ID: 326341
Cookbook: browseurl.jbs
Time: 10:11:34
Date: 03/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report http://pastebin.com 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
Networking: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 9
URLs from Memory and Binaries 10
Contacted IPs 12
Public 12
Private 14
General Information 14
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 16
IPs 16
Domains 16
ASN 17
JA3 Fingerprints 17
Dropped Files 17
Created / dropped Files 17
Static File Info 46
No static file info 46
Network Behavior 47
Network Port Distribution 47
TCP Packets 47
UDP Packets 48
DNS Queries 64
DNS Answers 68
HTTP Request Dependency Graph 94
HTTP Packets 94
HTTPS Packets 94
Code Manipulations 96
Statistics 96
Behavior 96
System Behavior 97

Analysis Process: chrome.exe PID: 6972 Parent PID: 1476 97
General 97
File Activities 97
Registry Activities 97
Key Value Modified 97
Analysis Process: chrome.exe PID: 5484 Parent PID: 6972 98
General 98
File Activities 98
Registry Activities 98
Disassembly 98

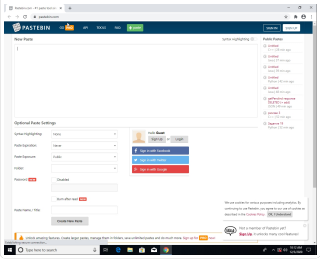
Analysis Report http://pastebin.com

Overview

General Information

Sample URL:	http://pastebin.com
Analysis ID:	326341

Most interesting Screenshot:



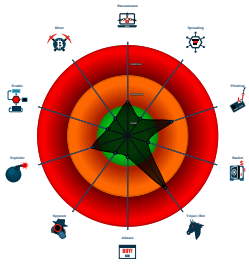
Detection

Score:	23
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Connects to a pastebin service (like…
- Allocates a big amount of memory (p…
- Connects to several IPs in different …
- Found iframes
- HTML body contains low number of …
- HTML title does not match URL
- Unusual large HTML page

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 6972 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'http://pastebin.com' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5484 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1500,13364953271334854619,5261983793971551056,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1672 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

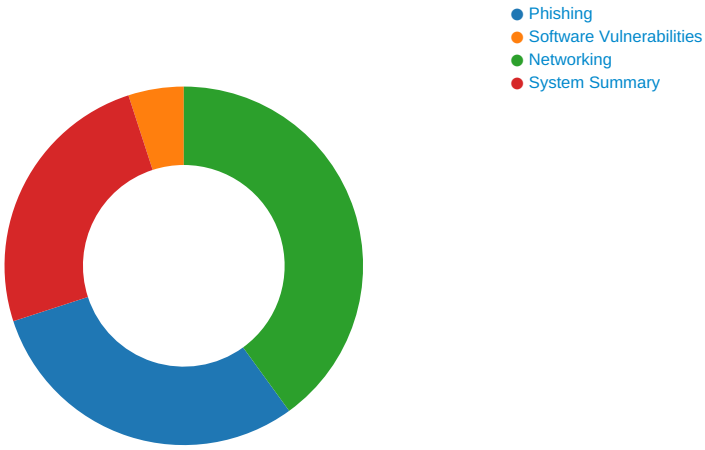
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

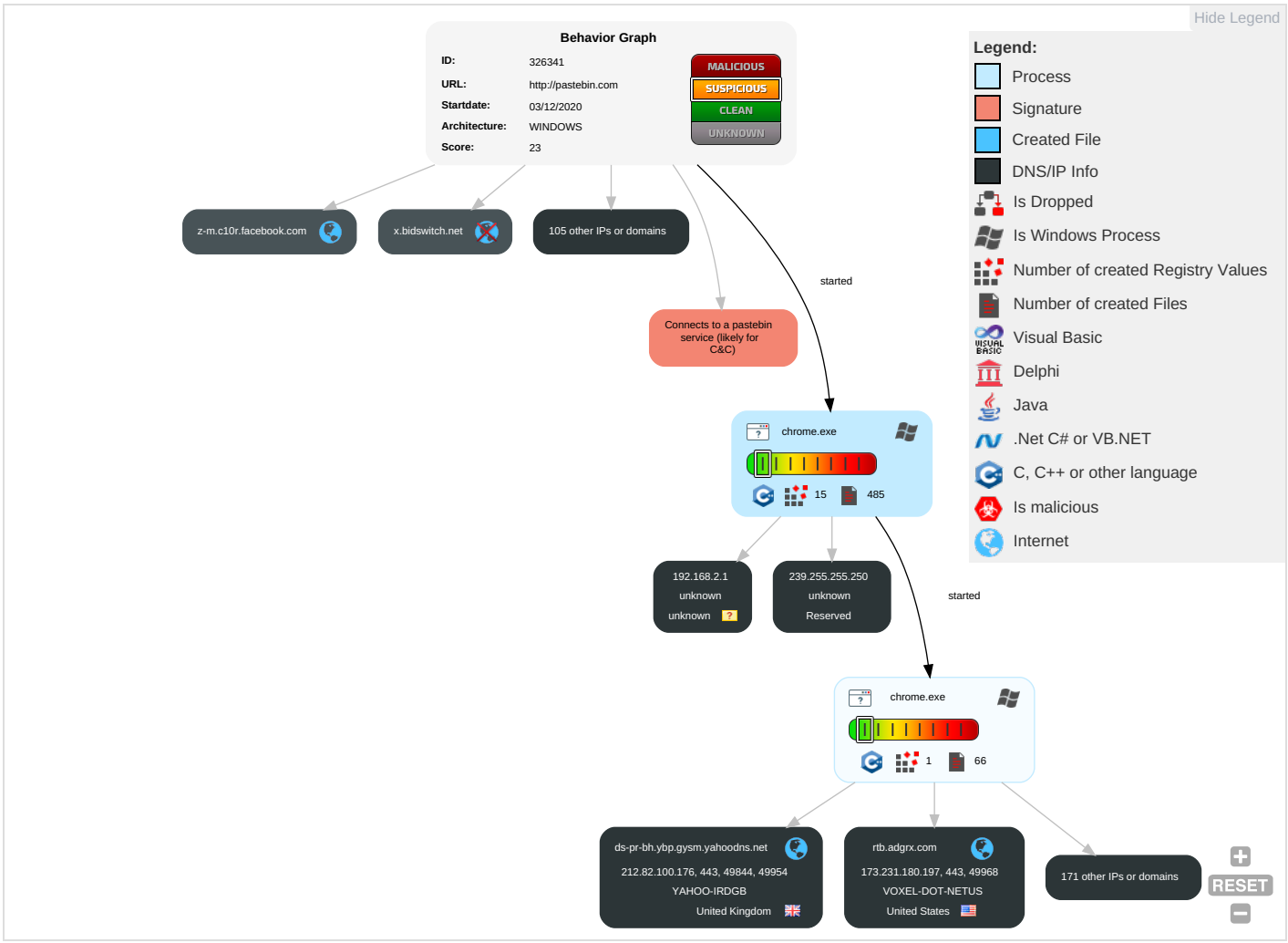
Networking:

Connects to a pastebin service (likely for C&C)

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
Drive-by Compromise 1	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	Web Service 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encrypted Channel 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Extra Window Memory Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
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	Application Layer Protocol 3	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Ingress Tool Transfer 1	Manipulate Device Communication	

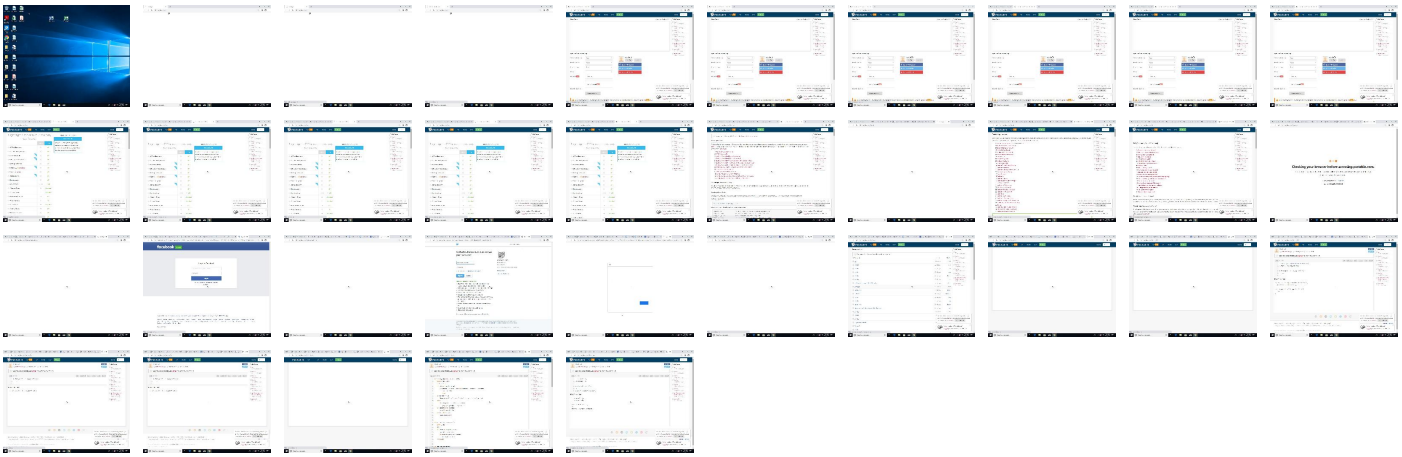
Behavior Graph

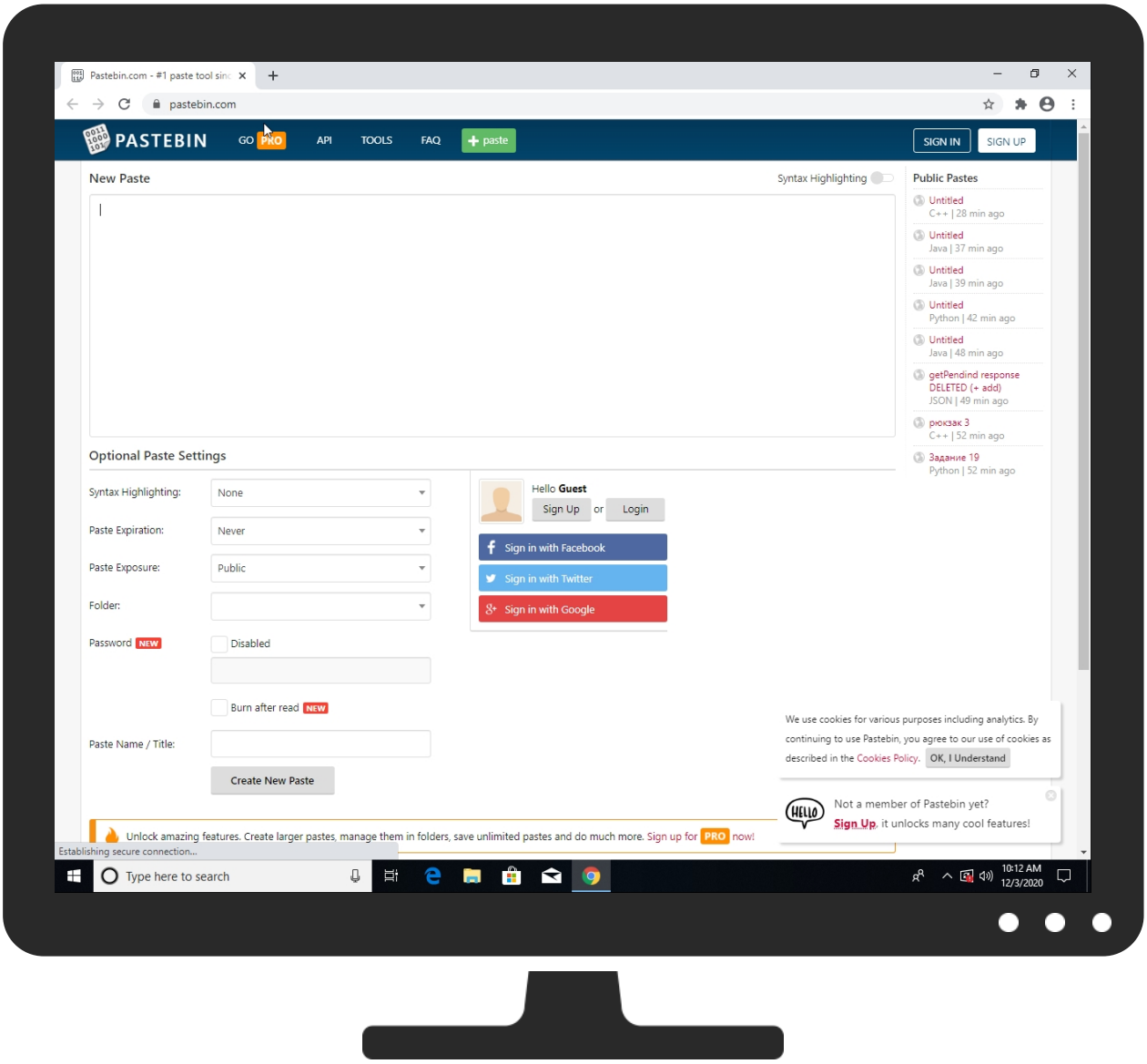


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://pastebin.com	0%	Virustotal		Browse
http://pastebin.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
tls13.taboola.map.fastly.net	0%	Virustotal		Browse
bttrack.com	0%	Virustotal		Browse
i.connectad.io	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://sync-eu.connectad.io/syncer/1?bidder=yahoo&dataid=data18&uuid=y-mFKX9L11l2Tkwg4QkxJUZtBAh7.x	0%	Avira URL Cloud	safe	
http://https://cdn.connectad.io	0%	Avira URL Cloud	safe	
http://https://ads.pubmatic.com$	0%	Avira URL Cloud	safe	
http://https://ssum.casalemedia.com$	0%	Avira URL Cloud	safe	
http://https://pastebin.comh	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
um.simpli.fi	159.253.128.183	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	• 0%, Virustotal, Browse	unknown
global.px.quantserve.com	91.228.74.189	true	false		high
pixel-a.sitescout.com	66.155.71.149	true	false		high
rtb.openx.net	35.186.253.211	true	false		high
bttrack.com	192.132.33.46	true	false	• 0%, Virustotal, Browse	unknown
mwzeom.zeotap.com	172.67.13.182	true	false		high
facebook.com	31.13.92.36	true	false		high
match-1943069928.eu-west-1.elb.amazonaws.com	52.17.171.52	true	false		high
bcp.crwdcntrl.net	52.48.137.92	true	false		high
eu2-ice.360yield.com	54.93.141.230	true	false		high
i.connectad.io	104.22.55.206	true	false	• 1%, Virustotal, Browse	unknown
match.prod.bidr.io	54.171.14.147	true	false		unknown
uip.semasio.net	77.243.60.138	true	false		high
gum.par.vip.prod.criteo.com	178.250.0.157	true	false		high
pixel.onaudience.com	51.210.112.63	true	false		unknown
d1ykf07e75w7ss.cloudfront.net	65.9.83.127	true	false		high
pugm-lhr.pubmatic.com	185.64.190.78	true	false		high
pool.4finance.iponweb.net	35.210.181.65	true	false		unknown
ams-1-sync.go.sonobi.com	178.162.133.149	true	false		high
rtb.adgrx.com	173.231.180.197	true	false		unknown
googlehosted.l.googleusercontent.com	172.217.16.193	true	false		high
api.btloader.com	130.211.23.194	true	false		unknown
oeu.vap.lijit.com	72.251.249.9	true	false		high
nep.advangelists.com	18.204.112.31	true	false		high
scontent.xx.fbcdn.net	31.13.81.13	true	false		high
api.rlcdn.com	34.120.207.148	true	false		high
cdn.connectad.io	172.67.8.174	true	false		unknown
load-ams1.exelator.com	147.75.102.200	true	false		high
rtb.adentifi.com	52.4.242.89	true	false		unknown
sync.srv.stackadapt.com	52.202.170.46	true	false		high
d5p.de17a.com	213.155.156.164	true	false		high
pixel.tapad.com	35.227.248.159	true	false		high
pagead46.l.doubleclick.net	216.58.207.34	true	false		high
twitter.com	104.244.42.193	true	false		high
ssp.ads.betweendigital.com	96.46.183.20	true	false		high
sync.ipredictive.com	35.169.194.138	true	false		unknown
s.amazon-adsystem.com	72.21.206.140	true	false		high
aax-eu.amazon-adsystem.com	52.95.116.38	true	false		high
dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com	52.59.61.242	true	false		high
ad-delivery.net	172.67.69.19	true	false		unknown
um3.eqads.com	54.85.167.1	true	false		high
ams02-usadmm-ds.dotomi.com	64.158.223.137	true	false		high
match.adsby.bidtheatre.com	174.138.12.104	true	false		unknown
ib.anycast.adnxs.com	185.33.221.11	true	false		high
prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud	3.126.56.137	true	false		unknown
aorta.clickagy.com	52.22.205.135	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
optomaton.geo.iponweb.net	35.210.178.101	true	false		unknown
geo-eu.snigelweb.com	172.64.102.21	true	false		high
pug-lhr.pubmatic.com	185.64.190.80	true	false		high
eu-u.openx.net	34.98.64.218	true	false		high
pastebin.com	104.23.98.190	true	false		high
elb-aws-fr-clickdistrict-1651093077.eu-central-1.elb.amazonaws.com	18.195.7.149	true	false		high
tpop-api.twitter.com	104.244.42.2	true	false		high
widget.am5.vip.prod.criteo.com	178.250.2.151	true	false		high
sync-eu.connectad.io	104.22.54.206	true	false		unknown
pagead.l.doubleclick.net	172.217.21.226	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
sync.1rx.io	213.19.147.150	true	false		high
ds-pr-bh.ybp.gysm.yahoodns.net	212.82.100.176	true	false		unknown
sync.connectad.io	104.22.55.206	true	false		unknown
ads.playground.xyz	3.121.163.163	true	false		unknown
star-mini.c10r.facebook.com	31.13.92.36	true	false		high
bidder.par.vip.prod.criteo.com	178.250.0.165	true	false		high
us-u.openx.net	35.244.159.8	true	false		high
stats.l.doubleclick.net	108.177.15.154	true	false		high
eqx.smartadserver.com	185.86.137.113	true	false		high
dsp.adfarm1.adition.com	85.114.159.93	true	false		high
cs.emxdgt.com	18.195.155.181	true	false		unknown
a.tribalfusion.com	104.18.12.5	true	false		high
eventd-eu.avct.cloud	54.194.211.3	true	false		unknown
btloader.com	104.26.6.139	true	false		unknown
adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com	54.77.74.200	true	false		high
dart.l.doubleclick.net	172.217.18.102	true	false		high
pixel-origin.mathtag.com	185.29.132.30	true	false		high
s.tribalfusion.com	104.18.13.5	true	false		high
ams01-login-ds.dotomi.com	63.215.202.140	true	false		high
cs45.wac.edgecastcdn.net	93.184.220.70	true	false		high
u.openx.net	34.98.64.218	true	false		high
snigelweb-com.videoplayerhub.com	172.67.74.207	true	false		unknown
rtb.gumgum.com	54.154.144.178	true	false		high
cm.smadex.com	65.9.86.12	true	false		high
ssbsync-itx4.smartadserver.com	185.86.139.103	true	false		high
static.par.vip.prod.criteo.net	178.250.0.130	true	false		high
alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com	35.156.245.144	true	false		high
z-m.c10r.facebook.com	31.13.92.37	true	false		high
dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com	18.185.170.181	true	false		high
pug22000nf.pubmatic.com	185.64.189.110	true	false		high
spug22000nf.pubmatic.com	185.64.189.114	true	false		high
partnerad.l.doubleclick.net	172.217.21.194	true	false		high
green.erne.co	87.98.252.5	true	false		high
onetag-sys.com	51.89.9.253	true	false		unknown
cdn.snigelweb.com	172.64.102.21	true	false		high
abs-zero.twimg.com	104.244.43.131	true	false		high
visitor.fiftyt.com	104.26.13.50	true	false		unknown
adserver-vpc-alb-0-1578609942.eu-west-1.elb.amazonaws.com	63.35.200.21	true	false		high
securepubads.g.doubleclick.net	unknown	unknown	false		high
a.volvelle.tech	unknown	unknown	false		high
d.adroll.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://aax-eu.amazon-adsystem.com/s/ecm3?id=17797123819684764 79&ex=appnexus.com&gdpr=0	false		high
http://https://simage2.pubmatic.com/AdServer/Pug?vcode=bz0yJnR5cGU9MSZjb2RlPTMzOTkmdGw9NDMyMDA=&piggybackCookie=6901955540651997325	false		high

Name	Malicious	Antivirus Detection	Reputation
http://https://sync-eu.connectad.io/syncer/1?bidder=yahoo&dataid=data18&uuid=y-mFKX9L11l2Tkwg4QkxJUZtBAh7.xHg--	true		unknown
http://https://onetag-sys.com/usync/?cb=1606986778757&us_privacy=1---	true		unknown
http://https://sync-eu.connectad.io/syncer/1?us_privacy=1---&	true		unknown
http://https://pastebin.com/doc_api	false		high
http://https://onetag-sys.com/usync/?cb=1606986804988&us_privacy=1---	true		unknown
http://https://aax-eu.amazon-adsystem.com/s/v3/pr?exlist=pm-db5_n-emx_rx_snb_ox-db5_dm_smrt_an-db5_sovrn_3lift&fv=1.0&a=cm&cm3ppd=1&gdpr=0	false		high
http://https://aax-eu.amazon-adsystem.com/s/ecm3?id=17797123819684764 79&ex=districtm&gdpr=0	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://u.openx.net/w/1.0/cm?cc=1&id=e818ca1e-0c23-caa8-0dd3-096b0ada08b7&ph=2d1251ae-7f3a-47cf-bd2a-2f288854a0ba&plm=5&r=https%3A%2F%2Faax-eu.amazon-adsystem.com%2Fs%2Fecm3%3Fex%3Dopenx.com%26id%3D%7BOPENX_ID%7D&gdpr=0	false		high
http://https://aax-eu.amazon-adsystem.com/s/v3/pr?exlist=rx_snb&fv=1.0&a=cm&cm3ppd=1&gdpr=0	false		high
http://https://simage2.pubmatic.com/AdServer/Pug?vcode=bz0yJnR5cGU9MSZjb2RlPTMyMDMmdGw9NDMyMDA=&piggybackCookie=RX-6d355ea9-1a84-43da-81d4-b6980f597991-003	false		high
http://https://pastebin.com/C31QJabQ	false		high
http://https://onetag-sys.com/usync/?cb=1606986812537&us_privacy=1---	true		unknown
http://https://acdn.adnxs.com/dmp/async_usersync.html	false		high
http://https://onetag-sys.com/usync/?cb=1606986748247&us_privacy=1---	true		unknown
http://https://pastebin.com/login	false		high
http://https://aax-eu.amazon-adsystem.com/s/ecm3?id=29A8C016-71A4-40E9-B9FD-3D8155395C81&ex=pubmatic.com	false		high
http://https://simage2.pubmatic.com/AdServer/Pug?vcode=bz0yJnR5cGU9MSZjb2RlPTMwNzQmdGw9MTI5NjAw&piggybackCookie=uid:szgbymTo1KKKFh5&gdpr=0&gdpr_consent=	false		high
http://https://pastebin.com/pro	false		high
http://https://aax-eu.amazon-adsystem.com/s/ecm3?ex=smart.com&id=5882865552118630403	false		high

