHA-256:	3F47570F560EC4F187540609335096F7F81DE18B1C404EE86F5F009C53098794
SHA-512:	F7D26458CDD5DF2AD304E2408532FA6B9D5C90D60D16B115ADF8848078641DE2D06BE930F71DC5EF2E76DE5DE0E789D7A111440F31914D4CD36F610CB4F0DE E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d....._keyhttps://www.googletagmanager.com/gtag/js?id=G-LZZ5Y9M58K&l=dataLayer&cx=c .https://hatena.ne.jp/.....%/.....{FQ.U.`.7...z...}.-..n.<.O.. ...A..Eo.....].....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7b2a5235503b4b88_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.512041380455129
Encrypted:	false
SSDEEP:	6:mW9YGLHaNuaCcOo9S1vyVGCH/TP4hlZK6t:99aNjTRG+GCfT0lT
MD5:	E212BBAC82B0CD6543F8B7CAE704AA9B
SHA1:	252F87F57A68321944255373F959008C65962732
SHA-256:	5DF04562722EED7DD6C3F3BEC4C520C7C59453EB8A5C8862D2E84B24315EC78D
SHA-512:	CBE0685EABCE0A2C0DFF341DC658CAAE882F1758B1E41756CC0411D72FE02A75DE66A6B179EC6DF0080922CA91BC0B6C1D4C529A7DB3F69A8ED5263E074CE D80
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K....v....._keyhttps://www.stopcovid19.jp/Chart.bundle.min.js .https://stopcovid19.jp/y3...%/.....e0.f.J...+GK...]..........]..0.A..Eo.....T.w.....A..Eo..... ...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7c21be5089b61970_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	5.651857596975349
Encrypted:	false
SSDEEP:	6:m3EYAWTfHdezFOllSqKuzql0grY71K6t:ufcZpauul0kM
MD5:	8BD94AB6F3A8C8DFD200459677C3AD3B
SHA1:	7930B153ED9E3EF761257C5E5D011520844D7312
SHA-256:	7A4F2B9CE1243B73027FBB50B7C6CFC4A7B5416703B87254F3503218AB9364DB
SHA-512:	7D8DAB72A562FD29B0DA3B3A93C801B8DE65430CF5F255ADC3505BBB7E4978488BDC41E3FC16D2DF0CE8AE5B6F89EEB07054039DDA2F6EBF81543284CC473 D4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....l....._keyhttps://connect.facebook.net/ja_JP/sdk.js?hash=717430068f18341031a2bf06d6ad5a88 .https://stopcovid19.jp/.a...%/.....p.....S...A..n.E ...HL..D.v5 ..7Tz=...A..Eo.....).....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7c6c430c5b32df45_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	195
Entropy (8bit):	5.382495347454884
Encrypted:	false
SSDEEP:	3:m+l3uBa8RzYzTgWi6tVM0DYsHl91/tlHCBglYNtiQPTZd13JVyP5mq5lpK5kt:mzYL39Tl91/Sp/9P93JY4mK6t
MD5:	06F0CCA86E18ABAC4B6D1377B6F94A4E
SHA1:	D7FCF162AC27FA1F2DA9D1FC5D8240587C5C3F42
SHA-256:	ABB571A2BE65DB0BF400E30F91E0FB8E1F828A10C6DDBFA82906BCDDA2234E13
SHA-512:	33427B9518C76E887C4EE424E838CA9D6740ED2D9FBE45D22A5507D099C67E14E1FAA82BAB50014E409C12CB30A6B9FBBFE0EBE25759C362CA9C8E8872B075 9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....?.....T...._keyhttps://yads.c.yimg.jp/uadf/yads_vimps.js .https://yimg.jp/.b4..%/.....a.....t...\..J.....n.8.....6.I.A..Eo.....ts.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7df5b6e20f2af607_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	5.494912897763853
Encrypted:	false
SSDEEP:	6:mXPYGL8lGKXVYAscrZEzGzW+g1/S+lq2PsnSpK4yK6t:2lvxZyGQB3Eno4
MD5:	C4900AD23B66B76E6CB2C4AB9E4CB8FF
SHA1:	66FF53B4CFF036B744FD37E571FE5DA81A3B0CC3
SHA-256:	77CE46014E73F764824294529E817C87417FD1729438A0D405DABA93A2AD1CB6

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7df5b6e20f2af607_0	
SHA-512:	29EFAB7B2F1EAEA425950379CC4A43A4068093E183B06EC2BB2DF6D126E1F708FC392C2F545423FBB5D2450CC6609933A1723AAF8BD989BA02790DE5E7003AE1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....x...^....._keyhttps://www.ja-ces.or.jp/wordpress/wp-content/plugins/page-links-to/dist/new-tab.js?ver=3.3.5 .https://ja-ces.or.jp/V_...%/.....?w.....w..n.~.z.2.j...0..6*F.,...A..Eo.....W.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\802e1bfb59a9db13_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.462034556025162
Encrypted:	false
SSDEEP:	3:m+lOlBfl/a8RzYP2wuEu8CiSE+tyWFvNdOdd1MAatlHCKl1y/iQHQLU9hMmyvpK+:mJJPYeBEfCiSEodO6vSKl2QQhnyRK6t
MD5:	BBBB1104184CEAB94320867427639777
SHA1:	2CC1C6FC5C1E223E084E7ACA64798EC995946A97
SHA-256:	B9C22BAB7BC96F62A4B4BB00105DF3066D817A5BC98A4AA0A8392304E61A74B8
SHA-512:	1DC05F8084E18BFBFF1DF4E65DEAD5D3DE0D7EF12CB433AA352B7512FEA5650B361A330254C21CC7152E9D4488CDAFAD6C28F527E2E938E27B9EB6D7123BE6E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O...Q@d ...._keyhttps://code4sabae.github.io/kafumon/lib/Chart.mjs .https://stopcovid19.jp/e....%/.....s%.....Il.....X...vEt..|...A..Eo.....w%.h.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8478470334b58522_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	246
Entropy (8bit):	5.650868010768318
Encrypted:	false
SSDEEP:	6:mBnYGLlgcZbEhyN2zY292slzEtJ3YTWhK6t:xBZ/oki2slz2qW7
MD5:	9DFC6A7B20229F6718344C79070EC8D2
SHA1:	0CEA1ACAB26F340F24016013D2F697F37AABC77F
SHA-256:	415A8CB678DC3F387EC1C124078FE02F17FA0A1994F9AFA47EA834BA27CB57E6
SHA-512:	7ADACC0ED44B36713ECFE2063719F6A324C6CBFB35B6769DB833456614386 80F29ED115C763BE4B030975E7254D8D586B16B1C83648BFB6A1AB1A05A6FE5F80
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r...TI....._keyhttps://www.google.com/cse/static/element/b54a745638da8bbb/cse_element__ja.js?usqp=CAI%3D .https://mhlw.go.jp/vPT..%/.....~.....HPp.$a-.>.wp....>z...r....A..Eo.....(.I.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\89a981ce4d0a0464_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.676957586876334
Encrypted:	false
SSDEEP:	6:mSYk+f2pomdMGw1VwhmJ2AHSFU3IGH4Z4K6t:L++amdnkJfHLIGHIa
MD5:	22CD9E7473451AE8221CB596243F423C
SHA1:	A2D89483897674B20CF8094DAFC85A1F286F719E
SHA-256:	2322AA5C142ACBDBA932CB9EC4B79440059EE80AE8CDE5C0657E5E8BC100098D
SHA-512:	77828216A485F4692392AA7DD3F2332C07129976FE65E03BEAD7284F96A6AD4E257FA38C032C6083BD2B4836BD9D4D29CE39210D5C685F489B9EA708CDD5801
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yv/r/eRfcZJxUwCV.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/r...%/.....C.I.GI:.....8.~....[x.?.."...A..Eo.....O.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8cfa1199efdab160_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\8cfa1199efdab160_0	
Size (bytes):	247
Entropy (8bit):	5.7938628049358005
Encrypted:	false
SSDEEP:	6:m6q9Yk+f2pomWw2AOMC1MhmJ2xCSTEyDh3k4hbRK6t:fW++amXOx1MkJOCk3T3
MD5:	EDB267B57CFE812B301515D9C9E2729E
SHA1:	4A4B78EB305786CC1E33531222A7ED5AEF80005C
SHA-256:	CBB529F3389EA2025B7DAEEADE91379B33E4D304E7D4DB7E9B045CBA350501E1
SHA-512:	4E796FD60B48446425C629DAFB33982CC78AF70CC842E1DD0ED9DAB2247A45A54ECDC51AE632275A62DC89B2CBCB97E7C73FEFF519AD326D78A86272E6374A4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....>....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3i5ED4/yz/l/de_DE/63GuVXEYA0F.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/1e..%/.....:....U...'.|..W#v..%.s...~z...A..Eo.....y.*.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\97b834ef0803d9e7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	197
Entropy (8bit):	5.295913797202354
Encrypted:	false
SSDEEP:	6:mylEYGLKd7AK01u2YvT9SJtmk1KliDIRIUDK6t:RhlJqjog5U1
MD5:	EEEE22B59489C475A3812C227C6E03AE
SHA1:	2C8EA393D1B98DA37A987407C5A8DF495FF1C6EE
SHA-256:	850A063C5EBB0585FA57CC7D1FACBCAB8E73ED15B685DF3D767AFBD2CA8899C9
SHA-512:	D380D323C5E6FFCC6097107B324F499802B2A4C83043EF5AF0349E0E96565EBA6861C5264C6BBDCB67B4682C35174AB52D3EA842A22227A83E51A1CDFF65EE9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....A...k.%n...._keyhttps://www.gstatic.com/prose/brandjs.js .https://mhlw.go.jp/.V...%/.....w.....|.....0..s_.....*.rP...#..?H.r.A..Eo.....0me.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9b2160d82b9e4faa_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.475027247453838
Encrypted:	false
SSDEEP:	6:mYXyWPYGL8YLEJIvg/IhYF99SaZfu+Hly4fRK6t:FiWUYqIqI6F99xmi
MD5:	7C4E8E96C64DA8E87E5E0A234DC22FA9
SHA1:	817542AE53E37BDD4DBCBE3A3682C59AB853CBC4
SHA-256:	7410E1DBC33A53A6E0C5F1E510C4D621F1CE0BDADC2AB858D1C9B1F7C8263C28
SHA-512:	8164202E05F226A756472ECA0AF7A65F63692E035EBF25E4E43C671DDF2402A88B5DDA3D47158C96EB566C2B159BF06BB5EE1E1298EE9953C337AAA2F3747DF
Malicious:	false
Reputation:	low
Preview:	0\r..m....._....z....._keyhttps://www.mhlw.go.jp/common/scripts/flatHeights.paddingbugfix-ver.js .https://mhlw.go.jp/A.B..%/.....y:.....S+..M..I.S...."b#..l....A..Eo.....8.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9e285134dde499bf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	206
Entropy (8bit):	5.469973533310232
Encrypted:	false
SSDEEP:	6:mknYGL+MIwJJ6OM7HSVpLoyzS6EN4fX5/ZK6t:dIwv6HHmpDW6U0Z
MD5:	416EE6D32F132CEA5856080D0149D0EC
SHA1:	C1E096F4912A4CA8687F47E3604765DCBEBF7D63
SHA-256:	8FF60671483F1FEE65A7629E866292C141FBEC3CCC72A6D0B13BB361F8C62E1D
SHA-512:	BEE3382478C21DC2CBBAABE973E3D4B6E819EEFDF14908B94C7C9F0B86C7E04A26B701DF38A25C1AD766D535B36BF6CEECBC0D85691350695F3684189B2DD15
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9e285134dde499bf_0	
Preview:	0\r..m.....J...IH.b...._keyhttps://www.google-analytics.com/analytics.js .https://stopcovid19.jp/q....%/.....i.*..W...0LZ.%..<.....L..P.Kl..A..Eo.....z.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9ef6dd16e6c04320_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	265
Entropy (8bit):	5.520408704659259
Encrypted:	false
SSDEEP:	6:m1iEYGL8lGKXVYAscpEC/hmFPdTMGzWY3ScEJT4zfQtXiYDnK6t:qiqvL/8PdTMGx36CzQy6p
MD5:	064DC8ACDEF1780C04448AC47001B533
SHA1:	4411BB4BB9B6F913BFDFCD52A11638D341FE7584
SHA-256:	C5C538EA2546F8F41B16B78E2E7E4261BB50EDFD75F8FFA6F3FEEF0C953348DA
SHA-512:	8A409250982BE4401889A106119EA919CA98E02A79E808966353F7C482878B8CCB37CF9D3691FD94941611851866CC4D3CC022C3972C51A6094F59D11244DA58
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f....._keyhttps://www.ja-ces.or.jp/wordpress/wp-content/plugins/vk-all-in-one-expansion-unit/js/all.min.js?ver=6.6.2 .https://ja-ces.or.jp/.L...%/.....Qw..... {.v...G,..v..Z....'..E`.\.4..A..Eo.....r+{.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a11713cbf11dbe8c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	203
Entropy (8bit):	5.338366028499891
Encrypted:	false
SSDEEP:	6:mwp9YVQfCYKi9Q8EI76lSLL/jahRLK47hK6t:dpUQfCYKSQVI7ODRLz
MD5:	4F3DC4E33E35BD5EDA551BD3FF4EA0B4
SHA1:	27028AFA86DBBF9C9C5C7D43618BBAFBF0D5CD93
SHA-256:	7016A6D3FDC6CEA802F51670CEF99DC8D5C091A7826CF771A930189017B3F4C3
SHA-512:	4BC516CFAB95857408AF0A6EC7D3E8C6ADF82D7C214BE0E9E27A4DD648AC1F13E2786BBB07EEA6096459C687CD38BB6D2E3B1C87D9107FF2B0631F9358FC3 F2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G...Ej6....._keyhttps://c.amazon-adsystem.com/aax2/apstag.js .https://hatena.ne.jp/.....%/.....S`@...|'i;.XaE_..G(.....nA.F..A..Eo.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a562e271c28ce1cb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	412
Entropy (8bit):	5.726066792423515
Encrypted:	false
SSDEEP:	12:2/0GKjqoDIHBDa0/aYjWXiSVI7eWR81p/+cN:4UZCk0TyXiSVI7eV1p/+cN
MD5:	9853715AC1114F5A68D1BDAD795583CD
SHA1:	165E3CCF988C86EEE5D96DFAB9290A06B66D8387
SHA-256:	AF6BAACE557C2EDBC6D005EBB2D8776CC6FB8D2E8ED9B919245EB45088FD43A6
SHA-512:	4A5B4008FBC110272732733E4CED616A027919BCB02D5A0BAB3E26DD285C9F2E5BC92E623D1967CA7B6FC93A30B21D3AD5161D7D247C4EA165EDE0D8083321 C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`.w....._keyhttps://i.socdm.com/sdk/js/adg-script-loader.js?displayid=1&async=true&flexibleOL=true&autoPadding=true&tagver=2.0.0&id=92279&targetID=adg- slot-wrapper-entry-double-rectangle-right&adType=RECT&width=300&height=250&apsamznbid=2&apsamzniid=&label_random=6 .https://hatena.ne.jp/u.L..%/..... ..<..-.'...+..uF.4.^.y...p..y\...A..Eo.....^.9c.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a5e7cb262c05eea2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	254
Entropy (8bit):	5.657171153849947
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a5e7cb262c05eea2_0	
SSDEEP:	6:mDPYkmLf+kWNXCUkAFuAEQK8EI7W1lSK/lsGyIQQb5hK6t:7+kldLAE9Vl76JtTyIQQ97
MD5:	D8A9F226B00753236C067D5F7D418EB4
SHA1:	1DBBCE11077D8326D269DBA8014135E049198A1C
SHA-256:	6735B358A1E57238B85705A115CF4553194A9987954CCDBA6FA05F7127E12259
SHA-512:	F737D6596AB5F12A6BE2D936740F3B79715517CBDC48E1AB80DB04E8B8EBAE360348B667D5DF87951E8C0C2D2B36C7F7A3BE55965AC14D5394856E43F2D850A A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z.....r....._keyhttps://b.st-hatena.com/js/v4/bookmark.star.js?version=b28e833a092c996f374596d23318dea9e3c5a9c8 .https://hatena.ne.jp/.R...%/.....w... .....R..6.u.0K..q.S.Y....C...?.o.q.A..Eo.....a.)3.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a782bc86a3b81da4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	239
Entropy (8bit):	5.531502252181308
Encrypted:	false
SSDEEP:	6:mUw/PYGL8IGKXVUfIQKjWwpiGzW2Kl9SR1l//+mvhl4m4/K6t:pwlKfIQKqFGG9iHRvhlX2
MD5:	3D5E8762037D3B0345FD59AE7AD44676
SHA1:	7A54AD9F07DF82328033301B40113564BAFEB04A
SHA-256:	37CD6EB82B08AA6E288079247BCCBD88EC1319E3495FF846E6DA7F89B35DDB0D
SHA-512:	AE398AFDFAEE5F09A6D0AF24E4C185057CCBBBABE7E30EA4E04A47C0AEB3A11D8C814FF821DB7C3B44D9693D9EFAF997C36D83E0A77F9DFD19723213E23EF 46C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k.....g....._keyhttps://www.ja-ces.or.jp/wordpress/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp .https://ja-ces.or.jp/^....%/.....4u....."..f./.L../jz.."..B.$xn..E5.... A..Eo.....,.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a8021a103cac1926_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.411192921322115
Encrypted:	false
SSDEEP:	3:m+l8nO8RzYrSL8Y4GK1JlWx7LozY4/V7tlHCBtVJfPebIea4dApp4mWltpK5kt:mfYGL8YLEJlqKY4SLCS4dmhWZK6t
MD5:	49BD82F85966C012B62089B202E0B920
SHA1:	DD1849E69BBBDCA07085E9BE3AB913E352C34F2F
SHA-256:	1DC8942F287BCC157C913FD824EA5FB776415FDE71CB06D32A3432CFF4409A9C
SHA-512:	4ACCE224DC26C3062FA33874DB67C557AFEE21D1AB419970B42205C5F6F27C9556C650DE7C8BAEEFC4370F5D7286761FD087A634C4E3D6BE4EDC2CD714E7A 63
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R.....s!...._keyhttps://www.mhlw.go.jp/common/scripts/jquery.mk_cookie.js .https://mhlw.go.jp/..>..%/.....p*T.M.(LLMz....T.6.m....V%x.(-E.A..Eo.....fS... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ad1ee8a46673fd3d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270
Entropy (8bit):	5.521016820250625
Encrypted:	false
SSDEEP:	6:mZYGL8IGKXVYAscOGrDACEqGzW//91/SW/eMRYwvzaS4r7DK6t:Wv0GfACDGi9P/5+wunl
MD5:	86C8CD6229A45D800337ED0DCD37D985
SHA1:	7E9212E7F2A4CDC17687AB25AC7688AFDA1ED45B
SHA-256:	0A91C6BB872C576E28EA048834C0E8DB594E6D0ADB31B3DEB4BC07B8B4F9249A
SHA-512:	208AB1D696F522ED0F401F20836B2AE198625C590438012DDEBCF781B2FD0DFCCA7AD66573D12A7F0991713C1CEEDCCAB746F78BCE12AD8C39E4A587445331 3
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://www.ja-ces.or.jp/wordpress/wp-content/plugins/contact-form-7-add-confirm/includes/js/scripts.js?ver=5.1 .https://ja-ces.or.jp/.\...%/..... ..Lv.....;..c...}....q....E.J.....J.j~.A..Eo.....P..F.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ad93ac35a63b43df_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.3660633789346
Encrypted:	false
SSDEEP:	6:mNYE5LOmLoBj8EI7avlSHaVsY1X2hp5bK6t:AUVI7a96a6Y2h1
MD5:	10802ACA0D4431746B353FCC25BE0D24
SHA1:	3EB009968DAB4D32A93AC814EF753A6FC48A3975
SHA-256:	07339C53873F6511DB362C9A524C28DF74F2BD94C772CA947087B229D6E0340D
SHA-512:	8F654F0CD97ADEA53883CCFF95B1B2C1E1A6DB53106A0B7CDF7D46C11F6235CB9B6946BC7F2820ED97CCC7DCAC3B12CAFF83935E3E0816A4CA2AE06C8AB6B3D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H....._keyhttps://cdn.pool.st-hatena.com/valve/valve.js .https://hatena.ne.jp/.j...%/.....z.4....%K?..1s-|-...|:..YuL.A..Eo.....l.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\adf7722569fd0bc6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.765393033500388
Encrypted:	false
SSDEEP:	6:m49Yk+f2pomX8N7yhmJ2YvSNFY/SIrNeniK6t:rl++amX8okJLv+FYD3
MD5:	9D4A165AFE3AEDF4877A856293394EED
SHA1:	14FC92A74E6EB753BE6EF54E8161A6D063210338
SHA-256:	E554FB598201828598FABBF5CC2EBA0AB9C4F60FED4424DFC788D757F458A9FF
SHA-512:	2D6BFD4DD7A2862D1673703E917F50ED490EC60BCE91CE6409125C63B1C7A789CB68CB153797F2D595FE63EC290A4428BA6534565CF78337FFEBB1379CD6159
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....'....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y3/r/CrII4R3C1FT.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/aS..%/.....(.....7.6I.#....1.Y.z.....D6...#-Go...A..Eo.....~^.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b03c983cdd03da8d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.411985330330933
Encrypted:	false
SSDEEP:	3:m+lQY/v8RzYrSL8Y4GK1JlW/H7WVDzY4fl3tlHCQhgt3T4Ll+pS1kj1Y4WmMDhlP:mK8YGL8YLEJlrYs3S0ZlwyOAlhK6t
MD5:	EE9DC996FA814CC7447B073B69BA4A2E
SHA1:	55001F6C45539A47631D28A510F65931C09B1B0D
SHA-256:	E9F8B6098654CBB7AA9ADC8211A7EFA056015B14FFDC6A7CD86DA33C86753D9A
SHA-512:	131F37D97465A7FAABC0FE247D068EBD8AD3F25F1BB1BDB04BB22B9C4BBE571CACA168272E42EC29365EE9F162F4815D459D6C48D6AFAD5B8BC3D751D8235AD6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...<.!....._keyhttps://www.mhlw.go.jp/common/scripts/jquery.closeUp.js .https://mhlw.go.jp/..@..%/.....5.....H...[].....|.....gtr../.. .h6.A..Eo.....;.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b1ace53f1483ebae_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	200
Entropy (8bit):	5.389045020243544
Encrypted:	false
SSDEEP:	3:m+lMx8RzYl4J13y0TPC7HOdd5oUo+9tlHC3ll/8adLjpjnBSI14mYg/lpK5kt:msYKxDCLOeUo+9SVt8SLjJB71rbK6t
MD5:	125B8448E44AFB24A2CCE97C01192BDE
SHA1:	14358E6036540397790CD54143F13688EA1A0954
SHA-256:	2648F087257CA8C8760F2BE574F0E8B6B1AC1C7EB8516E3264347CB2D4C18C25
SHA-512:	756362B2AB862371B48D81031082DBB4840D38FE2CE6FA483B73522C1618C8BFBCA659BF7DAED0B000621DC97ED3581E692F4437F6C261737CC17EA9709C029

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b1ace53f1483ebae_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....D....1....._keyhttps://platform.twitter.com/widgets.js .https://stopcovid19.jp/X....%/.....I.....?..F...AE|7- .3...P...m.I..$....A..Eo.....i.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b1ce1a24dbd33c5b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.396309441087955
Encrypted:	false
SSDEEP:	6:mUv/XYGLH0c4OlfA+9SKly+qFLqbfbK6t:pngZa1I+Q2
MD5:	62554BC40FABCB343B38DEB7E5331176
SHA1:	CFEB3FF52DCA56FCE33D62B49E3E95CF0F101C6D
SHA-256:	04E8D31029EE09F38A0AF72804BF62CB064E1A0AF7FE190CF5A15D29B4ACB72F
SHA-512:	935B21B53E2192F287A2BD62CD22EE3B89C04055E181648DC9B9984907B1D67BF8A3299AB90867ACF99C3984651AD2AA854A8DE6BEB386E0498B2FB11230AED
Malicious:	false
Reputation:	low
Preview:	0\r..m.....F...0....._keyhttps://www.stopcovid19.jp/mhlw-graph.mjs .https://stopcovid19.jp/.1...%/....."....h.R..A....}.....W...A..Eo.....,kE.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b2c8341815361ffa_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.6894590477121385
Encrypted:	false
SSDEEP:	6:mQYk+f2pomJ4MWawhmJ2paSKxqRP7wbyQhK6t:t++amJxdwkJgaxqP7wbF
MD5:	A2DD5F91ED54171A5557F4184EA15032
SHA1:	F82B9117E939B853113906C007579FD79C2326ED
SHA-256:	E737976508EC7C009315ADADF92D5440D04EDD5AC5540D3D9BD6452652769162
SHA-512:	B31AA4B7403D1E43E66690D2359A5FA2808F814971A914170C9CEE81F5B01737F1A9705A1926262982B637C226B87553B2CACA46D3E04CD9C7B9C90E0D265E26
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yb/r/UHlXKQHdl3t.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/@Z..%/.....h.....4.Yj.G..>~...r.....j/.@ I.B+.{.A..Eo.....^.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b33e1f449eb327db_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.782511361059564
Encrypted:	false
SSDEEP:	6:mXPYk+f2pomWr2Ky2rN5hmJ2VKHS9kPUjD39hneK6t:2b++amyy2XkJ/HAGa396
MD5:	528DB2E2678B066802638A76AC2FF5A6
SHA1:	40C3B98CE2AE4BDE69F9B2D8817A51A0946FE3F0
SHA-256:	DB79091206351C69A68B9FC7695A6099235EFF437460447851AC68CBF76B4F2F
SHA-512:	5FA72B8D26B1226E1AA088ECBB45B34119143F2A9B852BF779D55FFBFE84EDF8C70C66548E134EBA99FAFDC0180984564D6E795C00D5CE433CE7CDD240BFB2E3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....{K....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iN_84/y6/l/de_DE/6d1QoB2_uVs.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/&\..%/.....{.....mt.....b.~+...zt.df.....A..Eo.....Q.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b343428e4e214036_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.704596149602445
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b343428e4e214036_0	
SSDEEP:	6:mv8gl/VYk+f2pomWmoO+oLahmJ2JSV0w5a4jlhK6t:48gN++amGO+FkJym0fu7
MD5:	0FF275D33363C04C984625652D2334DC
SHA1:	A8710AC5A6D47B0B217E9449FC5E4A4FD7FBF6C9
SHA-256:	761DB383BD919F6DCEA399C9B4EB1122C463D51F1523CCB2AA53C5A094A439F7
SHA-512:	DE9989DF722D69811BBCCC9DB4E08FD470DF6A12D0F0FC9A55F9A8A6B6C3D43CC0080C524378CDB49FD78698A6FCB52042022EBE5D979B9C48E23B2AC1B682A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....T....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iOTn4/yF/l/de_DE/AghE3rjighB.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/....%/.....Bt."..%R..... ..o...oK.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b513e1192537baeb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	213
Entropy (8bit):	5.368345621540867
Encrypted:	false
SSDEEP:	3:m+lZwMlll08RzYggb8epWFvDYsrl99tlHC6gLi2YZpjzda7dWoMmUHPllpK5kt:mlMnYDFml99S6gEpjRa7cYepK6t
MD5:	7A1C38E14A7E113FDCF598B4810008E1
SHA1:	9C9DA007629D53B112E42647BFDC844A9B99F7B9
SHA-256:	9636C6CE88C2AC1D9D82D3038D4633672FE6C34C5890FF8C410512BDDC6E298F
SHA-512:	783A7CF7E033CA882A33C55C488943156C6A37BCA6E651D7650341DABF0A473D1D7F01380A3F72DD84FE7DCA5F8FAD5EA34FA142C015AE1062FE1B592923840
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....a.i..._keyhttps://s.yimg.jp/images/advertising/common/js/iicon.min.js .https://yimg.jp/.Z<..%/.....h.....f=....]....m|.Sj4....+r...f..x...A..Eo.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b848f038f264e3cc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	202
Entropy (8bit):	5.50964534697697
Encrypted:	false
SSDEEP:	3:m+lvbis8RzYPIXXHKhfTSoHOddJv/tlHCitvHQ9xWZdyMEDyP5mx1lpK5kt:mIeYAWZOxHSiJQaZpZP4xRK6t
MD5:	6B08D66715BEC1F13DBB18EAE9210FDC
SHA1:	338376EEF4ADA2122819F45FCCCCFB191309EEFE
SHA-256:	AA6E1123FB3F0A7323961F5DB1D8A967774D36C096E7802B8045659AEB535260
SHA-512:	BE9FABE90E343CD42BF3394E28E8B44FCD5046591F33085998F78E1719C05CAED566A5D4259C5AF249BA67EE09F7C1E20B32CAF25BF7761FB4198EC190A3955
Malicious:	false
Reputation:	low
Preview:	0\r..m.....F...)'....._keyhttps://connect.facebook.net/ja_JP/sdk.js .https://stopcovid19.jp/.....%/.....9...+.....T.....Vxi!.y.A..Eo.....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 15, 2021 09:20:43.301651001 CEST	192.168.2.4	8.8.8.8	0xaecc	Standard query (0)	www.stopcovid19.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:44.256953955 CEST	192.168.2.4	8.8.8.8	0xa522	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:44.279403925 CEST	192.168.2.4	8.8.8.8	0x5bc4	Standard query (0)	platform.twitter.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:44.287300110 CEST	192.168.2.4	8.8.8.8	0x6c3b	Standard query (0)	b.st-hatena.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:44.954101086 CEST	192.168.2.4	8.8.8.8	0xcc34	Standard query (0)	code4sabae.github.io	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:44.968410015 CEST	192.168.2.4	8.8.8.8	0xc5a	Standard query (0)	taisukef.github.io	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:45.038386106 CEST	192.168.2.4	8.8.8.8	0xc56b	Standard query (0)	b.hatena.ne.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:45.122127056 CEST	192.168.2.4	8.8.8.8	0xbe3b	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:45.461610079 CEST	192.168.2.4	8.8.8.8	0x4b2e	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:46.069135904 CEST	192.168.2.4	8.8.8.8	0xd361	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:46.596673012 CEST	192.168.2.4	8.8.8.8	0x522f	Standard query (0)	syndication.twitter.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:46.985733032 CEST	192.168.2.4	8.8.8.8	0x8d85	Standard query (0)	twitter.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:47.364135981 CEST	192.168.2.4	8.8.8.8	0x935d	Standard query (0)	tk3-805-12365.vw.sakura.ne.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:48.248827934 CEST	192.168.2.4	8.8.8.8	0x252d	Standard query (0)	r3.i.lencr.org	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:49.024199009 CEST	192.168.2.4	8.8.8.8	0xd62c	Standard query (0)	www.stopcovid19.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:50.361486912 CEST	192.168.2.4	8.8.8.8	0x2055	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:50.619060993 CEST	192.168.2.4	8.8.8.8	0x515e	Standard query (0)	tk3-805-12365.vw.sakura.ne.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:54.560976028 CEST	192.168.2.4	8.8.8.8	0x2e66	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:55.052417994 CEST	192.168.2.4	8.8.8.8	0x929b	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:02.483704090 CEST	192.168.2.4	8.8.8.8	0x3be2	Standard query (0)	cdn.pool.st-hatena.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:02.498198032 CEST	192.168.2.4	8.8.8.8	0xc19d	Standard query (0)	cdn-ak2.favicon.st-hatena.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:02.512798071 CEST	192.168.2.4	8.8.8.8	0xff26	Standard query (0)	cdn.profile-image.st-hatena.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:03.200907946 CEST	192.168.2.4	8.8.8.8	0xb62c	Standard query (0)	cdn-ak-scissors.favicon.st-hatena.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:03.313405037 CEST	192.168.2.4	8.8.8.8	0x6936	Standard query (0)	s.hatena.ne.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:03.449323893 CEST	192.168.2.4	8.8.8.8	0xea2b	Standard query (0)	c.amazon-adsystem.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:03.591470003 CEST	192.168.2.4	8.8.8.8	0xba0f	Standard query (0)	static.ads-twitter.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:03.594217062 CEST	192.168.2.4	8.8.8.8	0xc76a	Standard query (0)	www.clarity.ms	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:03.735688925 CEST	192.168.2.4	8.8.8.8	0xac53	Standard query (0)	dmp.im-apps.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.062832117 CEST	192.168.2.4	8.8.8.8	0x7601	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.076358080 CEST	192.168.2.4	8.8.8.8	0xcfa3	Standard query (0)	ib.adnxs.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.084821939 CEST	192.168.2.4	8.8.8.8	0x7794	Standard query (0)	bidder.criteo.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.106236935 CEST	192.168.2.4	8.8.8.8	0x8f23	Standard query (0)	pb.ladsp.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 15, 2021 09:21:04.109908104 CEST	192.168.2.4	8.8.8.8	0xbe25	Standard query (0)	ad.as.amanad.adtdp.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.124361992 CEST	192.168.2.4	8.8.8.8	0xa7b6	Standard query (0)	d.socdm.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.133069992 CEST	192.168.2.4	8.8.8.8	0x551c	Standard query (0)	hbopenbid.pubmatic.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.135240078 CEST	192.168.2.4	8.8.8.8	0x6538	Standard query (0)	s-rtb-pb.send.microad.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.146400928 CEST	192.168.2.4	8.8.8.8	0x34cc	Standard query (0)	hatena-d.openx.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.147351027 CEST	192.168.2.4	8.8.8.8	0x17e8	Standard query (0)	fastlane.rubiconproject.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.147876978 CEST	192.168.2.4	8.8.8.8	0x1d76	Standard query (0)	y.one.impact-ad.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.356960058 CEST	192.168.2.4	8.8.8.8	0x1d37	Standard query (0)	cnt.fout.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.366936922 CEST	192.168.2.4	8.8.8.8	0x9f16	Standard query (0)	t.co	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.367856979 CEST	192.168.2.4	8.8.8.8	0x19a6	Standard query (0)	c.clarity.ms	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.432233095 CEST	192.168.2.4	8.8.8.8	0x435c	Standard query (0)	aax-eu.amazon-adsystem.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.479264021 CEST	192.168.2.4	8.8.8.8	0xd8f7	Standard query (0)	cdn.bigmining.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:05.492258072 CEST	192.168.2.4	8.8.8.8	0x4c	Standard query (0)	i.socdm.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:05.686810970 CEST	192.168.2.4	8.8.8.8	0x1fe	Standard query (0)	static.criteo.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.418143034 CEST	192.168.2.4	8.8.8.8	0xded	Standard query (0)	tg.socdm.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.418560028 CEST	192.168.2.4	8.8.8.8	0xd901	Standard query (0)	imp-adedge.i-mobile.co.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.481960058 CEST	192.168.2.4	8.8.8.8	0xe49e	Standard query (0)	yads.c.yimg.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.594952106 CEST	192.168.2.4	8.8.8.8	0xf3ec	Standard query (0)	repository.secomtrust.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.260516882 CEST	192.168.2.4	8.8.8.8	0x3d71	Standard query (0)	ssp-bidapi.i-mobile.co.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.411741018 CEST	192.168.2.4	8.8.8.8	0x50b7	Standard query (0)	b.hatena.ne.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.421981096 CEST	192.168.2.4	8.8.8.8	0x6c2e	Standard query (0)	b.st-hatena.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.465291977 CEST	192.168.2.4	8.8.8.8	0x4b6a	Standard query (0)	cdn-ak2.favicon.st-hatena.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.528129101 CEST	192.168.2.4	8.8.8.8	0xe7d5	Standard query (0)	s.yimg.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.529372931 CEST	192.168.2.4	8.8.8.8	0xd86d	Standard query (0)	yads.yjtag.yahoo.co.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.541564941 CEST	192.168.2.4	8.8.8.8	0x1399	Standard query (0)	cdn.profile-image.st-hatena.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.840228081 CEST	192.168.2.4	8.8.8.8	0x5fdf	Standard query (0)	cdn-ak-scissors.favicon.st-hatena.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.859560966 CEST	192.168.2.4	8.8.8.8	0xaba6	Standard query (0)	eus.rubiconproject.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.929116964 CEST	192.168.2.4	8.8.8.8	0xf90f	Standard query (0)	ads.pubmatic.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:08.619270086 CEST	192.168.2.4	8.8.8.8	0x345b	Standard query (0)	spnativeapi-tls.i-mobile.co.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:08.623224020 CEST	192.168.2.4	8.8.8.8	0x5ad2	Standard query (0)	cr-p31.ladsp.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:08.628782034 CEST	192.168.2.4	8.8.8.8	0x55ec	Standard query (0)	eu-u.openx.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:08.632672071 CEST	192.168.2.4	8.8.8.8	0xed96	Standard query (0)	y.one.impact-ad.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:08.633812904 CEST	192.168.2.4	8.8.8.8	0x7487	Standard query (0)	acdn.adnxs.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:09.105787039 CEST	192.168.2.4	8.8.8.8	0x218b	Standard query (0)	image6.pubmatic.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:09.126308918 CEST	192.168.2.4	8.8.8.8	0x76b9	Standard query (0)	cr-pall.ladsp.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 15, 2021 09:21:11.152590990 CEST	192.168.2.4	8.8.8.8	0x9def	Standard query (0)	match.adsrvr.org	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:12.043181896 CEST	192.168.2.4	8.8.8.8	0xba9b	Standard query (0)	im.ov.yahoo.co.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:12.289339066 CEST	192.168.2.4	8.8.8.8	0xdbb2	Standard query (0)	penta.a.one.impact-ad.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.755934954 CEST	192.168.2.4	8.8.8.8	0xa44c	Standard query (0)	pm.w55c.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.760998011 CEST	192.168.2.4	8.8.8.8	0x63a3	Standard query (0)	x.bidswitch.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.769920111 CEST	192.168.2.4	8.8.8.8	0xdf0c	Standard query (0)	match.prod.bidr.io	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.772300959 CEST	192.168.2.4	8.8.8.8	0xb3ec	Standard query (0)	sync.mathtag.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.777756929 CEST	192.168.2.4	8.8.8.8	0xbdc3	Standard query (0)	pixel.quantserve.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.779161930 CEST	192.168.2.4	8.8.8.8	0x86c	Standard query (0)	c1.adform.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.786365986 CEST	192.168.2.4	8.8.8.8	0x5291	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:14.330032110 CEST	192.168.2.4	8.8.8.8	0xa0d4	Standard query (0)	us-u.openx.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:14.581542969 CEST	192.168.2.4	8.8.8.8	0x292a	Standard query (0)	ads.creative-serving.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:14.793909073 CEST	192.168.2.4	8.8.8.8	0x35df	Standard query (0)	pixel-eu.rubiconproject.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:14.923738956 CEST	192.168.2.4	8.8.8.8	0xa4b6	Standard query (0)	dis.criteo.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:14.975544930 CEST	192.168.2.4	8.8.8.8	0xfa7f	Standard query (0)	rtb-csync.smartadserver.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.067918062 CEST	192.168.2.4	8.8.8.8	0x5869	Standard query (0)	match.deepintent.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.160267115 CEST	192.168.2.4	8.8.8.8	0xf718	Standard query (0)	idsync.rlcdn.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.170581102 CEST	192.168.2.4	8.8.8.8	0x128a	Standard query (0)	bh.contextweb.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.194991112 CEST	192.168.2.4	8.8.8.8	0x3696	Standard query (0)	ad.turn.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.209711075 CEST	192.168.2.4	8.8.8.8	0xec2	Standard query (0)	sync-tm.everesttech.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.215645075 CEST	192.168.2.4	8.8.8.8	0xce0c	Standard query (0)	pr-bh.ybp.yahoo.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.222846031 CEST	192.168.2.4	8.8.8.8	0x9859	Standard query (0)	ups.analytics.yahoo.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.222989082 CEST	192.168.2.4	8.8.8.8	0x7e54	Standard query (0)	um.simpli.fi	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.241314888 CEST	192.168.2.4	8.8.8.8	0xc0f7	Standard query (0)	pubmatic-match.dotomi.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.332366943 CEST	192.168.2.4	8.8.8.8	0xfc95	Standard query (0)	rtb.adentifi.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.338776112 CEST	192.168.2.4	8.8.8.8	0x6fff	Standard query (0)	image2.pubmatic.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.452775002 CEST	192.168.2.4	8.8.8.8	0x5c03	Standard query (0)	token.rubiconproject.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.452914000 CEST	192.168.2.4	8.8.8.8	0xb59e	Standard query (0)	id.rlcdn.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.453087091 CEST	192.168.2.4	8.8.8.8	0xbad4	Standard query (0)	pixel.rubiconproject.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.574071884 CEST	192.168.2.4	8.8.8.8	0x8dd0	Standard query (0)	sync.ipredictive.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.659990072 CEST	192.168.2.4	8.8.8.8	0x4339	Standard query (0)	pixel-sync.sitescout.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.946455002 CEST	192.168.2.4	8.8.8.8	0x92fe	Standard query (0)	image4.pubmatic.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.954991102 CEST	192.168.2.4	8.8.8.8	0xc572	Standard query (0)	simage2.pubmatic.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.971554041 CEST	192.168.2.4	8.8.8.8	0xea8d	Standard query (0)	r.scoota.co	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.999620914 CEST	192.168.2.4	8.8.8.8	0x99b5	Standard query (0)	pmp.mxptint.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:16.173269987 CEST	192.168.2.4	8.8.8.8	0xc093	Standard query (0)	sync.1rx.io	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 15, 2021 09:21:16.238296032 CEST	192.168.2.4	8.8.8.8	0xffb5	Standard query (0)	cm.adgrx.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:16.509507895 CEST	192.168.2.4	8.8.8.8	0x5273	Standard query (0)	ads.yahoo.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:16.570548058 CEST	192.168.2.4	8.8.8.8	0x6722	Standard query (0)	sync.targeting.unrulymedia.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:16.855938911 CEST	192.168.2.4	8.8.8.8	0x4b80	Standard query (0)	px.owneriq.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.075294018 CEST	192.168.2.4	8.8.8.8	0x1fc6	Standard query (0)	a.tribalfusion.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.231060028 CEST	192.168.2.4	8.8.8.8	0xf1d7	Standard query (0)	match.bnmla.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.354314089 CEST	192.168.2.4	8.8.8.8	0x167e	Standard query (0)	s.tribalfusion.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.411189079 CEST	192.168.2.4	8.8.8.8	0xc62e	Standard query (0)	pixel.onaudience.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.412108898 CEST	192.168.2.4	8.8.8.8	0x5e5c	Standard query (0)	visitor.fiftyt.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.420802116 CEST	192.168.2.4	8.8.8.8	0xec07	Standard query (0)	aa.agkn.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.434314966 CEST	192.168.2.4	8.8.8.8	0x7a02	Standard query (0)	rtb.gumgum.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.434533119 CEST	192.168.2.4	8.8.8.8	0x71d2	Standard query (0)	io.narrative.io	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:18.596082926 CEST	192.168.2.4	8.8.8.8	0x6d60	Standard query (0)	simage4.pubmatic.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.237687111 CEST	192.168.2.4	8.8.8.8	0xe56	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.246959925 CEST	192.168.2.4	8.8.8.8	0xf535	Standard query (0)	idsync.rlcdn.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.280467987 CEST	192.168.2.4	8.8.8.8	0xf8d4	Standard query (0)	sync.mathtag.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.287281990 CEST	192.168.2.4	8.8.8.8	0x146d	Standard query (0)	match.adsrvr.org	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.296545982 CEST	192.168.2.4	8.8.8.8	0x75b4	Standard query (0)	ad.turn.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.313779116 CEST	192.168.2.4	8.8.8.8	0x7fba	Standard query (0)	sync-tm.everesttech.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.331202030 CEST	192.168.2.4	8.8.8.8	0x2a8a	Standard query (0)	pr-bh.ybp.yahoo.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.340843916 CEST	192.168.2.4	8.8.8.8	0x77e6	Standard query (0)	ups.analytics.yahoo.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.350408077 CEST	192.168.2.4	8.8.8.8	0xc57d	Standard query (0)	um.simpli.fi	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.357578993 CEST	192.168.2.4	8.8.8.8	0x956c	Standard query (0)	ib.adnxs.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.364037991 CEST	192.168.2.4	8.8.8.8	0xaa64	Standard query (0)	ads.pubmatic.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.368736029 CEST	192.168.2.4	8.8.8.8	0xbe92	Standard query (0)	pubmatic-match.dotomi.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.374650955 CEST	192.168.2.4	8.8.8.8	0x656b	Standard query (0)	rtb.adentifi.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.375178099 CEST	192.168.2.4	8.8.8.8	0x4335	Standard query (0)	image2.pubmatic.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.387561083 CEST	192.168.2.4	8.8.8.8	0x35f8	Standard query (0)	sync.ipredictive.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.400904894 CEST	192.168.2.4	8.8.8.8	0xf36c	Standard query (0)	pixel-sync.sitescout.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.408442974 CEST	192.168.2.4	8.8.8.8	0xc89	Standard query (0)	x.bidswitch.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.418004990 CEST	192.168.2.4	8.8.8.8	0xbf13	Standard query (0)	image4.pubmatic.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.418050051 CEST	192.168.2.4	8.8.8.8	0x6519	Standard query (0)	pmp.mxptint.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.423826933 CEST	192.168.2.4	8.8.8.8	0x9507	Standard query (0)	aud.pubmatic.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.428845882 CEST	192.168.2.4	8.8.8.8	0xd3ba	Standard query (0)	simage2.pubmatic.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.435941935 CEST	192.168.2.4	8.8.8.8	0x7ff6	Standard query (0)	pixel.quantserve.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.552434921 CEST	192.168.2.4	8.8.8.8	0x567b	Standard query (0)	a.volvelle.tech	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.638694048 CEST	192.168.2.4	8.8.8.8	0xdd7d	Standard query (0)	sync.crwdcntrl.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 15, 2021 09:21:19.911833048 CEST	192.168.2.4	8.8.8.8	0xc8ad	Standard query (0)	spl.zeotap.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.061311007 CEST	192.168.2.4	8.8.8.8	0x1073	Standard query (0)	mwzeom.zeotap.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.064310074 CEST	192.168.2.4	8.8.8.8	0xd1ef	Standard query (0)	pm.w55c.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.090034008 CEST	192.168.2.4	8.8.8.8	0xc7bc	Standard query (0)	match.prod.bidr.io	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.142049074 CEST	192.168.2.4	8.8.8.8	0x3013	Standard query (0)	inv-nets.admixer.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.157469034 CEST	192.168.2.4	8.8.8.8	0x1278	Standard query (0)	c1.adform.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.161181927 CEST	192.168.2.4	8.8.8.8	0xde7e	Standard query (0)	eu-u.openx.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.202240944 CEST	192.168.2.4	8.8.8.8	0x3e3f	Standard query (0)	analytics.twitter.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.242707968 CEST	192.168.2.4	8.8.8.8	0xc89	Standard query (0)	gum.criteo.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.266544104 CEST	192.168.2.4	8.8.8.8	0x6c14	Standard query (0)	us-u.openx.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.545711994 CEST	192.168.2.4	8.8.8.8	0x600b	Standard query (0)	rtb-csync.smartadserver.