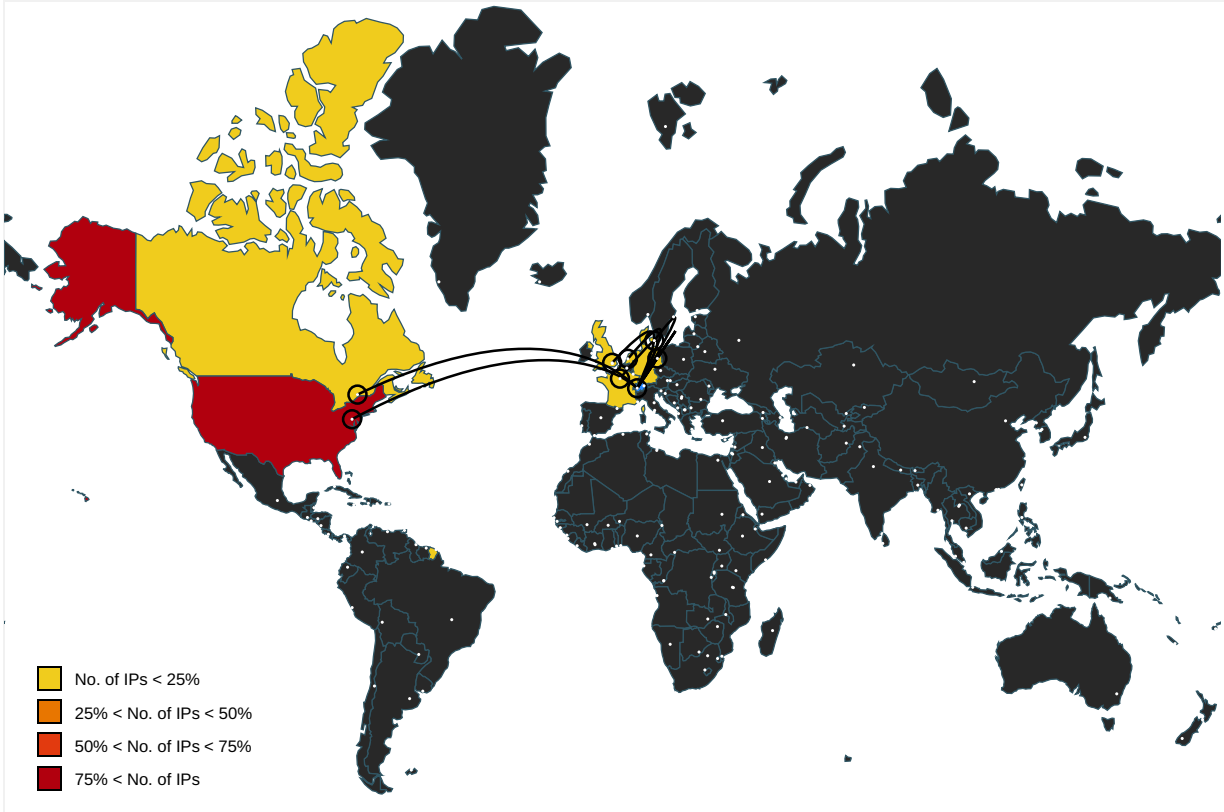
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://image6.pubmatic.com/AdServer/PugMaster?kdntuid=1&rnd=19252284&p=156077&s=0&a=0&ptask=ALL&np=	87cba9c64d845c0d_0.0.dr	false		high
http://https://pastebin.com/themes/pastebin/js/vendors.bundle.js?677fa6bd2113231028dd	cf6d21810551f26a_0.0.dr	false		high
http://https://securepubads.g.doubleclick.net/gpt/pubads_impl_2020111901.js	7a69c8c98ea1b6d5_0.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/yo/r/iRmz9lCMBD2.ico$	Favicons.0.dr	false		high
http://https://a.nel.cloudflare.com/report?s=8ueMsIQcbkiPdSVqmUp3Oo9dRtnazL9cZyGUf%2BYhi2eC3wltgqXzaBL4i5qa	Reporting and NEL.1.dr	false		high
http://https://onetag-sys.com/usync/?cb=1606986800434&us_privacy=1---	Current Session.0.dr	false		unknown
http://https://pastebin.com/assets/1745bc3b/yii.activeForm.jsaD	1b63c6e73bda96a4_0.0.dr	false		high
http://https://pastebin.com/cg	60c0828071489bda_0.0.dr	false		high
http://https://sync-eu.connectad.io/syncer/1?bidder=yahoo&dataid=data18&uuid=y-mFKX9L11l2Tkwg4QkxJUZtBAh7.x	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://static.xx.fbcdn.net/rsrc.php/v3iaLv4/yE/l/en_GB/ubsVV_mono5.js?_nc_x=Ij3Wp8lg5Kz	2a3a31f51ba217b7_0.0.dr	false		high
http://https://cdn.connectad.io	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.snigelweb.com/adconsent/adconsent.jsaD	8f06da9be8297fca_0.0.dr	false		high
http://https://pastebin.com/assets/ae9b8d97/jquery.min.js	707c02e9a3e299c0_0.0.dr	false		high
http://https://image2.pubmatic.com/AdServer/Pug?vcode=bz0yJnR5cGU9MSZjb2RlPTI3NDUmdGw9MTI5NjAw&gdpr=0&gdpr_	Current Session.0.dr	false		high
http://https://onetag-sys.com/usync/?cb=1606986760370&us_privacy=1---	Current Session.0.dr	false		unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://securepubads.g.doubleclick.net/	8b95103176f2e077_0.0.dr	false		high
http://https://pastebin.com/site/auth-google	Current Session.0.dr	false		high
http://https://ads.pubmatic.com$	Current Session.0.dr	false	• Avira URL Cloud: safe	low
http://https://onetag-sys.com/usync/?cb=1606986798950&us_privacy=1---	Current Session.0.dr	false		unknown
http://https://api.twitter.com/oauth/authenticate	Current Session.0.dr	false		high
http://https://pastebin.com/site/auth-googleSign	History-journal.0.dr	false		high
http://https://a.nel.cloudflare.com/report?s=aS48KQ9EY%2FZjl4sophnUIt8w9JjK4yYh%2F%2FgN9wyE%2Fvk3ddKQNX3wwj	Reporting and NEL.1.dr	false		high
http://https://pastebin.com/qxkve6Xr;while(jugadorTU	Current Session.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3iYXl4/yz/l/en_GB/bOtHsRxDkOf.js?_nc_x=Ij3Wp8lg5Kz	8995dfb6624f2499_0.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/yo/r/iRmz9lCMBD2.ico	Favicons.0.dr	false		high
http://https://image2.pubmatic.com/AdServer/Pug?vcode=bz0yJnR5cGU9MSZjb2RlPTI4ODQmdGw9MTI5NjAw&piggybackCoo	Current Session.0.dr	false		high
http://pastebin.com/Q	Favicons-journal.0.dr	false		high
http://https://ssum.casalemedia.com$	Current Session.0.dr	false	• Avira URL Cloud: safe	low
http://https://cm.adgrx.com/bridge?AG_PID=pubmatic&AG_SETCOOKIE&gdpr=0&gdpr_consent=	Current Session.0.dr	false		unknown
http://https://pastebin.comh	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://s0.2mdn.net/ads/richmedia/studio_canary/mu/templates/hifi/hifi_canary.js	db650fda12315775_0.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3iPrS4/yl/l/en_GB/ZjRaTSQ42RF.js?_nc_x=Ij3Wp8lg5Kz	78431f791492b110_0.0.dr	false		high
http://https://pastebin.com/g	60c0828071489bda_0.0.dr	false		high
http://https://pastebin.com/6YJs2dr9_	Current Session.0.dr	false		high
http://https://abs-0.twimg.com/	Network Action Predictor-journal.0.dr	false		high
http://https://pastebin.com/Pastebin.com	History-journal.0.dr	false		high
http://https://aax-eu.amazon-adsystem.com/s/iu3?cm3ppd=1&d=dtb-pub&csif=t&gdpr=0&dl=n-emx_rx_snb	Current Session.0.dr	false		high
http://https://c1.adform.net/serving/cookie/match?party=14&cid=29A8C016-71A4-40E9-B9FD-3D8155395C81	Current Session.0.dr	false		high
http://https://static.criteo.net/images/pixel.gif?ch=2	74845533764f80c7_0.0.dr	false		high
http://https://eus.rubiconproject.com/usync.html	bbf6347a22a48602_0.0.dr	false		high
http://https://static.criteo.net/images/pixel.gif?ch=1	74845533764f80c7_0.0.dr	false		high
http://https://www.googletagservices.com/tag/js/gpt.jsaD	8b95103176f2e077_0.0.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/codemirror/5.58.2/addon/mode/multiplex.min.jsa	753e6439691a724e_0.0.dr	false		high
http://https://pastebin.com/Ns3rF0f9System.out.print(	History-journal.0.dr	false		high
http://https://pastebin.com/themes/pastebin/js/app.bundle.js?677fa6bd2113231028ddaD	a8e071ae86cd7f79_0.0.dr	false		high
http://https://pixel.tapad.com/idsync/ex/receive/check?partner_id=PUBMATIC_RTB	Current Session.0.dr	false		high
http://https://securepubads.g.doubleclick.net/pagead/js/rum.js	db650fda12315775_0.0.dr	false		high
http://https://ib.adnxs.com/ut/v3/prebid	bbf6347a22a48602_0.0.dr	false		high
http://https://cdn.connectad.io/connectmyusers.php?us_privacy=1---&	Current Session.0.dr	false		unknown
http://https://dmx.districtm.io/b/v1	bbf6347a22a48602_0.0.dr	false		high
http://https://ads.pubmatic.com/AdServer/js/showad.js	Current Session.0.dr	false		high
http://https://securepubads.g.doubleclick.net/pagead/js/rum_debug.js	db650fda12315775_0.0.dr	false		high
http://https://pastebin.com/(Pastebin.com	Current Session.0.dr	false		high
http://https://pastebin.com/BLw7LJjee	Current Session.0.dr	false		high
http://https://cdn.snigelweb.com/prebid/latest/prebid.jsaD	bbf6347a22a48602_0.0.dr	false		high
http://https://pastebin.com/y	18b9130c1e45de41_0.0.dr	false		high
http://https://onetag-sys.com/usync/?cb=1606986778757&us_privacy=1---	Current Session.0.dr	false		unknown
http://https://static.xx.fbcdn.net/rsrc.php/v3/yA/r/P2xVPF9XJCl.js?_nc_x=Ij3Wp8lg5Kz	89f65cd09ba91171_0.0.dr	false		high
http://https://pastebin.com/signup	Current Session.0.dr, Favicons-journal.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aax-eu.amazon-adsystem.com/s/v3/pr?exlist=snb&fv=1.0&a=cm&cm3ppd=1&gdpr=0	Current Session.0.dr	false		high
http://https://pastebin.com/doc_api&	Current Session.0.dr	false		high
http://https://sync-eu.connectad.io/syncer/1?us_privacy=1---&	Current Session.0.dr	false		unknown
http://https://onetag-sys.com/usync/?cb=1606986773394&us_privacy=1---	Current Session.0.dr	false		unknown
http://https://image6.pubmatic.com/AdServer/PugMaster?kdntuid=1&rnd=89367292&p=156657&s=0&a=0&ptask=ALL&np=	e3606adf4b207cfe_0.0.dr	false		high
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://prebid.adnxs.com/pbc/v1/cache	bbf6347a22a48602_0.0.dr	false		high
http://https://api.twitter.com/oauth/authenticate?oauth_token=Pp6EjQAAAAAADnp_AAABdifgcN8Twitter	History-journal.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3iril4/yW/l/en_GB/3V96puac_8e.js?_nc_x=Ij3Wp8lg5Kz	990da70a3b3900c1_0.0.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/codemirror/5.58.2/addon/mode/multiplex.min.js	753e6439691a724e_0.0.dr	false		high
http://https://pastebin.com/Ni	c671a1e6d1566d7a_0.0.dr	false		high
http://https://cdn.snigelweb.com/snhb/snhbGlobalSettings.js	ffeb292a4c56ab10_0.0.dr	false		high
http://https://pastebin.com/favicon.ico	Favicons-journal.0.dr	false		high
http://https://cdn.jsdelivr.net/gh/prebid/currency-file	bbf6347a22a48602_0.0.dr	false		high
http://https://onetag-sys.com/usync/?cb=1606986804988&us_privacy=1---	Current Session.0.dr	false		unknown
http://https://acdn.adnxs.com/dmp/async_usersync.html	Current Session.0.dr	false		high
http://https://static.xx.fbcdn.net/rsrc.php/v3/yx/r/RPpa71t4yWJ.js?_nc_x=Ij3Wp8lg5Kz	df10c594f19545b9_0.0.dr	false		high
http://https://um2.eqads.com/um/cs&eq_cc=1	Current Session.0.dr	false		high
http://https://image2.pubmatic.com/AdServer/Pug?vcode=bz0yJnR5cGU9MSZjb2RlPTMyOTcmdGw9MTI5NjAw&piggybackCoo	Current Session.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
178.250.0.157	unknown	France		44788	ASN-CRITEO-EUROPEFR	false
216.52.2.30	unknown	United States		29791	VOXEL-DOT-NETUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.33.221.11	unknown	Netherlands		29990	ASN-APPNEXUS	false
130.211.23.194	unknown	United States		15169	GOOGLEUS	false
185.64.190.80	unknown	United Kingdom		62713	AS-PUBMATICUS	false
185.33.220.241	unknown	Netherlands		29990	ASN-APPNEXUS	false
35.227.248.159	unknown	United States		15169	GOOGLEUS	false
51.89.20.86	unknown	France		16276	OVHFR	false
192.132.33.46	unknown	United States		18568	BIDTELLECTUS	false
178.250.2.151	unknown	France		44788	ASN-CRITEO-EUROPEFR	false
72.251.249.9	unknown	United States		29791	VOXEL-DOT-NETUS	false
54.154.144.178	unknown	United States		16509	AMAZON-02US	false
87.98.252.5	unknown	France		16276	OVHFR	false
52.22.205.135	unknown	United States		14618	AMAZON-AESUS	false
213.19.147.151	unknown	United Kingdom		26120	RHYTHMONEUS	false
213.19.147.150	unknown	United Kingdom		26120	RHYTHMONEUS	false
104.22.55.206	unknown	United States		13335	CLOUDFLARENETUS	false
178.250.0.165	unknown	France		44788	ASN-CRITEO-EUROPEFR	false
185.86.137.113	unknown	France		201081	SMARTADSERVERFR	false
151.101.1.44	unknown	United States		54113	FASTLYUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.212.162	unknown	United States		15169	GOOGLEUS	false
104.18.12.5	unknown	United States		13335	CLOUDFLARENETUS	false
54.93.141.230	unknown	United States		16509	AMAZON-02US	false
66.155.71.149	unknown	Canada		13768	COGECO-PEER1CA	false
54.171.14.147	unknown	United States		16509	AMAZON-02US	false
172.67.74.207	unknown	United States		13335	CLOUDFLARENETUS	false
178.250.0.130	unknown	France		44788	ASN-CRITEO-EUROPEFR	false
172.217.21.226	unknown	United States		15169	GOOGLEUS	false
185.64.189.110	unknown	United Kingdom		62713	AS-PUBMATICUS	false
96.46.183.20	unknown	United States		7979	SERVERS-COMUS	false
185.64.189.114	unknown	United Kingdom		62713	AS-PUBMATICUS	false
18.185.170.181	unknown	United States		16509	AMAZON-02US	false
52.48.137.92	unknown	United States		16509	AMAZON-02US	false
104.23.98.190	unknown	United States		13335	CLOUDFLARENETUS	false
213.155.156.164	unknown	European Union		1299	TELIANETTeliaCarrierEU	false
185.64.190.78	unknown	United Kingdom		62713	AS-PUBMATICUS	false
147.75.102.200	unknown	Switzerland		54825	PACKETUS	false
52.17.171.52	unknown	United States		16509	AMAZON-02US	false
172.217.23.162	unknown	United States		15169	GOOGLEUS	false
52.95.116.38	unknown	United States		16509	AMAZON-02US	false
104.26.13.50	unknown	United States		13335	CLOUDFLARENETUS	false
104.16.19.94	unknown	United States		13335	CLOUDFLARENETUS	false
104.26.6.139	unknown	United States		13335	CLOUDFLARENETUS	false
108.177.15.154	unknown	United States		15169	GOOGLEUS	false
35.156.245.144	unknown	United States		16509	AMAZON-02US	false
172.67.13.182	unknown	United States		13335	CLOUDFLARENETUS	false
216.58.207.66	unknown	United States		15169	GOOGLEUS	false
77.243.60.138	unknown	Denmark		42697	NETIC-ASDK	false
212.82.100.176	unknown	United Kingdom		34010	YAHOO-IRDGB	false
172.217.22.66	unknown	United States		15169	GOOGLEUS	false
185.29.132.30	unknown	United Kingdom		30419	MEDIAMATH-INCUS	false
172.64.102.21	unknown	United States		13335	CLOUDFLARENETUS	false
18.195.155.181	unknown	United States		16509	AMAZON-02US	false
18.195.7.149	unknown	United States		16509	AMAZON-02US	false
185.86.139.103	unknown	France		201081	SMARTADSERVERFR	false
178.162.133.149	unknown	Netherlands		60781	LEASEWEB-NL-AMS-01NetherlandsNL	false
159.253.128.183	unknown	Netherlands		36351	SOFTLAYERUS	false
64.158.223.137	unknown	United States		41041	VCLK-EU-SE	false
172.217.18.102	unknown	United States		15169	GOOGLEUS	false
3.126.56.137	unknown	United States		16509	AMAZON-02US	false
172.217.21.194	unknown	United States		15169	GOOGLEUS	false
172.217.16.193	unknown	United States		15169	GOOGLEUS	false
72.21.206.140	unknown	United States		16509	AMAZON-02US	false
52.202.170.46	unknown	United States		14618	AMAZON-AESUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
51.210.112.63	unknown	France		16276	OVHFR	false
91.228.74.189	unknown	United Kingdom		27281	QUANTCASTUS	false
35.210.181.65	unknown	United States		19527	GOOGLE-2US	false
52.59.61.242	unknown	United States		16509	AMAZON-02US	false
54.77.74.200	unknown	United States		16509	AMAZON-02US	false
85.114.159.93	unknown	Germany		24961	MYLOC-ASIPBackboneofmyLocmanagedITAGDE	false
65.9.83.127	unknown	United States		16509	AMAZON-02US	false
35.169.194.138	unknown	United States		14618	AMAZON-AESUS	false
198.148.27.140	unknown	United States		19189	PULSEPOINTUS	false
65.9.86.12	unknown	United States		16509	AMAZON-02US	false
54.194.211.3	unknown	United States		16509	AMAZON-02US	false
172.67.69.19	unknown	United States		13335	CLOUDFLARENETUS	false
216.58.207.34	unknown	United States		15169	GOOGLEUS	false
173.231.180.197	unknown	United States		29791	VOXEL-DOT-NETUS	false
34.120.207.148	unknown	United States		15169	GOOGLEUS	false
174.138.12.104	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
35.186.253.211	unknown	United States		15169	GOOGLEUS	false
51.89.9.253	unknown	France		16276	OVHFR	false
34.98.64.218	unknown	United States		15169	GOOGLEUS	false
54.85.167.1	unknown	United States		14618	AMAZON-AESUS	false
52.4.242.89	unknown	United States		14618	AMAZON-AESUS	false

Private

IP
192.168.2.1
192.168.2.4
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	326341
Start date:	03.12.2020
Start time:	10:11:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://pastebin.com
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:	8
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:	SUS
Classification:	sus23.troj.win@89/268@169/89

Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://pastebin.com/ • Browse: https://pastebin.com/pro • Browse: https://pastebin.com/doc_api • Browse: https://pastebin.com/tools • Browse: https://pastebin.com/faq • Browse: https://pastebin.com/login • Browse: https://pastebin.com/signup • Browse: https://pastebin.com/site/auth-facebook • Browse: https://pastebin.com/site/auth-twitter • Browse: https://pastebin.com/site/auth-google • Browse: https://pastebin.com/archive • Browse: https://pastebin.com/6YJs2dr9 • Browse: https://pastebin.com/Ns3rF0f9 • Browse: https://pastebin.com/qxkve6Xr • Browse: https://pastebin.com/C31QJabQ • Browse: https://pastebin.com/BLw7LJje
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.64.90.137, 172.217.16.142, 172.217.18.13, 216.58.212.163, 216.58.206.14, 173.194.151.123, 172.217.23.168, 172.217.23.142, 216.58.208.42, 204.13.202.71, 2.20.142.209, 2.20.142.210, 92.122.147.28, 172.217.21.225, 172.217.23.97, 37.157.4.25, 37.157.6.253, 37.157.3.29, 37.157.2.239, 37.157.6.241, 37.157.6.247, 37.157.5.142, 37.157.4.24, 91.199.212.52, 46.228.164.11, 151.101.2.49, 151.101.66.49, 151.101.130.49, 151.101.194.49, 92.122.145.117, 37.157.2.235, 37.157.6.251, 37.157.4.40, 37.157.3.30, 37.157.4.39, 37.157.3.28, 37.157.4.29, 37.157.2.234, 104.43.193.48, 92.122.147.230, 204.79.197.222, 93.184.220.29, 172.217.16.170, 172.217.18.106, 172.217.23.106, 216.58.212.138, 172.217.22.42, 172.217.22.74, 216.58.212.170, 172.217.23.170, 142.250.74.202, 172.217.22.106, 216.58.205.234, 172.217.16.138, 172.217.21.202, 172.217.21.234, 51.104.139.180, 216.58.205.227, 172.217.21.227, 172.217.18.14, 216.58.208.36, 172.217.16.131, 172.217.18.99, 74.125.173.233, 92.122.213.247, 92.122.213.194, 20.54.26.129, 52.155.217.156, 173.194.188.42, 173.194.165.171 • Excluded domains from analysis (whitelisted): fp.msedge.net, gstaticadssl.l.google.com, ssl.gstatic.com, uipglob.trafficmanager.net, arc.msn.com.nsatc.net, clientservices.googleapis.com, 584d8ccbb49ccf988fb43167f391ebbc.safeframe.googlesyndication.com, track-eu.adformnet.akadns.net, ssum.casalemedia.com.edgekey.net, a-0019.a-msedge.net, clients2.google.com, ocsp.digicert.com, audownload.windowsupdate.nsatc.net, afp.dotomi.weighted.com.akadns.net, update.googleapis.com, www.google.com, watson.telemetry.microsoft.com, www.gstatic.com, 24d55f2e779b71ae84830a3eebf266ed.safeframe.googlesyndication.com, au-bg-shim.trafficmanager.net, secure-adnxs.edgekey.net, e8cebfedb9e276799155c422dd3969db.safeframe.googlesyndication.com, www.google-analytics.com, pagead-googlehosted.l.google.com, 23b26c62870fa23d9efc7a12c15fb6b3.safeframe.googlesyndication.com, content-autofill.googleapis.com, 2-01-275d-0028.cdx.cedexis.net, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ssl.trustwave.com, pagead2.googlesyndication.com, www.googleapis.com, skypedataprdcolcus15.cloudapp.net, 03d8bd4c87e529c6f89d805376aa7d3f.safeframe.googlesyndication.com, ris.api.iris.microsoft.com, r5---sn-4g5ednse.gvt1.com, 43d2c973d504de06853a74a8aa45f4c2.safeframe.googlesyndication.com, www3.l.google.com, blobcollector.events.data.trafficmanager.net, e6603.g.akamaiedge.net, dsum-sec.casalemedia.com.edgekey.net, clients.l.google.com, r5.sn-4g5edn7y.gvt1.com,

h2.shared.global.fastly.net, au.download.windowsupdate.com.edgesuite.net, cs2-wac.apr-8315.edgecastdns.net, r5.sn-4g5edney.gvt1.com, adservice.google.com, track.adformnet.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e94a5a8d1fd72f1787c271c674c62fbe.safeframe.googlesyndication.com, 9e16dfc4a8b87d4f8125198eb23e3f73.safeframe.googlesyndication.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e8037.g.akamaiedge.net, redirector.gvt1.com, www.googletagmanager.com, dc911c7fd8279b5b09546b2e1ee86da5.safeframe.googlesyndication.com, pubmatic.edgekey.net, r5---sn-4g5edney.gvt1.com, r4---sn-4g5ednz7.gvt1.com, 1.perf.msedge.net, 4b59331a563429ce121717d1495de25d.safeframe.googlesyndication.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, b527a9f15742bc337d1ca3e556de4388.safeframe.googlesyndication.com, r5.sn-4g5ednse.gvt1.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, accounts.google.com, www-google-analytics.l.google.com, fonts.gstatic.com, www-googletagmanager.l.google.com, ctldl.windowsupdate.com, a767.dscg3.akamai.net, ad.turn.com.akadns.net, r5---sn-4g5edn7y.gvt1.com, r4.sn-4g5ednz7.gvt1.com, dsum.casalemedia.com.edgekey.net, play.google.com, 2-01-275d-0035.cdx.cedexis.net, tpc.googlesyndication.com, crt.usertrust.com, ssum-sec.casalemedia.com.edgekey.net, 2-01-275d-002f.cdx.cedexis.net, 5322d77b112933525e277c2f9aef7f0f.safeframe.googlesyndication.com, e6115.g.akamaiedge.net, 5b53f8a210aa91d532b73fed2c2be7e4.safeframe.googlesyndication.com, c34edbe947c918439ed24a99b77ff08f.safeframe.googlesyndication.com

- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.
- Report size getting too big, too many NtWriteFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:12:27	API Interceptor	2x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\4CA77D36767B6202D4786BF3D1EC5242	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	956
Entropy (8bit):	7.3478006141797225
Encrypted:	false
SSDEEP:	12:AQ8f+rvA5L3jGKQvA5L3j27QqUEpnJ0vec4HIbMqoilagtzsTfLsqTSR2My3Oux1:t9vguPvg+7QqUESjQLscZ3Oywr9ICRk
MD5:	DC32C3A76D2557C768099DEA2DA9A2D1
SHA1:	8782C6C304353BCFD29692D2593E7D44D934FF11
SHA-256:	F1C1B50AE5A20DD8030EC9F6BC24823DD367B5255759B4E71B61FCE9F7375D73
SHA-512:	0709087318438E54CFC687B3C16CD8789E1CC3438720E39E79E00519184B03E7F84AD92C2B0C0B91592743DCA04D4A5CE02A6C31A0A5AA9674A45C4D96B0ADC
Malicious:	false
Reputation:	low
Preview:	0...0.....\....B...'.Y.0...*.H.....0H1.0...U....US1 0...U....SecureTrust Corporation1.0...U....SecureTrust CA0...0611071931l8Z..291231194055Z0H1.0...U....US1 0 ...U....SecureTrust Corporation1.0...U....SecureTrust CA0.."0...*.H.....0.....O...x.X.A...@$.9.3f..b\...$[a....A..n.....H.....A>...).....m.g.W.....f%H...].....O. F..\..^..m.....o1BlR>h...4...V.&....o.....d.KD.....c.f.v.q..6.hzw..../.z.r..k.....Y?.r.D$..s...W/B&..t..R.K.S\|G.6..f....4W.f....pT...(.Y.....0..0...+.....7.....C.A0...U.....0...U.....0... .0...U.....B2.....]Kz...L@.ZC.04..U...-0+0).'.%.#http://crl.securetrust.com/STCA.crl0...+.....7.....0...*.H.....0.OJ.X:Rr[...e...Q;w...\.Ee{..[.pP.....I.A..s.~.#!....`.Zr.....z o]....iB..q..&....j.q....!T+.X..W).....&.....i.....+.64{$.xL....&..dR6_`g...t..g#.....0.7~..2.-.D00l....4...@.K.fF.T..2.c&0k...G...b...g.x)c.o....L...7...(K..,.h....1

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	117872
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	1536:i/LAvEZrGclx0hoW6qCLdNz2p+/LAvEZrGclx0hoW6qCLdNz2pj:UcMqZVCp8pwcMqZVCp8pj
MD5:	DB381E85D86EA4484D20078E9EC667A6
SHA1:	4871FDAF0C2EEC8183FC3CE7710B18FD3C647CEA
SHA-256:	C3520E3A6EB43F6D416852C454414C5D7823A96FB9070BC30301ADDEBB334D4D
SHA-512:	D9E03A617D1D9505D3ADA3C41FC8A53504F4F1C44F92AF00869F2FE150D6677FD4450E85EB1E3D920D32BA01F190E7F14BF130F8CC69EB47D834CCE43CAA765 0
Malicious:	false
Reputation:	low
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:.(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC... 3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.... ....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G..... ..b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u. .s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`...........A$:.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\8A4AA6A226E1870F0261713C59F1CB84	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	983
Entropy (8bit):	7.131487105347442
Encrypted:	false

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\8A4AA6A226E1870F0261713C59F1CB84	
SSDEEP:	24:EJm3RW857Ij3e1CyAQxESMrVAVsNFrcHqHmk27mz:mL854PTQxMrGVmFrcHqHmkek
MD5:	42F8529FE545103FDD848980A8647F29
SHA1:	CA7788C32DA1E4B7863A4FB57D00B55DDACBC7F9
SHA-256:	A6CF64DBB4C8D5FD19CE48896068DB03B533A8D1336C6256A87D00CBB3DEF3EA
SHA-512:	1A3994C12D65E9C96B4C4EBCF79E8B291B620177520A7D0482A2B6043DD150A9F2CE1627D130309390E3AC6BE98AF5F2B50C1993C478976D0C9A9638C46A61B
Malicious:	false
Reputation:	low
Preview:	0...0.....Vg...O.Lo..GY.u.0...*.H.....0{1.0...U....GB1.0...U....Greater Manchester1.0...U....Salford1.0...U....Comodo CA Limited1!0...U....AAA Certificate Service s0...190312000000Z..281231235959Z0..1.0...U....US1.0...U....New Jersey1.0...U....Jersey City1.0...U....The USERTRUST Network1.0,..U...%USERTrust ECC Certification Authority0v0...*.H.=....+...".b....TZ..h#.z.$oS.Z.K.....sq....a.....W..]?.!....y.~-..a...%.c..0..p..3...\S._.}2..4.yy...0..0...U.#..0.....#>.....)...0..0...U.....:.....vtlv..5.cc.0...U..... .....0...U.....0....0...U. ..0.0...U. .0C..U...<0:08.6.4.2http://crl.comodoca.com/AAACertificateServices.crl04..+.....(0&0$..+.....0...http://ocsp.comodoca.com0...*.H.....,, ...B.r..2...u[,..)@m..r.....=.rB.P..9.l.....u+..V.....|..9...ds.F...#.....3tv;(L..B...#B..zuj..|.g!.3:9mS..b"...Ul.lCk.....iwl..M...x...../.B;.t.H..l....^..gG.....(.J.D1&.7..t6..".tI.....)... ..._...t.....c....x.n..

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\4CA77D36767B6202D4786BF3D1EC5242	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	2.9642397348892784
Encrypted:	false
SSDEEP:	3:kkFklCxX3lXfllXlE/nCzsl/dllelzR3N2verH+Ot1Wv8+u15lsdlynl8sLFl/:kKdxWCzx3N2veVtcE+IIndO
MD5:	E314B3F0B7AB0FC87643843C056A2DDB
SHA1:	9F638425E588633CC93D2D65843A1E8BFBA58ABF
SHA-256:	8B8BD0097C97DD666C647A4C0E2C7A4C6A93327DA3C14780E5FF5185DEAF5BA1
SHA-512:	FB87BF2E7D9E46D5FC84BC78B629606E1B1AC27EE85431DA2CE55E1B0B0EB3A7346D0FDA65F7C0549F66EE2FB3932D235EE849B64F983FC59C082CBAF3FDDB FB
Malicious:	false
Reputation:	low
Preview:	p..... ....T....h.kT...(..... .....B.....(.....h.t.t.p.:.//.s.s.l...t.r.u.s.t.w.a.v.e...c.o.m./.i.s.s.u.e.r.s./.S.T.C.A...c.r.t..".3.b.c.-.5.b.3.f.f.3 .1.8.e.6.0.4.0."...

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):	652
Entropy (8bit):	3.1229696180105786
Encrypted:	false
SSDEEP:	12:GkPlE99SNxAhUegeTCjkPlE99SNxAhUegeT2:GkPcUQU76CjkPcUQU762
MD5:	D9AAD824A5DF18D844CA74033CE5D517
SHA1:	B7D22592754D9781B46DF8E2132830B6CF146699
SHA-256:	3F54FFC4E00C6E46B3A94D4CD3327BB235FE4650DDD2D1F417719764E2EB4D3C
SHA-512:	CC26857106D2AD38490662C4624DB45B0133687622E83CC93E5B6A2C9D7791EE02A00CF9055168A736175E273333FE6790B352B454BA8B143F75840F9AFD5CA6
Malicious:	false
Reputation:	low
Preview:	p..... .....K.kT...(..... .....Y.....$.....8...h.t.t.p.:.//.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...p..... .....kT...(..... .....Y.....$.....8...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...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\8A4AA6A226E1870F0261713C59F1CB84	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	250
Entropy (8bit):	2.9792482755074907
Encrypted:	false
SSDEEP:	3:kkFklNlJY3lXfllXlE/lQcjxlzR8tlwiANjpU+plgh3Cfax3QbaLU15lqErtdYll:kKNEQMlLjMulgkfaWbLOWw/
MD5:	5A4BAA745A5071FB014AB551BAB0D498
SHA1:	05E5BEA26D56C6E160FD10B61F849E2EAFE2D8DB
SHA-256:	94AF632A0BB4D7519970AEC3123A551FBFAF616795A26C554788B4AE681232BB
SHA-512:	D3F36C4112AA04F0D9F16A9CE81020586BBAE5545725F12EE46671083184D38F113078289EBC80837CB40010D3D8C9AFB7B1FEC93650A90ADB8F84B4F4A32A3E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\8A4AA6A226E1870F0261713C59F1CB84	
Preview:	p..... ....h....GxmT...(..... .....(.f...@8.....h.t.t.p.:././.c.r.t...u.s.e.r.t.r.u.s.t...c.o.m./.U.S.E.R.T.r.u.s.t.E.C.C.A.d.d.T.r.u.s.t.C.A...c.r.t...".5.c.8.6.f.6.8.0.-.3.d.7."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\1e19f240-83e3-43b8-bf7e-3a23997053ec.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	160448
Entropy (8bit):	6.084177568922665
Encrypted:	false
SSDEEP:	3072:1uK/JowiK5POmR8DsYYlhFcbXafIB0u1GOJmA3iuRA:NJdRMmynYlvaqfIlUOoSiuRA
MD5:	1B88F0D6FC5452B5D14CFC43A75F586E
SHA1:	092D3216137D16866DB9AA65619EEF8CCCE75096
SHA-256:	E08FFE6AA3D91FC6F65581ABC9EFAA4C4EF97FF730CED86D57116AF55E060A1F
SHA-512:	6A2E349241853076983B056AD3EFA34A1DB489D8373A19AA79A616D1CD398DED4EAB265F2C986EC7FB678C8A14F055CD8BCAA300545379EF7A5F2D2E5A35FC9
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":1.60698674374801e+12,"network":1.606986746e+12,"ticks":304171919.0,"uncertainty":4454872.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715948744"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\4d4cd37a-710c-412e-9967-e967ed072066.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):	160197
Entropy (8bit):	6.083805317576096
Encrypted:	false
SSDEEP:	3072:3JPK/JowiK5POmR8DsYYlhFcbXafIB0u1GOJmA3iuRA:5OJdRMmynYlvaqfIlUOoSiuRA
MD5:	57D34176B555CCAEDF7F3FD51E45CF1C
SHA1:	8A3DCD87CE1F9C96176194E0FF032C4CA2FCAFA8
SHA-256:	A783CF27CCE187D01F1B98EB619794965EA6592BB6AFC101E07D25E7975944E5
SHA-512:	9AACF8AC946D410E3196A5C7E24291CABE290455D7CCADA983C977FBCB34584387F470B54297749831667053C08FD42B6F86D24E47B5D39B5CD2B052480E1A6
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":1.60698674374801e+12,"network":1.606986746e+12,"ticks":304171919.0,"uncertainty":4454872.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqlYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\5cc7e8e1-2f79-40af-8564-a4461458fd29.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):	160448
Entropy (8bit):	6.0841788731354685
Encrypted:	false
SSDEEP:	3072:17K/JowiK5POmR8DsYYlhFcbXafIB0u1GOJmA3iuRA:EJdRMmynYlvaqfIlUOoSiuRA
MD5:	F7AD2633168C05343C7706891F212AAA
SHA1:	04E46E5D46C1235C97B1A216144CEE6A6C27994E
SHA-256:	9975D4DF9DDE59A6FE2186D7E53C7F508164E569D4FC2B31C7FE5883F49152EB
SHA-512:	E6DC269B28A0034A44C21B7F891201F175DADA690AD2874CAD92B4A30D2CC75A506743A7AB56317AA4FBEF1173A305125136244BC7C4DA400B2FCF1826F92F5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\5cc7e8e1-2f79-40af-8564-a4461458fd29.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.60698674374801e+12,"network":1.606986746e+12,"ticks":304171919.0,"uncertainty":4454872.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715948744"},"plugins":{"metadata":{"adobe-flash-player":{"di

C:\Users\user\AppData\Local\Google\Chrome\User Data\6e5c85c4-1af5-42d5-8d94-1e4b83a53ece.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):	160197
Entropy (8bit):	6.083804491539982
Encrypted:	false
SSDEEP:	3072:3UnK/JowiK5POmR8DsYYlhFcbXafIB0u1GOJmA3iuRA:EWJdRMmynYlvaqfllUOoSiuRA
MD5:	A4F6DD5E86BE3F4575DF688BEA155BAC
SHA1:	2AF062F841D2266762ABC7A048D0CF14A7D3E7F9
SHA-256:	4495B5D0C1390A939B30D3766AC981C34F182AF2416714FA3D41B374F3E830D3
SHA-512:	E14605BFB64377228D044BA4D8369423127D8C94E46274B85DF2E2087BD71E9FB25717F0AE93713186C97FBD23B2D07B36578AF20F56C45D1E1FDD47A770882D
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":1.60698674374801e+12,"network":1.606986746e+12,"ticks":304171919.0,"uncertainty":4454872.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABaHlwIoHYlQKZwuwW8V0yxAAAAAAIAAAAAABBmAAAAAQAAIAAAAOT4j8Zm9U1zXX6oEUpPqIYBIjSlOiLGeiMKiIFJZDroAAAAAA6AAAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMTt0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245922715401452"},"plugins":{"metadata":{"adobe-flash-player":{"di

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:	19B28BFE66708B294AB033C2F87D219E1C29D4F9363AC92E89B9406F6E2ACB13AD5DF73DD7E163D1ADEC0AF89C42DA112AE153EB23378EC29302F91192B7C59
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\007a3b44-1984-454c-8d87-9c314ae983d1.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
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\013c7a64-f2b3-4c9b-9f84-de192776af0a.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):	5726
Entropy (8bit):	5.167908757624649
Encrypted:	false
SSDEEP:	96:nlOg04KOQHIV85k0JCKL8Ank91JbOTlVuHn:nlOB47kIGh4Kxk9B
MD5:	517DF8884BC210A9E1950F7B7C6986E3
SHA1:	322FE8600589B729C9F31F292FF7CEE6F842E920
SHA-256:	3A743FC9891C49FE9ED8E3C53E77219E028B074E1C9CD06C9A6C43A961DBF728
SHA-512:	CAE33CE4C0BFBFED01A5058CD6219B44B18329AA68B3C3381858F5E1E7600039F14893E3A1537139E6E643E24797A98359F48FA4F009EC3D52959BCCDC8DFA9
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13251460341162165","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":{"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","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\166e634c-4e94-4c1f-9a19-3f237303d6b3.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):	16763
Entropy (8bit):	5.5775423392708445
Encrypted:	false
SSDEEP:	384:KZDtKLlNPXg1kXqKf/pUZNCgVLH2HfDQrUg+bb74Y:3Llxg1kXqKf/pUZNCgVLH2HfcrUl7P
MD5:	4AD0A7C56FC6B11089B3C6B42346DE3C
SHA1:	A513A269668252E746B3D0A21A3E54794BE106A6
SHA-256:	C1E05F2CBFABED690A4AA1FADB1B2D3A53BE418CD81496D1BD297226BBA3562E
SHA-512:	8D376EBB7F165A2A58A7260A103F85ED7E9781C7A520D196DBD8DA817F7C08788184A28ADEB32C069B30CB18E4C65D857279B75C02307DED2D48BB48BAC8AD 7
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":"13251460340969004","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2624f128-dddd-4093-b5b6-01e7b27a72f4.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):	12188
Entropy (8bit):	4.900402340009727
Encrypted:	false
SSDEEP:	192:JzMKxDHXTz6VFODk8gXr1iJh/9Ucn6UQ55siJoXe6fLut5V3K+0ibBFznLWa+umZ:JoKx7XTz6VFOo8gXr1Yh/9Ucn6U82iJC
MD5:	191FBEC3C81E59ACD97C0318007A575C
SHA1:	FC52431ADF050FBD2B0F117F76FF542A03FE220D
SHA-256:	B6F5A35DD1A36D77FBB8CCCD130B483F6173F7A1CBAC3A8ACA96E731BCE95445
SHA-512:	CD86BE04D4FB519CFD031F312F766D33F26BAF68CB1072F911696E875755DECE86A63708140C851A6F3C6CF0AC5F3994313666A2F49AC005BC9E7876D6B1410E
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://fonts.googleapis.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://btloader.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13254052346876540","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://stats.g.doubleclick.net","supports_spdy":true},{"isolation":[],"server":"https://u.openx.net","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13254052348712551","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://c34edbe947c918439ed24a

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2903f021-3e38-4332-9206-18bbe61c39f4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2903f021-3e38-4332-9206-18bbe61c39f4.tmp

Category:	dropped
Size (bytes):	22620
Entropy (8bit):	5.535384756212785
Encrypted:	false
SSDEEP:	384:KZDtPLlNPXg1kXqKf/pUZNCgVLH2HfDQrUtHGOnZI+8R748:YLlxg1kXqKf/pUZNCgVLH2HfcrURGOnc
MD5:	53E1FB61FAEA6E72EE47C211A5DFDD07
SHA1:	D0A67B5F369C1ED027F625052A5B9356BD6BB7BE
SHA-256:	19C9B38CB0F00063DBBA904E8A6124806B0B493CBCFD0A5C539381E9D26114B7
SHA-512:	8B5A61D8640DB220F6AF5BD68AEDD6649077D2A9E711E5D60ED7A0B794D0FF8632D9A8C603952E3F44981CC6B006B3F960F0687909AE974417418C5C69748C66
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":"13251460340969004","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4ad1d1dd-c9e3-4f1a-9f45-30703f698a72.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):	3553
Entropy (8bit):	5.600982244932505
Encrypted:	false
SSDEEP:	96:7UqUQUTUPUneUPkieUOr5sUjUU2UcUvUAKUzweUlUGPeU3UDUZUFUqUd:7UqUQUTUPUneUP0UOr5sUjUU2UcUvUAu
MD5:	E00A5A204E053A9C8D3E772748581E61
SHA1:	BE5B9B2C0AB07A1C8798F11F212E8001B6368BD2
SHA-256:	F8AF464EC4E65E5E2A3AC5737D78EF41FF6A7ACE2F6238D3F99FE5A5580523AC
SHA-512:	A117870F3C8AD246DF90DE74DEF6A28228B4852604934CC6AF4AFD8B5CBE502BA3CA5DD5A377BF1CB373517E37BC69A9786F89CDE908E0071B5327F108FD21I8
Malicious:	false
Reputation:	low

Preview:

{"expect_ct":[],"sts":[{"expiry":1622754758.606976,"host":"BBOugrewRBSrzXkoKc6fle0sVpb0Ep+WZj0hzmox9d0=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1606986758.606978},{"expiry":1609578749.881558,"host":"Dg14fIaciUHGX6Lc+OnYmaNiAA/ADiwumtIyPrC3d6U=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1606986749.881562},{"expiry":1622766746.164556,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1606986746.164559},{"expiry":1638522760.896578,"host":"HGgWuImG7OKoFG+SVLyzGa2Q/Pc92nvPSMCzgHENRl0=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1606986760.896582},{"expiry":1638522762.524955,"host":"Hi4bEdMq563Qsqn4sVyUls/uVk7U80lxMa3wyWVUqWU=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1606986762.524959},{"expiry":1617873146.876595,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4e9b0eca-7e36-4a6a-9c1c-d02014ff249a.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):	5699
Entropy (8bit):	5.165223508906853
Encrypted:	false
SSDEEP:	96:nlV04KOQHIVl5k0JCKL8Ank91JbOTlVuHn:nlm47kI7h4Kxk9B
MD5:	81C6060A5D80DD617627440A8B149514
SHA1:	D0C734B449B166C0F3F99B287A0DAFC72CD045C6
SHA-256:	522CCBD0CC343CC1D763D161C5D5479E5ED112B6DF94F0C866A0E9E443F1FD6D
SHA-512:	E6A6AE01E398176C9844C4CAA50B7514C8B41FAF0BD414B1DCEF90BFE7DD37F25706CDCE4ECCFABF3DED511EF74ECF3CAC7AFC9A5CF89D41A2A77F7731CIBFC1
Malicious:	false
Reputation:	low

Preview:

{"account_id_migration_state":2,"account_tracker_service_last_update":"13251460341162165","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":{"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","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\54e21646-27f7-4688-a8fd-abebf52ecd8a.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\Default\54e21646-27f7-4688-a8fd-abebf52ecd8a.tmp	
Size (bytes):	4559
Entropy (8bit):	5.600706722692137
Encrypted:	false
SSDEEP:	96:7UqUQUTUPUoeLUveUPkieUOr5sUjUUAiUtUhyUfUvUAKUzknUfZUHeUlUGPeU3UF:7UqUQUTUPUoeLUveUP0UOr5sUjUU5Ut7
MD5:	3808B3AC2DC0D4D781FBDDFCC7D0D19A
SHA1:	950DAC938C66D31B7913EB6E779DF1CD7073AEDA
SHA-256:	7A0C99124BE8A16D66003AFBEDCCE1EBAACF466950185E8DBCA05945ABEFBE06
SHA-512:	D2995BC1C5325DBB0AB47BC9924058D423B8A6EDDE6891CB02F1BCF4836A37F7DF58FB980F71B7A0FA2E85F5253EA2E626D8C48CC7E2CAAC4735A520D9002D B6
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1622754758.606976,"host":"BBOugrewRBSrzXkoKc6fle0sVpb0Ep+WZj0hzmox9d0=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1606986758.606978},{"expiry":1609578749.881558,"host":"Dg14fIaciUHGX6Lc+OnYmaNiAA/ADiwumtIyPrC3d6U=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1606986749.881562},{"expiry":1622766746.164556,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1606986746.164559},{"expiry":1638522760.896578,"host":"HGgWuImG7OKoFG+SVLyzGa2Q/Pc92nvPSMCzgHENRl0=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1606986760.896582},{"expiry":1638522762.524955,"host":"Hi4bEdMq563Qsqn4sVyUls/uVk7U80lxMa3wyWVUqWU=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1606986762.524959},{"expiry":1638522788.602925,"host":"I/1WWzGC3ORCzIiApYPQWeHZLoi50Q2mdlTs65nBysI=","mode":"force-https","sts_include_subdomains":false,"sts

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\61f03a8e-959a-4e65-918a-a75537b1564a.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):	4726
Entropy (8bit):	5.6010461652524945
Encrypted:	false
SSDEEP:	96:7UqUQUTUPUoeLUveUPkieUOr5sUjUU6UqUhyUfUvUAKUzknUNcUNZUHeUlUGPeUH:7UqUQUTUPUoeLUveUP0UOr5sUjUU6Uqi
MD5:	BB2FC3DCB374776429A1B4613AD2AC65
SHA1:	FA95A5F3500B5E8E984100AD715373EBC28C4515
SHA-256:	800A836E5D9FD97FCA39FF1CB184620327E45634C792E694F43489C95ECEC9C1
SHA-512:	674A53AF8BF7BB75FBBDDD4C7D8F6C31047DC0FD18CFE847472B784B2B4CA41E9B6427B2CD9DA5BAAD3471922625D9E79437C585F13CE6392E008A06138BC5 A
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1622754758.606976,"host":"BBOugrewRBSrzXkoKc6fle0sVpb0Ep+WZj0hzmox9d0=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1606986758.606978},{"expiry":1609578749.881558,"host":"Dg14fIaciUHGX6Lc+OnYmaNiAA/ADiwumtIyPrC3d6U=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1606986749.881562},{"expiry":1622766746.164556,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1606986746.164559},{"expiry":1638522760.896578,"host":"HGgWuImG7OKoFG+SVLyzGa2Q/Pc92nvPSMCzgHENRl0=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1606986760.896582},{"expiry":1638522762.524955,"host":"Hi4bEdMq563Qsqn4sVyUls/uVk7U80lxMa3wyWVUqWU=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1606986762.524959},{"expiry":1638522788.602925,"host":"I/1WWzGC3ORCzIiApYPQWeHZLoi50Q2mdlTs65nBysI=","mode":"force-https","sts_include_subdomains":false,"sts

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6b5f50f2-550b-4444-a898-42ae527ad4fe.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):	5102
Entropy (8bit):	4.955200766962195
Encrypted:	false
SSDEEP:	48:YcSAkMkli4qAORqTlYGlQuoTw0irN4MqM8C1Nfct/9BhUJo3KhmeSnpAnk9Jb5G2:nlLt4pIVQ5k0JCKL8Ank91JbOTlVuHn
MD5:	37EA574E414CAC056B7B30BB622F2D6F
SHA1:	E63E6E05FE72226882B5424B269FDF59FC5EDB50
SHA-256:	EF5B0BCC7DEF11A4D7F5D01F750907791B16D8CDA56DEA8B4A6E2484405AA887
SHA-512:	A11B158630FA53AD4F3D848E01C536269D9E593658CC14CF60C354386D1B34409EA4E861762EA1361B7E0D960DC7B7BCAF718573D7BE78A9B6B99E546CA4BE5 C
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13251460341162165","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":{"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_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8af65672-2f2e-44a4-a262-df5f0223930f.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8af65672-2f2e-44a4-a262-df5f0223930f.tmp	
Size (bytes):	22619
Entropy (8bit):	5.53562191150879
Encrypted:	false
SSDEEP:	384:KZDtPLlNPXg1kXqKf/pUZNCgVLH2HfDQrUtHGDnZI+8k74mA:YLlxg1kXqKf/pUZNCgVLH2HfcrURGDnc
MD5:	9014F385BC7B531EBC3DB4EDA9C33AE8
SHA1:	C0D362D73A693E4A7058559880D6D2E831BAAD21
SHA-256:	ADC4575E33CA42CDF85761FBE3FDD0E142B80D57DD2B4F51377EC805EA7A9D6B
SHA-512:	44C4AF7F1AACDD68A1C18F91B76EECF04B4529563DB6AA3F7A8A4CF3495647900C6780C88E80576E14CE347D114635E7D3351284AB0513B65836474A24D5FEA
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13251460340969004","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\99d8f14c-9c82-472e-96a0-0ceb3cb19fe3.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):	5102
Entropy (8bit):	4.953741608945042
Encrypted:	false
SSDEEP:	48:YcSAkMklirqALRqTlYGlQuoTw0ir74MqM8C1Nfct/9BhUJo3KhmeSnpAnk9Jb5G2:nlw04pIVu5k0JCKL8Ank91JbOTlVuHn
MD5:	F9B90D67CF0244CC7C61A0A4004D4FA2
SHA1:	D190C905055725680BBA2B2DC7999BDDA4AB9362
SHA-256:	7F2A9A5A9491894D7A8E60E91CAA120A7FC21835DB307FC176A3CFF2F42006E6
SHA-512:	7745BD75E2422613197237580895E01CBBF504510E1C6A1AB163BB47EAFFA810DDAB788C4F0A34EDB6D259DB01D28E024F6DF8B8F8573EF9C4B5D58CB6FFF12 E
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13251460341162165","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245924509391818","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"bookmark_bar":{"show_on_al l_tabs":false},"browser":{"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,"d ata_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","2042016"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0"

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9f149523-671f-49a6-b0bb-276ad9c5fbed.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):	4727
Entropy (8bit):	5.59969314304794
Encrypted:	false
SSDEEP:	96:7UqUQUTUPUoeLUQeUukieUOr5sUjUU6UqUhyUfUvUAKUzknURcUNvZUHeUlUGPej:7UqUQUTUPUoeLUQeUu0UOr5sUjUU6Uqz
MD5:	BE8C71A1A23DE03B045FA16B604109D7
SHA1:	4445E2D3F2DDB765540D07B64014D9C40150BF24
SHA-256:	1BBA7E022937A07A7660D0E2DF0DAA4F34BFADDC55A7BE3CF58CFD6B6AA1D725
SHA-512:	731FC8C3CD9E6479340D83E1D44F9239F7FD69FEC7D8170C49D734833F054E58B75C4B043F252DD7E5CF0C13444C82722D5E756458BDA54E6204F74AFE8B961
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1622754758.606976,"host":"BBOugrewRBSrzXkoKc6fle0sVpb0Ep+WZj0hzmox9d0=","mode":"force-https","sts_include_subdomains" :false,"sts_observed":1606986758.606978},{"expiry":1609578749.881558,"host":"Dg14fIaciUHGX6Lc+OnYmaNiAA/ADiwumtIyPrC3d6U=","mode":"force-https","sts_i nclude_subdomains":true,"sts_observed":1606986749.881562},{"expiry":1622766746.164556,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=", "mode":"force-https","sts_include_subdomains":false,"sts_observed":1606986746.164559},{"expiry":1638522760.896578,"host":"HGgWuImG7OKoFG+SVLyzGa2Q/Pc9 2nvPSMCzgHENRl0=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1606986760.896582},{"expiry":1638522762.524955,"host":"Hi4bEdMq56 3Qsqn4sVyUls/uVk7U80lxMa3wyWVUqWU=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1606986762.524959},{"expiry":1638522788.602925, "host":"I/1WWzGC3ORCzIiApYPQWeHZLoi50Q2mdlTs65nBysI=","mode":"force-https","sts_include_subdomains":false,"sts

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):	334

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Entropy (8bit):	5.181489425048587
Encrypted:	false
SSDEEP:	6:hsWfiN+q2Pwkn23iKKdK9RXXTZIFUtwssWF2FZZmwyssWF2FNVkwOwkn23iKKdKT:Ja+vYf5Kk7XT2FUtwEF2X/yEF23V5Jfv
MD5:	324E5A12EBE357F712196DE11C1F2D69
SHA1:	A83C089D484CDDD654A560B1BD28A0458C1365FA
SHA-256:	51B66B7378ADB54EFF469C1C0AC35544218294090A5AF57B2A5ECB602F430224
SHA-512:	897D2754407191EB41DA25267BC83B6CAEB355D259123049A38FEC5864849250E441102F80AF3EF89D5B380AECAEA2E5DEA5287BDB212687A9AB3F1301A5879F
Malicious:	false
Reputation:	low
Preview:	2020/12/03-10:12:43.084 24dc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2020/12/03-10:12:43.086 24dc Recovering log #3.2020/12/03-10:12:43.086 24dc 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):	5.1470224171486
Encrypted:	false
SSDEEP:	6:hsWiq2Pwkn23iKKdKyDZIFUtwssWjeXZmwyssWVkwOwkn23iKKdKyJLJ:JivYf5Kk02FUtwEjeX/yEV5Jf5KkWJ
MD5:	003817162FBAE9A456259A24E0AAB558
SHA1:	92DCA3CBC32EB692B7FF2A2DA0BBA49668E332EA
SHA-256:	EACAA5B75C77EC16525B8FAA16BC3C45B4AC470123E60C0F98498E77504CE023
SHA-512:	50CAA1EBFA045F5577ADF215321D12E864A326AFFFFFD47FE48A1E13B2108880083E4401ABADB6E56C1EB7BF0E1FDB1B10E1BD51D73EA8ED5DBA26201539DAED
Malicious:	false
Reputation:	low
Preview:	2020/12/03-10:12:43.160 1bd4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2020/12/03-10:12:43.163 1bd4 Recovering log #3.2020/12/03-10:12:43.164 1bd4 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\02920c9647a0fdc3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2264
Entropy (8bit):	5.4033362685240744
Encrypted:	false
SSDEEP:	48:GN4Jy/wsWm1pQI3yAgPLKrA9ipj+igQ/HqECW5:GNMy/wsWupQI3GWxj+igQ/7j
MD5:	AF4B79C047421059BED249CC513FC873
SHA1:	1B52AA53D4A30673B99FB258F9067515EBACDC03
SHA-256:	42A7E3E00383DFCA264594E77904B7F524DFBF8F68049A734AFEC03BD4AE4F57
SHA-512:	D178994894F7DE50367372E5D2721B6600241E934E0F88EA4F150A80B2168723BB003A8DCB19457527B29820CC1A32D55425D5462431E57D3520C5478A8E5CB8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.....P...._keyhttps://pastebin.com/assets/54b66ebb/js/select2-krajee.min.js .https://pastebin.com/*..."./.....%.....7..Rm.=.x....hT...(....?.uo.A..Eo.....N>.....A..Eo.....*..."./.....'.l.....O....x....S8.....(S.h..`.....<L`.....L`.....Qe.....initS2ToggleAll...Qd.....initS2Order...Qe..y.....initS2Loading.....Qd.....initS2Change..Qe..H,....initS2Unselect...(S.....a`...d....E.@.-....LP.!.....=...https://pastebin.com/assets/54b66ebb/js/select2-krajee.min.js...a.....D`....D`....D`.....x...`8...&...&....&.(S.....ay...}....E....d.....&.(S.....q.a.....E.d.....&.(S.....a.....E.d.....&.(S.....A.a.....E.d.....&.(S....`.....,L`.....Q.@2..[....define....Qb..s.....amd.....`.....M`.....QcR.!.....jquery....Q.@.P.....module....QcZ.;N....exports...Qc..C.....require.....Qc..dm....window....Q.@..g....jQuery....K`...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\056c7341c0a0787f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.6344571409691495
Encrypted:	false
SSDEEP:	6:mwXXYH5PLHmfxMZJZwltgdjMGiU2fkH4b5tbK6t:lW5boaXwXgdjHckCtN
MD5:	353430B27F7DD168AC64AEEFE1B65390
SHA1:	DB666374F6472F96561ECAFB2736E77ECFE4B957
SHA-256:	CFC0BC938CB6C2EEDE7C383B34988AAB5DCE45E2A11CFBB3CA7BE4E4CEF64AE0
SHA-512:	0F8ED873F1BF7BBD1B832327A4A97D05D7B5FD06B4905843F018DB19A0E30FB39E5CA18202A44336772B18F78C108A5D1F628D10975E839FC8ACFA35FFF80CD
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\056c7341c0a0787f_0	
Reputation:	low
Preview:	0\r..m.....h.....G...._keyhttps://abs-0.twimg.com/login/base.7ced3ee3ff61dadf91a9c9bd7082adc8f158a360.js .https://twitter.com/=.5."./.....R.....-I.;@$y.L-.....a)#(3n.. ..(SZIV..A..Eo.....z.;.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\06637864d920d6f7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.905600225531717
Encrypted:	false
SSDEEP:	6:mpXYGL+MIwJJaKo5CygDDIKb1Br/8DK6tNK6DJjRtMfaIKb1Brh:glwva5cXDsaG137W/a
MD5:	97297F820DE5F3CF16D7AABA07199281
SHA1:	AFBE1A40DD64937308F5A9B11932FFABE672C1E2
SHA-256:	02B46A0E35790F37D914AD6EB81DE1CD89E34C88E367DB6630116C892E0475B6
SHA-512:	25355463630D9E771215043C386EDC4ACBFDE82C65C5AEFF5F616D49E419D9935533E9BA5946C1A76D265A7D3260647A547F104DD002DCF2C30DBD232C428A0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H....{....._keyhttps://www.google-analytics.com/analytics.js .https://pastebin.com/...."./.....W.....g...v....$..lE.R9...x....+J.A..Eo.....A..Eo..... ....."./.@"..F3518CFB7854036E5EE3FE896491BA14743028034CA4DFBAD6FF0F8241E9EA90....g...v....$..lE.R9...x....+J.A..Eo....."..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\07e7c48acd14fc16_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.4322889272769554
Encrypted:	false
SSDEEP:	6:mM36EYoK2hVH4/VRKIpQJt+XzBbY6hK6t:zK46wKf7
MD5:	F0852971607B044C26BF5341B3B0C785
SHA1:	3288E7FA9FAB9C42F6CA806292ABB8E2D084525C
SHA-256:	5AD377BCD7C71AE10713351B6299B6718BB2C91A9CAC247502F62EC5C1113C1D
SHA-512:	58CB938CAAF2C9AAB53792675C22D22A8F7A935FD7DB50CF399458A86D43313B4442C0E4B436524032BE639C1D7C77A090336BB320A657DA19C7D652FB83C27
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N....._keyhttps://pastebin.com/assets/1745bc3b/yii.captcha.js .https://pastebin.com/...."./.....gJ.....,:T.4u#."....}.v.J.WZ..$.'.A..Eo.....k..q.....A..Eo .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0f9a200ae7ca6f25_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	24140
Entropy (8bit):	5.643347571561368
Encrypted:	false
SSDEEP:	384:6vdrV1Wv/AcGPWus1cGSs+pRtkaNfrcN6x61ZlvA99:6v3kv/FGPWdhSHKaNfrc0017499
MD5:	F3E5700A5F5AE46D40E60D0FFB2E3415
SHA1:	B1AC0F5C6B2B33A2B6B4B6A353D8268E75BD687A
SHA-256:	B9D3BB4C33C0F530E66261C28F801F0833338A4947A0DDFD923A7E1C09CA6BAA
SHA-512:	2CC8CE84F6E7EBF932183B67D5A9761F54BCF4357E9E29169ADE587103D7CE88FFA13797EE375D7EE526B23462F92DD0CDB02DAF6F0B9C0683B203D7BD95EC A2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L...0..*...._keyhttps://tpc.googlesyndication.com/sodar/sodar2.js .https://pastebin.com/..../.....`7.d..9.q\.C.pM;Q....-.Z..X..A..Eo.....,r".....A..Eo... .....',?....O....\...2.....(S.<..`2....L`.....(S.u..`.....L`.....RcJ.....Qb.....aa....Qb.*w....ba....Qb.!n.....ca....Qbn.....q.....Q b.g8.....r.....Qb.B.....t.....Qb.A;.....m.....Qb.Q.....v.....Qb.?8....p.....Qb.....A.....Qb..Z.....C.....Qb.H.....D.....QbB..Z....E.....Qb.$.}....F.....Qb.j.....ha....Qb>.&.....ia....QbR..... G.....Qb.....H.....Qb..$.....ja....Qb...4....I.....Qb._hY....ka....Qb..OU....J.....Qb2.m.....la....Qb.%.}....K.....Qbf.....ma....Qb*.|.....L.....Qb:.....M.....Qb..h.....O.....Qb..q....na....Qb. oN.....N.....QbfK.....P.....QbR..X....Q.....Qb.b.....U.....QbF.....V.....Qb.O.....pa....QbV.y.....qa....Qb..X"....sa....Qb.z.....ra....Qb.....oa....Qb.i4.....W.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\116f16bda2dcabee_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\116f16bda2dcabee_0	
Entropy (8bit):	5.673354930574723
Encrypted:	false
SSDEEP:	6:m6lXYk+f2pomWmnKlJKHjfLhmJ2mlvYpXDrvHygEm4dK6t:FN++amulJKHjfLkJpl4vHLj0
MD5:	A97612752C58D4463134B5F6DC18548B
SHA1:	BC09679A5B0F72FFEAE803FEA1401B9730645EE6
SHA-256:	C575A6219D96C794C85BD649478EA43409F469290CF60BD71EF4C4762D75FC2E
SHA-512:	1637854CC3D00159CE219E0990F7ABCBF6C4FE72B6D8A4036A65483DFFA23656CD93C812757D86E674CB30A3A0F784D37DF906E48B9EC234C440AD0094D77D1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....iYh...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3ivjG4/yB/l/en_GB/WqGe59t5V9c.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...."./.....HE.....8.. .TG.A.D.H..ac!j.....VFo.....A..Eo.....3AQ.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\11a305796880f718_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.801713733913515
Encrypted:	false
SSDEEP:	6:m7PYGLSqfJPnRKw/iUKGnzrfHK6tmlSmkgNnGnzr:IxvRi+zLJAlSmkCGz
MD5:	766F76FE708069723C762268E676DFF9
SHA1:	861F1FF90A10F53E2585716DF87B9EE872E7474D
SHA-256:	F6190370BF68AB28A7BBD6C0203A7C82BF3FE7EC2D0A20FE9D94B0F948A1703F
SHA-512:	1823EC56D79A08602694704B5CC33AABFD55DBCB6D73166D682BB9E6AFA8250CA7B35EFC5AD1E2395EEDA6D3B08AF386D2BE82EEF293EE89290A22BF0D62C 4BB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J.....E...._keyhttps://www.googletagservices.com/tag/js/gpt.js .https://pastebin.com/,O..".//.....m.....m..1.Ez..C'.K.md..o.....I...A..Eo.....D.....A..Eo..... .....,O..".//..k..7FE7E78F69CBF79B3C48FFFF5EA179F40C5C324B187E5B3895C0A12F3EC034BE.m..1.Ez..C'.K.md..o.....I...A..Eo.....s.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\182f2026d29d0de8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	74472
Entropy (8bit):	6.052048644969269
Encrypted:	false
SSDEEP:	1536:TffQJpFRtYanlmjDjY61YehxrhuuI8lTg6EA4ef5mHY9nj5E:DfczSanU/jY61zldlEgm/IY9nm
MD5:	E2B65359625C95E9F16AB48B80B516F2
SHA1:	370861FAAC1E55BF3178F43D7562ADDFE9DEE6A3
SHA-256:	9D169D927CE93208D18F103F9AF5DC9BD448C898F037647547D167A04CFEC3FF
SHA-512:	1C43C8D4AA194134F8BD46D4B69A9B0F5D4F5996D8BE8878FB4B20F6BD9A275E0E38230FCB6F532CF3AAAD5083C6E95C4E9A660E9F107921DD9668213D7C2F5 A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....?.#....F3518CFB7854036E5EE3FE896491BA14743028034CA4DFBAD6FF0F8241E9EA90.....'.....O....!..v.....4..... .....(S.D..`B.....L`.....(S.a..`|.....L`b....}.Rc.....T.....Qb..!U....l.....Qbn.....q.....Qb.g8.....r.....Qb.B.....t.....R....Qb.Q.....v.....Qb^..M....w.....Qb..+.. ...x.....Qb..0.....y.....Qbz@.....z.....Qb.....A.....Qb.H.....D....Qb..Z.....C.....QbZo.....B.....QbB..Z....E.....Qb.$.}....F.....Qb.....H.....QbR.....G.....Qb...4....I.....Qb..OU....J.... .Qb.%.}....K.....Qb*.|.....L.....Qb.oN.....N.....Qb..h.....O.....QbfK.....P.....Qb:.....M.....Qb.!n.....ca....Qb.c.....da....QbR..X....Q.....Qb..T....S.....Qb.D.....R.....Qb.m1.....fa.. ..Qb.b.....U.....Qb.n.'....ea....Qb./X.....T.....QbF.....V.....Qb.i4.....W.....Qb..3.....Z.....Qb.u;&....Y.....Qb2.....X.....Qb.....aa....Qb.*w.....ba.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\18b9130c1e45de41_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1972
Entropy (8bit):	5.486302011970915
Encrypted:	false
SSDEEP:	48:X8Pi/dX98ezEdg0y8PdieZBhgEKXBKMwASV5gaM4AY9ecOi:XGirSDyGxiIZ5gT4Auei
MD5:	A55FAD0CFC215A153E27D10151E24E88
SHA1:	7F2AC537764B0472D31CD4D50519CCA358721571
SHA-256:	7840ABF8A5262DAC12B4493999E071D259D3F96A39EC100929F1586F287FBFEC
SHA-512:	CE80F98B031B3622252022487FCB06D0A1528CE993F110483A321660638A5FF80E03CF57D1CBC255669ADCDD33B123A95BC95F20B9EC71FFC92C792E8E0CEDA
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\18b9130c1e45de41_0	
Reputation:	low
Preview:	0\r..m.....l...$..p...._keyhttps://cdnjs.cloudflare.com/ajax/libs/codemirror/5.58.2/addon/mode/simple.min.js .https://pastebin.com/y..."./.....1h...K.8%\|5...i.....B.j.K.X..A..Eo.....Y.....A..Eo.....y..."./.....'.....O....@....-{.....t.....(S.8..`(....L`.....(S.t.`.....(L`.....Q.@Z.;N....exports...Q.@.P.....module....Qc..C.....require.. QfZ.Y...../../lib/codemirror..Q.@2..[....define....Qb..s.....amd.....`.....M`.....Q.PN.....CodeMirror....K`....Dw.....s.....s.....&...&.]...&.]..../...s.....&.(.....&.z..%&.^.....&.]....(Rc.....I`....Da....r.....e.....`...p...0.....@.-....`P.q.....Q...https://cdnjs.cloudflare.com/ajax/libs/codemirror/5.58.2/addon/mode/simple.min.js...a.....D`....D`:...D`.....P...`$...&...&....&.(S.d.`.....0L`.....XRc(.....Qb..T....S.....Qb.A;.....m.....Qb6.u.....s.....Qb.Q.....v.....Qbvwf.....d.....Qbze.....k...e$.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1b63c6e73bda96a4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6161
Entropy (8bit):	5.661259240752245
Encrypted:	false
SSDEEP:	192:fSii78x/VYMtm5S00d46uk3tKOsggBaK9YAH2ZU:anEKM4or3tKOucK+VG
MD5:	364EF134A83F831129F130A342600C10
SHA1:	2C322CFBA5A9F8D5D9AFAC521BC99CEB02A53C12
SHA-256:	0C717AE693F0F7291949623D397C21D5D4F6E36D2FACF145DC7712EB7A24A1ED
SHA-512:	A07A3AE8AD05BBACDB41AA7ED3D40CFC0254828D7AB497F1092D83262753C9A5D9952D02B2EAED371F6793FBF25C65514434A0DE9A4F339B79EBB2AB32201BEB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q...1..c...._keyhttps://pastebin.com/assets/1745bc3b/yii.activeForm.js .https://pastebin.com/...."./.....(.....0...>>..R.Xvi.*Jj....7....A..Eo.....<.....A..Eo.....'.....O.....8.....`.....(S.<..`0.....L`.....(S.e..`.....L`v.....Rc|.....6.....Qc.v.P....events....Qc...j....defaults. Qf..W_....attributeDefaults.....Qd~.cJ....submitDefer..$Qg.4^.....setSubmitFinalizeDefer....QezT7.....submitFinalize....Qc.ceQ....methods...QezJL.....watchAttribute....Qe...~....unwatchAttribute.Qf.IO.....validateAttribute.....Qc.....isEqual...QeB.....isObjectsEqual....Qe.9.....isArraysEqual.....Qe.....deferredArray.....QeBO}.....buttonOptions.....Qe..:h....getFormOptions... Qfb:.....applyButtonOptions... Qf.Hn....restoreButtonOptions..Qd.#.Y....updateInputs. QfF.....updateHiddenButton....Qd..N.....updateInput...Qd.....attrHasError..Qe.?.]....updateSummary.....Qc&.....getValue..Qd.R