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.667406082 CEST	192.168.2.4	8.8.8.8	0x6487	Standard query (0)	adc.auone.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.755621910 CEST	192.168.2.4	8.8.8.8	0x4a37	Standard query (0)	bh.contextweb.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.878344059 CEST	192.168.2.4	8.8.8.8	0x8ee6	Standard query (0)	pixel.onaudience.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.882162094 CEST	192.168.2.4	8.8.8.8	0x1af3	Standard query (0)	visitor.fiftyt.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.885832071 CEST	192.168.2.4	8.8.8.8	0xf352	Standard query (0)	io.narrative.io	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.886583090 CEST	192.168.2.4	8.8.8.8	0x91ae	Standard query (0)	aa.agkn.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.891629934 CEST	192.168.2.4	8.8.8.8	0xd4bc	Standard query (0)	rtb.gumgum.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:22.023510933 CEST	192.168.2.4	8.8.8.8	0x409a	Standard query (0)	spl.zeotap.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:22.026444912 CEST	192.168.2.4	8.8.8.8	0xf006	Standard query (0)	aud.pubmatic.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:22.158107042 CEST	192.168.2.4	8.8.8.8	0x4da8	Standard query (0)	mwzeom.zeotap.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:31.286335945 CEST	192.168.2.4	8.8.8.8	0x2e56	Standard query (0)	www.ja-ces.or.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:35.727377892 CEST	192.168.2.4	8.8.8.8	0xdebb	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:35.741154909 CEST	192.168.2.4	8.8.8.8	0x58de	Standard query (0)	oss.maxcdn.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:35.741251945 CEST	192.168.2.4	8.8.8.8	0x2a2a	Standard query (0)	s.w.org	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:41.127629042 CEST	192.168.2.4	8.8.8.8	0xd77d	Standard query (0)	www.ja-ces.or.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:41.314383030 CEST	192.168.2.4	8.8.8.8	0x310	Standard query (0)	www.mhlw.go.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:41.699157000 CEST	192.168.2.4	8.8.8.8	0x501f	Standard query (0)	ewb-c.infocreate.co.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:44.910521030 CEST	192.168.2.4	8.8.8.8	0x193f	Standard query (0)	www.mhlw.go.jp	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:46.533631086 CEST	192.168.2.4	8.8.8.8	0x12a5	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:54.752821922 CEST	192.168.2.4	8.8.8.8	0xb799	Standard query (0)	sync.srv.stackadapt.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:54.804025888 CEST	192.168.2.4	8.8.8.8	0x46af	Standard query (0)	ums.acuityplatform.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:55.034729004 CEST	192.168.2.4	8.8.8.8	0xad1	Standard query (0)	trc.taboola.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:55.040649891 CEST	192.168.2.4	8.8.8.8	0x80d4	Standard query (0)	sync.resetdigital.co	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:55.188615084 CEST	192.168.2.4	8.8.8.8	0xc69e	Standard query (0)	match.taboola.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:22:25.686719894 CEST	192.168.2.4	8.8.8.8	0x3199	Standard query (0)	gocm.c.appier.net	A (IP address)	IN (0x0001)
Jul 15, 2021 09:22:25.768043995 CEST	192.168.2.4	8.8.8.8	0xa623	Standard query (0)	jadserve.postrelease.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 15, 2021 09:22:25.823106050 CEST	192.168.2.4	8.8.8.8	0xc1f2	Standard query (0)	csync.loopme.me	A (IP address)	IN (0x0001)
Jul 15, 2021 09:22:25.857131004 CEST	192.168.2.4	8.8.8.8	0x8e4a	Standard query (0)	ads.playground.xyz	A (IP address)	IN (0x0001)
Jul 15, 2021 09:22:25.894049883 CEST	192.168.2.4	8.8.8.8	0x9232	Standard query (0)	pixel.tapad.com	A (IP address)	IN (0x0001)
Jul 15, 2021 09:22:26.015996933 CEST	192.168.2.4	8.8.8.8	0x32b	Standard query (0)	secure.adnxs.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:20:43.360604048 CEST	8.8.8.8	192.168.2.4	0xaecc	No error (0)	www.stopcovid19.jp	code4sabae.github.io		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:20:43.360604048 CEST	8.8.8.8	192.168.2.4	0xaecc	No error (0)	code4sabae.github.io		185.199.109.153	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:43.360604048 CEST	8.8.8.8	192.168.2.4	0xaecc	No error (0)	code4sabae.github.io		185.199.110.153	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:43.360604048 CEST	8.8.8.8	192.168.2.4	0xaecc	No error (0)	code4sabae.github.io		185.199.111.153	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:43.360604048 CEST	8.8.8.8	192.168.2.4	0xaecc	No error (0)	code4sabae.github.io		185.199.108.153	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:44.270942926 CEST	8.8.8.8	192.168.2.4	0xa522	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:20:44.270942926 CEST	8.8.8.8	192.168.2.4	0xa522	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:44.307898998 CEST	8.8.8.8	192.168.2.4	0x5bc4	No error (0)	platform.twitter.com	cs472.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:20:44.307898998 CEST	8.8.8.8	192.168.2.4	0x5bc4	No error (0)	cs472.wac.edgecastcdn.net	cs1-apr-8315.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:20:44.307898998 CEST	8.8.8.8	192.168.2.4	0x5bc4	No error (0)	cs1-apr-8315.wac.edgecastcdn.net	wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:20:44.307898998 CEST	8.8.8.8	192.168.2.4	0x5bc4	No error (0)	cs1-lb-eu.8315.ecdns.net	cs41.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:20:44.307898998 CEST	8.8.8.8	192.168.2.4	0x5bc4	No error (0)	cs41.wac.edgecastcdn.net		93.184.220.66	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:44.310305119 CEST	8.8.8.8	192.168.2.4	0x6c3b	No error (0)	b.st-hatena.com		143.204.98.89	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:44.310305119 CEST	8.8.8.8	192.168.2.4	0x6c3b	No error (0)	b.st-hatena.com		143.204.98.91	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:44.310305119 CEST	8.8.8.8	192.168.2.4	0x6c3b	No error (0)	b.st-hatena.com		143.204.98.117	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:44.310305119 CEST	8.8.8.8	192.168.2.4	0x6c3b	No error (0)	b.st-hatena.com		143.204.98.77	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:44.975657940 CEST	8.8.8.8	192.168.2.4	0xcc34	No error (0)	code4sabae.github.io		185.199.108.153	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:44.975657940 CEST	8.8.8.8	192.168.2.4	0xcc34	No error (0)	code4sabae.github.io		185.199.109.153	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:44.975657940 CEST	8.8.8.8	192.168.2.4	0xcc34	No error (0)	code4sabae.github.io		185.199.110.153	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:44.975657940 CEST	8.8.8.8	192.168.2.4	0xcc34	No error (0)	code4sabae.github.io		185.199.111.153	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:44.992010117 CEST	8.8.8.8	192.168.2.4	0xc5a	No error (0)	taisukef.github.io		185.199.109.153	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:44.992010117 CEST	8.8.8.8	192.168.2.4	0xc5a	No error (0)	taisukef.github.io		185.199.111.153	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:20:44.992010117 CEST	8.8.8.8	192.168.2.4	0xc5a	No error (0)	taisukef.github.io		185.199.108.153	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:44.992010117 CEST	8.8.8.8	192.168.2.4	0xc5a	No error (0)	taisukef.github.io		185.199.110.153	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:45.057100058 CEST	8.8.8.8	192.168.2.4	0xc56b	No error (0)	b.hatena.ne.jp		143.204.98.109	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:45.057100058 CEST	8.8.8.8	192.168.2.4	0xc56b	No error (0)	b.hatena.ne.jp		143.204.98.93	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:45.057100058 CEST	8.8.8.8	192.168.2.4	0xc56b	No error (0)	b.hatena.ne.jp		143.204.98.15	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:45.057100058 CEST	8.8.8.8	192.168.2.4	0xc56b	No error (0)	b.hatena.ne.jp		143.204.98.67	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:45.135354996 CEST	8.8.8.8	192.168.2.4	0xbe3b	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:20:45.135354996 CEST	8.8.8.8	192.168.2.4	0xbe3b	No error (0)	star-mini.c10r.facebook.com		157.240.195.35	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:45.474910021 CEST	8.8.8.8	192.168.2.4	0x4b2e	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:20:45.474910021 CEST	8.8.8.8	192.168.2.4	0x4b2e	No error (0)	stats.l.doubleclick.net		74.125.128.155	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:45.474910021 CEST	8.8.8.8	192.168.2.4	0x4b2e	No error (0)	stats.l.doubleclick.net		74.125.128.154	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:45.474910021 CEST	8.8.8.8	192.168.2.4	0x4b2e	No error (0)	stats.l.doubleclick.net		74.125.128.157	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:45.474910021 CEST	8.8.8.8	192.168.2.4	0x4b2e	No error (0)	stats.l.doubleclick.net		74.125.128.156	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:46.083803892 CEST	8.8.8.8	192.168.2.4	0xd361	No error (0)	www.google.ch		172.217.168.3	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:46.609662056 CEST	8.8.8.8	192.168.2.4	0x522f	No error (0)	syndication.twitter.com		104.244.42.200	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:46.609662056 CEST	8.8.8.8	192.168.2.4	0x522f	No error (0)	syndication.twitter.com		104.244.42.8	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:46.609662056 CEST	8.8.8.8	192.168.2.4	0x522f	No error (0)	syndication.twitter.com		104.244.42.136	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:46.609662056 CEST	8.8.8.8	192.168.2.4	0x522f	No error (0)	syndication.twitter.com		104.244.42.72	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:46.999150991 CEST	8.8.8.8	192.168.2.4	0x8d85	No error (0)	twitter.com		104.244.42.1	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:46.999150991 CEST	8.8.8.8	192.168.2.4	0x8d85	No error (0)	twitter.com		104.244.42.193	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:47.617036104 CEST	8.8.8.8	192.168.2.4	0x935d	No error (0)	tk3-805-12365.vw.sakura.ne.jp		27.134.249.119	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:48.273871899 CEST	8.8.8.8	192.168.2.4	0x252d	No error (0)	r3.i.lencr.org	crl.root-x1.letsencrypt.org.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:20:49.037194014 CEST	8.8.8.8	192.168.2.4	0xd62c	No error (0)	www.stopcovid19.jp	code4sabae.github.io		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:20:49.037194014 CEST	8.8.8.8	192.168.2.4	0xd62c	No error (0)	code4sabae.github.io		185.199.109.153	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:49.037194014 CEST	8.8.8.8	192.168.2.4	0xd62c	No error (0)	code4sabae.github.io		185.199.110.153	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:20:49.037194014 CEST	8.8.8.8	192.168.2.4	0xd62c	No error (0)	code4sabae.github.io		185.199.111.153	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:49.037194014 CEST	8.8.8.8	192.168.2.4	0xd62c	No error (0)	code4sabae.github.io		185.199.108.153	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:50.374562025 CEST	8.8.8.8	192.168.2.4	0x2055	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:20:50.374562025 CEST	8.8.8.8	192.168.2.4	0x2055	No error (0)	scontent.xx.fbcdn.net		157.240.196.15	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:50.633277893 CEST	8.8.8.8	192.168.2.4	0x515e	No error (0)	tk3-805-12365.vw.sakura.ne.jp		27.134.249.119	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:54.573529005 CEST	8.8.8.8	192.168.2.4	0x2e66	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:20:54.573529005 CEST	8.8.8.8	192.168.2.4	0x2e66	No error (0)	scontent.xx.fbcdn.net		157.240.196.15	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:55.079940081 CEST	8.8.8.8	192.168.2.4	0x929b	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:20:55.079940081 CEST	8.8.8.8	192.168.2.4	0x929b	No error (0)	googlehosted.l.googleusercontent.com		172.217.168.33	A (IP address)	IN (0x0001)
Jul 15, 2021 09:20:56.403048992 CEST	8.8.8.8	192.168.2.4	0x52b2	No error (0)	a-0019.a.dns.azurefd.net	a-0019.standard.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:02.562969923 CEST	8.8.8.8	192.168.2.4	0xff26	No error (0)	cdn.profile-image.st-hatena.com	cdn.profile-image.st-hatena.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:02.737970114 CEST	8.8.8.8	192.168.2.4	0x3be2	No error (0)	cdn.pool.st-hatena.com	cdn.pool.st-hatena.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:02.762974024 CEST	8.8.8.8	192.168.2.4	0xc19d	No error (0)	cdn-ak2.favicon.st-hatena.com	cdn-ak2.favicon.st-hatena.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:03.220870018 CEST	8.8.8.8	192.168.2.4	0xb62c	No error (0)	cdn-ak-scissors.favicon.st-hatena.com	cdn-ak-scissors.favicon.st-hatena.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:03.332077026 CEST	8.8.8.8	192.168.2.4	0x6936	No error (0)	s.hatena.ne.jp		18.182.163.232	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:03.332077026 CEST	8.8.8.8	192.168.2.4	0x6936	No error (0)	s.hatena.ne.jp		54.64.231.89	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:03.471371889 CEST	8.8.8.8	192.168.2.4	0xea2b	No error (0)	c.amazon-adsystem.com	d1ykf07e75w7ss.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:03.471371889 CEST	8.8.8.8	192.168.2.4	0xea2b	No error (0)	d1ykf07e75w7ss.cloudfront.net		143.204.95.188	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:03.608843088 CEST	8.8.8.8	192.168.2.4	0xba0f	No error (0)	static.ads-twitter.com	platform.twitter.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:03.608843088 CEST	8.8.8.8	192.168.2.4	0xba0f	No error (0)	platform.twitter.map.fastly.net		199.232.136.157	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:03.623613119 CEST	8.8.8.8	192.168.2.4	0xc76a	No error (0)	www.clarity.ms	clarity.azurefd.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:03.623613119 CEST	8.8.8.8	192.168.2.4	0xc76a	No error (0)	clarity.azurefd.net	global-geo-afdthirdparty-unicast.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:03.755652905 CEST	8.8.8.8	192.168.2.4	0xac53	No error (0)	dmp.im-apps.net	cf.im-apps.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:04.081643105 CEST	8.8.8.8	192.168.2.4	0x7601	No error (0)	cdn.jsdelivr.net	cdn.jsdelivr.net.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:04.090064049 CEST	8.8.8.8	192.168.2.4	0xcfa3	No error (0)	ib.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:04.090064049 CEST	8.8.8.8	192.168.2.4	0xcfa3	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:21:04.090064049 CEST	8.8.8.8	192.168.2.4	0xcfa3	No error (0)	ib.anycast .adnxs.com		37.252.172.249	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.090064049 CEST	8.8.8.8	192.168.2.4	0xcfa3	No error (0)	ib.anycast .adnxs.com		37.252.172.38	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.090064049 CEST	8.8.8.8	192.168.2.4	0xcfa3	No error (0)	ib.anycast .adnxs.com		37.252.173.27	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.090064049 CEST	8.8.8.8	192.168.2.4	0xcfa3	No error (0)	ib.anycast .adnxs.com		37.252.172.36	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.090064049 CEST	8.8.8.8	192.168.2.4	0xcfa3	No error (0)	ib.anycast .adnxs.com		37.252.172.37	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.090064049 CEST	8.8.8.8	192.168.2.4	0xcfa3	No error (0)	ib.anycast .adnxs.com		37.252.173.62	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.090064049 CEST	8.8.8.8	192.168.2.4	0xcfa3	No error (0)	ib.anycast .adnxs.com		37.252.172.250	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.090064049 CEST	8.8.8.8	192.168.2.4	0xcfa3	No error (0)	ib.anycast .adnxs.com		37.252.173.38	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.097630024 CEST	8.8.8.8	192.168.2.4	0x7794	No error (0)	bidder.cri teo.com	bidder.am5.vip.prod.criteo .com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:04.097630024 CEST	8.8.8.8	192.168.2.4	0x7794	No error (0)	bidder.am5 .vip.prod. criteo.com		178.250.2.131	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.119224072 CEST	8.8.8.8	192.168.2.4	0x8f23	No error (0)	pb.ladsp.com		54.95.166.26	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.119224072 CEST	8.8.8.8	192.168.2.4	0x8f23	No error (0)	pb.ladsp.com		18.176.77.239	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.119224072 CEST	8.8.8.8	192.168.2.4	0x8f23	No error (0)	pb.ladsp.com		18.176.108.153	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.119224072 CEST	8.8.8.8	192.168.2.4	0x8f23	No error (0)	pb.ladsp.com		52.69.137.156	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.119224072 CEST	8.8.8.8	192.168.2.4	0x8f23	No error (0)	pb.ladsp.com		52.199.32.151	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.119224072 CEST	8.8.8.8	192.168.2.4	0x8f23	No error (0)	pb.ladsp.com		18.181.155.39	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.129889011 CEST	8.8.8.8	192.168.2.4	0xbe25	No error (0)	ad.as.aman ad.adtdp.com		143.204.98.55	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.129889011 CEST	8.8.8.8	192.168.2.4	0xbe25	No error (0)	ad.as.aman ad.adtdp.com		143.204.98.53	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.129889011 CEST	8.8.8.8	192.168.2.4	0xbe25	No error (0)	ad.as.aman ad.adtdp.com		143.204.98.109	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.129889011 CEST	8.8.8.8	192.168.2.4	0xbe25	No error (0)	ad.as.aman ad.adtdp.com		143.204.98.69	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.137183905 CEST	8.8.8.8	192.168.2.4	0xa7b6	No error (0)	d.socdm.com		202.241.208.56	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.137183905 CEST	8.8.8.8	192.168.2.4	0xa7b6	No error (0)	d.socdm.com		124.146.215.44	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.137183905 CEST	8.8.8.8	192.168.2.4	0xa7b6	No error (0)	d.socdm.com		124.146.215.43	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.137183905 CEST	8.8.8.8	192.168.2.4	0xa7b6	No error (0)	d.socdm.com		124.146.215.42	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.137183905 CEST	8.8.8.8	192.168.2.4	0xa7b6	No error (0)	d.socdm.com		124.146.215.52	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.137183905 CEST	8.8.8.8	192.168.2.4	0xa7b6	No error (0)	d.socdm.com		202.241.208.100	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:21:04.137183905 CEST	8.8.8.8	192.168.2.4	0xa7b6	No error (0)	d.socdm.com		202.241.208.53	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.137183905 CEST	8.8.8.8	192.168.2.4	0xa7b6	No error (0)	d.socdm.com		124.146.215.46	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.137183905 CEST	8.8.8.8	192.168.2.4	0xa7b6	No error (0)	d.socdm.com		124.146.215.45	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.137183905 CEST	8.8.8.8	192.168.2.4	0xa7b6	No error (0)	d.socdm.com		202.241.208.52	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.137183905 CEST	8.8.8.8	192.168.2.4	0xa7b6	No error (0)	d.socdm.com		124.146.215.51	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.137183905 CEST	8.8.8.8	192.168.2.4	0xa7b6	No error (0)	d.socdm.com		202.241.208.54	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.137183905 CEST	8.8.8.8	192.168.2.4	0xa7b6	No error (0)	d.socdm.com		124.146.215.48	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.137183905 CEST	8.8.8.8	192.168.2.4	0xa7b6	No error (0)	d.socdm.com		124.146.215.49	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.137183905 CEST	8.8.8.8	192.168.2.4	0xa7b6	No error (0)	d.socdm.com		124.146.215.47	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.137183905 CEST	8.8.8.8	192.168.2.4	0xa7b6	No error (0)	d.socdm.com		202.241.208.55	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.137183905 CEST	8.8.8.8	192.168.2.4	0xa7b6	No error (0)	d.socdm.com		202.241.208.57	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.137183905 CEST	8.8.8.8	192.168.2.4	0xa7b6	No error (0)	d.socdm.com		124.146.215.50	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.146466970 CEST	8.8.8.8	192.168.2.4	0x551c	No error (0)	hbopenbid.pubmatic.com	hbopenbid22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:04.146466970 CEST	8.8.8.8	192.168.2.4	0x551c	No error (0)	hbopenbid22000nfc.pubmatic.com	hbopenbid22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:04.146466970 CEST	8.8.8.8	192.168.2.4	0x551c	No error (0)	hbopenbid22000nf.pubmatic.com		185.64.189.112	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.162147999 CEST	8.8.8.8	192.168.2.4	0x34cc	No error (0)	hatena-d.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.162147999 CEST	8.8.8.8	192.168.2.4	0x34cc	No error (0)	hatena-d.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.162169933 CEST	8.8.8.8	192.168.2.4	0x1d76	No error (0)	y.one.impact-ad.jp	pool-gce.dac-yieldone.iponweb.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:04.162169933 CEST	8.8.8.8	192.168.2.4	0x1d76	No error (0)	pool-gce.dac-yieldone.iponweb.net	dac-yieldone-gce.pool.iponweb.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:04.162169933 CEST	8.8.8.8	192.168.2.4	0x1d76	No error (0)	dac-yieldone-gce.pool.iponweb.net		35.213.109.249	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.176517010 CEST	8.8.8.8	192.168.2.4	0x6538	No error (0)	s-rtb-pb.send.microad.jp	s-rtb-pb.send.microad.jp.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:04.181705952 CEST	8.8.8.8	192.168.2.4	0x17e8	No error (0)	fastlane.rubiconproject.com	tagged-by.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:04.379343987 CEST	8.8.8.8	192.168.2.4	0x9f16	No error (0)	t.co		104.244.42.5	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.379343987 CEST	8.8.8.8	192.168.2.4	0x9f16	No error (0)	t.co		104.244.42.133	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.379343987 CEST	8.8.8.8	192.168.2.4	0x9f16	No error (0)	t.co		104.244.42.197	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.379343987 CEST	8.8.8.8	192.168.2.4	0x9f16	No error (0)	t.co		104.244.42.69	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:21:04.381123066 CEST	8.8.8.8	192.168.2.4	0x19a6	No error (0)	c.clarity.ms	c.msn.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:04.381123066 CEST	8.8.8.8	192.168.2.4	0x19a6	No error (0)	c.msn.com	c-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:04.400238991 CEST	8.8.8.8	192.168.2.4	0x1d37	No error (0)	cnt.fout.jp		202.232.238.39	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.445770025 CEST	8.8.8.8	192.168.2.4	0x435c	No error (0)	aax-eu.amazon-adsystem.com		52.95.124.170	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.497997999 CEST	8.8.8.8	192.168.2.4	0xd8f7	No error (0)	cdn.bigmining.com		143.204.98.58	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.497997999 CEST	8.8.8.8	192.168.2.4	0xd8f7	No error (0)	cdn.bigmining.com		143.204.98.37	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.497997999 CEST	8.8.8.8	192.168.2.4	0xd8f7	No error (0)	cdn.bigmining.com		143.204.98.6	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:04.497997999 CEST	8.8.8.8	192.168.2.4	0xd8f7	No error (0)	cdn.bigmining.com		143.204.98.123	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:05.509953022 CEST	8.8.8.8	192.168.2.4	0x4c	No error (0)	i.socdm.com	i.socdm.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:05.699418068 CEST	8.8.8.8	192.168.2.4	0x1fe	No error (0)	static.criteo.net	static.am5.vip.prod.criteo.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:05.699418068 CEST	8.8.8.8	192.168.2.4	0x1fe	No error (0)	static.am5.vip.prod.criteo.net		178.250.2.130	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.430869102 CEST	8.8.8.8	192.168.2.4	0xded	No error (0)	tg.socdm.com	tg.dr.socdm.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:06.430869102 CEST	8.8.8.8	192.168.2.4	0xded	No error (0)	tg.dr.socdm.com		124.146.215.52	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.430869102 CEST	8.8.8.8	192.168.2.4	0xded	No error (0)	tg.dr.socdm.com		202.241.208.53	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.430869102 CEST	8.8.8.8	192.168.2.4	0xded	No error (0)	tg.dr.socdm.com		124.146.215.45	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.430869102 CEST	8.8.8.8	192.168.2.4	0xded	No error (0)	tg.dr.socdm.com		124.146.215.46	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.430869102 CEST	8.8.8.8	192.168.2.4	0xded	No error (0)	tg.dr.socdm.com		202.241.208.55	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.430869102 CEST	8.8.8.8	192.168.2.4	0xded	No error (0)	tg.dr.socdm.com		202.241.208.56	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.430869102 CEST	8.8.8.8	192.168.2.4	0xded	No error (0)	tg.dr.socdm.com		124.146.215.42	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.430869102 CEST	8.8.8.8	192.168.2.4	0xded	No error (0)	tg.dr.socdm.com		124.146.215.50	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.430869102 CEST	8.8.8.8	192.168.2.4	0xded	No error (0)	tg.dr.socdm.com		124.146.215.49	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.430869102 CEST	8.8.8.8	192.168.2.4	0xded	No error (0)	tg.dr.socdm.com		124.146.215.48	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.430869102 CEST	8.8.8.8	192.168.2.4	0xded	No error (0)	tg.dr.socdm.com		202.241.208.57	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.430869102 CEST	8.8.8.8	192.168.2.4	0xded	No error (0)	tg.dr.socdm.com		124.146.215.44	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.430869102 CEST	8.8.8.8	192.168.2.4	0xded	No error (0)	tg.dr.socdm.com		202.241.208.52	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.430869102 CEST	8.8.8.8	192.168.2.4	0xded	No error (0)	tg.dr.socdm.com		124.146.215.47	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:21:06.430869102 CEST	8.8.8.8	192.168.2.4	0xded	No error (0)	tg.dr.socdm.com		202.241.208.54	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.430869102 CEST	8.8.8.8	192.168.2.4	0xded	No error (0)	tg.dr.socdm.com		202.241.208.100	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.430869102 CEST	8.8.8.8	192.168.2.4	0xded	No error (0)	tg.dr.socdm.com		124.146.215.43	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.430869102 CEST	8.8.8.8	192.168.2.4	0xded	No error (0)	tg.dr.socdm.com		124.146.215.51	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.437849045 CEST	8.8.8.8	192.168.2.4	0xd901	No error (0)	imp-adedge.i-mobile.co.jp	d1g3u69q0yy58t.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:06.437849045 CEST	8.8.8.8	192.168.2.4	0xd901	No error (0)	d1g3u69q0yy58t.cloudfront.net		143.204.98.70	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.437849045 CEST	8.8.8.8	192.168.2.4	0xd901	No error (0)	d1g3u69q0yy58t.cloudfront.net		143.204.98.117	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.437849045 CEST	8.8.8.8	192.168.2.4	0xd901	No error (0)	d1g3u69q0yy58t.cloudfront.net		143.204.98.21	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.437849045 CEST	8.8.8.8	192.168.2.4	0xd901	No error (0)	d1g3u69q0yy58t.cloudfront.net		143.204.98.41	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.495579004 CEST	8.8.8.8	192.168.2.4	0xe49e	No error (0)	yads.c.yimg.jp	edge.g.yimg.jp		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:06.495579004 CEST	8.8.8.8	192.168.2.4	0xe49e	No error (0)	edge.g.yimg.jp		182.22.24.124	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:06.608217001 CEST	8.8.8.8	192.168.2.4	0xf3ec	No error (0)	repository.secomtrust.net		61.114.177.151	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.279180050 CEST	8.8.8.8	192.168.2.4	0x3d71	No error (0)	ssp-bidapi.i-mobile.co.jp	ssp-pc-layer7-lb-1418692822.ap-northeast-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:07.279180050 CEST	8.8.8.8	192.168.2.4	0x3d71	No error (0)	ssp-pc-layer7-lb-1418692822.ap-northeast-1.elb.amazonaws.com		13.230.7.5	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.279180050 CEST	8.8.8.8	192.168.2.4	0x3d71	No error (0)	ssp-pc-layer7-lb-1418692822.ap-northeast-1.elb.amazonaws.com		18.177.223.75	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.279180050 CEST	8.8.8.8	192.168.2.4	0x3d71	No error (0)	ssp-pc-layer7-lb-1418692822.ap-northeast-1.elb.amazonaws.com		3.115.182.199	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.279180050 CEST	8.8.8.8	192.168.2.4	0x3d71	No error (0)	ssp-pc-layer7-lb-1418692822.ap-northeast-1.elb.amazonaws.com		18.182.222.164	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.279180050 CEST	8.8.8.8	192.168.2.4	0x3d71	No error (0)	ssp-pc-layer7-lb-1418692822.ap-northeast-1.elb.amazonaws.com		18.179.235.202	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.433361053 CEST	8.8.8.8	192.168.2.4	0x50b7	No error (0)	b.hatena.ne.jp		143.204.98.15	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.433361053 CEST	8.8.8.8	192.168.2.4	0x50b7	No error (0)	b.hatena.ne.jp		143.204.98.67	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.433361053 CEST	8.8.8.8	192.168.2.4	0x50b7	No error (0)	b.hatena.ne.jp		143.204.98.109	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.433361053 CEST	8.8.8.8	192.168.2.4	0x50b7	No error (0)	b.hatena.ne.jp		143.204.98.93	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.436726093 CEST	8.8.8.8	192.168.2.4	0x6c2e	No error (0)	b.st-hatena.com		143.204.98.89	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:21:07.436726093 CEST	8.8.8.8	192.168.2.4	0x6c2e	No error (0)	b.st-hatena.com		143.204.98.91	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.436726093 CEST	8.8.8.8	192.168.2.4	0x6c2e	No error (0)	b.st-hatena.com		143.204.98.117	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.436726093 CEST	8.8.8.8	192.168.2.4	0x6c2e	No error (0)	b.st-hatena.com		143.204.98.77	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.542376995 CEST	8.8.8.8	192.168.2.4	0xe7d5	No error (0)	s.yimg.jp	edge.g.yimg.jp		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:07.542376995 CEST	8.8.8.8	192.168.2.4	0xe7d5	No error (0)	edge.g.yimg.jp		182.22.31.252	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.542823076 CEST	8.8.8.8	192.168.2.4	0xd86d	No error (0)	yads.yjtag.yahoo.co.jp	edge.g.yimg.jp		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:07.542823076 CEST	8.8.8.8	192.168.2.4	0xd86d	No error (0)	edge.g.yimg.jp		183.79.248.124	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:07.555214882 CEST	8.8.8.8	192.168.2.4	0x1399	No error (0)	cdn.profile-image.st-hatena.com	cdn.profile-image.st-hatena.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:07.727859974 CEST	8.8.8.8	192.168.2.4	0x4b6a	No error (0)	cdn-ak2.favicon.st-hatena.com	cdn-ak2.favicon.st-hatena.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:07.853308916 CEST	8.8.8.8	192.168.2.4	0x5fdf	No error (0)	cdn-ak-scissors.favicon.st-hatena.com	cdn-ak-scissors.favicon.st-hatena.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:07.880455971 CEST	8.8.8.8	192.168.2.4	0xaba6	No error (0)	eus.rubiconproject.com	eus.rubiconproject.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:07.948709965 CEST	8.8.8.8	192.168.2.4	0xf90f	No error (0)	ads.pubmatic.com	pubmatic.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:08.641967058 CEST	8.8.8.8	192.168.2.4	0x5ad2	No error (0)	cr-p31.ladsp.jp		143.204.98.44	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:08.641967058 CEST	8.8.8.8	192.168.2.4	0x5ad2	No error (0)	cr-p31.ladsp.jp		143.204.98.83	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:08.641967058 CEST	8.8.8.8	192.168.2.4	0x5ad2	No error (0)	cr-p31.ladsp.jp		143.204.98.56	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:08.641967058 CEST	8.8.8.8	192.168.2.4	0x5ad2	No error (0)	cr-p31.ladsp.jp		143.204.98.106	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:08.641998053 CEST	8.8.8.8	192.168.2.4	0x55ec	No error (0)	eu-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:08.641998053 CEST	8.8.8.8	192.168.2.4	0x55ec	No error (0)	eu-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:08.645304918 CEST	8.8.8.8	192.168.2.4	0xed96	No error (0)	y.one.impact-ad.jp	pool-gce.dac-yieldone.iponweb.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:08.645304918 CEST	8.8.8.8	192.168.2.4	0xed96	No error (0)	pool-gce.dac-yieldone.iponweb.net	dac-yieldone-gce.pool.iponweb.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:08.645304918 CEST	8.8.8.8	192.168.2.4	0xed96	No error (0)	dac-yieldone-gce.pool.iponweb.net		35.213.109.249	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:08.647334099 CEST	8.8.8.8	192.168.2.4	0x345b	No error (0)	spnativeapi-tls.i-mobile.co.jp	d1o24znjkq68c8.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:08.647334099 CEST	8.8.8.8	192.168.2.4	0x345b	No error (0)	d1o24znjkq68c8.cloudfront.net		143.204.98.37	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:08.647334099 CEST	8.8.8.8	192.168.2.4	0x345b	No error (0)	d1o24znjkq68c8.cloudfront.net		143.204.98.86	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:08.647334099 CEST	8.8.8.8	192.168.2.4	0x345b	No error (0)	d1o24znjkq68c8.cloudfront.net		143.204.98.59	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:08.647334099 CEST	8.8.8.8	192.168.2.4	0x345b	No error (0)	d1o24znjkq68c8.cloudfront.net		143.204.98.73	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:21:08.652296066 CEST	8.8.8.8	192.168.2.4	0x7487	No error (0)	acdn.adnxs.com	secure-adnxs.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:09.118552923 CEST	8.8.8.8	192.168.2.4	0x218b	No error (0)	image6.pubmatic.com	pugm22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:09.118552923 CEST	8.8.8.8	192.168.2.4	0x218b	No error (0)	pugm22000nfc.pubmatic.com	pugm22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:09.118552923 CEST	8.8.8.8	192.168.2.4	0x218b	No error (0)	pugm22000nf.pubmatic.com		185.64.189.115	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:09.148627043 CEST	8.8.8.8	192.168.2.4	0x76b9	No error (0)	cr-pall.ladsp.com		143.204.98.24	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:09.148627043 CEST	8.8.8.8	192.168.2.4	0x76b9	No error (0)	cr-pall.ladsp.com		143.204.98.42	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:09.148627043 CEST	8.8.8.8	192.168.2.4	0x76b9	No error (0)	cr-pall.ladsp.com		143.204.98.102	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:09.148627043 CEST	8.8.8.8	192.168.2.4	0x76b9	No error (0)	cr-pall.ladsp.com		143.204.98.47	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:11.184186935 CEST	8.8.8.8	192.168.2.4	0x9def	No error (0)	match.adsrvr.org	match-aga.adsrvr.org		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:11.184186935 CEST	8.8.8.8	192.168.2.4	0x9def	No error (0)	match-aga.adsrvr.org	a97adde81b00f2ca4.awsglobalaccelerator.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:11.184186935 CEST	8.8.8.8	192.168.2.4	0x9def	No error (0)	a97adde81b00f2ca4.awsglobalaccelerator.com		13.248.242.197	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:11.184186935 CEST	8.8.8.8	192.168.2.4	0x9def	No error (0)	a97adde81b00f2ca4.awsglobalaccelerator.com		76.223.111.131	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:12.056519032 CEST	8.8.8.8	192.168.2.4	0xba9b	No error (0)	im.ov.yahoo.co.jp	edge.g.yimg.jp		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:12.056519032 CEST	8.8.8.8	192.168.2.4	0xba9b	No error (0)	edge.g.yimg.jp		182.22.16.123	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:12.302938938 CEST	8.8.8.8	192.168.2.4	0xdbb2	No error (0)	penta.a.one.impact-ad.jp		107.178.248.96	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.768141985 CEST	8.8.8.8	192.168.2.4	0xa44c	No error (0)	pm.w55c.net	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:13.768141985 CEST	8.8.8.8	192.168.2.4	0xa44c	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		3.124.143.99	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.768141985 CEST	8.8.8.8	192.168.2.4	0xa44c	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		18.193.131.224	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.768141985 CEST	8.8.8.8	192.168.2.4	0xa44c	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		3.123.143.157	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.768141985 CEST	8.8.8.8	192.168.2.4	0xa44c	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		3.125.99.7	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.768141985 CEST	8.8.8.8	192.168.2.4	0xa44c	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		18.159.182.76	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.768141985 CEST	8.8.8.8	192.168.2.4	0xa44c	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		3.127.92.82	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:21:13.768141985 CEST	8.8.8.8	192.168.2.4	0xa44c	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		18.158.226.176	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.768141985 CEST	8.8.8.8	192.168.2.4	0xa44c	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		52.57.110.162	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.773691893 CEST	8.8.8.8	192.168.2.4	0x63a3	No error (0)	x.bidswitch.net	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:13.773691893 CEST	8.8.8.8	192.168.2.4	0x63a3	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		54.93.69.146	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.773691893 CEST	8.8.8.8	192.168.2.4	0x63a3	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		3.121.66.166	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.773691893 CEST	8.8.8.8	192.168.2.4	0x63a3	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		3.124.165.65	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.773691893 CEST	8.8.8.8	192.168.2.4	0x63a3	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		52.59.128.17	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.773691893 CEST	8.8.8.8	192.168.2.4	0x63a3	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		35.157.168.25	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.773691893 CEST	8.8.8.8	192.168.2.4	0x63a3	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		18.195.73.36	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.773691893 CEST	8.8.8.8	192.168.2.4	0x63a3	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		52.57.47.211	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.773691893 CEST	8.8.8.8	192.168.2.4	0x63a3	No error (0)	alb-aws-fr-bswx-2-1673521430.eu-central-1.elb.amazonaws.com		35.158.9.168	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.784296036 CEST	8.8.8.8	192.168.2.4	0xb3ec	No error (0)	sync.mathtag.com	pixel-origin.mathtag.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:13.784296036 CEST	8.8.8.8	192.168.2.4	0xb3ec	No error (0)	pixel-origin.mathtag.com		185.29.132.144	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.784296036 CEST	8.8.8.8	192.168.2.4	0xb3ec	No error (0)	pixel-origin.mathtag.com		185.29.135.227	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.784296036 CEST	8.8.8.8	192.168.2.4	0xb3ec	No error (0)	pixel-origin.mathtag.com		185.29.135.226	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.784296036 CEST	8.8.8.8	192.168.2.4	0xb3ec	No error (0)	pixel-origin.mathtag.com		185.29.135.190	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.790841103 CEST	8.8.8.8	192.168.2.4	0xdf0c	No error (0)	match.prod.bidr.io		52.16.214.249	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.790841103 CEST	8.8.8.8	192.168.2.4	0xdf0c	No error (0)	match.prod.bidr.io		52.49.238.187	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.790841103 CEST	8.8.8.8	192.168.2.4	0xdf0c	No error (0)	match.prod.bidr.io		54.246.13.173	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.790841103 CEST	8.8.8.8	192.168.2.4	0xdf0c	No error (0)	match.prod.bidr.io		34.247.100.44	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:21:13.790841103 CEST	8.8.8.8	192.168.2.4	0xdf0c	No error (0)	match.prod.bidr.io		52.30.92.119	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.790841103 CEST	8.8.8.8	192.168.2.4	0xdf0c	No error (0)	match.prod.bidr.io		52.30.222.33	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.790841103 CEST	8.8.8.8	192.168.2.4	0xdf0c	No error (0)	match.prod.bidr.io		52.17.245.120	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.790841103 CEST	8.8.8.8	192.168.2.4	0xdf0c	No error (0)	match.prod.bidr.io		34.252.144.15	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.799087048 CEST	8.8.8.8	192.168.2.4	0xbdc3	No error (0)	pixel.quantserve.com	global.px.quantserve.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:13.799087048 CEST	8.8.8.8	192.168.2.4	0xbdc3	No error (0)	global.px.quantserve.com		91.228.74.134	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.799087048 CEST	8.8.8.8	192.168.2.4	0xbdc3	No error (0)	global.px.quantserve.com		91.228.74.189	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.799087048 CEST	8.8.8.8	192.168.2.4	0xbdc3	No error (0)	global.px.quantserve.com		91.228.74.226	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.799087048 CEST	8.8.8.8	192.168.2.4	0xbdc3	No error (0)	global.px.quantserve.com		91.228.74.198	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.799087048 CEST	8.8.8.8	192.168.2.4	0xbdc3	No error (0)	global.px.quantserve.com		91.228.74.133	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.812923908 CEST	8.8.8.8	192.168.2.4	0x5291	No error (0)	cm.g.doubleclick.net		216.58.215.226	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:13.878340006 CEST	8.8.8.8	192.168.2.4	0x86c	No error (0)	c1.adform.net	track.adformnet.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:14.342869997 CEST	8.8.8.8	192.168.2.4	0xa0d4	No error (0)	us-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:14.342869997 CEST	8.8.8.8	192.168.2.4	0xa0d4	No error (0)	us-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:14.594907999 CEST	8.8.8.8	192.168.2.4	0x292a	No error (0)	ads.creative-serving.com	elb-aws-fr-clickdistrict-1651093077.