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1ef7d216b0421f0f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.7689689401367
Encrypted:	false
SSDEEP:	6:m9kYk+f2pomWqKJnV6zhmJ2vABteh/mMo0nhh/bK6t:/++amfKJQzkJBeh/doG
MD5:	C228CAFF1A8EAD6D6FDC86360F84FC25
SHA1:	3EED9D14DCA2E562D6DB1024443237E309FA4A60
SHA-256:	91DE8A605B04CC0448777CB6626F24A05244A38A0F1F8DDC1A010A71AD2EA5B1
SHA-512:	9F205F17B05140995F1FB4EAA368D870A8AD7DA16D0CD07D2D122A9D754535D7EA1D8BCACFD12A020A359D4B26E54F151A876BF742F4F05669513631131E32B3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3id2q4/yE/l/en_GB/BVpZI4bmBYG.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.\..."./.....F.....X..;D5O<L.!...C...C...(;.e.\....A..Eo.....+.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\20ab2bbebc418a61_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.631668693226811
Encrypted:	false
SSDEEP:	6:mVlVYk+f2pomHEh5hmJ2WMlA7ruOj3pkYnDK6t:E++am45kJuIb6q
MD5:	F5C9491CB06DF03AC539F7468E4C32D3
SHA1:	DEDAD149905879C681918114561E230D6D64A458
SHA-256:	E3B768FF767A87EF4D32322F4F4BC438AD86BEC194D11D076165E3B3EFFB2000
SHA-512:	22B85574932BCE77EE297D24447D7300C1B61CCC6580A1F977D99ADC7B1130B37B27AFF13743F8B331CEF4FBEA56A01E103A7AE1E0AD4CC35B898A5BBC8104A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yl/r/1d5nFTij4Ob.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/y]..."./.....F.....X../..1..nQ/.gC.'U%..T.....K.A..Eo.....ur.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\22b37a349d2034b2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.722440445060799
Encrypted:	false
SSDEEP:	6:mzLYk+f2pomWvrtJKApyJawhmJ2KALty3qvBr+5RK6t:wv++amiK8ynkJLGeqG
MD5:	462B1199C273371A401029F478DDC988
SHA1:	8E81C9042D5640AE39AB7A5791340AF0AE877FF7
SHA-256:	A7299C824395F5B10C147AB45F2B8FFDE57C7717202D7C5BCE0846C63BD8D9D0
SHA-512:	BFA723D7EC76392D6EC08F91AEEC96C7F33D2495BB0DB8BAF8C514322FD9E43560CCC5B6448D76225199206EB849878CD8F17B52E5F62E21F8AA0B1582FB00A 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s.....H....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iJq44/yd/l/en_GB/eZdBZ6fWkcm.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/*]..".../.....F.....)M.0../.z&Y. M.e....T8...EbP.Z..A..Eo.....B.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\22bbeef81bd7c9c7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.743190511232818
Encrypted:	false
SSDEEP:	6:mq+nYk+f2pomWMBlJKjo46zhmJ24naMlAztKHIzsk4/MbK6t:fG++am5lJKF6zkJYk+XCMN
MD5:	9BC605AB929E00FEDE20FCFDE4A16946
SHA1:	9E963179215677F9D8F3094DF203D48ED7DC102B
SHA-256:	80A07C3865F4694C13A4483CD3EF2EDA5141B61D2B131F95B453BCE4309C37F5
SHA-512:	6C8B7AE878983DE7585A9DBD0AB3BBB4C27311DF379AD56ECDD4FB140B6A41F440C8203CCB148122EAF643D6757B15C7C52C1198BD3BB5F3ABE1379A755B0I A8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...4Z.k...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3ibcU4/yN/l/en_GB/KRKMSAK751s.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.;.."./.....F.....tr.....S... I.m1.7.....z;*q.l.A..Eo.....&u.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2a3a31f51ba217b7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.7217321106411285
Encrypted:	false
SSDEEP:	6:moYk+f2pomWuPnKQqJhmJ2d/kZ5IH4SnK6t:N++amHKzkJwzDp
MD5:	35AFBF8E3C0DE10FD3AAE2475006989E
SHA1:	CCD7BB329063A785176F4827DC8E8F5E16AE3624
SHA-256:	5433D1D7088D352E031E9385DC72CE40C899D90EC71F7043CFF59F3C58BB54FD
SHA-512:	BFA7CDDB53169814DC02636FAC2B092EF32CCCC3D3B09D59D2277EEE3F126891935BF526CF169E0EB5EEBA9FA0A267D7DD9A5ACF7F8E9D67E798E275A04CC 69C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...Rf|....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iaLv4/yE/l/en_GB/ubsVV_mono5.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...."./.....F.....01...3....>&. <ej>.p.....$Q.5".l.A..Eo.....J.~.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2adde3a5c70003ec_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.7007272499036095
Encrypted:	false
SSDEEP:	6:mW9Yk+f2pomCr2Lu5hmJ2fAI/6kuIGH45K6t:9l++am23kJy66+w
MD5:	0E45902010B3097DE0691BB48BA6FFC9
SHA1:	803D9CD288D75234A19B4817468E0346848F4A1E
SHA-256:	944C886728E8ECB9DD2683EAD5DECFC6081C5E255AB8DB41D37027D38DF699EB

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2adde3a5c70003ec_0	
SHA-512:	82D7D600FF026375D4B6322DBAF2FFD52C8AE7AD74D7E4FC378B9566CA3B6B44AE796DEC63CB69EB4753E2A3FF8DF3E12B4B70C6EC4884F9D22A02F2362B4C50
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h..._.....,_keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yN/r/ZdsAnrSMdhj.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.:.."./.....VF.....|s....'8..7..{F1@..O..w..9C#.A..Eo.....Y9.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2fe6116701ae5007_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.6573007665329005
Encrypted:	false
SSDEEP:	6:mPXXYk+f2pomZXGndQjhmJ2QoR1cgtW+pBfhxAzbK6t:iz++amZXGnIkJSEgWsQzN
MD5:	B09DB6144599E7257B35B4FA52510091
SHA1:	BBD69CEBBA458A109AA31DF852BBBDF9F71761A0
SHA-256:	9BBBAA286D04E89D4397D1153571DA69AB1F7CC55B13A0DF2FCA622CF6F1CCDF
SHA-512:	93D1D42F80844CEB5F79AC52D2851B21DE68C5850E4A81A56F2E8950B5F39A8A79B4A198A2B16751ABE660D27290733E08FE11E007F4F51D0DAB70C0534F225F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....'....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yr/r/FZmFG4Q8g6o.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/'<..".../.....[F.....wx.Wj...m1.b..b...|.....a..d.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3324640353af4668_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	80304
Entropy (8bit):	5.760265620405299
Encrypted:	false
SSDEEP:	1536:3VcEE6y0FJdxto59FcSyoAG+YAcAqLzMca+lS/0FF3HxCf:nE6XJdx+7Lt+ALi+L3HxCf
MD5:	8D0D373B642FFFDF6A485FC6EA500F8F
SHA1:	2BF72342FE3A697CF161900FBD0255F1015D6B00
SHA-256:	18F3DE3296868BE5B7B1A556ACE36BD417F00D036264C9F18FDCF100289C9728
SHA-512:	4C3EAAB9F1374DF74114B3A853443BA792651FBC286981B6A0108B1517779FC45EBA3D5B345EC8FE9B19E5AC2A433890FD4A92232AF4E43D0D6F30480667BE4F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...o..^....0022C50DCF3F3028B96B8F51741FC3AB8D142E025FD7C0789A5C43B53519DFB5.....'.....O....p8.....1..X.....<.....(S.0..`.....L`.....(S....1.`.a.....Y.L`(.....Rc.....Qb".....data....Qb.*w....ba....Qb.!n.....ca....Qb._hY....ka....Qb.....oa....Qb..X"....sa....Qb.%=.....ta....Qb.z.....ra....QbV.y.....qa....QbZs.p....ua....Qb.x).....wa....Qb~.I.....xa....Qb.?.O....ya.....Qbnf!.....za....Qb.....Aa....Qb.}.....Ba....Qb..H.....Ca....Qb.:.H....Da....Qb.A.....Ga....Qb..m.....Ha....Qb6F\.....Ia....Qb.....Ja....Qb"..P....Ka....Qb6.....La....Qb.....Na....Qb.....Ea....Qb.....Oa....Qb.A.....Pa....Qb.....Qa....Qb.f....Ra....Qb.!Z.....Ta....Qb~.....Ua....Qbn..b....Wa....Qb..}.....Xa....Qb..X(....Ya....Qb*.{.....Za....Qb^c!.....$a....Qb.A;.....m.....Qb.d#.....ab....Qb>.....zb....Qbn.F.....Ab....Qb..Os....Bb....Qb.^.....C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\370a660deb3efd3b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.643550289847155
Encrypted:	false
SSDEEP:	6:mAYk+f2pomDkQhmJ2mx1y1ukGahLDK6t:p++amFkJLsp3
MD5:	CAFCC8FD900B5DFF358A51B56527E7B4
SHA1:	AE3B9E9B834D5FD091AB87F330523BBDF7744FA3
SHA-256:	B0349C433C9AD195C9EC201905D827AF859E34A260077BC55B7461DD682F75AD
SHA-512:	0F00A71505322C51A0B5C3F198319179DE358CC182F960BB692C444FC72821CF6301AA8CA133930662F233E211231A45BB94170C6887754EFED9BE98DEBF9C8B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....M...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yh/r/sbJIxk8bYkn.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/Z3..".../.....G.....e0.@LB..]...j.....U....ddQG...A..Eo.....P.4.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3bbba9d520641b16_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3bbba9d520641b16_0	
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.720697773302749
Encrypted:	false
SSDEEP:	6:m9XYk+f2pom/am0hmJ2VNyzWhZ+2lK4rHhZK6t:Az++am/am0kJWYWvrnhT
MD5:	F3D38CF79E6CCA163C46E3C38EF906D7
SHA1:	B7829280DFCE771D31565529BAF5252FE21A48C6
SHA-256:	A6BFAE759F7F9FA59F84198FCCD8CF54E7A442A42D52422303EF14CAADF7EA45
SHA-512:	24C69BC8C415123F6279B5CE63A09728B826EB299E345E15A1067DF6BD9952871BC9C683A116F8B627298E547ED747A85ABF8CBE13B1A0B959D02E4C51ED081(
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....>9....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yV/r/cKYG5jgbj2D.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.[..'./.....]F.....J4X..]..<`g+.....sV-L. M...^...A..Eo.....yA.r.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4c72ccd69cf67e9b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	90152
Entropy (8bit):	5.697265741262994
Encrypted:	false
SSDEEP:	1536:8/9ZM8OzZ2ucWwGOP+6x0jhzU11H7r2gKM6gTOo5iWmN28mygT:3rcKo+lWVrPwFpgT
MD5:	39AF56DED653CA6C3C059BAFBAD0B07E
SHA1:	57D289C39BFB160F4E576A4EE09356DB8190E72E
SHA-256:	C0F4C57DACB0F1F4E069B6AD1A47D42CAA4DDC1E4DF67A6501C9F0D3F9BBE091
SHA-512:	081C41ED5006F1A2790EA99129BC0FD6BFE2D819E4817EBAC59F7755509047C3CC5D951F67EEA0907DD63F7C1B1AE44BD143EB99B893DFDFBFF68F41AB1CE7 7A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....g.R....573159DA2CBEFEEDC05D0227D0957B81C75E41C86B2B36BD5BC7F7D97C52A5F1.....'.....O ....^..D..(.....T.....x.....P..... .....L.....(S.A...`6....hL`0....(S...`.....LL`'....@Rc.....Qb.B.....t.....Qb~.k.....e.....Qbv.....n...b$.....I`....Da.....(S...`.....L`... ...Q.@Z.;N....exports..$..a.....S.C..Qb..!U....I...H.....a.....Qb*`.3....call.....K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&. ..&.'..W.....-...(.....,Rc.....I.`....Da.....e..... P.....@....@.-....8P.....,...https://c.amazon-adsystem.com/aax2/apstag.jsa.....D`....D`@...D`.....`.... &...&..A.&..a.&.(S.X..`I.....L`.....Qb.P.....o.....e.....a.....G...C...K`....Dp(... .....&.(...&.Z.....$...&.(...&.}..)&.%./...'..'..W.....,Rc.....I`.....Pb.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4ec9ee8aabbd7f70_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	335
Entropy (8bit):	5.902832915129304
Encrypted:	false
SSDEEP:	6:mwJYVQfCYKi9oKcKynLEiY8eHh7CZK6tOZK+Qe1jgvKMUSlfCEFY8eHhA:dAQfCYKSozSv8eHcTSRpgi2fCE+8eH
MD5:	274E81958F5D9B8670D9D99C9FF0CFD5
SHA1:	0C446D67A3837A457B26B46687F278ED2334E3FB
SHA-256:	C538E3A712E932AFF0A35BC6EFBB687F5C7C2BB4E452B5A4F6D4551D5B23A77A
SHA-512:	602183C7FD1D8325D8F4CB2C4A480DD0D08485FCBBD7DF69D5E9BFEFF1D21BCF3496F12EC1C9C2DE564515B8E1227F136FB05BABCD81B7C70DEADE9404E5(F74
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G.....o....._keyhttps://c.amazon-adsystem.com/aax2/apstag.js .https://pastebin.com/...../.....D.....%..~.==.ZX.*.,L.j.....8.r.A..Eo.....A..Eo..... ....."./..._..573159DA2CBEFEEDC05D0227D0957B81C75E41C86B2B36BD5BC7F7D97C52A5F1D.....%..~.==.ZX.*.,L.j.....8.r.A..Eo.....& .L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\508797177f1f805e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.648971000224664
Encrypted:	false
SSDEEP:	6:mSYk+f2pom8FS5hmJ2oMlAuWBiErLrDynK6t:3++am8AkJshg1LXq
MD5:	D87C917226A7CDE4736A32A896D46E72
SHA1:	0AF1527617EA217069FB91418CAF8624A4E939A4

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\508797177f1f805e_0	
SHA-256:	A4838356BC300A48C90F8AA7FD159BB5CB026E9786FA7873DB68E065CBB6EBAE
SHA-512:	57908553856632B6FE8FFD4F92385FC2B6EB3EE6D332A6B5B09C0A4515182034DE47390A47FD45C01BF657C528E7B7646DC65E2F84D921D186F3D9F773B47F17
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....a...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yU/r/WNPbD2XSPbr.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/+9.."./.....TF.....U.m.L...8".V..... .h.)....A..Eo.....f.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\56a7c474ef8e9ce0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.467769999598611
Encrypted:	false
SSDEEP:	6:mwoYxwSEBW2PYmBnRKJlAebW0+CAAUYsz9konRZK6t:DdoDQqnREle0iYsRP
MD5:	FF67A3792EFA3F2BA9ADD0CC61185970
SHA1:	FF040304D396BB8064EA044491944A938B1D76CA
SHA-256:	51DE2AB2F5BC4F2C1687C8F4BF2332413E52261F04172CB9FF6ED85C24145BCD
SHA-512:	6E0D99F61696BF33506FC333762E84942C047B825037B34D1EB2465738EB0E2378248FF00F9E82CFD8682582191FAB2E22FA4154545C3532AE672FF6BE8E2C68
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O...R.6....._keyhttps://securepubads.g.doubleclick.net/tag/js/gpt.js .https://pastebin.com/M..."./.....3QB...9.T.../...v...b....XW8..A..Eo.....A..E o.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\59e0c850d4f2d2a9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	121760
Entropy (8bit):	5.862637325973189
Encrypted:	false
SSDEEP:	1536:oc1bHwJoilFyoWOdsFJ4WKzvFTS3tLePBuFxLMO1oN2Gr1oG/BhmLpexLebD:oOQJnl8oWg+UzvpWtLegFJMO1oN9TuDD
MD5:	AFAFEB8A7375C34E0980A6F67F34F682
SHA1:	0D343A63CD2D8839885D1D6B824676D0C3AC14F8
SHA-256:	616675D498498F6C40216A963FCBFA2F1D1515A6CECC9C722C9A2C297E5AA2E5
SHA-512:	E2FD9CD6BF280F5CED99E03FB9434D119CE08253B1A957436465909C79C6F3D785F3723572CA0461662F8DFBD0658EC54EF4207453AD2A1D6B0B38C85A9BACD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....2280C8D6A0B73FE576A5A22DE0863CFB1404AB2AB9A234FA6B1D5CEAB3952335.....'.....O'...0...&8.....2.. ....4...H....#.....(S.<..`2....L`.....(S....2.`je....!.L`.....Rc.....Qb.....aa....Qb.*w.....ba....Qb.c.....da....Qb.n. '....ea....Qbn.....q.....Qb.m1.....fa....Qb.g8.....r.....Qb.j.....ha....Qb..0.....y.....Qb..$....ja....Qb._hY....ka....Qb.O.....pa....QbV.y.....qa....Qb.z.....ra....Qb..X"....sa....Qb.%=....ta. ...QbZs.p....ua....Qb.....A.....Qb...w....va....Qbnf!.....za....Qb.?.O....ya....Qb~.I.....xa....Qb.....Aa....Qb.:.H....Da....Qb.....Ea....Qb.25c....Fa....Qb.A.....Ga....Qb..m.....Ha.. ..Qb6F\.....Ia....Qb.....Ja....Qb"..P....Ka....Qb6.....La....Qb.....Ma....Qb.....Na....Qb.....Oa....Qb.A.....Pa....Qb.....Qa....Qb.f.....Ra....Qb.....Sa....Qb.!Z.....Ta....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\60c0828071489bda_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3290
Entropy (8bit):	5.599012841095256
Encrypted:	false
SSDEEP:	96:lA/lM0A/9MJA/rMZA/RMNA/uMRVA/dDMoA/zMLA/IMHA/qM2A/ZDMqA/hQMzA/Oh:lATACAgAaAXAVRAiANASARPAfApAwAu
MD5:	56D6A7C3875743B3A9D47B56F846EDCA
SHA1:	BB22166700F103E0204D773C6A0278191075C7CB
SHA-256:	199E8ADE7D799FA91A914A32738159C0C420F45DC4B1FC8156C0D4EE22AE4A67
SHA-512:	2483EF29D11E3A5562ACD49E3FDABCA9DD87F86849376E2666A1FBE08D6162B81A3991B07E88B0043F0E579A311A16EB564600B22EE890B532AC273F9D856CD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g....(|+...._keyhttps://cdn.snigelweb.com/pub/pastebin.com/20200826/snhb-pastebin.com.min.js .https://pastebin.com/1..."./.....>.....ZT..3.?..X.....+E..... O\r+F'..A..Eo.....L.....A..Eo.....0\r..m.....g....(|+...._keyhttps://cdn.snigelweb.com/pub/pastebin.com/20200826/snhb-pastebin.com.min.js .https://pastebin.co m/..".."./.....D.....ZT..3.?..X.....+E.....O\r+F'..A..Eo.....e.....A..Eo.....0\r..m.....g....(|+...._keyhttps://cdn.snigelweb.com/pub/pastebin.com/20200826/snhb- pastebin.com.min.js .https://pastebin.com/..}."./.....ZT..3.?..X.....+E.....O\r+F'..A..Eo.....A..Eo.....0\r..m.....g....(|+...._keyhttps://cdn.snigelw eb.com/pub/pastebin.com/20200826/snhb-pastebin.com.min.js .https://pastebin.com/..6."./.....ZT..3.?..X.....+E.....O\r+F'..A..Eo....._.1.....A..Eo.....0\r. .m.....g....(|+...._keyhttps://cdn.snigelweb.com/pub/pa

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6c623839cc7f42fb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	470
Entropy (8bit):	6.1218189653272885
Encrypted:	false
SSDEEP:	12:rEm80vbmMZdbWKv4B0jUG4p+Q3ma++YJlo3:rfnvbtZdn20E4Xm
MD5:	8C8BB615437A9E3FE6CC91DE18F1645A
SHA1:	E5AB875777004041A3D891D41F3D8E9463ED9944
SHA-256:	5EFFDF5AAB007E348164E8AA5C385F6787C85F0E1EDF42D21552BC78EA94AE68
SHA-512:	76E91F9A6D2EAE430894EADFCCAB53B627444104AEBEDF71015B793E4CEE9EEF7710399414197315954A6B667A63532BFE6D31A1D60749B81E55DC6020CCCD0 5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...(....._keyhttps://ssl.gstatic.com/accounts/static/_/js/k=gaia.gaiafe_glif.en_GB.GR-XoYWnyYo.O/am=KwAAdiABMOAHAALMAwAAAAAAAAAMIBPKMk49rfD- JQ/d=0/ct=zgms/rs=ABkqax3dKZEgcQmwrv5rqONCea3zpQrSjg/m=NpD4ec,SF3gsd,YLQSd,lCVo3d,o02Jie,rHjpXd,pB6Zqd,QLpTOd,oWOlDb,n73qwf,MpJwZc,blf8 i,omf1Od,zbML3c,zy0vNb,K0PMbc,otPmVb,rlNAl .https://accounts.google.com/..j."./.............a.....zE`.....#..[.L.p.....p....A..Eo.....F.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6f085bbdaf305688_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	346
Entropy (8bit):	5.810467976806244
Encrypted:	false
SSDEEP:	6:myl/PYGLSmXZCjVRnKqRMyi/e8dLC3bAJK6tMXK31scZqNZ8dLC3bAo:7XiVRnVRMP/e8dLaQaalTZddLa
MD5:	4EF3C0CC56F6EC9CB53315CC95480630
SHA1:	F8F804A2EE23E91B11BF301CE81F2485B138E109
SHA-256:	4269C1E23011455BFCB741CAEF37AD44B13CA077ABA60E2A07B7E3ACCC852E6E
SHA-512:	5EEC0CDFFC859B771FA9E36C9A4CA8BD7B7734E746F535801411814BF807EE00F345D35A5382432FC9CB157BDB3CFA6CAD514627CA42B52CB067B5931F604C 9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....b....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-58643-34 .https://pastebin.com/-$.."./.....:...BX.....7.UB.b..j... ..N..4...A..Eo.....,=.....A ..Eo.....-$.."./..9..0022C50DCF3F3028B96B8F51741FC3AB8D142E025FD7C0789A5C43B53519DFB5:...BX.....7.UB.b..j... ..N..4...A..Eo.....^J:L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\707c02e9a3e299c0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	341
Entropy (8bit):	5.836593662444386
Encrypted:	false
SSDEEP:	6:met4YoK2hx3D3KsHZTrz65/ZK6tKYHnQWlmSRioEUZTr4:O3D31STVH/lmin
MD5:	5E4C3BEDD1A87CEB64828143587E68B6
SHA1:	7E56C6D804809872DFE73CFB203DA2118BB20A4A
SHA-256:	877708106F536890A0EB1EB0390828385439 17BE688054509F66572B75564415
SHA-512:	13F354DBDCA09AA20057290F18AAAA0D52F4B85FF2ECD987FCB76A02F5EFC39278C9BEF5F94C605360FC8307000EE00597462CF89E3CA468C699B4B2A843752
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....@.W...._keyhttps://pastebin.com/assets/ae9b8d97/jquery.min.js .https://pastebin.com/T..."./.....P.....w#3.....7a..:.....hB....A..Eo.....B.....A..Eo... .....T..."./..}..FA9B0BADD9BCEAFBBBCD8BC74F58D34C55C2DDDA8EE0F26FC4B30C20B1342943P.....w#3.....7a..:.....hB....A..Eo.....f=L~L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\74845533764f80c7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	50609
Entropy (8bit):	5.749679202940811
Encrypted:	false
SSDEEP:	768:DZHJydnCKPE0uoJ8H67fFxPCyPff1vUZlKkmbQKOGBVakfVAXwxyK1WVeQ5Rn8mT:DS5CBKIlKHQKOGB8kfVYwWeQHk0
MD5:	66FC2ECA3DA999A72820C69EC3E05F36
SHA1:	2DA127743C2426BE21179C822A2CF2AEB7E61637
SHA-256:	06257B9256D68BCA8B46D93DA1A7BF4E141773D35C6A9282C36269F22E302267

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\74845533764f80c7_0	
SHA-512:	43E1474AC59CEC922EC622470423D1D9663B467DF8FC61D0DABD1A38AB2D1732936B824883E31E6DA78122C646BB6E7CB10AF03E352C62D90AC6D8629F839F5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q...a....._keyhttps://static.criteo.net/js/ld/publishertag.prebid.js .https://pastebin.com/...."./.....rj..'i.1y.}..{./^+.....uGQ.A..Eo.....e$.....A..Eo.....'.D2....O.....K.....h.....(S.0..`.....L`.....(S...i..`.<.....L`.....Y.Rc.....Qb.g8.....r.....Qbjm_"...._.....S...Qbv.....n.....Qb./X.....T.....Qb~.k.....e.....Qb.P.....o.....Qb.:.....c.....Qb.....A.....Qbvwf.....d.....Qb.D.....R.....Qb..!U....l.....Qb:.....M.....Qb.Q.....v.....Qb.h.....f.....Qb..Z.....C.....QbfK.....P.....O...Qb..+.....x.....Qb...4....I.....Qb..h.....O.....Qb.H.....D.....QbZo.....B.....Qbze.....k.....Qb.$.}....F.....Qb.oN.....N.....Qb*.|.....L.....Qb.....H.....Qb.i4.....W.....Qbz@.....z.....QbR.....G.....QbF.....V.....Qb.....j.....Qb.u;&....Y.....Qb..OU....J.....Qb2.....X.....Qb..3.....Z.....QbR..X....Q.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\753e6439691a724e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1423
Entropy (8bit):	5.589011478780016
Encrypted:	false
SSDEEP:	24:1fEPG38CUuVXuqHclwzEdc39lIs64cfEPyOtb9jOGzttuCgte46e:18PGxBVX98ezEdg0l8PVN9jHuTcte
MD5:	D3A87D88800D8E135CF0F940CB4EFB20
SHA1:	57B5A143A592541F5078916CFF058BA47408C617
SHA-256:	42AB1280A0E17F83DC945F3013E2F17967603D8E9C149A5B1B59CAD02D388137
SHA-512:	5B7FAB031A748FD7ED75BEB5BA6007D0FFCA3D7D0DADB2DD2105B9771AF8E4C0406940452DAB2220DD2B0370A1B5C3D070EA801E95F8C50B787B14BC5D665A5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o.....}...._keyhttps://cdnjs.cloudflare.com/ajax/libs/codemirror/5.58.2/addon/mode/multiplex.min.js .https://pastebin.com/...."./.....F..Ho..m=..B.....p...i...KP..A..Eo.....n.....A..Eo....."./.X.....'.....O.....~.....(S.8..`(.....L`.....(S.t.`.....(L`.....Q.@Z.;N....exports...Q.@.P.....module....Qc..C.....require.. QfZ.Y...../../lib/codemirror..Q.@2..[....define....Qb..s.....amd.....`.....M`.....Q.PN.....CodeMirror....K`....Dw.....s.....s.....&...&.]...&.]..../...s.....&.(.....&.z..%&.^.....&.]....(Rc.....I`....Da....r.....e.....`...p...0.....@.-....`P.q.....T...https://cdnjs.cloudflare.com/ajax/libs/codemirror/5.58.2/addon/mode/multiplex.min.jsa.....D`....D`8...D`.....4...`....&...&....&.(S.<.`.....L`.....0Rc.....Qb.?8....p...`$...I`....Da....D....(S.....5.a.....a.....QeB.....multiplexing

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\78431f791492b110_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.795912349173355
Encrypted:	false
SSDEEP:	6:m9x/PYk+f2pomW1FKUwoKhmJ2f+ABvdcr+G4rfDK6t:u++amyFKroKkJ2zvdK+GO
MD5:	97EA4AB2E4DF9FDF21576F3945B17B79
SHA1:	B6A730B166345902BDDC79207C088B86C70A4648
SHA-256:	A57A104C35BBA0FFD2D646373E46259EE6A72E0972D812FD2AC504A2F52B68E7
SHA-512:	60F72627977EC354093729B7CDE60018DEC85ACD44B196A59D1A593010A43F086B820E832ECA31F3F0943E259DACA146C0CD2FD63D73D4666FDA9EB3DD170B5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s.....V...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iPrS4/yl/l/en_GB/ZjRaTSQ42RF.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/u8.."./.....QF.....u...~. ..fLD...[R.+?..B.\$..A..Eo....._U.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7a69c8c98ea1b6d5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	359
Entropy (8bit):	5.907538740440559
Encrypted:	false
SSDEEP:	6:mYPlPYxwSEBW2PYuVrp+wRKkXCg+z360j4QBZK6tWZyU+7iZD3hTBGWzz360j4h:FP6doDQR80FK0j7BTUZyUWiVx1GGK0jc
MD5:	6FAC917AAD8424248AC8576C569464BF
SHA1:	558C96F2F640048E721E29D32A23E5B12B12660A
SHA-256:	D948674C9FCC0A1C50DE6C9B20667DFD1DDEB0AD605C9708AECC6CF43A78A08A
SHA-512:	C1DE96C23D81DC36640396F6B575B5253E8D0C8E3E5381DAEC4D160C9D65552F3E7C02131A3FC6163AB79EA76AFE9C56CB5B91C23448206D656838C8FDC228
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...{j".....keyhttps://securepubads.g.doubleclick.net/gpt/pubads_impl_2020111901.js .https://pastebin.com/...."./.....T.....biy?.....a%...8....A..Eo....._.....A..Eo....."./.@P..34DF60C745AE4FCA779EC05816092C46C1A710BF7E6B92F2BF3F2F3BFAD66246...T.....biy?.....a%...8....A..Eo.....7.p.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7c15ca074beae818_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.719823554632696
Encrypted:	false
SSDEEP:	6:mJPYk+f2pomWv1iKHzazhmJ2qWzAc6EAz6BnvP496w/lbK6t:A++amqoKHzQkJVc363WBvc
MD5:	A82ADDD59130EA233CBC4DCE03EA84EF
SHA1:	4418367CD8C843000C9C3D31E37EC3D87A719F89
SHA-256:	2259EFA49203FE5C7514DF2C5190750DB217AE9829FE7459224D9E757105C3D2
SHA-512:	9657EE3163CBA275E68289308587842E9B111CC518D9FA7BE80C89E5C7452DF658CBFAF9FEA3A03CAB21583DF3F03E7F7D02CE33EC07EF11BD1DE4C4B0E9A196
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...8.;...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3i8jc4/ym/l/en_GB/KDuWd9CaxC9.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.9..".../.....ZF.....,.....^..._.....6..C..)....n...A..Eo.....8.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7d42b962309cabbb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	365
Entropy (8bit):	5.917714852802953
Encrypted:	false
SSDEEP:	6:mm7YET08N0JNCoKGET99dSpnOJGYQdK6tJR1STTCs1cQly9dSpnOJGYhe:/g8NCQoiTbdSpnOJGHifCs1c2y9dSpnq
MD5:	B4F7AB3872A4E7FB7DEE250EA518B4F3
SHA1:	F7060934B60A4BA41640F30A65EAF3CE42F19847
SHA-256:	D8B6845CE847F5B171364AE9969F42DCBEB7586ED7CCA730203A6F74B1EE2774
SHA-512:	D6BA3140F3F789ACB21AEADFBAB7D6256D4750BFD84D90605083287C7C82B84948142216619C5E9F1D05B3C28C161E624CC2EA6BA06F20A00BDCCCA79B262CD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e.....H...._keyhttps://cdnjs.cloudflare.com/ajax/libs/codemirror/5.58.2/codemirror.min.js .https://pastebin.com/X..."./.....6.....C&.i\..I....4..._...k[.~.A..Eo.....dX.....A..Eo.....X..."./.xT..99D872E9225507790D479DBBA384FCA601D8F8486026934D14F6955BB1F6CC75.6.....C&.i\..I....4..._...k[.~.A..Eo.....CwL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\817ea1e483f22797_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	386
Entropy (8bit):	5.96117820628637
Encrypted:	false
SSDEEP:	6:mEYvEdCN8uVvUCllDCMRFqsTNYxcbqoDq3Yhw+GvA1rqQPLcNmY3TbK6t:CEm80vbmMZdbqoYYK+Go7GN
MD5:	33D25603B23BCBAB0DB3B0BE3DCCB20B
SHA1:	F97DB53BB97E730D7A1BDA8F19518E6F0DA32A0B
SHA-256:	B9CE049539523BE4118C1716CE85AAB2D4886531BD66791D4E3B98106DB31A5B
SHA-512:	3E7272D6D19EC1308317DEFDA8A7CD843AF7D60AD8323BAD9FF1259D532F4A1B7F8F3A97001B1C95D593808F3F1DCDEF8D6AFA00BCA371B316837F1885DC91F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....5...._keyhttps://ssl.gstatic.com/accounts/static/_/js/k=gaia.gaiafe_glif.en_GB.GR-XoYWnyYo.O/am=KwAAdiABMOAHAALMAwAAAAAAAAAMIBPKMk49rfD-JQ/d=0/ct=zgms/rs=ABkqax3dKZEgcQmwrv5rqONCea3zpQrSjg/m=syl,i5dxUd,RAnnUd,syi,syj,uu7UOe,soHxf .https://accounts.google.com/..n."./.....a.....d8(.e.....u.L.@...[.Y....4.A..Eo.....q|."".....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\82eb4abb40f6c298_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1305
Entropy (8bit):	5.446077281235305
Encrypted:	false
SSDEEP:	24:ngn3w/At54gqHjw6CAqqYQnterl2v2II:G3Q3TYMtal8ZI
MD5:	E13D8B83B1558D992C24FEFC83DAD5B2
SHA1:	3A6AF6FF921F52392316DC83895ED6A852D9F875

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\82eb4abb40f6c298_0	
SHA-256:	5D3143A5A1A5211050601F51A8FAD068B15CF5395BB98B441AFDDAF68ED2B648
SHA-512:	C2A9442E007E006D6D75080F9C37674F6DA4C1EA58E887390CA20AB0EAA97C99C976CD9E4E914AF84580C5AC025211350B0963481F3EC2C4CD7B4AD802571AC D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q.....S...._keyhttps://btloader.com/tag?o=5658536637890560&upapi=true .https://pastebin.com/.A..".../.....^.....+. ...E-3.d.i7....!'.n..2..A..Eo.....p.....A. .Eo.....A..".../.....\.....+. ...E-3.d.i7....!'.n..2..A..Eo.....A..".../.....+. ...E-3.d.i7....!'.n..2..A..Eo.....Q.....A..".../.....+. ...E-3.d.i 7....!'.n..2..A..Eo.....<.....A..".../....."".....+. ...E-3.d.i7....!'.n..2..A..Eo.....S.....A..".../.....+.....+. ...E-3.d.i7....!'.n..2..A..Eo.....'S.....A..".../.....&P..... ..+. ...E-3.d.i7....!'.n..2..A..Eo.....VQy.....A..".../.....f.....+. ...E-3.d.i7....!'.n..2..A..Eo.....Ej.....A..".../.....Hk.....+. ...E-3.d.i7....!'.n..2..A..Eo.....T.....A.. "./.....x.....+. ...E-3.d.i7....!'.n..2..A..Eo.....A..".../.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8422562e17d84495_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.638256970595558
Encrypted:	false
SSDEEP:	6:mVYnYk+f2pomTnI3GhmJ2PT//ll8z9DT0GaGYTcnK6t:qYD++amL/kJytmJDrUcp
MD5:	2FDA2F46C617380A77CF5F932012BD94
SHA1:	D611101627CC668DBA1669DDD57F7E7A3429B427
SHA-256:	F6EFD74C4C47B6C6913769781615BBEC108CB35067F3BCBA03B6D06FFB16050B
SHA-512:	2B031BE1EA3AE31AFA522258830F35EEC9E62DE81823DD6FEDAF3DEBF35EE89729F204B8BA90B830226A73844F65B220971F45208ED01428E841797D899CBBE A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....,....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y8/r/v-R2pLq3QHO.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...."./.....E.....YZ0.aq.]....L..P..v?.... rr....o.A..Eo.....p.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\849c3de6865d8565_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.376720894851798
Encrypted:	false
SSDEEP:	6:mEanYiMs8pMjBcZ6HF/llXj8IcNupgLrzK6t:MrNyQngIc8p6
MD5:	3F799F7A7EC92CE5D1818EE67B48E84F
SHA1:	1CC690AC49CDD029C2976449BD82A0F426315BD1
SHA-256:	497F622EF9E4622D9349895A4C3CB3D77E341803F7A03CB080B254745AE9A760
SHA-512:	14ABC0B17715C07085BB2BCAFC4348DB738493334E8A3380086E56434B909A70B840D60B09B016688FE05857692801CF34D82B13E082FE4808CE56F23A0B6804
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I....._keyhttps://twitter.com/i/js_inst?c_name=ui_metrics .https://twitter.com/..9."./.....S.....D...L...9..g.....-...m...oN.B.A..Eo.....-.c.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\87cba9c64d845c0d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	329
Entropy (8bit):	5.711953475600255
Encrypted:	false
SSDEEP:	6:mGFXYBZsrRZPaxo1r/9LvHZifAR4tgoIkon/XhK6t:lYarRxbr/9LfQoR4Qh/X7
MD5:	8AE6B065979965D917535C8452EF6DE4
SHA1:	94CAFB04F33AA3A7316C2A057B7C9AD465EFE79C
SHA-256:	FFF4DCC8993CD7811526F4D3C0EE5E26D75C8D416A5123D313DA5297DE532F18
SHA-512:	2635D9E60457B0EE68DF3E3C1C19851B149AEAE365994654C48A33B398FF21F5664AF621C79EE3F0075CB9EC2DFE39D85D0A0572390033A6DA60B18B971AC0C
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://image6.pubmatic.com/AdServer/PugMaster?kdntuid=1&rnd=19252284&p=156077&s=0&a=0&ptask=ALL&np=0&fp=0&mpc=0&spug=1&co ppa=0&gdpr=0&gdpr_consent=&us_privacy=1---&sec=1 .https://pubmatic.com/.[..".../.....7...lk.~)D2.(.G.....:..2b.7;L.A..Eo.....T.1.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8995dfb6624f2499_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8995dfb6624f2499_0	
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.732206529361576
Encrypted:	false
SSDEEP:	6:mzYlPYk+f2pomWsJ9WKK+jVahmJ22oR1+/6J0+fH43ZK6t:kYlb++amX9WKK+4kJ6W/b+/GT
MD5:	95A2E20DFF48FA43257C77A76A68A6B8
SHA1:	287C358CAEA1FF8169E5A5B9DB490761677D397D
SHA-256:	B2EC356B0A29046C87D042BD8189E44A3F8A12D5C63BBE0CE2F22B9C9A710555
SHA-512:	FDE6248D5C5BC1FF860368D972489A0EF38B05159F24370065BEBD0671E101139EE868C2874DC3DB9D64B66A8AF5C47409FA6B99348721DABC51599C32753DD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...W@....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iYXl4/yz/l/en_GB/bOtHsRxDkOf.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...."./.....F.....ER.....9...@%..a:..b8.xGP}!gw.A..Eo.....:.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\89f65cd09ba91171_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.7093995916396665
Encrypted:	false
SSDEEP:	6:meVYk+f2pomRuXk927dwhmJ2tMlvYlFXYiZA0LjJK6t:pN++amRYk92pwkJO9FXHOkD
MD5:	942FAE331B23E9ADE8420390E273FC15
SHA1:	D1A0F468CB727D5710DCCE8611B2AE3C48A45FE5
SHA-256:	39454A1EFA8217819CD3F323F9EA5FC44077200B88F76B53DB1510B314835DA3
SHA-512:	8666317BB19B374642511232ED620B040D4ABA0597DE10295F1F2097B44E026059CD2C75CE29E127A33181348E449F8042FB91CA29B6E07D0BD007E375D4128A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yA/r/P2xVPF9XJCl.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/t".."./.....IC.....%`...z.{o}..S:TwRG.E.V=..X./.$[.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8ab9deeb5de6b942_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	15955
Entropy (8bit):	5.947678787521587
Encrypted:	false
SSDEEP:	192:ToIsStuddKloc+Jl6B/a0UySXTSFFhLhQ58yImKkCWO7+SFcJcVXRc+bkOobsY1C:uf3u9P3SnaPRhVTYvToChIhkcATaTd
MD5:	82ED4AC330EC753F0BA9D2AAE00B13FC
SHA1:	40999619F5746AF4D2B3BDA34821E4B4BE7A7F3B
SHA-256:	38429494932886487D639D6723905DD2EA944277E801E0FFA374281F75849CBB
SHA-512:	085B65F84D0F6B2FAE02BCF8821703185E55B2DCE300C2E04401CBAEFD0F51A8CF9135ACCDE7327B8E8DDBA037797AABD21A1D8CC491253DE149419289EF07A9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....{...%2o....._keyhttps://pagead2.googlesyndication.com/bg/PbZvCEkorD5rxjWOexle1_regFmuc5-vrUA2zacPm4s.js .https://googlesyndication.com/...."./.....9.....[...0V."./b.t.uS..e...P<.(...A..Eo.....?\,.....A..Eo.....'..6....O.....<....|.....D....5..t.....(S.<..`2.....L`.....(S...`.....8L`.....\Rc*.....Qb.....J.....Qb..2....r.....Qb...m....v.....f.....I`....Da.....m...(S...`.....4L`.....Qd~3.....trustedTypes..Qd..].....createPolicy..Qb"..P....bg...$..a.....QdN{qr....createHTML..C..Qd...O....createScriptC..Qe^0l.....createScriptURL.C.....q.. Rc.....Qb..;Q....h...`.....Qc.Vv.....console...QcZ.....error....m...Kd .....E...9.....D.Q.(.....&...&...(.....%..'..(...&...&.}..)&.../...../...../...Z.....&..>&....&...%.....&.(....#....&.(...&...&.(...&..Y.....%...,Rc.....Q.`.....a4.....e.....0.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8b95103176f2e077_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	93224
Entropy (8bit):	5.467203047500784
Encrypted:	false
SSDEEP:	1536:f9ZRD244vkf8xrQZCxvBpHifBVhW+5BeGBtWe8jT:PBMvy8xrQ4vCfTJ8v
MD5:	7347C55AFDA7CEDA64A1510F2B74957E
SHA1:	F475D711CF55E978E3A86EC0579B95DD8F5F67D3
SHA-256:	1D4567F0FBCD9543CCB9C305625412B41EEBCF58F1BA66E4A6AF00750B1C92E5

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8b95103176f2e077_0	
SHA-512:	88699A065F367F1BCFBD20BC8990963FE6D013945D02BD2F6238D5AA2F88C733A27980190B7C128634A93C1A2BCA6F519182A2B5058121A0055EDD5C2AB96D1E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....~T.....7FE7E78F69CBF79B3C48FFFF5EA179F40C5C324B187E5B3895C0A12F3EC034BE.....'.....O#....j...B..... .....\.....(S.l..`.....$L`.....(S.....`R.....a.L`.....e.Rc.....Q.@..dm....window....Qb.....aa....Qb.*w.....ba....Qb.n.'.... ea....Qb.m1.....fa....Qb.A;.....m.....Qb.j.....ha....Qbv.....n.....Qb>.&.....ia....Qb.g8....r.....Qb..$....ja....Qb._hY....ka....Qb2.m.....la....QbV.y.....qa....Qb.B.....t....Qb..X".. ..sa....Qb.%=.....ta....R....Qb.x).....wa....Qb~.l.....xa....Qb...w....va....QbZs.p....ua....Qb.?.O....ya....Qb.}.....Ba....Qbnf!.....za....Qb.....Aa....Qb..H.....Ca....Qb.:.H....Da....Q b..+.....x.....Qb.....Ea....Qb.25c....Fa....Qb.A.....Ga....Qb..m.....Ha....Qb6F\.....Ia....Qb"..P....Ka....Qb..0.....y.....Qb.....Na....Qbz@.....z.....Qb.....Ma....Qb6.....La....Qb .....A.....Qb.A...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8be92a48b627b287_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	87328
Entropy (8bit):	5.809993160158118
Encrypted:	false
SSDEEP:	1536:/xfG6YL9eJoSZ2KgkeMfOZflqXmDRvjMsJmc4OCGO:Q6YReJJZ1gkfslb1vjMsgc7O
MD5:	D0D63E1897DD40AAEA35B2F86174FC4D
SHA1:	B35F231854A27000272E481598AD441936B854DA
SHA-256:	4F3F9A7E224CF874A1AD7031CCAA0910381B86A499B7F2515C2C14C067578259
SHA-512:	AF49C479C9A79B1BBDF7074DF761C71F922906BA53E5B3DC70940548F970644E783D896EADC11330A18EA5715B48157B52A9AF4FF0B0CE0A1CCD95AF4A00EBF 8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....99D872E9225507790D479DBBA384FCA601D8F8486026934D14F6955BB1F6CC75.....'.....O.....S..d..%.....3..\..... ..0.....(S.<..`4....L`.....(S.x.`..... L`.....Q.@Z.;N....exports...Q.@.P.....module....Q.@2..[....define....Qb..s.....amd...Qb.=.....self..Q.PN..... ..CodeMirror....K`....Dx.....s.....s.....&.\..&.-...%..3...s.....&.(.....&.].....%.....&.\..&.-...%.....(Rc.....I`....Da....D.....e.....`...p...@... ..@.-....XP.Q.....J... https://cdnjs.cloudflare.com/ajax/libs/codemirror/5.58.2/codemirror.min.js..a.....D`....D`$...D`.....`F...&...&....&.(S....3.`.g.....].L`.....Rcl.....Qb..+.....x.....Qb. .Z.....C.....O...Qb..!U....l.....Qb.A;.....m.....Qb.:.....c.....Qb6.u.....s.....Qb.Q.....v.....M...R....Qb.L.....h.....Qb^..M....w.....Qbvwf.....d.....Qb..0.....y.....Qb..T....S.....Qb*.|....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8dae72a65858ac42_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.696652277032063
Encrypted:	false
SSDEEP:	6:mgPYk+f2pomZHhmJ2sAwgAS5NnIU+ZOsPAKR/bK6t:hb++amZHkJVgACrW
MD5:	7D1D43763F165EAF7E1AB29B69A1ECF2
SHA1:	81EFAD8BF781307F876600AD9E82BE34DB701017
SHA-256:	B9171958BCE1832170C2EA3DA0B87281C8624833371A3B68E888B41570B70FCB
SHA-512:	B5F4BD0822E449FD13980B855577EDCE86A9CB3F8CF5EFB0966985146F3E3B88A0C7563D20B9DCFF95601831D437D9F5A7A66807B1699A933FCAEBE780D2023
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...l.....,_keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yr/r/51t-ENp6yHv.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/q:../.....WF.....u..j.....F.1E.....h.....A.. Eo.....H.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8f06da9be8297fca_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	9067
Entropy (8bit):	5.841010126127589
Encrypted:	false
SSDEEP:	192:nEVlWLK0drd4iCxFoahTzpajKTa/uktq9Fv6pbNd1z:nEOLK0drY2gHTH4c8z
MD5:	149041E5B20A1B870E2E0BE0BBA50F61
SHA1:	ACAFE7235E62B3A496022978F5C1290E7612E610
SHA-256:	D3A4E076F8DD4CEFECDB69EE5FE854535165304B6B02AC24B97896B30DF4970A
SHA-512:	3C48BE74A3DEAC1A3EA5BC4C03CC17745350A545A0B94A9B9FA1686119311460C4FE8AABC7E1AE20A97F9C9871ADFA2116383F3F5929E058E683D5689D9721F D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8f06da9be8297fca_0	
Preview:	0\r..m.....K.....K...._keyhttps://cdn.snigelweb.com/adconsent/adconsent.js .https://pastebin.com/...."./.....^.....@.3b.]6...>BO.s..t.m.%I. _W.....A..Eo.....s.....A..Eo.....'.k.....O....!....F.....(S.|..`.....,L`.....(S....`:.....L`.....Q.Rc.....J.....Qb6.u.....s.....Qb.B.....t.....Qbv.....n.....Qb~.k.....e.....Qb..!U....I... ..Qb.:.....c.....R....Qb.?8....p.....Qb.h.....f.....Qbvwf.....d.....Qb.Q.....v.....Qb.A;.....m.....Qb..Z.....C.....Qbjm_"...._.....Qb.L.....h.....QbB..Z....E.....Qb*.|.....L.....Qb..T....S... ..Qb.....A.....Qb...4....I.....Qbze.....k.....Qb.H.....D.....Qb.oN.....N.....Qb.b.....U.....Qb^..M....w.....Qb./X.....T.....Qbn.....q.....QbfK.....P.....Qb.D.....R.....Qb..h.....O.....QbF.... ...V.....Qb.....j.....Qb..+.....x.....Qb:.....M.....Qb.$.}....F.....Qb..OU....J....Q.$...$.....$.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\990da70a3b3900c1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.685273720641507
Encrypted:	false
SSDEEP:	6:mmvYk+f2pomWLiKlZQvnS5hmJ2plAHll3rS43K6t:T7++amvKlZgmkJqlYW2
MD5:	E007F8FE4B9D572BFD776EF565F4FAF5
SHA1:	EC61CE56191DA8DAFA44A043B29D4F8553931B7E
SHA-256:	7E35803C6CD7DBFFBBEB71FD2442535D30C9DD98C95C3A48D4D4C6AE9CCD29AF
SHA-512:	0E41A42B06FE221B54FD30FBE8C5DCFE06D5E8306C1A65ECF012EF87F1542543767A8664A7713D6CC28EF8C1C004E3F74A76C468EA7A02D8D0C79BE468E1BA F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....fZ....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iril4/yW/l/en_GB/3V96puac_8e.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com//;.."./.....HG.....D..s..us.;..' .}u..I-!..n.....2..A..Eo.....[.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9b8a68cfae070dc9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.76357186976228
Encrypted:	false
SSDEEP:	6:m3Oq9Yk+f2pomWj6KHA3zhmJ2DAAkgLfd497K6t:gh++amfKHszkJdgLfdQ
MD5:	B3D7F39A2296E67C7DC65B8364A953E0
SHA1:	2AE4A06A8C19B24FBF3C9E565962380B9C804120
SHA-256:	A7BD0730B31BB686F6972D2607F1553D4044837C52DF717F5DD9178D0AA2D125
SHA-512:	36F3C65C136DF396EE7F8552D9E48FA474CA158B1ECF7182C1F9608C16043DF937817BFE284158C4B2489AB12CD17A96A2042FFDF13579B8D292FF64025543FA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....V....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3izT64/y6/l/en_GB/jC6WAaCopOO.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.:.."./.....G.....V...J..w....%.. .....fS.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a56d2be969db972e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.819290638690836
Encrypted:	false
SSDEEP:	6:m5JYk+f2pomW3nKHPjwhmJ2fAEg3mY9H+4zRK6t:W++am2KvUkJSg3mIrr
MD5:	6D5D92C4EC3BCA8ECB866A5FDA636D2C
SHA1:	5F88B9D4FFEF1E4B802E9622E6507455162A4481
SHA-256:	081D0692A322BFBE8EB86BD98594D66739E6F6405DC2D400E3C066765B935FC3
SHA-512:	77B55A2442004874E092D13D7008CF8F89CF3B3389229A64F94D458B80AD14D9DE9916AD498F78D4E7AE1D90E8AC35E6AB2DFBA0EF43ACA131F66DB36B4B8B F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....>8....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3ig1H4/y9/l/en_GB/2rv8CRYU2U8.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.8.."./.....SF.....`4. ....9.x?.A...+..gD...O..5...A..Eo.....2.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a8e071ae86cd7f79_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	9525

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a8e071ae86cd7f79_0	
Entropy (8bit):	5.7039212882434045
Encrypted:	false
SSDEEP:	192:drEoucT2D7P/Jh0jZcMWe7cW+nCk2tiJrlMkd7MbYew/GUHqM:pjSKWeanCkjBlfwbFw/GqB
MD5:	806E9CC73B6066AD2AEC99D3EE6ADC85
SHA1:	C2A6BE467B19F4F6D8533842971D35B9A4F5BB3A
SHA-256:	595BD2981FD236F58623E161ED1FC52D281B015B078FE68486AD997721F1DC9C
SHA-512:	C9F78F70DC139C592AA3D2551B4D6C0EF9DF4DE7F9194AA8C4173699FBFA8C7B35758FC3C40F3C1E5E209EA174E0B5C574F5D4A5D6A56D3297BC6CFDF6DD80D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e.....Q...._keyhttps://pastebin.com/themes/pastebin/js/app.bundle.js?677fa6bd2113231028dd .https://pastebin.com/.'..''./.....''F....s..4:..qk*D.Jd.o<.. ...A..Eo.....I.....A..Eo.....'.j7....O.....#....n.....(S.h..`.....L`.....(S.)..`.....pL`4....`Rc,.....Qb.B.....t.....Qbv.....n.....Qb.P.....o.... ..S....M...Qb6.u.....s.....R..f$.....I`....Da.....(S.M..`P....(L`.....M.....Qe.....hasOwnProperty....Qb*`.3....call..Qb.....push..Qc.}.....shift.....K`....D...x..... ....*..&...*..&...*..&..&.|.&.(...i...e%.*..&....&.(...&.(...&..(...&...&.Z.....).&.%.*....(...&...&.%.*..&..*..&.Y.....&..0.. %.L"&..i.%..Qw.....#.&...B....#.4&....&.(...&.(..$&.(..&&.Z....(....&.% .*.*&.0..,%..&..B.....&.]...(..0..(..2&.X..4&.\.6.....&.(...&.(..8&...&.%...|:&.Z....;..&.\.=....,Rc.....Qb~.k.....e...`....Da....P.....8..l?..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ad8d8e34f02141c1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.687467781273426
Encrypted:	false
SSDEEP:	3:m+lY3346v8RzYkwLf3G9Lomwp2zV2QufRJ2VnLlHCSUXIqtQSNQtoMmCB7XlpK5M:m2Yk+f2pomwpEhmJ2NEf4qz3n07DK6t
MD5:	82E24E9752F114376A68C531AA42BE97
SHA1:	E59803AF75E8C34166835C598CDB3E2988E45698
SHA-256:	C838EB183E781A1E278BAED5D3E5A1D6D73221654C90D1C3FC2C96DFB5347C0C
SHA-512:	987AD7B46B8E3DE7B7F1D53E705B7D71FF7E44374CBC4B05E31C58219AC615FA143B50017851E04CB7338419DC76505699A2C85D1BD8157BC7E1C5964501AF3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....~R....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yH/r/7oVtGLsr9D2.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/-...''./.....F.....d... ..yHe...~.. {..MF .W.N5U...A..Eo.....C~.2.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b2be8dd0840c2c39_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	246
Entropy (8bit):	5.610683105312271
Encrypted:	false
SSDEEP:	6:mQ/VYH5PLcNKPbGk626CtQHaMqbwll/0/E5/f6D+onIRK6t:LI5oSbR6TCiH50/Q/gXIr
MD5:	D58F589106176E79180CDC767172D197
SHA1:	DC22AC0FCBAFFF87EEE90972753F852226A7FF38
SHA-256:	FD613FD369BB00ECA9E5778C0FB0C2DF5BC0AD3F3F8F727C12D292AF494C85A9
SHA-512:	AA20434750E59913AAB08B950968FD36B95362E0329ED446CE449E639DD38AB8EE6EE1F4099588AE662BB2531999AB2EA763ABC34E717FAB6E246C80EAFF26FF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r...B4....._keyhttps://abs-0.twimg.com/login/authorize_page.c4edf9ccaf94a42b6963991691957aaa827aa56b.js .https://twitter.com/..5.''./.....R.....7...8..... :s....ff.....u.I..A..Eo.....L.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b768a36c464a700e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.690254925318816
Encrypted:	false
SSDEEP:	6:mS4ol/lXYk+f2pomBM0ahmJ2Gmlt+cn/KK41nK6t:r44lz++amBNakJ2XMhp
MD5:	1C02B0AF51F8C389CAFEC6589C940EB2
SHA1:	B3ED27B997BC468A96BD105BC766B0F0D41FE22C
SHA-256:	962623A5010CC8FF0602846ACA24D51E138A003BCE76303C0C44B41F1A2A0555
SHA-512:	42DCC63F575571E78B9811ACE541778715A0909C39FAC48EEB7E5E6A4D994A1F3F2EC421DC1644064C994F7589660ED4C5681EFB2AF1F41A771FC18CCFAF5F2
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b768a36c464a700e_0	
Reputation:	low
Preview:	0\r..m.....h.....]M...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yj/r/n3LKZtESrJ0.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.<..".../.....\F.....L.'....D-I.tq...}..%iJ..-Z..A..Eo.....E@O.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b9ee1cc115ed86f4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	340
Entropy (8bit):	5.878934354396993
Encrypted:	false
SSDEEP:	6:msvEYEoatRKelvt0z+MJJ66P41YhK6t9vMggSE0ei+MJJ66P4P/:bMoajYiMJJrAkLcTMJJre
MD5:	04FF77E121ABFB84BA050BD2F141C2E9
SHA1:	38BA4CB5EA3397D464B225055728D45283740E02
SHA-256:	11481DE1F1EF8BF4CC64A02CE2EA09DD5A318393B9AB6CB2634608FBB177F70C
SHA-512:	6A5E2974743B7053E492C6553063C2B36F6BB986B4D37AE6B5E6BFC4912C9860D85FB2BA4B8EB1EB1E17D4639BC560000616CDFAE9FADF6DC48457CA35E0327 9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L...g_.J...._keyhttps://cdn.snigelweb.com/prebid/latest/prebid.js .https://pastebin.com/..."./.....s".....)...F. y.OQ.1.....^.|5..A..Eo.....7.0c.....A..Eo..... ....."./.h...90C2920E4F15A78ABECDD9B4DE3F757D67A7E2A01AF692914D2B37396488930B.s".....)...F. y.OQ.1.....^.|5..A..Eo.....{.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bbf6347a22a48602_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	295696
Entropy (8bit):	5.8700565298097445
Encrypted:	false
SSDEEP:	3072:KvqvTaGiW1VirFZfnQXS+hNB4ceqGpOLuCCZ93bzgJdK6BV33Y7DRLyopl:E2Hq3nQphNuc/78ZhoRgLyoH
MD5:	4459162F0CB9968A492439C0B5E32EC7
SHA1:	2A42A6A24BB592E853D3FFD41E55C9E7E7A463BC
SHA-256:	776B17FC70F5E111D664F2FF684939BB7FB70C2840DC5F3DBD2B710473535411
SHA-512:	1C9D8A5ADA3CC4514D63270063F72C82E51C58FC3781C57E1089AEC778696528BC96B078E58BDD291C704E58E4F7A1D6184DA71B24C700B696CDE8301060865
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....C.....90C2920E4F15A78ABECDD9B4DE3F757D67A7E2A01AF692914D2B37396488930B.....'.....O[.....x.....(...d.....%..... .....D.....d.....T.....t..... .....(S...e...`.*.....).L`.....(S...`,....TL`&....PRc$.....R....Qb6.u.....s.....Qbv.....n.....Qbvwf.....d.....Qb.h.....f...d$.....l`....Dal..... (S...`.....L`.....Q.@Z.;N....exports..$..a.....S.C..Qb..!U....I...H..."...a.....Qb*`.3....call...#..K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&. (...&.(...&...&.'..W.....-...(.....,Rc.....q.`....Da.....q.....e..... P.....@....@.-....@P.....1.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bc432d8b882001fd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.776229726580351
Encrypted:	false
SSDEEP:	6:mJ/gEYk+f2pomW9WaiKhxhmJ2irbUll/s8GQlC+/T/ZK6t:qIU++am6piKjkJdMs+Y4/T
MD5:	9FF47432D4C88C5CBD1FCE5D607887D0
SHA1:	C02318F0522655534EAC149985220CC9C252A5D5
SHA-256:	A9DE0DD8ABDC2846CAB4F71D9677D1B201D06A900A5A34E1B399985C6A56005F
SHA-512:	76D6FD2473FDE363520409A992452BDC2B1F04BE9427B6B69A61704255E3CEC8169CC74B82A1803DFBF66C5DB127200540AF12951439CB49AA1585B0F4293335
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....'....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iX3c4/yP/l/en_GB/AMRwpQFJv6q.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...."./.....F.....T...L..?... ..lm.N.;....4...A..Eo.....J.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c4b5e6b0fcbddb62_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	35595