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:14.594907999 CEST	8.8.8.8	192.168.2.4	0x292a	No error (0)	elb-aws-fr-clickdistrict-1651093077.eu-central-1.elb.amazonaws.com		3.127.51.194	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:14.594907999 CEST	8.8.8.8	192.168.2.4	0x292a	No error (0)	elb-aws-fr-clickdistrict-1651093077.eu-central-1.elb.amazonaws.com		3.123.96.39	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:14.594907999 CEST	8.8.8.8	192.168.2.4	0x292a	No error (0)	elb-aws-fr-clickdistrict-1651093077.eu-central-1.elb.amazonaws.com		18.195.105.17	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:14.594907999 CEST	8.8.8.8	192.168.2.4	0x292a	No error (0)	elb-aws-fr-clickdistrict-1651093077.eu-central-1.elb.amazonaws.com		3.120.83.159	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:14.820063114 CEST	8.8.8.8	192.168.2.4	0x35df	No error (0)	pixel-eu.rubiconproject.com	pixel-eu.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:14.938536882 CEST	8.8.8.8	192.168.2.4	0xa4b6	No error (0)	dis.criteo.com	widget.par.vip.prod.criteo.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:14.938536882 CEST	8.8.8.8	192.168.2.4	0xa4b6	No error (0)	widget.par.vip.prod.criteo.com		178.250.0.163	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:21:14.998388052 CEST	8.8.8.8	192.168.2.4	0xfa7f	No error (0)	rtb-csync.smartadserver.com	2-01-275d-002d.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:14.998388052 CEST	8.8.8.8	192.168.2.4	0xfa7f	No error (0)	rtb-csync-eqx.smartadserver.com		185.86.137.131	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:14.998388052 CEST	8.8.8.8	192.168.2.4	0xfa7f	No error (0)	rtb-csync-eqx.smartadserver.com		185.86.137.110	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:14.998388052 CEST	8.8.8.8	192.168.2.4	0xfa7f	No error (0)	rtb-csync-eqx.smartadserver.com		185.86.137.133	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:14.998388052 CEST	8.8.8.8	192.168.2.4	0xfa7f	No error (0)	rtb-csync-eqx.smartadserver.com		185.86.137.132	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.081986904 CEST	8.8.8.8	192.168.2.4	0x5869	No error (0)	match.deepintent.com	g.deepintent.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:15.081986904 CEST	8.8.8.8	192.168.2.4	0x5869	No error (0)	g.deepintent.com		169.197.150.8	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.081986904 CEST	8.8.8.8	192.168.2.4	0x5869	No error (0)	g.deepintent.com		169.197.150.7	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.081986904 CEST	8.8.8.8	192.168.2.4	0x5869	No error (0)	g.deepintent.com		38.91.45.7	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.181608915 CEST	8.8.8.8	192.168.2.4	0xf718	No error (0)	idsync.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.184331894 CEST	8.8.8.8	192.168.2.4	0x128a	No error (0)	bh.contextweb.com	lga-bh.contextweb.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:15.184331894 CEST	8.8.8.8	192.168.2.4	0x128a	No error (0)	lga-bh.contextweb.com	lga-bh-bgp.contextweb.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:15.184331894 CEST	8.8.8.8	192.168.2.4	0x128a	No error (0)	lga-bh-bgp.contextweb.com		198.148.27.140	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.184331894 CEST	8.8.8.8	192.168.2.4	0x128a	No error (0)	lga-bh-bgp.contextweb.com		198.148.27.139	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.224399090 CEST	8.8.8.8	192.168.2.4	0xec2	No error (0)	sync-tm.everesttech.net	sync.tubemogul.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:15.224399090 CEST	8.8.8.8	192.168.2.4	0xec2	No error (0)	sync.tubemogul.com	syncf.tubemogul.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:15.224399090 CEST	8.8.8.8	192.168.2.4	0xec2	No error (0)	syncf.tubemogul.com	h2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:15.231327057 CEST	8.8.8.8	192.168.2.4	0x3696	No error (0)	ad.turn.com	ad.turn.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:15.231372118 CEST	8.8.8.8	192.168.2.4	0xce0c	No error (0)	pr-bh.ybp.yahoo.com	ds-pr-bh.ybp.gysm.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:15.231372118 CEST	8.8.8.8	192.168.2.4	0xce0c	No error (0)	ds-pr-bh.ybp.gysm.yahoodns.net		212.82.100.176	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.238563061 CEST	8.8.8.8	192.168.2.4	0x9859	No error (0)	ups.analytics.yahoo.com	prod.ups-ats.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:15.238563061 CEST	8.8.8.8	192.168.2.4	0x9859	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 15, 2021 09:21:15.238563061 CEST	8.8.8.8	192.168.2.4	0x9859	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 15, 2021 09:21:15.238563061 CEST	8.8.8.8	192.168.2.4	0x9859	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 15, 2021 09:21:15.247226000 CEST	8.8.8.8	192.168.2.4	0x7e54	No error (0)	um.simpli.fi		169.50.137.190	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:21:15.247226000 CEST	8.8.8.8	192.168.2.4	0x7e54	No error (0)	um.simpli.fi		159.253.128.188	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.247226000 CEST	8.8.8.8	192.168.2.4	0x7e54	No error (0)	um.simpli.fi		159.253.128.183	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.294714928 CEST	8.8.8.8	192.168.2.4	0xc0f7	No error (0)	pubmatic-match.dotomi.com	afp.dotomi.weighted.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:15.350574970 CEST	8.8.8.8	192.168.2.4	0xfc95	No error (0)	rtb.adentifi.com		54.236.227.29	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.350574970 CEST	8.8.8.8	192.168.2.4	0xfc95	No error (0)	rtb.adentifi.com		52.4.101.239	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.350574970 CEST	8.8.8.8	192.168.2.4	0xfc95	No error (0)	rtb.adentifi.com		54.210.14.23	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.350574970 CEST	8.8.8.8	192.168.2.4	0xfc95	No error (0)	rtb.adentifi.com		52.55.122.95	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.350574970 CEST	8.8.8.8	192.168.2.4	0xfc95	No error (0)	rtb.adentifi.com		52.45.11.130	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.350574970 CEST	8.8.8.8	192.168.2.4	0xfc95	No error (0)	rtb.adentifi.com		52.4.236.19	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.350574970 CEST	8.8.8.8	192.168.2.4	0xfc95	No error (0)	rtb.adentifi.com		52.44.116.71	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.350574970 CEST	8.8.8.8	192.168.2.4	0xfc95	No error (0)	rtb.adentifi.com		52.207.62.93	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.351421118 CEST	8.8.8.8	192.168.2.4	0x6fff	No error (0)	image2.pubmatic.com	pug22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:15.351421118 CEST	8.8.8.8	192.168.2.4	0x6fff	No error (0)	pug22000nfc.pubmatic.com	pug22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:15.351421118 CEST	8.8.8.8	192.168.2.4	0x6fff	No error (0)	pug22000nf.pubmatic.com		185.64.189.110	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.474423885 CEST	8.8.8.8	192.168.2.4	0xb59e	No error (0)	id.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.480333090 CEST	8.8.8.8	192.168.2.4	0xbad4	No error (0)	pixel.rubiconproject.com	pixel.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:15.494113922 CEST	8.8.8.8	192.168.2.4	0x5c03	No error (0)	token.rubiconproject.com	pixel.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:15.587162971 CEST	8.8.8.8	192.168.2.4	0x8dd0	No error (0)	sync.ipredictive.com		34.232.92.67	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.587162971 CEST	8.8.8.8	192.168.2.4	0x8dd0	No error (0)	sync.ipredictive.com		34.194.115.107	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.587162971 CEST	8.8.8.8	192.168.2.4	0x8dd0	No error (0)	sync.ipredictive.com		52.203.60.58	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.587162971 CEST	8.8.8.8	192.168.2.4	0x8dd0	No error (0)	sync.ipredictive.com		52.205.83.58	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.587162971 CEST	8.8.8.8	192.168.2.4	0x8dd0	No error (0)	sync.ipredictive.com		54.160.32.191	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.587162971 CEST	8.8.8.8	192.168.2.4	0x8dd0	No error (0)	sync.ipredictive.com		54.226.209.67	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.587162971 CEST	8.8.8.8	192.168.2.4	0x8dd0	No error (0)	sync.ipredictive.com		52.71.206.53	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.587162971 CEST	8.8.8.8	192.168.2.4	0x8dd0	No error (0)	sync.ipredictive.com		34.239.198.206	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.685980082 CEST	8.8.8.8	192.168.2.4	0x4339	No error (0)	pixel-sync.sitescout.com	pixel-a.sitescout.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:21:15.685980082 CEST	8.8.8.8	192.168.2.4	0x4339	No error (0)	pixel-a.si tescout.com		66.155.71.25	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.959280968 CEST	8.8.8.8	192.168.2.4	0x92fe	No error (0)	image4.pub matic.com	spug22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:15.959280968 CEST	8.8.8.8	192.168.2.4	0x92fe	No error (0)	spug22000n fc.pubmatic.com	spug22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:15.959280968 CEST	8.8.8.8	192.168.2.4	0x92fe	No error (0)	spug22000n f.pubmatic.com		185.64.189.114	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.967590094 CEST	8.8.8.8	192.168.2.4	0xc572	No error (0)	simage2.pu bmatic.com	pug-lhrc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:15.967590094 CEST	8.8.8.8	192.168.2.4	0xc572	No error (0)	pug-lhrc.p ubmatic.com	pug-lhr.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:15.967590094 CEST	8.8.8.8	192.168.2.4	0xc572	No error (0)	pug-lhr.pu bmatic.com		185.64.190.80	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.986202955 CEST	8.8.8.8	192.168.2.4	0xea8d	No error (0)	r.scoota.co	pool-scoota.rockabox.iponweb.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:15.986202955 CEST	8.8.8.8	192.168.2.4	0xea8d	No error (0)	pool-scoot a.rockabox .iponweb.net	elb-aws-ie-rockabox-scoota-2052063539.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:15.986202955 CEST	8.8.8.8	192.168.2.4	0xea8d	No error (0)	elb-aws-ie-rockabox-scoota-205 2063539.eu-west-1.el b.amazonaw s.com		52.17.35.107	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:15.986202955 CEST	8.8.8.8	192.168.2.4	0xea8d	No error (0)	elb-aws-ie-rockabox-scoota-205 2063539.eu-west-1.el b.amazonaw s.com		54.171.74.241	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:16.012603998 CEST	8.8.8.8	192.168.2.4	0x99b5	No error (0)	pmp.mxptint.net		204.2.255.233	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:16.196402073 CEST	8.8.8.8	192.168.2.4	0xc093	No error (0)	sync.1rx.io		213.19.147.44	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:16.265444040 CEST	8.8.8.8	192.168.2.4	0xffb5	No error (0)	cm.adgrx.com	rtb.adgrx.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:16.265444040 CEST	8.8.8.8	192.168.2.4	0xffb5	No error (0)	rtb.adgrx.com	rtb.adgrx.com.tech.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:16.522488117 CEST	8.8.8.8	192.168.2.4	0x5273	No error (0)	ads.yahoo.com	edge.gycpi.b.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:16.522488117 CEST	8.8.8.8	192.168.2.4	0x5273	No error (0)	edge.gycpi .b.yahoodns.net		87.248.118.22	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:16.522488117 CEST	8.8.8.8	192.168.2.4	0x5273	No error (0)	edge.gycpi .b.yahoodns.net		87.248.118.23	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:16.597191095 CEST	8.8.8.8	192.168.2.4	0x6722	No error (0)	sync.targe ting.unrul ymedia.com	sync.1rx.io		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:16.597191095 CEST	8.8.8.8	192.168.2.4	0x6722	No error (0)	sync.1rx.io		213.19.147.44	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:16.875226021 CEST	8.8.8.8	192.168.2.4	0x4b80	No error (0)	px.owneriq.net	wildcard.owneriq.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:17.094366074 CEST	8.8.8.8	192.168.2.4	0x1fc6	No error (0)	a.tribalfu sion.com		104.18.12.5	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.094366074 CEST	8.8.8.8	192.168.2.4	0x1fc6	No error (0)	a.tribalfu sion.com		104.18.13.5	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:21:17.243740082 CEST	8.8.8.8	192.168.2.4	0xf1d7	No error (0)	match.bnmla.com		38.27.122.158	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.391891956 CEST	8.8.8.8	192.168.2.4	0x167e	No error (0)	s.tribalfusion.com		104.18.12.5	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.391891956 CEST	8.8.8.8	192.168.2.4	0x167e	No error (0)	s.tribalfusion.com		104.18.13.5	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.423985004 CEST	8.8.8.8	192.168.2.4	0xc62e	No error (0)	pixel.onaudience.com		146.59.148.16	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.423985004 CEST	8.8.8.8	192.168.2.4	0xc62e	No error (0)	pixel.onaudience.com		51.79.83.225	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.423985004 CEST	8.8.8.8	192.168.2.4	0xc62e	No error (0)	pixel.onaudience.com		51.210.112.236	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.423985004 CEST	8.8.8.8	192.168.2.4	0xc62e	No error (0)	pixel.onaudience.com		51.222.80.231	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.423985004 CEST	8.8.8.8	192.168.2.4	0xc62e	No error (0)	pixel.onaudience.com		51.210.112.63	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.431240082 CEST	8.8.8.8	192.168.2.4	0x5e5c	No error (0)	visitor.fiftyt.com		35.201.96.126	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.432815075 CEST	8.8.8.8	192.168.2.4	0xec07	No error (0)	aa.agkn.com	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:17.432815075 CEST	8.8.8.8	192.168.2.4	0xec07	No error (0)	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com		52.29.225.117	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.432815075 CEST	8.8.8.8	192.168.2.4	0xec07	No error (0)	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com		3.120.52.200	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.432815075 CEST	8.8.8.8	192.168.2.4	0xec07	No error (0)	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com		52.58.248.2	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.432815075 CEST	8.8.8.8	192.168.2.4	0xec07	No error (0)	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com		3.127.52.31	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.452847958 CEST	8.8.8.8	192.168.2.4	0x71d2	No error (0)	io.narrative.io		52.212.225.58	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.452847958 CEST	8.8.8.8	192.168.2.4	0x71d2	No error (0)	io.narrative.io		52.215.52.168	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.456295967 CEST	8.8.8.8	192.168.2.4	0x7a02	No error (0)	rtb.gumgum.com		52.18.52.16	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.456295967 CEST	8.8.8.8	192.168.2.4	0x7a02	No error (0)	rtb.gumgum.com		54.247.114.64	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.456295967 CEST	8.8.8.8	192.168.2.4	0x7a02	No error (0)	rtb.gumgum.com		54.77.19.59	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.456295967 CEST	8.8.8.8	192.168.2.4	0x7a02	No error (0)	rtb.gumgum.com		52.48.175.241	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.456295967 CEST	8.8.8.8	192.168.2.4	0x7a02	No error (0)	rtb.gumgum.com		52.212.126.234	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.456295967 CEST	8.8.8.8	192.168.2.4	0x7a02	No error (0)	rtb.gumgum.com		34.251.173.19	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:21:17.456295967 CEST	8.8.8.8	192.168.2.4	0x7a02	No error (0)	rtb.gumgum.com		54.77.47.243	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:17.456295967 CEST	8.8.8.8	192.168.2.4	0x7a02	No error (0)	rtb.gumgum.com		52.208.210.171	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:18.608958960 CEST	8.8.8.8	192.168.2.4	0x6d60	No error (0)	simage4.pubmatic.com	spug22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:18.608958960 CEST	8.8.8.8	192.168.2.4	0x6d60	No error (0)	spug22000nfc.pubmatic.com	spug22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:18.608958960 CEST	8.8.8.8	192.168.2.4	0x6d60	No error (0)	spug22000nf.pubmatic.com		185.64.189.114	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.268910885 CEST	8.8.8.8	192.168.2.4	0xe56	No error (0)	cm.g.doubleclick.net		216.58.215.226	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.269162893 CEST	8.8.8.8	192.168.2.4	0xf535	No error (0)	idsync.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.295001030 CEST	8.8.8.8	192.168.2.4	0xf8d4	No error (0)	sync.mathtag.com	pixel-origin.mathtag.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.295001030 CEST	8.8.8.8	192.168.2.4	0xf8d4	No error (0)	pixel-origin.mathtag.com		185.29.135.227	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.295001030 CEST	8.8.8.8	192.168.2.4	0xf8d4	No error (0)	pixel-origin.mathtag.com		185.29.135.226	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.295001030 CEST	8.8.8.8	192.168.2.4	0xf8d4	No error (0)	pixel-origin.mathtag.com		185.29.135.234	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.295001030 CEST	8.8.8.8	192.168.2.4	0xf8d4	No error (0)	pixel-origin.mathtag.com		185.29.133.58	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.300986052 CEST	8.8.8.8	192.168.2.4	0x146d	No error (0)	match.adsrvr.org	match-aga.adsrvr.org		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.300986052 CEST	8.8.8.8	192.168.2.4	0x146d	No error (0)	match-aga.adsrvr.org	a97adde81b00f2ca4.awsglobalaccelerator.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.300986052 CEST	8.8.8.8	192.168.2.4	0x146d	No error (0)	a97adde81b00f2ca4.awsglobalaccelerator.com		13.248.242.197	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.300986052 CEST	8.8.8.8	192.168.2.4	0x146d	No error (0)	a97adde81b00f2ca4.awsglobalaccelerator.com		76.223.111.131	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.326394081 CEST	8.8.8.8	192.168.2.4	0x7fba	No error (0)	sync-tm.everesttech.net	sync.tubemogul.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.326394081 CEST	8.8.8.8	192.168.2.4	0x7fba	No error (0)	sync.tubemogul.com	syncf.tubemogul.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.326394081 CEST	8.8.8.8	192.168.2.4	0x7fba	No error (0)	syncf.tubemogul.com	h2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.337034941 CEST	8.8.8.8	192.168.2.4	0x75b4	No error (0)	ad.turn.com	ad.turn.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.343907118 CEST	8.8.8.8	192.168.2.4	0x2a8a	No error (0)	pr-bh.ybp.yahoo.com	ds-pr-bh.ybp.gysm.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.343907118 CEST	8.8.8.8	192.168.2.4	0x2a8a	No error (0)	ds-pr-bh.ybp.gysm.yahoodns.net		212.82.100.176	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.353744984 CEST	8.8.8.8	192.168.2.4	0x77e6	No error (0)	ups.analytics.yahoo.com	prod.ups-ats.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.353744984 CEST	8.8.8.8	192.168.2.4	0x77e6	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 15, 2021 09:21:19.353744984 CEST	8.8.8.8	192.168.2.4	0x77e6	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		18.156.0.31	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:21:19.353744984 CEST	8.8.8.8	192.168.2.4	0x77e6	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 15, 2021 09:21:19.364224911 CEST	8.8.8.8	192.168.2.4	0xc57d	No error (0)	um.simpli.fi		169.50.137.190	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.364224911 CEST	8.8.8.8	192.168.2.4	0xc57d	No error (0)	um.simpli.fi		159.253.128.188	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.364224911 CEST	8.8.8.8	192.168.2.4	0xc57d	No error (0)	um.simpli.fi		159.253.128.183	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.370224953 CEST	8.8.8.8	192.168.2.4	0x956c	No error (0)	ib.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.370224953 CEST	8.8.8.8	192.168.2.4	0x956c	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.370224953 CEST	8.8.8.8	192.168.2.4	0x956c	No error (0)	ib.anycast.adnxs.com		185.33.221.53	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.370224953 CEST	8.8.8.8	192.168.2.4	0x956c	No error (0)	ib.anycast.adnxs.com		185.33.221.11	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.370224953 CEST	8.8.8.8	192.168.2.4	0x956c	No error (0)	ib.anycast.adnxs.com		185.33.221.87	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.370224953 CEST	8.8.8.8	192.168.2.4	0x956c	No error (0)	ib.anycast.adnxs.com		185.33.221.91	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.370224953 CEST	8.8.8.8	192.168.2.4	0x956c	No error (0)	ib.anycast.adnxs.com		185.33.220.243	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.370224953 CEST	8.8.8.8	192.168.2.4	0x956c	No error (0)	ib.anycast.adnxs.com		185.33.221.15	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.370224953 CEST	8.8.8.8	192.168.2.4	0x956c	No error (0)	ib.anycast.adnxs.com		185.33.220.240	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.370224953 CEST	8.8.8.8	192.168.2.4	0x956c	No error (0)	ib.anycast.adnxs.com		185.33.221.90	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.382020950 CEST	8.8.8.8	192.168.2.4	0xbe92	No error (0)	pubmatic-match.dotomi.com	afp.dotomi.weighted.