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c4b5e6b0fcbddb62_0	
Entropy (8bit):	5.859713733814106
Encrypted:	false
SSDEEP:	384:CgFeZ3BFOmOtcub3TYQUMt6p8tc/OiIhHwxbW7KMs1Cdli+Yc/kl+s+mxrhNt4qq:vQfOxP0fS6p1/ORd7frYcrNvOb
MD5:	AED4B350D95667B6F55803154CA5797B
SHA1:	04CAC37D022A3C0F44CAC0F49C978CB8ADEADB81
SHA-256:	D316A2FA510C91EF36E5BD8BF4151FE5FE5849CBBEFB99947D827B168EC50DBE
SHA-512:	5B115964CDC2147E4CDA99C21870FC15873CDC55AE232BE76CF06144C83FFC7AA6A04066DD63AF459E9EA00BEE83312C6E72444E31610B0395C8C3C914C990
Malicious:	false
Reputation:	low
Preview:	0\r..m.....{...D.YN...._keyhttps://pagead2.googlesyndication.com/bg/UBVKjIgL52oAupqoau5bmS4QFq3D8gEqQe5TpWWG23I.js .https://googlesyndication.com/.O..''./..... .....\.....6.3).... ~,.3.>..H...Y>..>.I.{.A..Eo.....W..I.....A..Eo.....'.....O....h....i.....0.....t.....(S.<..`2.....L`.....(S...`.....8L`.....\Rc*..... ..Qbj.....r.....Qb.(N.....Z.....f.....I`....Da....:....(S...`.....,L`.....Qd..q8....trustedTypes..Qd..K....createPolicy.$..a.....Qd.Bf.....createHTML..C..Qd&:..... .createScriptC..Qe.....createScriptURL.C.....q..... Rc.....O.`.....Qc.,.....console..m...Kd .....C...).....D.Q.(...0.....&.(...&.'..%...(.....%..'..(...&.}..)&.../...../...../. ..Z.....&..?&....&...%.....&.(....$....&.(...&.%.*..&...&.(...&.Y.....%....,Rc.....Q.`.....a8.....e.....0.....@.-....dP.....W...https://pagead2.googlesyndica

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c574393b20fd444e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.628157374335539
Encrypted:	false
SSDEEP:	6:ma/VYk+f2pomoDkmhmJ2r15//sNAn+M59konnGbK6t:dl++amoDpkJyv8NAf9koGN
MD5:	2B236FE8A976B72D3B6C4906148A3F0C
SHA1:	DD88CADA0C2F9A59E8255BFC499D488CFE871BEF
SHA-256:	FED4EF5856E10E85DC6A03EC56D71CFFADD26D988D4A9C1E40F389150230F760
SHA-512:	23E0901BAA04256D31F9D5E9DB243A11ED22DDFF88BDD89A34E8EAB6B12295E8C3AF88B99602DAD7EB40EF172B45CA08F68DA8C95B7C8367834C6239B43FAE 83
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....sS....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y5/r/RCtYq7ukb3F.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/}<..''./.....G.....I.e..eVCy.W...h...Z..... hbba0E..A..Eo.....oD.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c671a1e6d1566d7a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	353
Entropy (8bit):	5.90651044623654
Encrypted:	false
SSDEEP:	6:ma/A/VYoDaZC1HEHIrDX+tJuKvLKy9lu6tMOi1J77KkyYbvNDK6tgF2MX8iRh40M:s52ZCRLoxHu6tWZyQWMMXPs0sZy
MD5:	CE5F640FA78CE9386A56FDCD84B2F39F
SHA1:	A5171DFA27C8FB8FB23600BF703A7E5FA84CF7ED
SHA-256:	4CB66258ED6DFD7D99EF04126B0D7A5A6C61023EFE237B1D78C970C1E46816EE
SHA-512:	94B45AE305B1969BC9F4A1E2093A0AAAD161254F72B0DFEC091BDE0161438FDEDECCD4F11311DAE67B57A3ED1A9C536BB3D323080C1417602AE7CE83C16770 20
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Y.....C%...._keyhttps://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js .https://pastebin.com/Ni..''./.....-.U..3..+.....A.m..'.....9.A..Eo.....)..... .....A..Eo.....Ni..''./.....2280C8D6A0B73FE576A5A22DE0863CFB1404AB2AB9A234FA6B1D5CEAB3952335.-.U..3..+.....A.m..'.....9.A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cc58fa0ab9a66ceb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	460
Entropy (8bit):	5.405531302571067
Encrypted:	false
SSDEEP:	6:mG09YoK0B/PEgcNKCANazKGp0YvjRY7n5qDK6tWG09YoK0B/PEgcNKCANazKQ80R:ylJP6NKCANYzY4QlJP6NKCANYBKqr
MD5:	4B05D2BD7F7BB8A94B40815F3ED568FC
SHA1:	6544641FB54559B822FC75FDE239BE8C7EF289CB
SHA-256:	7B5B967BF4823A8FB408E964B5BB393DD919CA617179ABF5A3015A7FD5B02312
SHA-512:	8EE46A5C32BA3560DF1F90FC4DB6897A867CF3535592C4E588736F8BFF88205EB346119AC9030C33A6D7B495776C286A41ADE24BED1A01D4B307AA59768E210
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cc58fa0ab9a66ceb_0	
Reputation:	low
Preview:	0\r..m.....b....4Q....._keyhttps://pastebin.com/cdn-cgi/challenge-platform/h/g/orchestrate/jsch/v1 .https://pastebin.com/pv..".../.....0.....Qc.~2#.s.T.....Q.....m}.| .A..Eo.....P.....A..Eo.....0\r..m.....b....4Q....._keyhttps://pastebin.com/cdn-cgi/challenge-platform/h/g/orchestrate/jsch/v1 .https://pastebin.com/...."./..... 6.....Qc.~2#.s.T.....Q.....m}.|.A..Eo.....1.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cf6d21810551f26a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	27737
Entropy (8bit):	5.975709128958262
Encrypted:	false
SSDEEP:	384:sD46yI7ZOUOZ/Y00IY7ZkDfxlNB8AZn97D6vfWwB+7lFORaSJFzygrTSao1zPSo9:m46yECSkDD1aWwcpkUgPqgx2JS6
MD5:	FD1ABB680F791E8F52F69D8527BF0EC2
SHA1:	CDBB1C367976E2EA28040CEE36C0EFBA324DF3C9
SHA-256:	9A821117378FAF4264118331C7570042E0FEFBB587589FEE4E318DA3F2FC339A
SHA-512:	3F9D1B6B22EE032D5B3DF6BDE7585D1563A96D043EA2DA639718B8906F0A3ACDF0473B2C4AC211B961EE65B09C4FC42237E971F587514620FDD1E68497557C8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i....,.I...._keyhttps://pastebin.com/themes/pastebin/js/vendors.bundle.js?677fa6bd2113231028dd .https://pastebin.com/J..."./.....#....v&..IL*o..b[f6...h >;oS.A..Eo.....Tr4.....A..Eo.....'.....O....j....M.....P.....$.....(S....`.....L`.....Qc..dm....window....Q.P...}....webpackJso np..Qb.....push....`.....L`.....`.....Ma.....`.....`.....L~.....E.q..... .....(S.....IaA...._.....E. ...!+.....@.....@.....@.....@.....@.....@.....@.....@.....@.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d6d3525fe6fa5ceb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.6100751435340594
Encrypted:	false
SSDEEP:	6:mr9Yk+f2pomA6WWxzhmJ20bTUEgSlDAsMl4g7DK6t:I++amFWW5kJQEg2AsMr1
MD5:	EB748D8134B9E070376581D78C142A14
SHA1:	2AF2D821B1B8FF6ED63B033145621EA391B3B9D0
SHA-256:	80FE7AC3CECD6365235D656B620CD296B2DB668146E91CCB3230FEFB3A947D56
SHA-512:	DAC6F1856E5872DAAF70EDE2A4E8C053583D323FB6C4C42AAFFAFCD9E26D415BB23C12470A30196A0E6B78F30B180A961094720BB9532FCFE554EC95A77B825 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...h..w...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yy/r/LavfStOeKlK.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.e..".../.....F.....a.n.....~w.....o.e?.....X..i- 6...A..Eo.....x.p.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\db650fda12315775_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	217320
Entropy (8bit):	5.687103362666854
Encrypted:	false
SSDEEP:	3072:vki202MvSWH1JmMabnyfhJ3rTy1WGt3ur3di2OtfxtHUT3lr:ciDVoj6J3UWMdnu3N
MD5:	861CB76939E3F291818A02F58D9E1FDA
SHA1:	D82A5140FE8DC76BD52683B1A0AFB8E879CE0896
SHA-256:	48ED1581F314F79A3D16AB98898080CAD9E90794B54FB084022DFEA004EE5C47
SHA-512:	93DB246B4DCD8DBEA1A57E369BCF9C413C8F84BCFC7B4941DEAD265AF5579953FCA77EA7AB1B79F6D68A3D4A047A7C52C541C8B11783E647C4B44E56C9DC9 451
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....N<a....34DF60C745AE4FCA779EC05816092C46C1A710BF7E6B92F2BF3F2F3BFAD66246.....'..T....O;...(O.....h.....,'.....\#..... ....d.....(S.@..`:....L`.....(S...i..`.....L`.....-'Rc..... .....Qbjm_"...._.....Qb.*w.....ba....Qb.....aa....Qb.c.....da....Qb.n.'....ea....Qb.m1.....fa....Qb..$.....ja....Qb2.m.....la....Qbf.....ma....Qb._hY....ka....Qb..q....na....Qb..... ...oa....Qb.O.....pa....Qb..X"....sa....QbZs.p....ua....Qb.x).....wa....Qb.?.O....ya....Qb.}.....Ba....Qb.:.H....Da....Qb.....Ea....Qb.25c....Fa....Qb.A.....Ga....Qb..m.....Ha....Qb..... ..Ja....Qb"..P....Ka....Qb.....Na....Qb.....Qa....Qbn..b....Wa....Qb*.{.....Za....Qb...|....gb....QbR].U....jb....Qb..n.....kb....Qb.....nb....Qbb.....ob....Qb...~....lb....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\de320dffa40055dd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	64902
Entropy (8bit):	5.7223892528471785
Encrypted:	false
SSDEEP:	1536:gPWv1Xnpxq4MEU9kwLNFnUyrfiUiLDMaJVNXI/HTNRAe:guB+FEU9ksNFnUyUDM0VNY/BRAe
MD5:	B92D353A95643591177E7E2FB1B7444A
SHA1:	A80E12155F5335613263815EC988EFCF3723DFBD
SHA-256:	1522E3AB5385746E4B619057939ECD14F6B7E8D279969E4257FAA6EACB91A890
SHA-512:	EACF283716224FEC9615D60C1E80E62C8ACC845BD52D53A08D14C9D1748CBE9A37F5897E35E3AF944A3516E65EAC5693048122D36E317C05D56438741300E77
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V...I.F...._keyhttps://pastebin.com/assets/7ba4275b/js/select2.full.min.js .https://pastebin.com/..".../.....#.....^#..Q4v[#../...m.j.....%9+.A..Eo....,..... ...A..Eo.....'.A0....O.....o.....4.....|...\.....t.....(S.8..`(.....L`.....(S..`.....(L`....0Rc.....Qbv..... n...`$...I`....Da.....Q.@2..[....define....Qb..s.....amd.....`.....M`.....QcR.!.....jquery....Q.@.P.....module....QcZ.;N....exports..(S.....5.a....(....!....a....".....a....!.....q....a..... ....a.....a....a.....a.....a.....a.....Pc.....exportsa....?...I..!..@.-....HP.....;...https://pastebin.com/assets/7ba4275b/js/select2.full.min.js.a.....D`....D`....D` .....`....&...&....&....&.(S.`..`\|....$L`.....0Rc.....Qbvwf.....d...`$...I`....Da....~`...(S.....`.....L`@.....Rc^.....&

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\de4cc5865d5834f8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	97832
Entropy (8bit):	5.831971069971875
Encrypted:	false
SSDEEP:	1536:3lzbgFMM7U70QNq8Y53rQHgnoUUg0U76fuwXQH7hHUThxdTwpRVamt:2GMewRMLdrN6t
MD5:	BECB2D8ED3B5CD798B55FB19E6CE0BD7
SHA1:	DCC09E7D7D8E6ADEA00F4E628917BBFA0DF5643F
SHA-256:	7626EA85645E1BBF8852DD5982C59A9608B3AF0399FECA1F2B305ECBF6075D8E
SHA-512:	90D15D9CE101098949458295FA6F7499C2A3C6DFD7E6A9A604BC17FEDD8EB9CDDC9BFA64AD8C5F3A471155592A8812ECC36AAF7E294528CA875D874A7DA0B 3C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...i,.....FA9B0BADD9BCEAFBBBCD8BC74F58D34C55C2DDDA8EE0F26FC4B30C20B1342943.....'..]....O!....|....@.....`&..... .....`.....(S.H..`L....L`.....(S.p.`.....L`.....0Rc.....Qb.B.....t..`....I`....Da....j....Q.@.P.....module....QcZ.;N....exports.. .QcN.....document.(S.....5.a.....a.....a.....A....a.....a.....Pc.....exportsa..../...I.....@.-....@P.....2...https://pastebin.com/assets/ae9b8d97/jquery. min.js..a.....D`....D`....D`.....`....&...&..!.&....&.(S...a&..`|L.....L`.....Rcd.....*.....Qb..Z.....C.....Qb.g8.....r.....Qb6.u.....s.....R.....S...Qbv.....n.....Qb.P.....o.... .Qb.Q.....v.....M...Qb..!U....I.....Qb..0.....y.....Qb.A;.....m.....Qb..+.....x.....QbB..Z....E.....Qb.:.....c.....O...Qb^..M....w.....Qb..T....S.....Qb.?8....p.....Qb.L.....h.....Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\df10c594f19545b9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.676394992917124
Encrypted:	false
SSDEEP:	6:mCYk+f2pomTDs3cyOhmJ2nEdXllAzCOsyP48K6t:D++amvsKkJLXlazCOsyZ
MD5:	8640E30A47C1B6BA7E6EAD399369F57C
SHA1:	72BE9662999C3BFA0ABBEBA2BB1A4F1B8264F617
SHA-256:	29D9115DC287D6695E8B11440819AB8348F2AF88B6036774A59F8ECDD5F3A592
SHA-512:	41F19A57AF1DD65FC0E415E8416F67E6A94D218D8BC8D9E275C66E5E56A4D428976F531DDDF18D7EE9EB46308E2C045AF65D157E740003501C970346F41E7F0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....|....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yx/r/RPpa71t4yWJ.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...."./.....E.....V..X!.V.$..qX.+#....ZA ..|.j9.H.A..Eo.....n.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e3606adf4b207cfe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	329
Entropy (8bit):	5.707786881323933
Encrypted:	false
SSDEEP:	6:mG7YBZsrRgBWHo1r/9LvHZCOsyUy6fWG4k5K6t:UarRQWGr/9Lfjsj+Gbz

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e3606adf4b207cfe_0	
MD5:	DF7B77B70B4742BE54663419A259BB56
SHA1:	C889076934A947B8DDA5C0776F8C9628641EEBAF
SHA-256:	32989D9425E17F84684070F639057075C93CFFCB9B685666D2F0E4A6B438BEB1
SHA-512:	C676BEF8378F1E62CB00F7D03254A109C32FC709AC79D233E301605C37409D00DA33B900F4D0D111D5E08C627A3E7B4553A86D98AA647034CF38E68190393074
Malicious:	false
Reputation:	low
Preview:	0\r..m.....1.-'...._keyhttps://image6.pubmatic.com/AdServer/PugMaster?kdntuid=1&rnd=89367292&p=156657&s=0&a=0&ptask=ALL&np=0&fp=0&mpc=0&spug=1&coppa=0&gdpr=0&gdpr_consent=&us_privacy=1---&sec=1 .https://pubmatic.com/.D..".../.....7S.n'}...)z...?...d...b...w.A..Eo.....]6.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e397d3c67960a568_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.690924073367813
Encrypted:	false
SSDEEP:	6:mv5lXYk+f2pomWPKtmhmJ2yHx12glXeuLSvz/oDK6t:4f++amWKtmkJvlNWM1
MD5:	7D2F1FBDC5DFCB66A7AFD36DB785D4A5
SHA1:	B131DC1B3FD03C987279D582D268DB8E758AB317
SHA-256:	5A386C0AE09615CDF4422C34EC7E3DDEA44164A947933BA8B6FD1CE3868D776F
SHA-512:	9FB8D80D762EB18BEF67861F301EBF868611A4AD13E96CF86F5BCAC2444151D5B4617AB0B18330C5F65AE0C438526F3C98840371A0E5CD28DF1E13AF338F2BD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...K].@...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3ivYP4/y0/l/en_GB/CxSTYUY_wMJ.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/./..".../.....NG..... ..".n.cR/j....0...N...".9.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e4bd527a79e8a665_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	386
Entropy (8bit):	5.9173137179757935
Encrypted:	false
SSDEEP:	6:mgYvEdCN8uVvUCllDCMRFqsTNYxcb7WdYlGSHbK1VDw+yx+A+XcsVwCLvP49szbD:2Em80vbmMZdb7ySGSH3+iA9rDisp
MD5:	C13912A2A9ABE794F3F385AB4C0D1CF1
SHA1:	00A2B0E39E1A1B3B45791A1F4C29E661EA8EC72D
SHA-256:	A649502A5198C4546FACAF22CA0B220B3A5E11DEE0D4EADF4BBDE2292F833C7B
SHA-512:	F5FDFDB970B5255A7A8477216A15C66BAB343CBF283B12175DA7DF2A366B3E0690275DCDEC64E6CF6177368EC6837B338CC3775658B902CB4F4C4B13A8F7554
Malicious:	false
Reputation:	low
Preview:	0\r..m.....q...._keyhttps://ssl.gstatic.com/accounts/static/_/js/k=gaia.gaiafe_glif.en_GB.GR-XoYWnyYo.O/am=KwAAdiABMOAHAALMAwAAAAAAAAAMIBPKMk49rfD-JQ/d=0/ct=zgms/rs=ABkqax3dKZEgcQmwrv5rqONCea3zpQrSjg/m=sy1a,sy1b,sy1c,sy1e,sy1f,sy35,pwd_view .https://accounts.google.com/..p."./.....a.....#d?S)...4..rz..._.%.l.....Qj...A..Eo.....q.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e5dc652ef4939d65_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.676035262232318
Encrypted:	false
SSDEEP:	6:mVTXXYk+f2pomWyoKpLzhmJ2fAAXlZZD+NngK4ibK6t:4z++amYKhkJ2TJgnB
MD5:	BE5A9346BEF2BEA56F37FD5877AE59E9
SHA1:	A4DA8995FDACA5F020389BC724BE67C22462D452
SHA-256:	B1979857969C87854DA73976D7480B31937A97A53A2CF315C242ED6EE73706FD
SHA-512:	AC89CC8A5D42028D17ACDFC31324BDC96EA9D0BFD29298DEDD51FB52042DF1929BF292B09524D8BDCFA0224EA39021792BE2E518D7995415CEEDDB646D03E81
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s...q...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3ibnX4/yg/l/en_GB/nm3fR8eb6my.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.\.."./.....%G.....y.....-.mZ.q.|%}%x....6[6d....A..Eo.....h..G.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e8c668b936c8e2c4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.705893694602225
Encrypted:	false
SSDEEP:	6:m7/lgEYk+f2pomR37hmJ28fvpw5YiDK6t:itgU++amRrkJzaV
MD5:	E7676D04336EB7CD60316B24CD00395D
SHA1:	523AD45D109C410F6E86AED135F39253C89B44AB
SHA-256:	B7028D4C948302C571053FD86FB632E7EF0685B6486AB22702BC35C4C56E2F87
SHA-512:	24DEBBEF11F3A36F0FB775F450863E4F267B145BF3DCF4D5CEE2D2C86D4313A60AFD758BCB87CB8F97A1EE01E328BDC7F3434122CFB55F80A3BDD5523B3B7D16
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...D.M....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yU/r/aLxU7-VSlzO.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/...."./.....E.....u 4QM6E.6#Cp.....(.....<.r..A..Eo.....c,Dr.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f18a6f4c1dce03e1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4134
Entropy (8bit):	5.309158153853303
Encrypted:	false
SSDEEP:	96:WCJLO9HHrbiFzabDDh5iz1cjaV2Ed65kN:rOxHrOFz8DDh5i2jod65kN
MD5:	2D9B60A5040ADCAB4A62915966B342C2
SHA1:	739064515FF0C33D99F85BF186ADC32650BDD5DF
SHA-256:	8CFED9A86DC9119BC8BBA4C4E6C25AF8C752347ACD2784F12134AAC6208F236B
SHA-512:	C7ECE04E703876DF1676421FC834D27608A6A5918A66352617BE9D76241DB48174947367C6CD77DCEDDB18C4C00DD971C0CFC9BADE977AE02EBA9DFDC44870
Malicious:	false
Reputation:	low
Preview:	0\r..m.....F....._keyhttps://pastebin.com/assets/1745bc3b/yii.js .https://pastebin.com/...."./.....\8....7...L.v\....=P.....2.B.A..Eo.....7.V.....A..Eo..... "./.....'..Q....O.....M.....8.....(S.\..`n.....L`.....Qc..dm....window...(S..`J.....L`D....pRc4.....Qb.....pub...Qe.e.l....initCsrfHandler.. Qf...(....initRedirectHandler...QeBA.T....initAssetFilters..Qe..sg....initDataMethods.. Qf...k....isReloadableAsset.....Qdf2.....escapeRegExp..Qe...E....getAbsoluteUrl..h$..... .....I`....Da.....(S.....Ia.8..W9.....d.....p.r.....@.-....8P.....+...https://pastebin.com/assets/1745bc3b/yii.js.a.....D`....D`,...D`.....`N...&...&....&.(S.....5.a..... .....a.....a.....Qb...*....yii....a.....a.....a.....Qd.1.....getCsrfParama.....A.d.....&.(S.....a.....

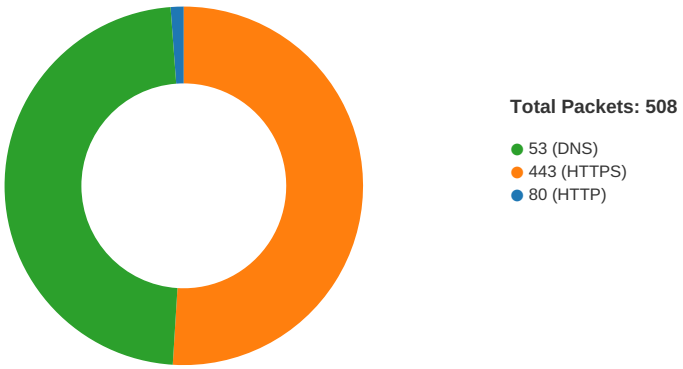
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f49494b8265cf4a1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.6513265735913025
Encrypted:	false
SSDEEP:	6:mhYk+f2pomynbLxzhmJ29/l1NaF44Hcm4IK6t:Q++amsv5kJoAaFXb9
MD5:	2C6F2311A111037A7801CBBBE759F4E0
SHA1:	5E7E5440BE53178F2780A718A65A0A210A5D0CA3
SHA-256:	FFC7F12675E3747765AB7C59DE50052875438B8DB5182EB3A54A1064787CCC3D
SHA-512:	85FFA43344E5309C3FD7D02FF9B986ADE1ADD63A1C801697160EE72A8D057B21DBF2A02B822F711BA400CEE8A5669EAC0FDB6D36AFEEFE7FF21EBB6948E79C0A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....be...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yk/r/PVV3KMbMu_m.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.4.."./.....G.....Hq...}H..j..`1I.s..):o.., ..._.A..Eo.....w.....A..Eo.....

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:12:26.336673021 CET	49742	80	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.337466002 CET	49743	80	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.352963924 CET	80	49742	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.353499889 CET	49742	80	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.353768110 CET	49742	80	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.353849888 CET	80	49743	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.354018927 CET	49743	80	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.370120049 CET	80	49742	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.379285097 CET	80	49742	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.391675949 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.408066034 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.408168077 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.408548117 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.420984983 CET	49742	80	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.424869061 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.429279089 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.429313898 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.429366112 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.573252916 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.573549032 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.573846102 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.589520931 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.589580059 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.589766026 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.589804888 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.589862108 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.590049028 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.592720032 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.608886003 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.815417051 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.815465927 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.815505981 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.815527916 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.815531969 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.815570116 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.815577030 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.815608978 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.815645933 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.815649986 CET	49746	443	192.168.2.4	104.23.98.190

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:12:26.815686941 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.815725088 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.815735102 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.815771103 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.815792084 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.815819025 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.815835953 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.815886021 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.901738882 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.902316093 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.902802944 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.903238058 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.903687000 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.904602051 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.904902935 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.917989016 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.918428898 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.918992996 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.919435024 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.919833899 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.920768023 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.921205044 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.925668001 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.925698996 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.925735950 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.925767899 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.925775051 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.925811052 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.925822973 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.925831079 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.925862074 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.925900936 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.925913095 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.925929070 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.925946951 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.925965071 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.926008940 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.926012039 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.926054001 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.926090956 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.926100016 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.926119089 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.926156998 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.926157951 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.926204920 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.926220894 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.926259995 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.926273108 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.926297903 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.926307917 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.926335096 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.926372051 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.926381111 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.926400900 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.926425934 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.926440954 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.926460028 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.926501036 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.926506042 CET	49746	443	192.168.2.4	104.23.98.190
Dec 3, 2020 10:12:26.926532030 CET	443	49746	104.23.98.190	192.168.2.4
Dec 3, 2020 10:12:26.926568031 CET	443	49746	104.23.98.190	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:12:17.245426893 CET	63153	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:17.272476912 CET	53	63153	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:18.225800037 CET	52991	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:18.252837896 CET	53	52991	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:19.314163923 CET	53700	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:19.341337919 CET	53	53700	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:20.385189056 CET	51726	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:20.412635088 CET	53	51726	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:22.813240051 CET	56794	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:22.848704100 CET	53	56794	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:24.524373055 CET	64078	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:24.551578999 CET	53	64078	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:26.299901962 CET	61522	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:26.300029039 CET	52337	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:26.300647974 CET	55046	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:26.301744938 CET	49612	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:26.327651024 CET	53	55046	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:26.335483074 CET	53	61522	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:26.343347073 CET	53	52337	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:26.344528913 CET	53	49612	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:26.657056093 CET	49285	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:26.700726986 CET	53	49285	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:26.744187117 CET	50601	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:26.802608967 CET	53	50601	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:26.917963982 CET	60875	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:26.918000937 CET	56448	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:26.918109894 CET	59172	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:26.945103884 CET	53	56448	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:26.945133924 CET	53	59172	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:26.961659908 CET	53	60875	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:27.325207949 CET	62420	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:27.326231003 CET	60579	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:27.327378988 CET	50183	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:27.327467918 CET	61531	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:27.354110956 CET	53	60579	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:27.364053011 CET	53	50183	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:27.369671106 CET	53	62420	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:27.372205019 CET	53	61531	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:27.748723984 CET	49228	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:27.775727034 CET	53	49228	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:27.782821894 CET	59794	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:27.783704996 CET	55916	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:27.810651064 CET	53	55916	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:27.829200983 CET	53	59794	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:27.842152119 CET	52752	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:27.885725975 CET	53	52752	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:27.919291019 CET	60542	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:27.929992914 CET	60689	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:27.964337111 CET	53	60542	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:27.973257065 CET	53	60689	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:28.075761080 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:12:28.082495928 CET	64206	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:28.083225012 CET	50904	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:28.099659920 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:28.099699974 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:28.101353884 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:12:28.102123976 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:12:28.109671116 CET	53	64206	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:28.124882936 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:28.125794888 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:12:28.126619101 CET	53	50904	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:28.134988070 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:28.135031939 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:28.135070086 CET	443	60690	172.217.21.194	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:12:28.135107040 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:28.135142088 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:28.135188103 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:28.135230064 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:28.135266066 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:28.135303020 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:28.135339975 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:28.135375977 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:28.136094093 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:12:28.136145115 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:12:28.136197090 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:12:28.136254072 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:12:28.136271954 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:28.136302948 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:12:28.136320114 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:28.136360884 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:28.136390924 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:28.136465073 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:12:28.136507988 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:12:28.162749052 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:12:28.252854109 CET	57525	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:28.261504889 CET	53814	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:28.262861967 CET	53418	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:28.263695955 CET	62833	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:28.272394896 CET	59260	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:28.279916048 CET	53	57525	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:28.288590908 CET	53	53814	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:28.290676117 CET	53	62833	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:28.299287081 CET	53	59260	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:28.308960915 CET	53	53418	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:28.351464987 CET	49944	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:28.378444910 CET	53	49944	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:28.512655020 CET	63300	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:28.512725115 CET	61449	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:28.548233032 CET	53	63300	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:28.557843924 CET	53	61449	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:29.006472111 CET	51275	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:29.042259932 CET	53	51275	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:29.148386002 CET	63492	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:29.149069071 CET	58945	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:29.149506092 CET	60779	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:29.150163889 CET	64014	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:29.150311947 CET	57091	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:29.175544977 CET	53	63492	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:29.176031113 CET	53	58945	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:29.176489115 CET	53	60779	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:29.177083969 CET	53	64014	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:29.187496901 CET	49374	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:29.193732977 CET	50436	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:29.197278023 CET	53	57091	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:29.220659018 CET	53	50436	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:29.230644941 CET	53	49374	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:29.268937111 CET	62605	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:29.295989037 CET	53	62605	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:29.405745983 CET	54256	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:29.405982018 CET	52189	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:29.411670923 CET	56131	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:29.441415071 CET	53	52189	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:29.443034887 CET	53	54256	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:29.449024916 CET	53	56131	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:29.452529907 CET	62992	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:29.453927994 CET	54432	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:29.479554892 CET	53	62992	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:29.480864048 CET	53	54432	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:12:29.637636900 CET	57227	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:29.643055916 CET	58383	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:29.643812895 CET	63136	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:29.670764923 CET	53	63136	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:29.676676035 CET	53	57227	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:29.686672926 CET	53	58383	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:29.720144987 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:12:29.722402096 CET	50911	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:29.761771917 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:29.767719984 CET	53	50911	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:29.806308031 CET	63409	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:29.809192896 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:29.809223890 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:29.809509039 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:12:29.833322048 CET	53	63409	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:29.900875092 CET	59185	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:29.923171997 CET	64236	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:29.927848101 CET	53	59185	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:29.948225975 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:29.950113058 CET	53	64236	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:29.971879959 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:29.971932888 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:29.973247051 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:29.973468065 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:30.003994942 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:30.004491091 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:30.017759085 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:30.017802954 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:30.017838955 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:30.017884970 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:30.017925978 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:30.017960072 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:30.017988920 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:30.018218994 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:30.018269062 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:30.018275976 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:30.030256987 CET	56157	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:30.043545961 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:30.076150894 CET	53	56157	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:30.119482994 CET	55601	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:30.145016909 CET	52984	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:30.146634102 CET	53	55601	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:30.147664070 CET	51141	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:30.151262999 CET	53610	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:30.189182043 CET	53	53610	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:30.190382957 CET	53	52984	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:30.190975904 CET	53	51141	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:30.246006966 CET	61247	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:30.248989105 CET	65165	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:30.251054049 CET	52076	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:30.272983074 CET	53	61247	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:30.276062012 CET	53	65165	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:30.277926922 CET	53	52076	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:30.307475090 CET	54903	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:30.344809055 CET	53	54903	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:30.418351889 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:30.419997931 CET	55045	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:30.422847033 CET	54464	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:30.442011118 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:30.442049980 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:30.443463087 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:30.443744898 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:30.458209991 CET	53	54464	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:30.462146044 CET	53	55045	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:12:30.474416971 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:30.475374937 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:30.486135960 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:30.486167908 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:30.486520052 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:30.489217043 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:30.531256914 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:30.573213100 CET	50970	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:30.600167036 CET	53	50970	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:30.648503065 CET	55261	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:30.675499916 CET	53	55261	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:30.710931063 CET	59809	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:30.738059044 CET	53	59809	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:30.770858049 CET	51278	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:30.797924042 CET	53	51278	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:30.889931917 CET	51932	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:30.916914940 CET	53	51932	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:30.980268002 CET	59494	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:31.007373095 CET	53	59494	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:31.070089102 CET	55915	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:31.097199917 CET	53	55915	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:31.264655113 CET	49779	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:31.291832924 CET	53	49779	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:31.388993025 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:31.400249004 CET	49458	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:31.417011023 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:31.417041063 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:31.417627096 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:31.418373108 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:31.449318886 CET	53	49458	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:31.459903002 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:31.470916033 CET	57164	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:31.498030901 CET	53	57164	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:31.519596100 CET	49840	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:31.530765057 CET	57174	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:31.546766996 CET	53	49840	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:31.557796955 CET	53	57174	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:31.577774048 CET	58531	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:31.604883909 CET	53	58531	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:31.681754112 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:31.708538055 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:31.709022045 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:31.709196091 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:31.710391998 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:31.731976986 CET	49608	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:31.752904892 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:31.764400959 CET	55682	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:31.768565893 CET	62436	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:31.769035101 CET	53	49608	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:31.772485018 CET	61230	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:31.775664091 CET	64730	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:31.775944948 CET	60624	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:31.797760010 CET	62600	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:31.799555063 CET	53	61230	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:31.799654007 CET	53	55682	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:31.803966045 CET	53	62436	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:31.812740088 CET	53	60624	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:31.812983036 CET	53	64730	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:31.824805021 CET	53	62600	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:31.997955084 CET	53200	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:32.013290882 CET	61034	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:32.024908066 CET	53	53200	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:32.035903931 CET	57687	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:32.073081017 CET	53	57687	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:12:32.098479033 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:32.115386963 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:32.115432978 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:32.115484953 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:32.115523100 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:32.115561962 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:32.115906954 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:32.115940094 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:32.141417980 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:32.201543093 CET	53	61034	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:32.377227068 CET	49839	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:32.390736103 CET	57975	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:32.404186010 CET	53	49839	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:32.406308889 CET	57610	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:32.417644024 CET	53	57975	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:32.444205999 CET	53	57610	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:32.464236021 CET	55137	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:32.491159916 CET	53	55137	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:32.508452892 CET	59216	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:32.556216002 CET	53	59216	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:32.704899073 CET	63495	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:32.707390070 CET	64371	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:32.731950998 CET	53	63495	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:32.745358944 CET	53	64371	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:32.828732014 CET	54037	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:32.840478897 CET	53481	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:32.841274977 CET	58313	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:32.844875097 CET	58950	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:32.849318027 CET	55011	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:32.856019974 CET	53	54037	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:32.872056007 CET	53	58950	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:32.876769066 CET	53	58313	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:32.877597094 CET	53	53481	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:32.884644985 CET	53	55011	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:32.988020897 CET	57198	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:33.015130997 CET	53	57198	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:33.089584112 CET	60875	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:33.122256041 CET	55134	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:33.124979019 CET	53	60875	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:33.128129005 CET	53695	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:33.137598038 CET	50975	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:33.142302036 CET	65460	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:33.149255991 CET	53	55134	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:33.168677092 CET	53	53695	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:33.174869061 CET	53	50975	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:33.177757978 CET	53	65460	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:33.193928003 CET	63669	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:33.220918894 CET	53	63669	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:33.276611090 CET	51653	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:33.303751945 CET	53	51653	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:33.425713062 CET	56473	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:33.430361986 CET	61454	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:33.452225924 CET	54323	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:33.452867031 CET	53	56473	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:33.465816021 CET	53	61454	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:33.488857031 CET	53	54323	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:33.495254993 CET	59960	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:33.522258997 CET	53	59960	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:33.623888016 CET	50205	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:33.650801897 CET	53	50205	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:33.872941017 CET	50896	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:33.910077095 CET	53	50896	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:34.092277050 CET	59151	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:34.127713919 CET	53	59151	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:12:35.161489964 CET	61227	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:35.181368113 CET	54676	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:35.200778961 CET	53	61227	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:35.218913078 CET	53	54676	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:35.358144045 CET	65030	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:35.385051012 CET	53	65030	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:35.532684088 CET	61740	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:35.568140030 CET	53	61740	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:36.334948063 CET	59708	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:36.370603085 CET	53	59708	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:36.378434896 CET	54044	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:36.403470993 CET	56932	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:36.405549049 CET	53	54044	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:36.423006058 CET	57817	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:36.430538893 CET	53	56932	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:36.450054884 CET	53	57817	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:36.551656008 CET	59556	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:36.565273046 CET	57540	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:36.570408106 CET	62337	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:36.578702927 CET	53	59556	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:36.592137098 CET	57550	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:36.592196941 CET	53	57540	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:36.607680082 CET	53	62337	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:36.627707005 CET	53	57550	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:36.999288082 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:37.000471115 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:37.001869917 CET	63523	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:37.023058891 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:37.023103952 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:37.024152040 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:37.024189949 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:37.024457932 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:37.024724007 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:37.026292086 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:37.026783943 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:37.028755903 CET	53	63523	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:37.055316925 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:37.057060003 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:37.065764904 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:37.066910982 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:37.074501038 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:37.074919939 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:37.080372095 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:37.080817938 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:37.084546089 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:37.085248947 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:37.092108011 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:12:37.093359947 CET	59501	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:37.133897066 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:37.137325048 CET	53	59501	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:37.187093973 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:37.187145948 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:37.205301046 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:12:37.241095066 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:37.270267010 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:37.270320892 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:37.270360947 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:37.270399094 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:37.270437956 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:37.270464897 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:37.270500898 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:37.280102015 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:37.280139923 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:37.280145884 CET	64237	443	192.168.2.4	172.217.23.162

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:12:37.325416088 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:38.313595057 CET	60033	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:38.340480089 CET	53	60033	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:38.443984985 CET	62142	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:38.459532022 CET	54705	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:38.470942974 CET	53	62142	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:38.471903086 CET	54769	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:38.486473083 CET	53	54705	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:38.499622107 CET	60082	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:38.514048100 CET	60240	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:38.526689053 CET	59532	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:38.529767990 CET	53	54769	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:38.535257101 CET	53	60082	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:38.536422968 CET	50931	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:38.540898085 CET	53	60240	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:38.547060966 CET	56567	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:38.562277079 CET	53	59532	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:38.563225985 CET	53	50931	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:38.582454920 CET	53	56567	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:38.586107969 CET	59510	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:38.612987041 CET	53	59510	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:38.682240009 CET	53157	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:38.709140062 CET	53	53157	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:39.709233046 CET	62793	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:39.710745096 CET	51090	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:39.710797071 CET	57527	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:39.722665071 CET	55890	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:39.731103897 CET	51042	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:39.736223936 CET	53	62793	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:39.737694979 CET	53	57527	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:39.747378111 CET	53	51090	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:39.758143902 CET	53	51042	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:39.765779972 CET	53	55890	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:39.787273884 CET	49373	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:39.814460039 CET	53	49373	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:39.870150089 CET	52387	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:39.907367945 CET	53	52387	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:40.106012106 CET	50258	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:40.142749071 CET	53	50258	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:40.158488989 CET	52792	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:40.185560942 CET	53	52792	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:41.267451048 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:41.295042038 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:41.295892954 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:41.296067953 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:41.322088957 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:41.337872982 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:41.747684002 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:41.748280048 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:41.773547888 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:41.773590088 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:41.774183035 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:41.774673939 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:41.774738073 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:41.775886059 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:41.799839020 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:12:41.805007935 CET	54917	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:41.837750912 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:41.848396063 CET	53	54917	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:41.862052917 CET	65064	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:41.864684105 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:12:41.910768986 CET	53	65064	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:41.990834951 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:42.000933886 CET	54905	443	192.168.2.4	172.217.23.162

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:12:42.007431030 CET	49902	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:42.016918898 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:42.016954899 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:42.017376900 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:42.028120995 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:42.028162956 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:42.028497934 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:42.033735037 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:42.034549952 CET	53	49902	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:42.075583935 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:42.085128069 CET	58996	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:42.112282991 CET	53	58996	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:42.121320009 CET	54566	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:42.126751900 CET	55142	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:42.131171942 CET	54588	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:42.148340940 CET	53	54566	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:42.163594961 CET	53	55142	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:42.167993069 CET	53	54588	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:42.370783091 CET	50471	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:42.414362907 CET	53	50471	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:42.436039925 CET	50272	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:42.462907076 CET	53	50272	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:42.862761021 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:42.890459061 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:42.890485048 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:42.891138077 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:42.891904116 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:42.934163094 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:43.405514002 CET	53956	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:43.432596922 CET	53	53956	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:43.632168055 CET	63503	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:43.669836044 CET	53	63503	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:44.230539083 CET	59690	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:44.257546902 CET	53	59690	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:44.331191063 CET	49991	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:44.358285904 CET	53	49991	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:44.415224075 CET	51971	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:44.442217112 CET	53	51971	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:44.464871883 CET	65451	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:44.501203060 CET	53	65451	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:44.752403021 CET	63643	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:44.787878036 CET	53	63643	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:45.241067886 CET	54839	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:45.288408041 CET	53	54839	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:45.561433077 CET	51941	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:45.581865072 CET	59439	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:45.587245941 CET	50450	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:45.588421106 CET	53	51941	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:45.614321947 CET	53	50450	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:45.618840933 CET	53	59439	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:46.680464029 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:46.697555065 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:46.697613001 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:46.697659969 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:46.697701931 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:46.697737932 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:46.697776079 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:46.697813988 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:46.697849989 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:46.697886944 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:46.697925091 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:46.697972059 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:46.698123932 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:46.698163986 CET	54905	443	192.168.2.4	172.217.23.162

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:12:46.698210955 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:46.698232889 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:46.698277950 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:46.724493980 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:47.711899996 CET	59497	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:47.717400074 CET	59073	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:47.720416069 CET	50418	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:47.731456995 CET	51556	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:47.744323015 CET	53	59073	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:47.747181892 CET	53	59497	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:47.747236013 CET	53	50418	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:47.748384953 CET	55321	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:47.758385897 CET	53	51556	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:47.764879942 CET	63370	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:47.775279045 CET	53	55321	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:47.787503958 CET	64115	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:47.790451050 CET	49472	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:47.800344944 CET	53	63370	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:47.814398050 CET	53	64115	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:47.826941967 CET	53	49472	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:49.371934891 CET	57321	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:49.399090052 CET	53	57321	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:49.405606985 CET	57107	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:49.432542086 CET	53	57107	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:49.449692965 CET	64271	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:49.484996080 CET	53	64271	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:49.719980955 CET	55229	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:49.755558014 CET	53	55229	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:49.968158007 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:49.994762897 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:50.021003962 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:50.484672070 CET	59500	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:50.489850998 CET	64972	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:50.496196032 CET	54842	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:50.499064922 CET	54860	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:50.511682034 CET	53	59500	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:50.533435106 CET	53	64972	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:50.533998013 CET	53	54842	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:50.534235954 CET	53	54860	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:52.243437052 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:52.285900116 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:54.781471014 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:54.781997919 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:54.807331085 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:54.807351112 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:54.808020115 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:54.846304893 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:54.850054979 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:54.938306093 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:54.978029013 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:55.046726942 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:55.139995098 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:55.140069008 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:55.166435003 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:55.167900085 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:12:55.209464073 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:55.237042904 CET	60146	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:55.270814896 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:55.280544043 CET	53	60146	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:55.292368889 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:55.304339886 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:12:55.322432041 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:55.322484016 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:55.322531939 CET	443	64237	172.217.23.162	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:12:55.322577953 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:55.322602987 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:55.322630882 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:55.323009968 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:55.323076010 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:55.323126078 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:56.097414017 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:56.123421907 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:56.123442888 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:56.123764992 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:57.890603065 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:57.893498898 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:57.916831970 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:57.916944027 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:57.917145967 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:57.919289112 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:57.924012899 CET	51231	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:57.927701950 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:12:57.930841923 CET	54018	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:57.946525097 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:57.967593908 CET	53	51231	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:57.969465017 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:57.974610090 CET	53	54018	8.8.8.8	192.168.2.4
Dec 3, 2020 10:12:58.015562057 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:58.015582085 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:12:58.015918970 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:12:58.035906076 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:58.070204020 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:58.070246935 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:58.070285082 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:58.070322990 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:58.070358992 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:58.070394993 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:58.070420027 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:58.070698977 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:58.070743084 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:58.070791006 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:58.097053051 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:58.796497107 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:58.822645903 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:58.822683096 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:12:58.822998047 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:12:59.095681906 CET	60902	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:12:59.122622967 CET	53	60902	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:00.451426029 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:00.452404976 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:00.477294922 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:00.477435112 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:00.477636099 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:00.479428053 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:00.479558945 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:00.479743958 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:00.484375954 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:13:00.486578941 CET	54737	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:00.526189089 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:00.529118061 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:00.529272079 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:00.529402971 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:13:00.529930115 CET	53	54737	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:04.689882040 CET	59082	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:04.726794004 CET	53	59082	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:05.244848013 CET	60241	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:05.272008896 CET	53	60241	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:05.729074001 CET	55521	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:13:05.765806913 CET	53	55521	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:07.851084948 CET	55402	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:07.878066063 CET	53	55402	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:09.233455896 CET	60142	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:09.260493994 CET	53	60142	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:09.551033974 CET	58216	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:09.577992916 CET	53	58216	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:09.665031910 CET	62066	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:09.688903093 CET	63135	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:09.702414989 CET	53	62066	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:09.716006994 CET	53	63135	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:13.006922960 CET	53867	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:13.025361061 CET	55683	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:13.050339937 CET	53	53867	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:13.068871975 CET	53	55683	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:13.077656031 CET	58318	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:13.121139050 CET	53	58318	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:13.334676027 CET	50342	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:13.361890078 CET	53	50342	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:13.673285961 CET	58926	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:13.719034910 CET	53	58926	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:13.798049927 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:13.839673042 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:14.818121910 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:14.820359945 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:14.844372034 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:14.845221043 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:14.845642090 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:14.845997095 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:14.846194983 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:14.846785069 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:15.020675898 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:13:15.020719051 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:13:15.026041031 CET	64572	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:15.037781954 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:15.069808006 CET	53	64572	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:15.075124025 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:15.101315975 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:13:16.441600084 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:16.442085981 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:16.467533112 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:16.467580080 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:16.467889071 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:16.468025923 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:16.468235016 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:16.469058037 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:16.482911110 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:13:16.484944105 CET	63102	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:16.524652004 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:16.528453112 CET	53	63102	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:16.565500975 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:16.565576077 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:16.565788984 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:13:16.575365067 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:16.604054928 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:16.604127884 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:16.604176044 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:16.604218006 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:16.604255915 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:16.604285002 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:16.604871988 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:16.604926109 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:16.604938984 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:16.945094109 CET	56428	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:13:16.980637074 CET	53	56428	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:18.003808975 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:18.033691883 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:18.033773899 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:18.033823967 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:18.033863068 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:18.033900023 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:18.033935070 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:18.034125090 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:18.034161091 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:18.034169912 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:18.382405043 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:18.384815931 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:18.410845995 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:18.410875082 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:18.410918951 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:18.411413908 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:18.436443090 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:18.448575020 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:13:18.448743105 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:13:18.452951908 CET	52517	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:18.465434074 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:18.497560024 CET	53	52517	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:18.560516119 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:18.560551882 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:18.560913086 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:13:18.572197914 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:18.601846933 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:18.601928949 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:18.601983070 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:18.602030993 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:18.602080107 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:18.602122068 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:18.602277994 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:18.602313042 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:18.602328062 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:20.252512932 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:20.252991915 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:20.277885914 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:20.277914047 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:20.278218985 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:20.279731989 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:20.279859066 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:20.279974937 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:20.281996012 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:13:20.284666061 CET	61763	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:20.325146914 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:20.328452110 CET	53	61763	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:20.387918949 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:20.388456106 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:20.388643026 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:13:20.399286032 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:20.429492950 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:20.429522991 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:20.429547071 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:20.429570913 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:20.429594040 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:20.429613113 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:20.429792881 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:20.429815054 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:20.429847956 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:20.521322012 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:20.547386885 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:20.547431946 CET	443	54905	172.217.23.162	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:13:20.547663927 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:21.915126085 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:21.915522099 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:21.938422918 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:13:21.941242933 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:21.941811085 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:21.941843033 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:21.941966057 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:21.942244053 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:21.942369938 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:21.949475050 CET	53524	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:21.979937077 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:21.993094921 CET	53	53524	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:22.030270100 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:22.030390024 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:22.036777973 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:13:22.397058964 CET	51667	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:22.442774057 CET	53	51667	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:22.670528889 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:22.697984934 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:22.698040009 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:22.702775002 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:22.836236000 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:22.865861893 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:22.865951061 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:22.865964890 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:22.865997076 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:22.866036892 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:22.866065979 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:22.866095066 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:22.866285086 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:22.866322994 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:22.866338015 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:22.892323971 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:23.278876066 CET	50885	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:23.319611073 CET	53	50885	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:23.553833961 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:23.567329884 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:23.580223083 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:23.580281019 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:23.580599070 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:23.595396996 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:23.595509052 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:23.595674992 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:23.791817904 CET	50995	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:23.829029083 CET	53	50995	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:24.145277023 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:24.172828913 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:24.199065924 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:26.308093071 CET	55037	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:26.343746901 CET	53	55037	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:26.357685089 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:26.358478069 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:26.385185003 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:26.385607004 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:26.385749102 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:26.386200905 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:26.409631014 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:13:26.412749052 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:26.420345068 CET	58517	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:26.451299906 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:26.464145899 CET	53	58517	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:26.497728109 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:26.497819901 CET	443	60690	172.217.21.194	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:13:26.498059988 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:13:26.519324064 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:26.548770905 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:26.548794031 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:26.548808098 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:26.548823118 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:26.548834085 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:26.548845053 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:26.549256086 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:26.549299955 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:26.549305916 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:26.675632954 CET	63893	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:26.719012022 CET	53	63893	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:26.917551041 CET	56749	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:26.946188927 CET	60457	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:26.952876091 CET	53	56749	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:26.981618881 CET	53	60457	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:27.469137907 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:27.496568918 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:27.522252083 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:29.005183935 CET	58110	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:29.040354013 CET	53	58110	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:30.463134050 CET	51365	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:30.506563902 CET	53	51365	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:30.507807970 CET	51366	443	192.168.2.4	108.177.15.155
Dec 3, 2020 10:13:30.535393000 CET	443	51366	108.177.15.155	192.168.2.4
Dec 3, 2020 10:13:30.535413027 CET	443	51366	108.177.15.155	192.168.2.4
Dec 3, 2020 10:13:30.536811113 CET	51366	443	192.168.2.4	108.177.15.155
Dec 3, 2020 10:13:30.564723969 CET	443	51366	108.177.15.155	192.168.2.4
Dec 3, 2020 10:13:30.565112114 CET	51366	443	192.168.2.4	108.177.15.155
Dec 3, 2020 10:13:30.565382004 CET	51366	443	192.168.2.4	108.177.15.155
Dec 3, 2020 10:13:30.593297958 CET	443	51366	108.177.15.155	192.168.2.4
Dec 3, 2020 10:13:30.593317032 CET	443	51366	108.177.15.155	192.168.2.4
Dec 3, 2020 10:13:30.594090939 CET	51366	443	192.168.2.4	108.177.15.155
Dec 3, 2020 10:13:30.842605114 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:30.844027042 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:30.868274927 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:30.868391991 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:30.868591070 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:30.869827032 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:30.869947910 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:30.870091915 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:30.889579058 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:13:30.895068884 CET	54702	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:30.931440115 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:30.939419985 CET	53	54702	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:30.995749950 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:31.008730888 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:31.022329092 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:13:31.037412882 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:31.037461042 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:31.037496090 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:31.037509918 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:31.037532091 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:31.037550926 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:31.037842989 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:31.037894964 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:31.037956953 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:31.570251942 CET	64945	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:31.597203016 CET	53	64945	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:32.203246117 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:32.229284048 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:32.229305029 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:32.229639053 CET	54905	443	192.168.2.4	172.217.23.162