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.385018110 CEST	8.8.8.8	192.168.2.4	0xaa64	No error (0)	ads.pubmatic.com	pubmatic.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.386642933 CEST	8.8.8.8	192.168.2.4	0x656b	No error (0)	rtb.adentifi.com		54.236.227.29	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.386642933 CEST	8.8.8.8	192.168.2.4	0x656b	No error (0)	rtb.adentifi.com		52.3.173.52	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.386642933 CEST	8.8.8.8	192.168.2.4	0x656b	No error (0)	rtb.adentifi.com		52.44.116.71	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.386642933 CEST	8.8.8.8	192.168.2.4	0x656b	No error (0)	rtb.adentifi.com		52.202.1.196	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.386642933 CEST	8.8.8.8	192.168.2.4	0x656b	No error (0)	rtb.adentifi.com		52.4.236.19	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.386642933 CEST	8.8.8.8	192.168.2.4	0x656b	No error (0)	rtb.adentifi.com		52.45.16.192	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.386642933 CEST	8.8.8.8	192.168.2.4	0x656b	No error (0)	rtb.adentifi.com		52.45.215.106	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.386642933 CEST	8.8.8.8	192.168.2.4	0x656b	No error (0)	rtb.adentifi.com		52.207.62.93	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.387790918 CEST	8.8.8.8	192.168.2.4	0x4335	No error (0)	image2.pubmatic.com	pug-lhrc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.387790918 CEST	8.8.8.8	192.168.2.4	0x4335	No error (0)	pug-lhrc.pubmatic.com	pug-lhr.pubmatic.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:21:19.387790918 CEST	8.8.8.8	192.168.2.4	0x4335	No error (0)	pug-lhr.pubmatic.com		185.64.190.80	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.400202990 CEST	8.8.8.8	192.168.2.4	0x35f8	No error (0)	sync.ipredictive.com		54.226.209.67	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.400202990 CEST	8.8.8.8	192.168.2.4	0x35f8	No error (0)	sync.ipredictive.com		34.196.50.33	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.400202990 CEST	8.8.8.8	192.168.2.4	0x35f8	No error (0)	sync.ipredictive.com		23.22.239.72	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.400202990 CEST	8.8.8.8	192.168.2.4	0x35f8	No error (0)	sync.ipredictive.com		52.203.60.58	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.400202990 CEST	8.8.8.8	192.168.2.4	0x35f8	No error (0)	sync.ipredictive.com		3.220.196.160	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.400202990 CEST	8.8.8.8	192.168.2.4	0x35f8	No error (0)	sync.ipredictive.com		54.159.94.231	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.400202990 CEST	8.8.8.8	192.168.2.4	0x35f8	No error (0)	sync.ipredictive.com		34.232.92.67	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.400202990 CEST	8.8.8.8	192.168.2.4	0x35f8	No error (0)	sync.ipredictive.com		52.205.83.58	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.413791895 CEST	8.8.8.8	192.168.2.4	0xf36c	No error (0)	pixel-sync.sitescout.com	pixel-a.sitescout.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.413791895 CEST	8.8.8.8	192.168.2.4	0xf36c	No error (0)	pixel-a.sitescout.com		66.155.71.25	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.421084881 CEST	8.8.8.8	192.168.2.4	0xc89	No error (0)	x.bidswitch.net	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.421084881 CEST	8.8.8.8	192.168.2.4	0xc89	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		52.58.102.227	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.421084881 CEST	8.8.8.8	192.168.2.4	0xc89	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		35.156.223.207	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.421084881 CEST	8.8.8.8	192.168.2.4	0xc89	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		35.157.13.124	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.421084881 CEST	8.8.8.8	192.168.2.4	0xc89	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		18.195.177.11	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.421084881 CEST	8.8.8.8	192.168.2.4	0xc89	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		3.124.46.162	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.421084881 CEST	8.8.8.8	192.168.2.4	0xc89	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		35.156.19.236	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.421084881 CEST	8.8.8.8	192.168.2.4	0xc89	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		3.120.242.149	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.421084881 CEST	8.8.8.8	192.168.2.4	0xc89	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		52.58.182.33	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.431078911 CEST	8.8.8.8	192.168.2.4	0x6519	No error (0)	pmp.mxptint.net		204.2.255.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:21:19.431106091 CEST	8.8.8.8	192.168.2.4	0xbf13	No error (0)	image4.pubmatic.com	spug22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.431106091 CEST	8.8.8.8	192.168.2.4	0xbf13	No error (0)	spug22000nfc.pubmatic.com	spug22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.431106091 CEST	8.8.8.8	192.168.2.4	0xbf13	No error (0)	spug22000nf.pubmatic.com		185.64.189.114	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.437066078 CEST	8.8.8.8	192.168.2.4	0x9507	No error (0)	aud.pubmatic.com	avi-aud-k8s-ams.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.437066078 CEST	8.8.8.8	192.168.2.4	0x9507	No error (0)	avi-aud-k8s-ams.pubmatic.com		185.64.189.249	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.441680908 CEST	8.8.8.8	192.168.2.4	0xd3ba	No error (0)	simage2.pubmatic.com	pug-lhrc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.441680908 CEST	8.8.8.8	192.168.2.4	0xd3ba	No error (0)	pug-lhrc.pubmatic.com	pug-lhr.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.441680908 CEST	8.8.8.8	192.168.2.4	0xd3ba	No error (0)	pug-lhr.pubmatic.com		185.64.190.80	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.454787970 CEST	8.8.8.8	192.168.2.4	0x7ff6	No error (0)	pixel.quantserve.com	global.px.quantserve.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.454787970 CEST	8.8.8.8	192.168.2.4	0x7ff6	No error (0)	global.px.quantserve.com		91.228.74.226	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.454787970 CEST	8.8.8.8	192.168.2.4	0x7ff6	No error (0)	global.px.quantserve.com		91.228.74.134	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.454787970 CEST	8.8.8.8	192.168.2.4	0x7ff6	No error (0)	global.px.quantserve.com		91.228.74.189	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.454787970 CEST	8.8.8.8	192.168.2.4	0x7ff6	No error (0)	global.px.quantserve.com		91.228.74.198	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.454787970 CEST	8.8.8.8	192.168.2.4	0x7ff6	No error (0)	global.px.quantserve.com		91.228.74.133	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.593389034 CEST	8.8.8.8	192.168.2.4	0x567b	No error (0)	a.volvelle.tech	pool.optomaton.iponweb.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.593389034 CEST	8.8.8.8	192.168.2.4	0x567b	No error (0)	pool.optomaton.iponweb.net	optomaton.geo.iponweb.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:19.593389034 CEST	8.8.8.8	192.168.2.4	0x567b	No error (0)	optomaton.geo.iponweb.net		35.210.178.101	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.659168959 CEST	8.8.8.8	192.168.2.4	0xdd7d	No error (0)	sync.crwdcntrl.net		52.48.248.240	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.659168959 CEST	8.8.8.8	192.168.2.4	0xdd7d	No error (0)	sync.crwdcntrl.net		34.251.130.56	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.659168959 CEST	8.8.8.8	192.168.2.4	0xdd7d	No error (0)	sync.crwdcntrl.net		52.208.103.128	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.659168959 CEST	8.8.8.8	192.168.2.4	0xdd7d	No error (0)	sync.crwdcntrl.net		52.48.137.92	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.659168959 CEST	8.8.8.8	192.168.2.4	0xdd7d	No error (0)	sync.crwdcntrl.net		52.30.140.199	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.659168959 CEST	8.8.8.8	192.168.2.4	0xdd7d	No error (0)	sync.crwdcntrl.net		34.253.111.115	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.659168959 CEST	8.8.8.8	192.168.2.4	0xdd7d	No error (0)	sync.crwdcntrl.net		54.194.226.253	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.659168959 CEST	8.8.8.8	192.168.2.4	0xdd7d	No error (0)	sync.crwdcntrl.net		52.30.14.23	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.931649923 CEST	8.8.8.8	192.168.2.4	0xc8ad	No error (0)	spl.zeotap.com		104.22.25.87	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:21:19.931649923 CEST	8.8.8.8	192.168.2.4	0xc8ad	No error (0)	spl.zeotap.com		172.67.13.182	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:19.931649923 CEST	8.8.8.8	192.168.2.4	0xc8ad	No error (0)	spl.zeotap.com		104.22.24.87	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.077377081 CEST	8.8.8.8	192.168.2.4	0xd1ef	No error (0)	pm.w55c.net	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:20.077377081 CEST	8.8.8.8	192.168.2.4	0xd1ef	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		3.124.143.99	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.077377081 CEST	8.8.8.8	192.168.2.4	0xd1ef	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		18.193.131.224	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.077377081 CEST	8.8.8.8	192.168.2.4	0xd1ef	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		3.123.143.157	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.077377081 CEST	8.8.8.8	192.168.2.4	0xd1ef	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		3.125.99.7	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.077377081 CEST	8.8.8.8	192.168.2.4	0xd1ef	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		18.159.182.76	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.077377081 CEST	8.8.8.8	192.168.2.4	0xd1ef	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		3.127.92.82	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.077377081 CEST	8.8.8.8	192.168.2.4	0xd1ef	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		18.158.226.176	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.077377081 CEST	8.8.8.8	192.168.2.4	0xd1ef	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		52.57.110.162	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.079544067 CEST	8.8.8.8	192.168.2.4	0x1073	No error (0)	mwzeom.zeotap.com		104.22.24.87	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.079544067 CEST	8.8.8.8	192.168.2.4	0x1073	No error (0)	mwzeom.zeotap.com		172.67.13.182	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.079544067 CEST	8.8.8.8	192.168.2.4	0x1073	No error (0)	mwzeom.zeotap.com		104.22.25.87	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.111022949 CEST	8.8.8.8	192.168.2.4	0xc7bc	No error (0)	match.prod.bidr.io		34.252.144.15	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.111022949 CEST	8.8.8.8	192.168.2.4	0xc7bc	No error (0)	match.prod.bidr.io		52.16.214.249	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.111022949 CEST	8.8.8.8	192.168.2.4	0xc7bc	No error (0)	match.prod.bidr.io		52.30.222.33	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.111022949 CEST	8.8.8.8	192.168.2.4	0xc7bc	No error (0)	match.prod.bidr.io		52.17.245.120	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.111022949 CEST	8.8.8.8	192.168.2.4	0xc7bc	No error (0)	match.prod.bidr.io		52.49.238.187	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.111022949 CEST	8.8.8.8	192.168.2.4	0xc7bc	No error (0)	match.prod.bidr.io		34.247.100.44	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.111022949 CEST	8.8.8.8	192.168.2.4	0xc7bc	No error (0)	match.prod.bidr.io		52.30.92.119	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:21:20.111022949 CEST	8.8.8.8	192.168.2.4	0xc7bc	No error (0)	match.prod.bidr.io		54.246.13.173	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.154824972 CEST	8.8.8.8	192.168.2.4	0x3013	No error (0)	inv-nets.admixer.net	inv-nets-eu-s2.admixer.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:20.154824972 CEST	8.8.8.8	192.168.2.4	0x3013	No error (0)	inv-nets-eu-s2.admixer.net		146.0.227.109	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.173825026 CEST	8.8.8.8	192.168.2.4	0xde7e	No error (0)	eu-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.173825026 CEST	8.8.8.8	192.168.2.4	0xde7e	No error (0)	eu-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.196842909 CEST	8.8.8.8	192.168.2.4	0x1278	No error (0)	c1.adform.net	track.adformnet.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:20.217803955 CEST	8.8.8.8	192.168.2.4	0x3e3f	No error (0)	analytics.twitter.com	ads.twitter.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:20.217803955 CEST	8.8.8.8	192.168.2.4	0x3e3f	No error (0)	ads.twitter.com	s.twitter.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:20.217803955 CEST	8.8.8.8	192.168.2.4	0x3e3f	No error (0)	s.twitter.com		104.244.42.195	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.217803955 CEST	8.8.8.8	192.168.2.4	0x3e3f	No error (0)	s.twitter.com		104.244.42.3	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.217803955 CEST	8.8.8.8	192.168.2.4	0x3e3f	No error (0)	s.twitter.com		104.244.42.67	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.217803955 CEST	8.8.8.8	192.168.2.4	0x3e3f	No error (0)	s.twitter.com		104.244.42.131	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.256472111 CEST	8.8.8.8	192.168.2.4	0xc89	No error (0)	gum.criteo.com	gum.am5.vip.prod.criteo.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:20.256472111 CEST	8.8.8.8	192.168.2.4	0xc89	No error (0)	gum.am5.vip.prod.criteo.com		178.250.2.146	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.279273987 CEST	8.8.8.8	192.168.2.4	0x6c14	No error (0)	us-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.279273987 CEST	8.8.8.8	192.168.2.4	0x6c14	No error (0)	us-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.559398890 CEST	8.8.8.8	192.168.2.4	0x600b	No error (0)	rtb-csync.smartadserver.com	2-01-275d-002d.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:20.559398890 CEST	8.8.8.8	192.168.2.4	0x600b	No error (0)	rtb-csync-itx4.smartadserver.com		185.86.139.89	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.559398890 CEST	8.8.8.8	192.168.2.4	0x600b	No error (0)	rtb-csync-itx4.smartadserver.com		185.86.139.115	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.559398890 CEST	8.8.8.8	192.168.2.4	0x600b	No error (0)	rtb-csync-itx4.smartadserver.com		185.86.139.113	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.559398890 CEST	8.8.8.8	192.168.2.4	0x600b	No error (0)	rtb-csync-itx4.smartadserver.com		185.86.139.114	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.691595078 CEST	8.8.8.8	192.168.2.4	0x6487	No error (0)	adc.auone.jp		54.95.129.54	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.691595078 CEST	8.8.8.8	192.168.2.4	0x6487	No error (0)	adc.auone.jp		54.250.78.86	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.691595078 CEST	8.8.8.8	192.168.2.4	0x6487	No error (0)	adc.auone.jp		54.92.38.20	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.768696070 CEST	8.8.8.8	192.168.2.4	0x4a37	No error (0)	bh.contextweb.com	lga-bh.contextweb.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:20.768696070 CEST	8.8.8.8	192.168.2.4	0x4a37	No error (0)	lga-bh.contextweb.com	lga-bh-bgp.contextweb.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:21:20.768696070 CEST	8.8.8.8	192.168.2.4	0x4a37	No error (0)	lga-bh-bgp .contextweb.com		198.148.27.140	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:20.768696070 CEST	8.8.8.8	192.168.2.4	0x4a37	No error (0)	lga-bh-bgp .contextweb.com		198.148.27.139	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.891242027 CEST	8.8.8.8	192.168.2.4	0x8ee6	No error (0)	pixel.onau dience.com		51.210.112.63	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.891242027 CEST	8.8.8.8	192.168.2.4	0x8ee6	No error (0)	pixel.onau dience.com		146.59.148.16	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.891242027 CEST	8.8.8.8	192.168.2.4	0x8ee6	No error (0)	pixel.onau dience.com		51.79.83.225	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.891242027 CEST	8.8.8.8	192.168.2.4	0x8ee6	No error (0)	pixel.onau dience.com		51.210.112.236	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.891242027 CEST	8.8.8.8	192.168.2.4	0x8ee6	No error (0)	pixel.onau dience.com		51.222.80.231	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.899609089 CEST	8.8.8.8	192.168.2.4	0x91ae	No error (0)	aa.agkn.com	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:21.899609089 CEST	8.8.8.8	192.168.2.4	0x91ae	No error (0)	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		3.10.35.49	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.899609089 CEST	8.8.8.8	192.168.2.4	0x91ae	No error (0)	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		3.11.29.5	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.899609089 CEST	8.8.8.8	192.168.2.4	0x91ae	No error (0)	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		3.8.243.222	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.899609089 CEST	8.8.8.8	192.168.2.4	0x91ae	No error (0)	aa-agkn-com-https-1893222849.eu-west-2.elb.amazonaws.com		35.176.232.241	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.900484085 CEST	8.8.8.8	192.168.2.4	0x1af3	No error (0)	visitor.fiftyt.com		35.201.96.126	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.904989004 CEST	8.8.8.8	192.168.2.4	0xf352	No error (0)	io.narrative.io		52.215.52.168	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.904989004 CEST	8.8.8.8	192.168.2.4	0xf352	No error (0)	io.narrative.io		52.212.225.58	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.913180113 CEST	8.8.8.8	192.168.2.4	0xd4bc	No error (0)	rtb.gumgum.com		54.77.47.243	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.913180113 CEST	8.8.8.8	192.168.2.4	0xd4bc	No error (0)	rtb.gumgum.com		52.48.175.241	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.913180113 CEST	8.8.8.8	192.168.2.4	0xd4bc	No error (0)	rtb.gumgum.com		34.251.173.19	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.913180113 CEST	8.8.8.8	192.168.2.4	0xd4bc	No error (0)	rtb.gumgum.com		52.208.41.69	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.913180113 CEST	8.8.8.8	192.168.2.4	0xd4bc	No error (0)	rtb.gumgum.com		54.77.19.59	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.913180113 CEST	8.8.8.8	192.168.2.4	0xd4bc	No error (0)	rtb.gumgum.com		52.50.187.150	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:21.913180113 CEST	8.8.8.8	192.168.2.4	0xd4bc	No error (0)	rtb.gumgum.com		54.247.114.64	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:21:21.913180113 CEST	8.8.8.8	192.168.2.4	0xd4bc	No error (0)	rtb.gumgum.com		54.194.104.251	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:22.036192894 CEST	8.8.8.8	192.168.2.4	0x409a	No error (0)	spl.zeotap.com		104.22.25.87	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:22.036192894 CEST	8.8.8.8	192.168.2.4	0x409a	No error (0)	spl.zeotap.com		172.67.13.182	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:22.036192894 CEST	8.8.8.8	192.168.2.4	0x409a	No error (0)	spl.zeotap.com		104.22.24.87	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:22.039206982 CEST	8.8.8.8	192.168.2.4	0xf006	No error (0)	aud.pubmatic.com	avi-aud-k8s-ams.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:22.039206982 CEST	8.8.8.8	192.168.2.4	0xf006	No error (0)	avi-aud-k8s-ams.pubmatic.com		185.64.189.249	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:22.171634912 CEST	8.8.8.8	192.168.2.4	0x4da8	No error (0)	mwzeom.zeotap.com		104.22.24.87	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:22.171634912 CEST	8.8.8.8	192.168.2.4	0x4da8	No error (0)	mwzeom.zeotap.com		172.67.13.182	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:22.171634912 CEST	8.8.8.8	192.168.2.4	0x4da8	No error (0)	mwzeom.zeotap.com		104.22.25.87	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:31.560791969 CEST	8.8.8.8	192.168.2.4	0x2e56	No error (0)	www.ja-ces.or.jp	mail.ja-ces.or.jp		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:31.560791969 CEST	8.8.8.8	192.168.2.4	0x2e56	No error (0)	mail.ja-ces.or.jp		164.46.34.110	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:35.746838093 CEST	8.8.8.8	192.168.2.4	0xdebb	No error (0)	cdn.jsdelivr.net	cdn.jsdelivr.net.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:35.753882885 CEST	8.8.8.8	192.168.2.4	0x2a2a	No error (0)	s.w.org		192.0.77.48	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:35.753932953 CEST	8.8.8.8	192.168.2.4	0x58de	No error (0)	oss.maxcdn.com	osscdn.netdnasa9.netdna-cdn.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:35.753932953 CEST	8.8.8.8	192.168.2.4	0x58de	No error (0)	osscdn.netdnasa9.netdna-cdn.com		23.111.8.154	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:41.140650988 CEST	8.8.8.8	192.168.2.4	0xd77d	No error (0)	www.ja-ces.or.jp	mail.ja-ces.or.jp		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:41.140650988 CEST	8.8.8.8	192.168.2.4	0xd77d	No error (0)	mail.ja-ces.or.jp		164.46.34.110	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:41.332529068 CEST	8.8.8.8	192.168.2.4	0x310	No error (0)	www.mhlw.go.jp	www.mhlw.go.jp.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:41.712474108 CEST	8.8.8.8	192.168.2.4	0x501f	No error (0)	ewb-c.infocreate.co.jp	ifccloud6.infocreate.co.jp		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:41.712474108 CEST	8.8.8.8	192.168.2.4	0x501f	No error (0)	ifccloud6.infocreate.co.jp		169.56.3.74	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:44.931010008 CEST	8.8.8.8	192.168.2.4	0x193f	No error (0)	www.mhlw.go.jp	www.mhlw.go.jp.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:46.547259092 CEST	8.8.8.8	192.168.2.4	0x12a5	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:54.765932083 CEST	8.8.8.8	192.168.2.4	0xb799	No error (0)	sync.srv.stackadapt.com		54.81.207.173	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:54.765932083 CEST	8.8.8.8	192.168.2.4	0xb799	No error (0)	sync.srv.stackadapt.com		54.175.198.118	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:54.765932083 CEST	8.8.8.8	192.168.2.4	0xb799	No error (0)	sync.srv.stackadapt.com		34.204.22.100	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:54.765932083 CEST	8.8.8.8	192.168.2.4	0xb799	No error (0)	sync.srv.stackadapt.com		34.204.19.158	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:21:54.765932083 CEST	8.8.8.8	192.168.2.4	0xb799	No error (0)	sync.srv.stackadapt.com		54.87.192.123	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:54.765932083 CEST	8.8.8.8	192.168.2.4	0xb799	No error (0)	sync.srv.stackadapt.com		3.228.133.61	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:54.765932083 CEST	8.8.8.8	192.168.2.4	0xb799	No error (0)	sync.srv.stackadapt.com		34.205.3.24	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:54.765932083 CEST	8.8.8.8	192.168.2.4	0xb799	No error (0)	sync.srv.stackadapt.com		52.44.53.247	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:54.830615997 CEST	8.8.8.8	192.168.2.4	0x46af	No error (0)	ums.acuityplatform.com		154.59.122.79	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:55.047889948 CEST	8.8.8.8	192.168.2.4	0xad1	No error (0)	trc.taboola.com	dualstack.tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:55.047889948 CEST	8.8.8.8	192.168.2.4	0xad1	No error (0)	dualstack.tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:55.047889948 CEST	8.8.8.8	192.168.2.4	0xad1	No error (0)	dualstack.tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:55.047889948 CEST	8.8.8.8	192.168.2.4	0xad1	No error (0)	dualstack.tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:55.047889948 CEST	8.8.8.8	192.168.2.4	0xad1	No error (0)	dualstack.tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:55.054044962 CEST	8.8.8.8	192.168.2.4	0x80d4	No error (0)	sync.resetdigital.co		45.35.192.162	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:55.201464891 CEST	8.8.8.8	192.168.2.4	0xc69e	No error (0)	match.taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:21:55.201464891 CEST	8.8.8.8	192.168.2.4	0xc69e	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:55.201464891 CEST	8.8.8.8	192.168.2.4	0xc69e	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:55.201464891 CEST	8.8.8.8	192.168.2.4	0xc69e	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Jul 15, 2021 09:21:55.201464891 CEST	8.8.8.8	192.168.2.4	0xc69e	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)
Jul 15, 2021 09:22:25.702260971 CEST	8.8.8.8	192.168.2.4	0x3199	No error (0)	gocm.c.appier.net	cm119.appier.org		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:22:25.702260971 CEST	8.8.8.8	192.168.2.4	0x3199	No error (0)	cm119.appier.org		172.105.220.23	A (IP address)	IN (0x0001)
Jul 15, 2021 09:22:25.809582949 CEST	8.8.8.8	192.168.2.4	0xa623	No error (0)	jadserve.postrelease.com	jadserve.postrelease.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:22:25.837219954 CEST	8.8.8.8	192.168.2.4	0xc1f2	No error (0)	csync.loopme.me	generic-2.lb.lm5v.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:22:25.837219954 CEST	8.8.8.8	192.168.2.4	0xc1f2	No error (0)	generic-2.lb.lm5v.com		162.55.6.212	A (IP address)	IN (0x0001)
Jul 15, 2021 09:22:25.837219954 CEST	8.8.8.8	192.168.2.4	0xc1f2	No error (0)	generic-2.lb.lm5v.com		162.55.6.213	A (IP address)	IN (0x0001)
Jul 15, 2021 09:22:25.837219954 CEST	8.8.8.8	192.168.2.4	0xc1f2	No error (0)	generic-2.lb.lm5v.com		162.55.6.211	A (IP address)	IN (0x0001)
Jul 15, 2021 09:22:25.837219954 CEST	8.8.8.8	192.168.2.4	0xc1f2	No error (0)	generic-2.lb.lm5v.com		162.55.6.210	A (IP address)	IN (0x0001)
Jul 15, 2021 09:22:25.872947931 CEST	8.8.8.8	192.168.2.4	0x8e4a	No error (0)	ads.playground.xyz		34.98.107.212	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 15, 2021 09:22:25.917205095 CEST	8.8.8.8	192.168.2.4	0x9232	No error (0)	pixel.tapad.com		35.227.248.159	A (IP address)	IN (0x0001)
Jul 15, 2021 09:22:26.030664921 CEST	8.8.8.8	192.168.2.4	0x32b	No error (0)	secure.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:22:26.030664921 CEST	8.8.8.8	192.168.2.4	0x32b	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Jul 15, 2021 09:22:26.030664921 CEST	8.8.8.8	192.168.2.4	0x32b	No error (0)	ib.anycast.adnxs.com		37.252.173.38	A (IP address)	IN (0x0001)
Jul 15, 2021 09:22:26.030664921 CEST	8.8.8.8	192.168.2.4	0x32b	No error (0)	ib.anycast.adnxs.com		37.252.172.249	A (IP address)	IN (0x0001)
Jul 15, 2021 09:22:26.030664921 CEST	8.8.8.8	192.168.2.4	0x32b	No error (0)	ib.anycast.adnxs.com		37.252.172.37	A (IP address)	IN (0x0001)
Jul 15, 2021 09:22:26.030664921 CEST	8.8.8.8	192.168.2.4	0x32b	No error (0)	ib.anycast.adnxs.com		37.252.172.36	A (IP address)	IN (0x0001)
Jul 15, 2021 09:22:26.030664921 CEST	8.8.8.8	192.168.2.4	0x32b	No error (0)	ib.anycast.adnxs.com		37.252.172.38	A (IP address)	IN (0x0001)
Jul 15, 2021 09:22:26.030664921 CEST	8.8.8.8	192.168.2.4	0x32b	No error (0)	ib.anycast.adnxs.com		37.252.172.45	A (IP address)	IN (0x0001)
Jul 15, 2021 09:22:26.030664921 CEST	8.8.8.8	192.168.2.4	0x32b	No error (0)	ib.anycast.adnxs.com		37.252.172.250	A (IP address)	IN (0x0001)
Jul 15, 2021 09:22:26.030664921 CEST	8.8.8.8	192.168.2.4	0x32b	No error (0)	ib.anycast.adnxs.com		37.252.173.22	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- repository.secomtrust.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49918	61.114.177.151	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Jul 15, 2021 09:21:06.846488953 CEST	8446	OUT	GET /SC-Root2/SCRoot2ca.cer HTTP/1.1 Connection: Keep-Alive Accept: */* User-Agent: Microsoft-CryptoAPI/10.0 Host: repository.secomtrust.net

Timestamp	kBytes transferred	Direction	Data
Jul 15, 2021 09:21:07.075617075 CEST	8481	IN	HTTP/1.1 200 OK Date: Thu, 15 Jul 2021 07:21:06 GMT Server: Apache Last-Modified: Thu, 04 Jun 2009 08:43:57 GMT ETag: "30001d-37b-46b81c6cb2d40" Accept-Ranges: bytes Content-Length: 891 Connection: close Content-Type: application/pkix-cert Data Raw: 30 82 03 77 30 82 02 5f a0 03 02 01 02 02 01 00 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00 30 5d 31 0b 30 09 06 03 55 04 06 13 02 4a 50 31 25 30 23 06 03 55 04 0a 13 1c 53 45 43 4f 4d 20 54 72 75 73 74 20 53 79 73 74 65 6d 73 20 43 4f 2e 2c 4c 54 44 2e 31 27 30 25 06 03 55 04 0b 13 1e 53 65 63 75 72 69 74 79 20 43 6f 6d 6d 75 6e 69 63 61 74 69 6f 6e 20 52 6f 6f 74 43 41 32 30 1e 17 0d 30 39 30 35 32 39 30 35 30 30 33 39 5a 17 0d 32 39 30 35 32 39 30 35 30 30 33 39 5a 30 5d 31 0b 30 09 06 03 55 04 06 13 02 4a 50 31 25 30 23 06 03 55 04 0a 13 1c 53 45 43 4f 4d 20 54 72 75 73 74 20 53 79 73 74 65 6d 73 20 43 4f 2e 2c 4c 54 44 2e 31 27 30 25 06 03 55 04 0b 13 1e 53 65 63 75 72 69 74 79 20 43 6f 6d 6d 75 6e 69 63 61 74 69 6f 6e 20 52 6f 6f 74 43 41 32 30 82 01 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01 00 d0 15 39 52 b1 52 b3 ba c5 59 82 c4 5d 52 ae 3a 43 65 80 4b c7 f2 96 bc db 36 97 d6 a6 64 8c a8 5e f0 e3 0a 1c f7 df 97 3d 4b ae f6 5d ec 21 b5 41 ab cd b9 7e 76 9f be f9 3e 36 34 a0 3b c1 f6 31 11 45 74 93 3d 57 80 c5 f9 89 99 ca e5 ab 6a d4 b5 da 41 90 10 c1 d6 d6 42 89 c2 bf f4 38 12 95 4c 54 05 f7 36 e4 45 83 7b 14 65 d6 dc 0c 4d d1 de 7e 0c ab 3b c4 15 be 3a 56 a6 5a 6f 76 69 52 a9 7a b9 c8 eb 6a 9a 5d 52 d0 2d 0a 6b 35 16 09 10 84 d0 6a ca 3a 06 00 37 47 e4 7e 57 4f 3f 8b eb 67 b8 88 aa c5 be 53 55 b2 91 c4 7d b9 b0 85 19 06 78 2e db 61 1a fa 85 f5 4a 91 a1 e7 16 d5 8e a2 39 df 94 b8 70 1f 28 3f 8b fc 40 5e 63 83 3c 83 2a 1a 99 6b cf de 59 6a 3b fc 6f 16 d7 1f fd 4a 10 eb 4e 82 16 3a ac 27 0c 53 f1 ad d5 24 b0 6b 03 50 c1 2d 3c 16 dd 44 34 27 1a 75 fb 02 03 01 00 01 a3 42 30 40 30 1d 06 03 55 1d 0e 04 16 04 14 0a 85 a9 77 65 05 98 7c 40 81 f8 0f 97 2c 38 f1 0a ec 3c cf 30 0e 06 03 55 1d 0f 01 01 ff 04 04 03 02 01 06 30 0f 06 03 55 1d 13 01 01 ff 04 05 30 03 01 01 ff 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00 03 82 01 01 00 4c 3a a3 44 ac b9 45 b1 c7 93 7e c8 0b 0a 42 df 64 ea 1c ee 59 6c 08 ba 89 5f 6a ca 4a 95 9e 7a 8f 07 c5 da 45 72 82 71 0e 3a d2 cc 6f a7 b4 a1 23 bb f6 24 9f cb 17 fe 8c a6 ce c2 d2 db cc 8d fc 71 fc 03 29 c1 6c 5d 33 5f 64 b6 65 3b 89 6f 18 76 78 f5 dc a2 48 1f 19 3f 8e 93 eb f1 fa 17 ee cd 4e e3 04 12 55 d6 e5 e4 dd fb 3e 05 7c e2 1d 5e c6 a7 bc 97 4f 68 3a f5 e9 2e 0a 43 b6 af 57 5c 62 68 7c b7 fd a3 8a 84 a0 ac 62 be 2b 09 87 34 f0 6a 01 bb 9b 29 56 3c fe 00 37 cf 23 6c f1 4e aa b6 74 46 12 6c 91 ee 34 d5 ec 9a 91 e7 44 be 90 31 72 d5 49 02 f6 02 e5 f4 1f eb 7c d9 96 55 a9 ff ec 8a f9 99 47 ff 35 5a 02 aa 04 cb 8a 5b 87 71 29 91 bd a4 b4 7a 0d bd 9a f5 57 23 00 07 21 17 3f 4a 39 d1 05 49 0b a7 b6 37 81 a5 5d 8c aa 33 5e 81 28 7c a7 7d 27 eb 00 ae 8d 37 Data Ascii: 0w0_0*H0]10UJP1%0#USECOM Trust Systems CO.,LTD.1'0%USecurity Communication RootCA2009052 9050039Z290529050039Z0]10UJP1%0#USECOM Trust Systems CO.,LTD.1'0%USecurity Communication RootCA20"0* H09RRY]R:CeK6d^=K]!A~v>64;1Et=WjAB8LT6E{eM~;:VZoviRzj]R-k5j:7G~WO?gSU}x.aJ9p(?@^c<*kYj;oJN:'S$kP-<D4 'uB0@0Uwe\|@,8<0U0U00*HL:DE~BdYl_jJzErq:o#$q)l]3_de;ovxH?NU>|^Oh:.CW\bh|b+4j)V<7#lNtFl4D1rl|UG5Z[q)zW#!? J9I7]3^(|}'7

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 15, 2021 09:20:46.647386074 CEST	104.244.42.200	443	192.168.2.4	49757	CN=syndication.twitter.com, O="Twitter, 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	Fri Feb 05 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Feb 05 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=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 15, 2021 09:20:49.079498053 CEST	185.199.109.153	443	192.168.2.4	49782	CN=www.stopcovid19.jp CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Jul 12 17:05:52 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sun Oct 10 17:05:51 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	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=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 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
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Jul 15, 2021 09:20:49.079710960 CEST	185.199.109.153	443	192.168.2.4	49781	CN=www.stopcovid19.jp CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Jul 12 17:05:52 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sun Oct 10 17:05:51 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	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=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Jul 15, 2021 09:20:54.678373098 CEST	157.240.196.15	443	192.168.2.4	49809	CN=*.facebook.com, O="Facebook, Inc.", L=Menlo Park, 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	Wed May 26 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Wed Aug 25 01:59:59 CEST 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		
Jul 15, 2021 09:21:03.721019983 CEST	199.232.136.157	443	192.168.2.4	49847	CN=ads-twitter.com, OU=Twitter Security, O="Twitter, Inc.", L=San Francisco, 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	Fri Aug 14 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Thu Aug 19 14:00:00 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=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 15, 2021 09:21:03.800625086 CEST	18.182.163.232	443	192.168.2.4	49840	CN=s.hatena.ne.jp 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	Thu Jan 07 01:00:00 CET 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	Sun Feb 06 00:59:59 CET 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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 15, 2021 09:21:03.802815914 CEST	18.182.163.232	443	192.168.2.4	49843	CN=s.hatena.ne.jp 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	Thu Jan 07 01:00:00 CET 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	Sun Feb 06 00:59:59 CET 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 15, 2021 09:21:03.802980900 CEST	18.182.163.232	443	192.168.2.4	49842	CN=s.hatena.ne.jp 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	Thu Jan 07 01:00:00 CET 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	Sun Feb 06 00:59:59 CET 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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 15, 2021 09:21:03.804582119 CEST	18.182.163.232	443	192.168.2.4	49841	CN=s.hatena.ne.jp 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	Thu Jan 07 01:00:00 CET 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	Sun Feb 06 00:59:59 CET 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 15, 2021 09:21:04.024648905 CEST	18.182.163.232	443	192.168.2.4	49846	CN=s.hatena.ne.jp 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	Thu Jan 07 01:00:00 CET 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	Sun Feb 06 00:59:59 CET 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 15, 2021 09:21:04.169483900 CEST	37.252.172.249	443	192.168.2.4	49852	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 15, 2021 09:21:04.202135086 CEST	185.64.189.112	443	192.168.2.4	49869	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 15, 2021 09:21:04.419382095 CEST	104.244.42.5	443	192.168.2.4	49891	CN=t.co, O="Twitter, 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	Fri Feb 05 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Feb 05 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=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 15, 2021 09:21:04.527925014 CEST	52.95.124.170	443	192.168.2.4	49896	CN=aax-eu.amazon-adsystem.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	Fri Apr 09 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	Mon Mar 21 00:59:59 CET 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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 15, 2021 09:21:04.590226889 CEST	54.95.166.26	443	192.168.2.4	49858	CN=*.ladsp.com, O=SMN Corporation, OU=Technology & Development Dept., L=Shinagawa-ku, ST=Tokyo, C=JP CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri May 07 08:32:26 CEST 2021 Wed Nov 21 01:00:00 CET 2018	Wed Jun 08 08:32:26 CEST 2022 Tue Nov 21 01:00:00 CET 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=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
Jul 15, 2021 09:21:04.592050076 CEST	54.95.166.26	443	192.168.2.4	49856	CN=*.ladsp.com, O=SMN Corporation, OU=Technology & Development Dept., L=Shinagawa-ku, ST=Tokyo, C=JP CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri May 07 08:32:26 CEST 2021 Wed Nov 21 01:00:00 CET 2018	Wed Jun 08 08:32:26 CEST 2022 Tue Nov 21 01:00:00 CET 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=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
Jul 15, 2021 09:21:04.592526913 CEST	54.95.166.26	443	192.168.2.4	49854	CN=*.ladsp.com, O=SMN Corporation, OU=Technology & Development Dept., L=Shinagawa-ku, ST=Tokyo, C=JP CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri May 07 08:32:26 CEST 2021 Wed Nov 21 01:00:00 CET 2018	Wed Jun 08 08:32:26 CEST 2022 Tue Nov 21 01:00:00 CET 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=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
Jul 15, 2021 09:21:04.592936039 CEST	54.95.166.26	443	192.168.2.4	49857	CN=*.ladsp.com, O=SMN Corporation, OU=Technology & Development Dept., L=Shinagawa-ku, ST=Tokyo, C=JP CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri May 07 08:32:26 CEST 2021 Wed Nov 21 01:00:00 CET 2018	Wed Jun 08 08:32:26 CEST 2022 Tue Nov 21 01:00:00 CET 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=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
Jul 15, 2021 09:21:04.600625038 CEST	54.95.166.26	443	192.168.2.4	49855	CN=*.ladsp.com, O=SMN Corporation, OU=Technology & Development Dept., L=Shinagawa-ku, ST=Tokyo, C=JP CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri May 07 08:32:26 CEST 2021 Wed Nov 21 01:00:00 CET 2018	Wed Jun 08 08:32:26 CEST 2022 Tue Nov 21 01:00:00 CET 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
Jul 15, 2021 09:21:04.618340015 CEST	35.213.109.249	443	192.168.2.4	49872	CN=y.one.impact-ad.jp CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 17 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Mon Mar 21 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jul 15, 2021 09:21:04.618434906 CEST	35.213.109.249	443	192.168.2.4	49873	CN=y.one.impact-ad.jp CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 17 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Mon Mar 21 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jul 15, 2021 09:21:04.622035027 CEST	35.213.109.249	443	192.168.2.4	49871	CN=y.one.impact-ad.jp CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 17 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Mon Mar 21 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 15, 2021 09:21:04.623213053 CEST	35.213.109.249	443	192.168.2.4	49875	CN=y.one.impact-ad.jp CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 17 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Mon Mar 21 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jul 15, 2021 09:21:04.625262022 CEST	202.241.208.56	443	192.168.2.4	49868	CN=*.socdm.com, O=Supership inc., OU=AdPlatform Dev, L=Minato-ku, ST=Tokyo, C=JP CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri Apr 24 08:02:02 CEST 2020 Wed Nov 21 01:00:00 CET 2018	Thu Jun 02 10:59:24 CEST 2022 Tue Nov 21 01:00:00 CET 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=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
Jul 15, 2021 09:21:04.625382900 CEST	202.241.208.56	443	192.168.2.4	49865	CN=*.socdm.com, O=Supership inc., OU=AdPlatform Dev, L=Minato-ku, ST=Tokyo, C=JP CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri Apr 24 08:02:02 CEST 2020 Wed Nov 21 01:00:00 CET 2018	Thu Jun 02 10:59:24 CEST 2022 Tue Nov 21 01:00:00 CET 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=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
Jul 15, 2021 09:21:04.626758099 CEST	202.241.208.56	443	192.168.2.4	49866	CN=*.socdm.com, O=Supership inc., OU=AdPlatform Dev, L=Minato-ku, ST=Tokyo, C=JP CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri Apr 24 08:02:02 CEST 2020 Wed Nov 21 01:00:00 CET 2018	Thu Jun 02 10:59:24 CEST 2022 Tue Nov 21 01:00:00 CET 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=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
Jul 15, 2021 09:21:04.633157015 CEST	202.241.208.56	443	192.168.2.4	49864	CN=*.socdm.com, O=Supership inc., OU=AdPlatform Dev, L=Minato-ku, ST=Tokyo, C=JP CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri Apr 24 08:02:02 CEST 2020 Wed Nov 21 01:00:00 CET 2018	Thu Jun 02 10:59:24 CEST 2022 Tue Nov 21 01:00:00 CET 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
Jul 15, 2021 09:21:04.634377956 CEST	202.241.208.56	443	192.168.2.4	49867	CN=*.socdm.com, O=Supership inc., OU=AdPlatform Dev, L=Minato-ku, ST=Tokyo, C=JP CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri Apr 24 08:02:02 CEST 2020 Wed Nov 21 01:00:00 CET 2018	Thu Jun 02 10:59:24 CEST 2022 Tue Nov 21 01:00:00 CET 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=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
Jul 15, 2021 09:21:04.682601929 CEST	35.213.109.249	443	192.168.2.4	49874	CN=y.one.impact-ad.jp CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 17 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Mon Mar 21 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jul 15, 2021 09:21:04.811213017 CEST	54.95.166.26	443	192.168.2.4	49889	CN=*.ladsp.com, O=SMN Corporation, OU=Technology & Development Dept., L=Shinagawa-ku, ST=Tokyo, C=JP CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri May 07 08:32:26 CEST 2021 Wed Nov 21 01:00:00 CET 2018	Wed Jun 08 08:32:26 CEST 2022 Tue Nov 21 01:00:00 CET 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=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
Jul 15, 2021 09:21:04.846497059 CEST	202.241.208.56	443	192.168.2.4	49890	CN=*.socdm.com, O=Supership inc., OU=AdPlatform Dev, L=Minato-ku, ST=Tokyo, C=JP CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri Apr 24 08:02:02 CEST 2020 Wed Nov 21 01:00:00 CET 2018	Thu Jun 02 10:59:24 CEST 2022 Tue Nov 21 01:00:00 CET 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=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 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 15, 2021 09:21:04.892345905 CEST	35.213.109.249	443	192.168.2.4	49894	CN=y.one.impact-ad.jp CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 17 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Mon Mar 21 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jul 15, 2021 09:21:06.934844017 CEST	124.146.215.52	443	192.168.2.4	49911	CN=*.socdm.com, O=Supership inc., OU=AdPlatform Dev, L=Minato-ku, ST=Tokyo, C=JP CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri Apr 24 08:02:02 CEST 2020 Wed Nov 21 01:00:00 CET 2018	Thu Jun 02 10:59:24 CEST 2022 Tue Nov 21 01:00:00 CET 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=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
Jul 15, 2021 09:21:06.935689926 CEST	124.146.215.52	443	192.168.2.4	49912	CN=*.socdm.com, O=Supership inc., OU=AdPlatform Dev, L=Minato-ku, ST=Tokyo, C=JP CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri Apr 24 08:02:02 CEST 2020 Wed Nov 21 01:00:00 CET 2018	Thu Jun 02 10:59:24 CEST 2022 Tue Nov 21 01:00:00 CET 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=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
Jul 15, 2021 09:21:06.936829090 CEST	124.146.215.52	443	192.168.2.4	49913	CN=*.socdm.com, O=Supership inc., OU=AdPlatform Dev, L=Minato-ku, ST=Tokyo, C=JP CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri Apr 24 08:02:02 CEST 2020 Wed Nov 21 01:00:00 CET 2018	Thu Jun 02 10:59:24 CEST 2022 Tue Nov 21 01:00:00 CET 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=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
Jul 15, 2021 09:21:06.938452959 CEST	124.146.215.52	443	192.168.2.4	49910	CN=*.socdm.com, O=Supership inc., OU=AdPlatform Dev, L=Minato-ku, ST=Tokyo, C=JP CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri Apr 24 08:02:02 CEST 2020 Wed Nov 21 01:00:00 CET 2018	Thu Jun 02 10:59:24 CEST 2022 Tue Nov 21 01:00:00 CET 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
Jul 15, 2021 09:21:07.028341055 CEST	124.146.215.52	443	192.168.2.4	49917	CN=*.socdm.com, O=Supership inc., OU=AdPlatform Dev, L=Minato-ku, ST=Tokyo, C=JP CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri Apr 24 08:02:02 CEST 2020 Wed Nov 21 01:00:00 CET 2018	Thu Jun 02 10:59:24 CEST 2022 Tue Nov 21 01:00:00 CET 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=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
Jul 15, 2021 09:21:07.111609936 CEST	124.146.215.52	443	192.168.2.4	49919	CN=*.socdm.com, O=Supership inc., OU=AdPlatform Dev, L=Minato-ku, ST=Tokyo, C=JP CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Fri Apr 24 08:02:02 CEST 2020 Wed Nov 21 01:00:00 CET 2018	Thu Jun 02 10:59:24 CEST 2022 Tue Nov 21 01:00:00 CET 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=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
Jul 15, 2021 09:21:07.476707935 CEST	143.204.98.89	443	192.168.2.4	49927	CN=*.b.st-hatena.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	Sun Oct 25 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	Thu Nov 25 00:59:59 CET 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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=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 15, 2021 09:21:07.476731062 CEST	143.204.98.89	443	192.168.2.4	49928	CN=*.b.st-hatena.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	Sun Oct 25 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	Thu Nov 25 00:59:59 CET 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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=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 15, 2021 09:21:07.745918036 CEST	13.230.7.5	443	192.168.2.4	49924	CN=*.i-mobile.co.jp CN=JPRS Domain Validation Authority - G4, O="Japan Registry Services Co., Ltd.", C=JP	CN=JPRS Domain Validation Authority - G4, O="Japan Registry Services Co., Ltd.", C=JP OU=Security Communication RootCA2, O="SECOM Trust Systems CO.,LTD.", C=JP	Tue Aug 18 13:29:45 CEST 2020 Wed Jul 22 12:40:53 CEST 2020	Thu Mar 31 16:59:59 CEST 2022 Tue May 29 07:00:39 CEST 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=JPRS Domain Validation Authority - G4, O="Japan Registry Services Co., Ltd.", C=JP	OU=Security Communication RootCA2, O="SECOM Trust Systems CO.,LTD.", C=JP	Wed Jul 22 12:40:53 CEST 2020	Tue May 29 07:00:39 CEST 2029		
Jul 15, 2021 09:21:07.747379065 CEST	13.230.7.5	443	192.168.2.4	49925	CN=*.i-mobile.co.jp CN=JPRS Domain Validation Authority - G4, O="Japan Registry Services Co., Ltd.", C=JP	CN=JPRS Domain Validation Authority - G4, O="Japan Registry Services Co., Ltd.", C=JP OU=Security Communication RootCA2, O="SECOM Trust Systems CO.,LTD.", C=JP	Tue Aug 18 13:29:45 CEST 2020 Wed Jul 22 12:40:53 CEST 2020	Thu Mar 31 16:59:59 CEST 2022 Tue May 29 07:00:39 CEST 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=JPRS Domain Validation Authority - G4, O="Japan Registry Services Co., Ltd.", C=JP	OU=Security Communication RootCA2, O="SECOM Trust Systems CO.,LTD.", C=JP	Wed Jul 22 12:40:53 CEST 2020	Tue May 29 07:00:39 CEST 2029		
Jul 15, 2021 09:21:07.759681940 CEST	13.230.7.5	443	192.168.2.4	49923	CN=*.i-mobile.co.jp CN=JPRS Domain Validation Authority - G4, O="Japan Registry Services Co., Ltd.", C=JP	CN=JPRS Domain Validation Authority - G4, O="Japan Registry Services Co., Ltd.", C=JP OU=Security Communication RootCA2, O="SECOM Trust Systems CO.,LTD.", C=JP	Tue Aug 18 13:29:45 CEST 2020 Wed Jul 22 12:40:53 CEST 2020	Thu Mar 31 16:59:59 CEST 2022 Tue May 29 07:00:39 CEST 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=JPRS Domain Validation Authority - G4, O="Japan Registry Services Co., Ltd.", C=JP	OU=Security Communication RootCA2, O="SECOM Trust Systems CO.,LTD.", C=JP	Wed Jul 22 12:40:53 CEST 2020	Tue May 29 07:00:39 CEST 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 15, 2021 09:21:07.763350964 CEST	13.230.7.5	443	192.168.2.4	49922	CN=*.i-mobile.co.jp CN=JPRS Domain Validation Authority - G4, O="Japan Registry Services Co., Ltd.", C=JP	CN=JPRS Domain Validation Authority - G4, O="Japan Registry Services Co., Ltd.", C=JP OU=Security Communication RootCA2, O="SECOM Trust Systems CO.,LTD.", C=JP	Tue Aug 18 13:29:45 CEST 2020	Thu Mar 31 16:59:59 CEST 2022	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=JPRS Domain Validation Authority - G4, O="Japan Registry Services Co., Ltd.", C=JP	OU=Security Communication RootCA2, O="SECOM Trust Systems CO.,LTD.", C=JP	Wed Jul 22 12:40:53 CEST 2020	Tue May 29 07:00:39 CEST 2029		
Jul 15, 2021 09:21:07.944086075 CEST	13.230.7.5	443	192.168.2.4	49929	CN=*.i-mobile.co.jp CN=JPRS Domain Validation Authority - G4, O="Japan Registry Services Co., Ltd.", C=JP	CN=JPRS Domain Validation Authority - G4, O="Japan Registry Services Co., Ltd.", C=JP OU=Security Communication RootCA2, O="SECOM Trust Systems CO.,LTD.", C=JP	Tue Aug 18 13:29:45 CEST 2020	Thu Mar 31 16:59:59 CEST 2022	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=JPRS Domain Validation Authority - G4, O="Japan Registry Services Co., Ltd.", C=JP	OU=Security Communication RootCA2, O="SECOM Trust Systems CO.,LTD.", C=JP	Wed Jul 22 12:40:53 CEST 2020	Tue May 29 07:00:39 CEST 2029		
Jul 15, 2021 09:21:09.207079887 CEST	185.64.189.115	443	192.168.2.4	49969	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 15, 2021 09:21:09.230756044 CEST	35.213.109.249	443	192.168.2.4	49958	CN=y.one.impact-ad.jp CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 17 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Mon Mar 21 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 15, 2021 09:21:09.383497953 CEST	35.213.109.249	443	192.168.2.4	49966	CN=y.one.impact-ad.jp CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 17 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Mon Mar 21 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jul 15, 2021 09:21:11.825273037 CEST	13.248.242.197	443	192.168.2.4	49980	CN=*.adsrvr.org CN=GlobalSign GCC R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	CN=GlobalSign GCC R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3 CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Thu Mar 18 23:45:32 CET 2021 Tue Jul 28 02:00:00 CEST 2020 Wed Mar 18 11:00:00 CET 2009	Wed Apr 20 00:45:32 CEST 2022 Sun Mar 18 01:00:00 CET 2029 Sun Mar 18 11:00:00 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 GCC 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		
					CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Mar 18 11:00:00 CET 2009	Sun Mar 18 11:00:00 CET 2029		
Jul 15, 2021 09:21:13.813111067 CEST	185.29.132.144	443	192.168.2.4	50031	CN=*.mathtag.com, O="MediaMath, 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	Wed Apr 15 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Fri Apr 22 14:00:00 CEST 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 15, 2021 09:21:13.813239098 CEST	3.124.143.99	443	192.168.2.4	50028	CN=*.w55c.net 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 Aug 26 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	Sun Sep 26 14:00:00 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		
Jul 15, 2021 09:21:13.813324928 CEST	54.93.69.146	443	192.168.2.4	50029	CN=*.bidswitch.net CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Apr 23 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Thu May 05 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jul 15, 2021 09:21:13.842396021 CEST	91.228.74.134	443	192.168.2.4	50034	CN=*.quantserve.com, O=Quantcast Corporation, L=San Francisco, 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	Fri Oct 02 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Thu Oct 07 14:00:00 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=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 15, 2021 09:21:13.881946087 CEST	52.16.214.249	443	192.168.2.4	50033	CN=*.match.prod.bidr.io 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	Fri Feb 26 01:00:00 CET 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	Mon Mar 28 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 15, 2021 09:21:14.640676022 CEST	3.127.51.194	443	192.168.2.4	50050	CN=*.creative-serving.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 23 01:00:00 CET 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Mon Apr 04 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jul 15, 2021 09:21:15.345807076 CEST	169.50.137.190	443	192.168.2.4	50062	CN=*.simpli.fi, OU=IT, O=Simplifi Holdings Inc., L=Fort Worth, ST=Texas, 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 Sep 18 02:00:00 CEST 2019 Fri Mar 08 13:00:00 CET 2013	Sun Dec 12 13:00:00 CET 2021 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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 15, 2021 09:21:15.350725889 CEST	212.82.100.176	443	192.168.2.4	50060	CN=*.ybp.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	Mon Mar 29 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Thu Sep 23 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=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 15, 2021 09:21:15.406389952 CEST	185.64.189.110	443	192.168.2.4	50065	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 15, 2021 09:21:15.561455965 CEST	54.236.227.29	443	192.168.2.4	50064	CN=adentifi.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	Fri Oct 02 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	Tue Nov 02 13:00:00 CET 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 15, 2021 09:21:15.733498096 CEST	52.16.214.249	443	192.168.2.4	50076	CN=*.match.prod.bidr.io 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	Fri Feb 26 01:00:00 CET 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	Mon Mar 28 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 15, 2021 09:21:15.763329983 CEST	66.155.71.25	443	192.168.2.4	50079	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 15, 2021 09:21:15.877739906 CEST	34.232.92.67	443	192.168.2.4	50077	CN=*.ipredictive.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	Thu May 13 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	Sun Jun 12 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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 15, 2021 09:21:16.010565042 CEST	185.64.189.114	443	192.168.2.4	50084	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 15, 2021 09:21:16.035279036 CEST	185.64.190.80	443	192.168.2.4	50085	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 15, 2021 09:21:16.035995960 CEST	185.64.190.80	443	192.168.2.4	50086	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 15, 2021 09:21:16.043724060 CEST	185.64.190.80	443	192.168.2.4	50087	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 15, 2021 09:21:16.065993071 CEST	52.17.35.107	443	192.168.2.4	50088	CN=*.scoota.co, 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	Wed Jun 02 18:38:32 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	Mon Jul 04 18:38:32 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		
					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 15, 2021 09:21:16.275006056 CEST	213.19.147.44	443	192.168.2.4	50092	CN=*.1rx.io CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Jun 01 02:00:00 CEST 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Jul 03 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 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=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jul 15, 2021 09:21:16.316037893 CEST	204.2.255.233	443	192.168.2.4	50090	CN=*.mxptint.net, OU=Domain Control Validated CN=Starfield Secure Certificate Authority - G2, OU=http://certs.starfieldtech.com/repository/, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Starfield 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	CN=Starfield Secure Certificate Authority - G2, OU=http://certs.starfieldtech.com/repository/, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Starfield 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 OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue Jul 21 14:52:57 CEST 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:39:16 CEST 2004	Wed Jul 21 14:52:57 CEST 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 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=Starfield Secure Certificate Authority - G2, OU=http://certs.starfieldtech.com/repository/, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Starfield Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Starfield 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 Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Tue Jun 29 19:39:16 CEST 2004	Thu Jun 29 19:39:16 CEST 2034		
Jul 15, 2021 09:21:16.687647104 CEST	213.19.147.44	443	192.168.2.4	50096	CN=*.targeting.unrulymedia.com, O=Unruly Group Limited, L=London, C=GB 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 May 04 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Mon May 09 14:00:00 CEST 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 15, 2021 09:21:17.498945951 CEST	38.27.122.158	443	192.168.2.4	50105	CN=*.bnmla.com, 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	Wed Jan 06 03:24:20 CET 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	Mon Feb 07 03:24:20 CET 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

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 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 15, 2021 09:21:17.504554033 CEST	52.29.225.117	443	192.168.2.4	50109	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		
					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 15, 2021 09:21:17.539283991 CEST	52.212.225.58	443	192.168.2.4	50108	CN=*.narrative.io 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 Apr 07 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 May 07 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 15, 2021 09:21:17.544128895 CEST	52.18.52.16	443	192.168.2.4	50110	CN=*.gumgum.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	Sat Jun 05 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	Tue Jul 05 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 15, 2021 09:21:19.300422907 CEST	35.244.174.68	443	192.168.2.4	50119	CN=*.rlcdn.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Feb 25 01:00:00 CET 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Tue Mar 29 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	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=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 15, 2021 09:21:19.310117006 CEST	216.58.215.226	443	192.168.2.4	50118	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Jun 22 15:35:26 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Sep 14 15:35:25 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 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=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Jul 15, 2021 09:21:19.326921940 CEST	216.58.215.226	443	192.168.2.4	50120	CN=*.g.doubleclick.net CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Tue Jun 22 15:35:26 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Tue Sep 14 15:35:25 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 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=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Jul 15, 2021 09:21:19.379930973 CEST	13.248.242.197	443	192.168.2.4	50122	CN=*.adsrvr.org CN=GlobalSign GCC R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	CN=GlobalSign GCC R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3 CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Thu Mar 18 23:45:32 CET 2021 Tue Jul 28 02:00:00 CEST 2020 Wed Mar 18 11:00:00 CET 2009	Wed Apr 20 00:45:32 CEST 2022 Sun Mar 18 01:00:00 CET 2029 Sun Mar 18 11:00:00 CET 2029	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=GlobalSign GCC 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		
					CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Mar 18 11:00:00 CET 2009	Sun Mar 18 11:00:00 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 15, 2021 09:21:19.393060923 CEST	18.156.0.31	443	192.168.2.4	50128	CN=ups.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	Mon Mar 22 01:00:00 CET 2021 Tue Oct 22 14:00:00 CEST 2013	Thu Sep 16 01:59:59 CEST 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		
Jul 15, 2021 09:21:19.437715054 CEST	212.82.100.176	443	192.168.2.4	50127	CN=*.ybp.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	Mon Mar 29 02:00:00 CEST 2021 Tue Oct 22 14:00:00 CEST 2013	Thu Sep 23 01:59:59 CEST 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		
Jul 15, 2021 09:21:19.445503950 CEST	169.50.137.190	443	192.168.2.4	50130	CN=*.simpli.fi, OU=IT, O=Simplifi Holdings Inc., L=Fort Worth, ST=Texas, 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 Sep 18 02:00:00 CEST 2019 Fri Mar 08 13:00:00 CET 2013	Sun Dec 12 13:00:00 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 15, 2021 09:21:19.457844019 CEST	185.64.190.80	443	192.168.2.4	50135	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 15, 2021 09:21:19.484057903 CEST	185.64.189.114	443	192.168.2.4	50140	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert 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 15, 2021 09:21:19.492475986 CEST	66.155.71.25	443	192.168.2.4	50137	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=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 15, 2021 09:21:19.498972893 CEST	185.64.190.80	443	192.168.2.4	50141	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert 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 15, 2021 09:21:19.508979082 CEST	185.64.190.80	443	192.168.2.4	50144	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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 15, 2021 09:21:19.509083986 CEST	185.64.190.80	443	192.168.2.4	50143	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	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert 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		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 2936 Parent PID: 4944

General

Start time:	09:20:36
Start date:	15/07/2021
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://www.stopcovid19.jp/'
Imagebase:	0x7ff609c80000
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

Key Value Modified

Analysis Process: chrome.exe PID: 5976 Parent PID: 2936

General

Start time:	09:20:38
Start date:	15/07/2021
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=1532,11141525606934232942,4789934611024801501,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1756 /prefetch:8
Imagebase:	0x7ff609c80000
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