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:13:33.860944986 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:33.861433029 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:33.883217096 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:13:33.886058092 CET	51370	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:33.888032913 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:33.888091087 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:33.888468027 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:33.889374971 CET	443	57552	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:33.915271044 CET	57552	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:33.925232887 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:33.929454088 CET	53	51370	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:33.996395111 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:33.996488094 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:33.997426033 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:13:34.007323980 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:34.037125111 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:34.037151098 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:34.037162066 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:34.037175894 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:34.037194014 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:34.037545919 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:34.037868023 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:34.037954092 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:34.038018942 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:35.008083105 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:35.034671068 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:35.034717083 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:35.035140038 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:37.545548916 CET	60241	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:37.582803965 CET	53	60241	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:41.112668991 CET	54740	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:41.148135900 CET	53	54740	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:41.676204920 CET	54319	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:41.740191936 CET	53	54319	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:42.068949938 CET	50448	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:42.104346037 CET	53	50448	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:42.431977987 CET	63234	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:42.469069004 CET	53	63234	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:42.767379999 CET	62819	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:42.794636011 CET	53	62819	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:43.148334980 CET	59597	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:43.183990002 CET	53	59597	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:43.489761114 CET	64612	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:43.527565956 CET	53	64612	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:43.824121952 CET	58174	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:43.859793901 CET	53	58174	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:44.252876043 CET	63702	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:44.288516045 CET	53	63702	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:44.732774019 CET	64254	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:44.768213987 CET	53	64254	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:45.172022104 CET	50364	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:13:45.207614899 CET	53	50364	8.8.8.8	192.168.2.4
Dec 3, 2020 10:13:45.575592041 CET	51366	443	192.168.2.4	108.177.15.155
Dec 3, 2020 10:13:45.628603935 CET	443	51366	108.177.15.155	192.168.2.4
Dec 3, 2020 10:13:48.870563984 CET	57553	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:48.888091087 CET	60690	443	192.168.2.4	172.217.21.194
Dec 3, 2020 10:13:48.912523031 CET	443	57553	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:48.929773092 CET	443	60690	172.217.21.194	192.168.2.4
Dec 3, 2020 10:13:49.014379025 CET	64237	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:49.056370974 CET	443	64237	172.217.23.162	192.168.2.4
Dec 3, 2020 10:13:50.013560057 CET	54905	443	192.168.2.4	172.217.23.162
Dec 3, 2020 10:13:50.055574894 CET	443	54905	172.217.23.162	192.168.2.4
Dec 3, 2020 10:14:03.477158070 CET	52276	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:14:03.535589933 CET	53	52276	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:14:03.595725060 CET	54726	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:14:03.630949974 CET	53	54726	8.8.8.8	192.168.2.4
Dec 3, 2020 10:14:07.819307089 CET	57646	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:14:07.846405029 CET	53	57646	8.8.8.8	192.168.2.4
Dec 3, 2020 10:14:08.559931993 CET	60175	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:14:08.587106943 CET	53	60175	8.8.8.8	192.168.2.4
Dec 3, 2020 10:14:10.824155092 CET	61713	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:14:10.880455017 CET	53	61713	8.8.8.8	192.168.2.4
Dec 3, 2020 10:14:11.595580101 CET	55500	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:14:11.639333010 CET	53	55500	8.8.8.8	192.168.2.4
Dec 3, 2020 10:14:11.705616951 CET	64627	53	192.168.2.4	8.8.8.8
Dec 3, 2020 10:14:11.741028070 CET	53	64627	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 10:12:26.299901962 CET	192.168.2.4	8.8.8.8	0xfae0	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:26.918000937 CET	192.168.2.4	8.8.8.8	0x595a	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:26.918109894 CET	192.168.2.4	8.8.8.8	0x4d23	Standard query (0)	cdn.snigelweb.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:27.326231003 CET	192.168.2.4	8.8.8.8	0x14c4	Standard query (0)	snigelweb-com.videoplayerhub.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:27.327467918 CET	192.168.2.4	8.8.8.8	0xd16d	Standard query (0)	www.googletagservices.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:27.748723984 CET	192.168.2.4	8.8.8.8	0xc96b	Standard query (0)	btloader.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:27.782821894 CET	192.168.2.4	8.8.8.8	0xd6a9	Standard query (0)	c.amazon-adsystem.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:27.783704996 CET	192.168.2.4	8.8.8.8	0x80f2	Standard query (0)	geo-eu.snigelweb.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:27.842152119 CET	192.168.2.4	8.8.8.8	0x31ac	Standard query (0)	securepubads.g.doubleclick.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:27.919291019 CET	192.168.2.4	8.8.8.8	0xef34	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:28.082495928 CET	192.168.2.4	8.8.8.8	0x9917	Standard query (0)	ad-delivery.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:28.083225012 CET	192.168.2.4	8.8.8.8	0x3473	Standard query (0)	ad.doubleclick.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:28.252854109 CET	192.168.2.4	8.8.8.8	0xb21	Standard query (0)	gum.criteo.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:28.261504889 CET	192.168.2.4	8.8.8.8	0x8ebb	Standard query (0)	id5-sync.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:28.262861967 CET	192.168.2.4	8.8.8.8	0x4512	Standard query (0)	api.rlcdn.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:28.263695955 CET	192.168.2.4	8.8.8.8	0xaf8f	Standard query (0)	match.adsrvr.org	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:28.272394896 CET	192.168.2.4	8.8.8.8	0x6979	Standard query (0)	api.btloader.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:28.351464987 CET	192.168.2.4	8.8.8.8	0x987d	Standard query (0)	aax-eu.amazon-adsystem.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.006472111 CET	192.168.2.4	8.8.8.8	0x9f86	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.148386002 CET	192.168.2.4	8.8.8.8	0xadd6	Standard query (0)	onetag-sys.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.149069071 CET	192.168.2.4	8.8.8.8	0x6a1b	Standard query (0)	ib.adnxs.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.149506092 CET	192.168.2.4	8.8.8.8	0xb4b	Standard query (0)	i.connectad.io	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.150163889 CET	192.168.2.4	8.8.8.8	0xb473	Standard query (0)	bidder.criteo.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.150311947 CET	192.168.2.4	8.8.8.8	0x696b	Standard query (0)	prg.smartadserver.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.187496901 CET	192.168.2.4	8.8.8.8	0x8ee8	Standard query (0)	ad.doubleclick.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.193732977 CET	192.168.2.4	8.8.8.8	0x678c	Standard query (0)	ad-delivery.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.405745983 CET	192.168.2.4	8.8.8.8	0x39d2	Standard query (0)	cs.emxdgt.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 10:12:29.405982018 CET	192.168.2.4	8.8.8.8	0xee1d	Standard query (0)	sync.1rx.io	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.411670923 CET	192.168.2.4	8.8.8.8	0x169e	Standard query (0)	ads.pubmatic.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.452529907 CET	192.168.2.4	8.8.8.8	0x30a7	Standard query (0)	sync.go.sonobi.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.453927994 CET	192.168.2.4	8.8.8.8	0x4b35	Standard query (0)	u.openx.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.637636900 CET	192.168.2.4	8.8.8.8	0xfbdf	Standard query (0)	ssbsync.smartadserver.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.643055916 CET	192.168.2.4	8.8.8.8	0xd90c	Standard query (0)	adservice.google.co.uk	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.806308031 CET	192.168.2.4	8.8.8.8	0xbfbd	Standard query (0)	ap.lijit.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.900875092 CET	192.168.2.4	8.8.8.8	0x72cd	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.923171997 CET	192.168.2.4	8.8.8.8	0x6cbf	Standard query (0)	eb2.3lift.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.119482994 CET	192.168.2.4	8.8.8.8	0xda65	Standard query (0)	x.bidswitch.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.145016909 CET	192.168.2.4	8.8.8.8	0x5e9a	Standard query (0)	pixel.quantserve.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.147664070 CET	192.168.2.4	8.8.8.8	0x520c	Standard query (0)	c1.adform.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.151262999 CET	192.168.2.4	8.8.8.8	0x8a50	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.246006966 CET	192.168.2.4	8.8.8.8	0x6949	Standard query (0)	image6.pubmatic.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.248989105 CET	192.168.2.4	8.8.8.8	0x79ed	Standard query (0)	sync.mathtag.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.251054049 CET	192.168.2.4	8.8.8.8	0x4d5d	Standard query (0)	bh.contextweb.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.307475090 CET	192.168.2.4	8.8.8.8	0xab86	Standard query (0)	aorta.clickagy.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.419997931 CET	192.168.2.4	8.8.8.8	0x70f3	Standard query (0)	bcp.crwdcntrl.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.422847033 CET	192.168.2.4	8.8.8.8	0xe067	Standard query (0)	match.prod.bidr.io	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.573213100 CET	192.168.2.4	8.8.8.8	0xcfa8	Standard query (0)	ce.lijit.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.648503065 CET	192.168.2.4	8.8.8.8	0xa897	Standard query (0)	static.criteo.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.710931063 CET	192.168.2.4	8.8.8.8	0x2878	Standard query (0)	d5p.de17a.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.770858049 CET	192.168.2.4	8.8.8.8	0x786	Standard query (0)	dis.criteo.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.889931917 CET	192.168.2.4	8.8.8.8	0x7ad6	Standard query (0)	dsp.adfarm1.adition.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.980268002 CET	192.168.2.4	8.8.8.8	0x2ff2	Standard query (0)	image2.pubmatic.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.070089102 CET	192.168.2.4	8.8.8.8	0x62d0	Standard query (0)	simage2.pubmatic.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.264655113 CET	192.168.2.4	8.8.8.8	0xee78	Standard query (0)	green.erne.co	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.400249004 CET	192.168.2.4	8.8.8.8	0x6803	Standard query (0)	sync.targeting.unrulymedia.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.470916033 CET	192.168.2.4	8.8.8.8	0xa2d5	Standard query (0)	uipglob.semasio.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.519596100 CET	192.168.2.4	8.8.8.8	0x94f2	Standard query (0)	visitor.fiftyt.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.530765057 CET	192.168.2.4	8.8.8.8	0xc173	Standard query (0)	pixel.onaudience.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.731976986 CET	192.168.2.4	8.8.8.8	0x10eb	Standard query (0)	ad.turn.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.768565893 CET	192.168.2.4	8.8.8.8	0x342d	Standard query (0)	ups.analytics.yahoo.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.772485018 CET	192.168.2.4	8.8.8.8	0x78d3	Standard query (0)	pr-bh.ybp.yahoo.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.775664091 CET	192.168.2.4	8.8.8.8	0xcfb	Standard query (0)	pubmatic-match.dotomi.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.775944948 CET	192.168.2.4	8.8.8.8	0xb339	Standard query (0)	sync-tm.everesttech.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.797760010 CET	192.168.2.4	8.8.8.8	0x3d02	Standard query (0)	us-u.openx.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 10:12:31.997955084 CET	192.168.2.4	8.8.8.8	0x3cf5	Standard query (0)	eu-u.openx.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.013290882 CET	192.168.2.4	8.8.8.8	0x7bec	Standard query (0)	rtb.4finance.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.035903931 CET	192.168.2.4	8.8.8.8	0x71d2	Standard query (0)	pixel-sync .sitescout.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.377227068 CET	192.168.2.4	8.8.8.8	0x9bd0	Standard query (0)	ads.betwee ndigital.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.390736103 CET	192.168.2.4	8.8.8.8	0x74e6	Standard query (0)	match.adsb y.bidtheatre.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.406308889 CET	192.168.2.4	8.8.8.8	0x363a	Standard query (0)	um.simpli.fi	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.464236021 CET	192.168.2.4	8.8.8.8	0x642d	Standard query (0)	image4.pub matic.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.508452892 CET	192.168.2.4	8.8.8.8	0x5fc7	Standard query (0)	loada.exel ator.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.704899073 CET	192.168.2.4	8.8.8.8	0xced2	Standard query (0)	cdn.connectad.io	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.707390070 CET	192.168.2.4	8.8.8.8	0x73cb	Standard query (0)	acdn.adnxs.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.828732014 CET	192.168.2.4	8.8.8.8	0xb300	Standard query (0)	aax-eu.amazon-adsystem.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.840478897 CET	192.168.2.4	8.8.8.8	0x6e6b	Standard query (0)	c1.adform.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.841274977 CET	192.168.2.4	8.8.8.8	0x328e	Standard query (0)	pixel.quan tserve.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.844875097 CET	192.168.2.4	8.8.8.8	0x9981	Standard query (0)	match.adsrvr.org	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.849318027 CET	192.168.2.4	8.8.8.8	0x9798	Standard query (0)	cm.g.doubl eclick.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.988020897 CET	192.168.2.4	8.8.8.8	0xaab3	Standard query (0)	us-u.openx.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.122256041 CET	192.168.2.4	8.8.8.8	0x6268	Standard query (0)	bh.context web.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.128129005 CET	192.168.2.4	8.8.8.8	0x25b8	Standard query (0)	aorta.clic kagy.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.137598038 CET	192.168.2.4	8.8.8.8	0x669	Standard query (0)	bcp.crwdcntrl.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.142302036 CET	192.168.2.4	8.8.8.8	0xfaf8	Standard query (0)	match.prod .bidr.io	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.193928003 CET	192.168.2.4	8.8.8.8	0x587	Standard query (0)	sync-eu.co nnectad.io	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.276611090 CET	192.168.2.4	8.8.8.8	0x5310	Standard query (0)	ce.lijit.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.425713062 CET	192.168.2.4	8.8.8.8	0xb5da	Standard query (0)	simage4.pu bmatic.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.430361986 CET	192.168.2.4	8.8.8.8	0xc0d6	Standard query (0)	ads.creative-serving.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.452225924 CET	192.168.2.4	8.8.8.8	0x3ac	Standard query (0)	cm.adform.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.495254993 CET	192.168.2.4	8.8.8.8	0xe20e	Standard query (0)	rtb.openx.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.623888016 CET	192.168.2.4	8.8.8.8	0xa3ba	Standard query (0)	sync.conne ctad.io	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.872941017 CET	192.168.2.4	8.8.8.8	0xa739	Standard query (0)	ssum.casal emedia.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:35.161489964 CET	192.168.2.4	8.8.8.8	0x1298	Standard query (0)	cs.emxdgt.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:35.181368113 CET	192.168.2.4	8.8.8.8	0x20f0	Standard query (0)	sync.1rx.io	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:35.358144045 CET	192.168.2.4	8.8.8.8	0xb607	Standard query (0)	ib.adnxs.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:35.532684088 CET	192.168.2.4	8.8.8.8	0xf5b5	Standard query (0)	sync.targe ting.unrul ymedia.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:36.334948063 CET	192.168.2.4	8.8.8.8	0x4621	Standard query (0)	ads.pubmat ic.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:36.378434896 CET	192.168.2.4	8.8.8.8	0xe08e	Standard query (0)	uipglob.se masio.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:36.403470993 CET	192.168.2.4	8.8.8.8	0x5b7a	Standard query (0)	visitor.fiftyt.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:36.423006058 CET	192.168.2.4	8.8.8.8	0x5743	Standard query (0)	pixel.onau dience.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:36.551656008 CET	192.168.2.4	8.8.8.8	0x446b	Standard query (0)	sync.matht ag.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 10:12:36.565273046 CET	192.168.2.4	8.8.8.8	0x6f1d	Standard query (0)	image2.pubmatic.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:36.570408106 CET	192.168.2.4	8.8.8.8	0x5b5f	Standard query (0)	loada.exelator.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:36.592137098 CET	192.168.2.4	8.8.8.8	0x65fe	Standard query (0)	ad.turn.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:37.001869917 CET	192.168.2.4	8.8.8.8	0xf6e0	Standard query (0)	simage2.pubmatic.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.313595057 CET	192.168.2.4	8.8.8.8	0x5552	Standard query (0)	x.bidswitch.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.443984985 CET	192.168.2.4	8.8.8.8	0xb5d2	Standard query (0)	ups.analytics.yahoo.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.459532022 CET	192.168.2.4	8.8.8.8	0xc339	Standard query (0)	pr-bh.ybp.yahoo.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.471903086 CET	192.168.2.4	8.8.8.8	0x64ac	Standard query (0)	a.volvelle.tech	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.499622107 CET	192.168.2.4	8.8.8.8	0x36d1	Standard query (0)	sync-tm.everesttech.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.514048100 CET	192.168.2.4	8.8.8.8	0xd73c	Standard query (0)	pubmatic-match.dotomi.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.526689053 CET	192.168.2.4	8.8.8.8	0xf001	Standard query (0)	pixel-sync.sitescout.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.536422968 CET	192.168.2.4	8.8.8.8	0x8124	Standard query (0)	match.adsby.bidtheatre.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.547060966 CET	192.168.2.4	8.8.8.8	0x8e7a	Standard query (0)	um.simpli.fi	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.586107969 CET	192.168.2.4	8.8.8.8	0x450b	Standard query (0)	image4.pubmatic.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.709233046 CET	192.168.2.4	8.8.8.8	0x4dad	Standard query (0)	cm.adgrx.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.710745096 CET	192.168.2.4	8.8.8.8	0x35e9	Standard query (0)	trc.taboola.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.710797071 CET	192.168.2.4	8.8.8.8	0x8ab1	Standard query (0)	a.tribalfusion.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.722665071 CET	192.168.2.4	8.8.8.8	0x78cc	Standard query (0)	cm.smadex.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.731103897 CET	192.168.2.4	8.8.8.8	0xeed1	Standard query (0)	pm.w55c.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.787273884 CET	192.168.2.4	8.8.8.8	0x488e	Standard query (0)	mwzeom.zeotap.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.870150089 CET	192.168.2.4	8.8.8.8	0x240a	Standard query (0)	pixel.tapad.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:40.106012106 CET	192.168.2.4	8.8.8.8	0xe1cf	Standard query (0)	match.taboola.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:40.158488989 CET	192.168.2.4	8.8.8.8	0x408a	Standard query (0)	s.tribalfusion.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:41.862052917 CET	192.168.2.4	8.8.8.8	0xc525	Standard query (0)	loadm.exelator.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:42.007431030 CET	192.168.2.4	8.8.8.8	0xc671	Standard query (0)	secure.adnxs.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:42.121320009 CET	192.168.2.4	8.8.8.8	0x364c	Standard query (0)	um2.eqads.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:42.126751900 CET	192.168.2.4	8.8.8.8	0x53f1	Standard query (0)	ssum-sec.casalemedia.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:42.131171942 CET	192.168.2.4	8.8.8.8	0xcb68	Standard query (0)	dsum-sec.casalemedia.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:42.370783091 CET	192.168.2.4	8.8.8.8	0xb9ad	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:42.436039925 CET	192.168.2.4	8.8.8.8	0x9fa2	Standard query (0)	s.amazon-adsystem.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:43.632168055 CET	192.168.2.4	8.8.8.8	0xcb88	Standard query (0)	rtb.gumgum.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:44.331191063 CET	192.168.2.4	8.8.8.8	0xffa9	Standard query (0)	bttrack.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:44.415224075 CET	192.168.2.4	8.8.8.8	0x8407	Standard query (0)	rtb.adentifi.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:44.464871883 CET	192.168.2.4	8.8.8.8	0x4e6	Standard query (0)	ads.avct.cloud	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:44.752403021 CET	192.168.2.4	8.8.8.8	0x2258	Standard query (0)	d.adroll.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:45.561433077 CET	192.168.2.4	8.8.8.8	0x87b	Standard query (0)	sync.srv.stackadapt.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:45.581865072 CET	192.168.2.4	8.8.8.8	0xfa7c	Standard query (0)	dsum.casalemedia.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 10:12:45.587245941 CET	192.168.2.4	8.8.8.8	0xadc	Standard query (0)	sync.ipredictive.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.711899996 CET	192.168.2.4	8.8.8.8	0x97e0	Standard query (0)	dsum-sec.casalemedia.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.717400074 CET	192.168.2.4	8.8.8.8	0x7b1	Standard query (0)	s.amazon-adsystem.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.720416069 CET	192.168.2.4	8.8.8.8	0x74b0	Standard query (0)	nep.advangelists.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.731456995 CET	192.168.2.4	8.8.8.8	0x2d01	Standard query (0)	bttrack.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.748384953 CET	192.168.2.4	8.8.8.8	0xe09e	Standard query (0)	rtb.adentifi.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.764879942 CET	192.168.2.4	8.8.8.8	0x6e6b	Standard query (0)	sync.srv.stackadapt.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.787503958 CET	192.168.2.4	8.8.8.8	0xaa8a	Standard query (0)	sync.connectad.io	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.790451050 CET	192.168.2.4	8.8.8.8	0xfbc5	Standard query (0)	ssum-sec.casalemedia.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:49.371934891 CET	192.168.2.4	8.8.8.8	0x27b3	Standard query (0)	secure.adnxs.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:49.405606985 CET	192.168.2.4	8.8.8.8	0xd53d	Standard query (0)	d.adroll.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:49.449692965 CET	192.168.2.4	8.8.8.8	0xaa06	Standard query (0)	ads.avct.cloud	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:49.719980955 CET	192.168.2.4	8.8.8.8	0x78ec	Standard query (0)	dsum.casalemedia.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.484672070 CET	192.168.2.4	8.8.8.8	0xbfb4	Standard query (0)	mwzeom.zeotap.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.489850998 CET	192.168.2.4	8.8.8.8	0x1e1f	Standard query (0)	ads.playground.xyz	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.496196032 CET	192.168.2.4	8.8.8.8	0xd054	Standard query (0)	rtb.gumgum.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.499064922 CET	192.168.2.4	8.8.8.8	0xf31e	Standard query (0)	sync.ipredictive.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:57.924012899 CET	192.168.2.4	8.8.8.8	0xf3b5	Standard query (0)	ad.360yield.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:04.689882040 CET	192.168.2.4	8.8.8.8	0x6c3c	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:05.244848013 CET	192.168.2.4	8.8.8.8	0x25fd	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:05.729074001 CET	192.168.2.4	8.8.8.8	0x9124	Standard query (0)	facebook.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:07.851084948 CET	192.168.2.4	8.8.8.8	0x6a3e	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:09.233455896 CET	192.168.2.4	8.8.8.8	0xfe0	Standard query (0)	api.twitter.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:09.551033974 CET	192.168.2.4	8.8.8.8	0x1298	Standard query (0)	abs-0.twimg.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:09.665031910 CET	192.168.2.4	8.8.8.8	0x48d6	Standard query (0)	pbs.twimg.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:09.688903093 CET	192.168.2.4	8.8.8.8	0x83b8	Standard query (0)	twitter.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:13.077656031 CET	192.168.2.4	8.8.8.8	0x6178	Standard query (0)	accounts.youtube.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:23.791817904 CET	192.168.2.4	8.8.8.8	0x7f8a	Standard query (0)	pixel.facebook.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:29.005183935 CET	192.168.2.4	8.8.8.8	0x3fc	Standard query (0)	pastebin.com	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:30.463134050 CET	192.168.2.4	8.8.8.8	0x8558	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:31.570251942 CET	192.168.2.4	8.8.8.8	0x4720	Standard query (0)	sync.go.sonobi.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:26.335483074 CET	8.8.8.8	192.168.2.4	0xfae0	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:26.335483074 CET	8.8.8.8	192.168.2.4	0xfae0	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:26.945103884 CET	8.8.8.8	192.168.2.4	0x595a	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:26.945103884 CET	8.8.8.8	192.168.2.4	0x595a	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:26.945133924 CET	8.8.8.8	192.168.2.4	0x4d23	No error (0)	cdn.snigelweb.com		172.64.102.21	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:26.945133924 CET	8.8.8.8	192.168.2.4	0x4d23	No error (0)	cdn.snigelweb.com		172.64.103.21	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:27.354110956 CET	8.8.8.8	192.168.2.4	0x14c4	No error (0)	snigelweb-com.videoplayerhub.com		172.67.74.207	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:27.354110956 CET	8.8.8.8	192.168.2.4	0x14c4	No error (0)	snigelweb-com.videoplayerhub.com		104.26.9.50	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:27.354110956 CET	8.8.8.8	192.168.2.4	0x14c4	No error (0)	snigelweb-com.videoplayerhub.com		104.26.8.50	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:27.369671106 CET	8.8.8.8	192.168.2.4	0x7cf0	No error (0)	pagead46.l.doubleclick.net		216.58.207.34	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:27.372205019 CET	8.8.8.8	192.168.2.4	0xd16d	No error (0)	www.googletagservices.com	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:27.372205019 CET	8.8.8.8	192.168.2.4	0xd16d	No error (0)	pagead46.l.doubleclick.net		172.217.22.66	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:27.775727034 CET	8.8.8.8	192.168.2.4	0xc96b	No error (0)	btloader.com		104.26.6.139	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:27.775727034 CET	8.8.8.8	192.168.2.4	0xc96b	No error (0)	btloader.com		172.67.70.134	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:27.775727034 CET	8.8.8.8	192.168.2.4	0xc96b	No error (0)	btloader.com		104.26.7.139	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:27.810651064 CET	8.8.8.8	192.168.2.4	0x80f2	No error (0)	geo-eu.snigelweb.com		172.64.102.21	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:27.810651064 CET	8.8.8.8	192.168.2.4	0x80f2	No error (0)	geo-eu.snigelweb.com		172.64.103.21	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:27.829200983 CET	8.8.8.8	192.168.2.4	0xd6a9	No error (0)	c.amazon-adsystem.com	d1ykf07e75w7ss.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:27.829200983 CET	8.8.8.8	192.168.2.4	0xd6a9	No error (0)	d1ykf07e75w7ss.cloudfront.net		65.9.83.127	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:27.885725975 CET	8.8.8.8	192.168.2.4	0x31ac	No error (0)	securepubads.g.doubleclick.net	partnerad.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:27.885725975 CET	8.8.8.8	192.168.2.4	0x31ac	No error (0)	partnerad.l.doubleclick.net		172.217.21.194	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:27.964337111 CET	8.8.8.8	192.168.2.4	0xef34	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:27.964337111 CET	8.8.8.8	192.168.2.4	0xef34	No error (0)	stats.l.doubleclick.net		108.177.15.154	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:27.964337111 CET	8.8.8.8	192.168.2.4	0xef34	No error (0)	stats.l.doubleclick.net		108.177.15.157	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:27.964337111 CET	8.8.8.8	192.168.2.4	0xef34	No error (0)	stats.l.doubleclick.net		108.177.15.155	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:27.964337111 CET	8.8.8.8	192.168.2.4	0xef34	No error (0)	stats.l.doubleclick.net		108.177.15.156	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:28.109671116 CET	8.8.8.8	192.168.2.4	0x9917	No error (0)	ad-delivery.net		172.67.69.19	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:28.109671116 CET	8.8.8.8	192.168.2.4	0x9917	No error (0)	ad-delivery.net		104.26.2.70	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:28.109671116 CET	8.8.8.8	192.168.2.4	0x9917	No error (0)	ad-delivery.net		104.26.3.70	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:28.126619101 CET	8.8.8.8	192.168.2.4	0x3473	No error (0)	ad.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:28.126619101 CET	8.8.8.8	192.168.2.4	0x3473	No error (0)	dart.l.doubleclick.net		172.217.18.102	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:28.279916048 CET	8.8.8.8	192.168.2.4	0xb21	No error (0)	gum.criteo.com	gum.par.vip.prod.criteo.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:28.279916048 CET	8.8.8.8	192.168.2.4	0xb21	No error (0)	gum.par.vip.prod.criteo.com		178.250.0.157	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:28.290676117 CET	8.8.8.8	192.168.2.4	0xaf8f	No error (0)	match.adsrvr.org	match-1943069928.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:28.290676117 CET	8.8.8.8	192.168.2.4	0xaf8f	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.17.171.52	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:28.290676117 CET	8.8.8.8	192.168.2.4	0xaf8f	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		54.72.52.19	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:28.290676117 CET	8.8.8.8	192.168.2.4	0xaf8f	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		99.80.71.186	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:28.290676117 CET	8.8.8.8	192.168.2.4	0xaf8f	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.210.128.165	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:28.290676117 CET	8.8.8.8	192.168.2.4	0xaf8f	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		34.246.149.44	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:28.290676117 CET	8.8.8.8	192.168.2.4	0xaf8f	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		54.154.164.132	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:28.290676117 CET	8.8.8.8	192.168.2.4	0xaf8f	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		54.216.123.169	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:28.290676117 CET	8.8.8.8	192.168.2.4	0xaf8f	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.49.114.167	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:28.299287081 CET	8.8.8.8	192.168.2.4	0x6979	No error (0)	api.btloader.com		130.211.23.194	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:28.308960915 CET	8.8.8.8	192.168.2.4	0x4512	No error (0)	api.rlcdn.com		34.120.207.148	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:28.378444910 CET	8.8.8.8	192.168.2.4	0x987d	No error (0)	aax-eu.amazon-adsystem.com		52.95.116.38	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.042259932 CET	8.8.8.8	192.168.2.4	0x9f86	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.042259932 CET	8.8.8.8	192.168.2.4	0x9f86	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.175544977 CET	8.8.8.8	192.168.2.4	0xadd6	No error (0)	onetag-sys.com		51.89.9.253	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.175544977 CET	8.8.8.8	192.168.2.4	0xadd6	No error (0)	onetag-sys.com		51.89.9.254	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:29.175544977 CET	8.8.8.8	192.168.2.4	0xadd6	No error (0)	onetag-sys.com		51.89.9.252	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.175544977 CET	8.8.8.8	192.168.2.4	0xadd6	No error (0)	onetag-sys.com		51.89.9.251	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.176031113 CET	8.8.8.8	192.168.2.4	0x6a1b	No error (0)	ib.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:29.176031113 CET	8.8.8.8	192.168.2.4	0x6a1b	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:29.176031113 CET	8.8.8.8	192.168.2.4	0x6a1b	No error (0)	ib.anycast .adnxs.com		185.33.221.11	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.176031113 CET	8.8.8.8	192.168.2.4	0x6a1b	No error (0)	ib.anycast .adnxs.com		185.33.221.15	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.176031113 CET	8.8.8.8	192.168.2.4	0x6a1b	No error (0)	ib.anycast .adnxs.com		185.33.220.145	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.176031113 CET	8.8.8.8	192.168.2.4	0x6a1b	No error (0)	ib.anycast .adnxs.com		185.33.220.240	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.176031113 CET	8.8.8.8	192.168.2.4	0x6a1b	No error (0)	ib.anycast .adnxs.com		185.33.221.14	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.176031113 CET	8.8.8.8	192.168.2.4	0x6a1b	No error (0)	ib.anycast .adnxs.com		185.33.221.13	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.176031113 CET	8.8.8.8	192.168.2.4	0x6a1b	No error (0)	ib.anycast .adnxs.com		185.33.221.91	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.176031113 CET	8.8.8.8	192.168.2.4	0x6a1b	No error (0)	ib.anycast .adnxs.com		185.33.220.243	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.176489115 CET	8.8.8.8	192.168.2.4	0xb4b	No error (0)	i.connectad.io		104.22.55.206	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.176489115 CET	8.8.8.8	192.168.2.4	0xb4b	No error (0)	i.connectad.io		104.22.54.206	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.176489115 CET	8.8.8.8	192.168.2.4	0xb4b	No error (0)	i.connectad.io		172.67.8.174	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.177083969 CET	8.8.8.8	192.168.2.4	0xb473	No error (0)	bidder.cri teo.com	bidder.par.vip.prod.criteo. com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:29.177083969 CET	8.8.8.8	192.168.2.4	0xb473	No error (0)	bidder.par .vip.prod. criteo.com		178.250.0.165	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.197278023 CET	8.8.8.8	192.168.2.4	0x696b	No error (0)	prg.smarta dserver.com	prga.smartadserver.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:29.197278023 CET	8.8.8.8	192.168.2.4	0x696b	No error (0)	prga.smart adserver.com	2-01-275d-0028.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:29.197278023 CET	8.8.8.8	192.168.2.4	0x696b	No error (0)	eqx.smarta dserver.com		185.86.137.113	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.197278023 CET	8.8.8.8	192.168.2.4	0x696b	No error (0)	eqx.smarta dserver.com		185.86.137.17	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.197278023 CET	8.8.8.8	192.168.2.4	0x696b	No error (0)	eqx.smarta dserver.com		185.86.137.114	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.197278023 CET	8.8.8.8	192.168.2.4	0x696b	No error (0)	eqx.smarta dserver.com		185.86.137.32	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.220659018 CET	8.8.8.8	192.168.2.4	0x678c	No error (0)	ad-delivery.net		172.67.69.19	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.220659018 CET	8.8.8.8	192.168.2.4	0x678c	No error (0)	ad-delivery.net		104.26.2.70	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.220659018 CET	8.8.8.8	192.168.2.4	0x678c	No error (0)	ad-delivery.net		104.26.3.70	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:29.230644941 CET	8.8.8.8	192.168.2.4	0x8ee8	No error (0)	ad.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:29.230644941 CET	8.8.8.8	192.168.2.4	0x8ee8	No error (0)	dart.l.doubleclick.net		172.217.18.102	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.441415071 CET	8.8.8.8	192.168.2.4	0xee1d	No error (0)	sync.1rx.io		213.19.147.150	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.443034887 CET	8.8.8.8	192.168.2.4	0x39d2	No error (0)	cs.emxdgt.com		18.195.155.181	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.449024916 CET	8.8.8.8	192.168.2.4	0x169e	No error (0)	ads.pubmatic.com	pubmatic.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:29.479554892 CET	8.8.8.8	192.168.2.4	0x30a7	No error (0)	sync.go.sonobi.com	ams-1-sync.go.sonobi.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:29.479554892 CET	8.8.8.8	192.168.2.4	0x30a7	No error (0)	ams-1-sync.go.sonobi.com		178.162.133.149	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.480864048 CET	8.8.8.8	192.168.2.4	0x4b35	No error (0)	u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.480864048 CET	8.8.8.8	192.168.2.4	0x4b35	No error (0)	u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.670764923 CET	8.8.8.8	192.168.2.4	0x4808	No error (0)	pagead46.l.doubleclick.net		216.58.212.162	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.676676035 CET	8.8.8.8	192.168.2.4	0xfbdf	No error (0)	ssbsync.smartadserver.com	ssbsync-geo.smartadserver.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:29.676676035 CET	8.8.8.8	192.168.2.4	0xfbdf	No error (0)	ssbsync-geo.smartadserver.com	2-01-275d-0035.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:29.676676035 CET	8.8.8.8	192.168.2.4	0xfbdf	No error (0)	ssbsync-eu-secure.smartadserver.com	2-01-275d-002f.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:29.676676035 CET	8.8.8.8	192.168.2.4	0xfbdf	No error (0)	ssbsync-itx4.smartadserver.com		185.86.139.103	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.676676035 CET	8.8.8.8	192.168.2.4	0xfbdf	No error (0)	ssbsync-itx4.smartadserver.com		185.86.139.94	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.676676035 CET	8.8.8.8	192.168.2.4	0xfbdf	No error (0)	ssbsync-itx4.smartadserver.com		185.86.139.104	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.676676035 CET	8.8.8.8	192.168.2.4	0xfbdf	No error (0)	ssbsync-itx4.smartadserver.com		185.86.139.93	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.686672926 CET	8.8.8.8	192.168.2.4	0xd90c	No error (0)	adservice.google.co.uk	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:29.686672926 CET	8.8.8.8	192.168.2.4	0xd90c	No error (0)	pagead46.l.doubleclick.net		216.58.207.66	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.833322048 CET	8.8.8.8	192.168.2.4	0xbfbd	No error (0)	ap.lijit.com	vap.lijit.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:29.833322048 CET	8.8.8.8	192.168.2.4	0xbfbd	No error (0)	vap.lijit.com	emeas.vap.lijit.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:29.833322048 CET	8.8.8.8	192.168.2.4	0xbfbd	No error (0)	emeas.vap.lijit.com	oeu.vap.lijit.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:29.833322048 CET	8.8.8.8	192.168.2.4	0xbfbd	No error (0)	oeu.vap.lijit.com		72.251.249.9	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.833322048 CET	8.8.8.8	192.168.2.4	0xbfbd	No error (0)	oeu.vap.lijit.com		72.251.249.13	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.833322048 CET	8.8.8.8	192.168.2.4	0xbfbd	No error (0)	oeu.vap.lijit.com		216.52.2.48	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.833322048 CET	8.8.8.8	192.168.2.4	0xbfbd	No error (0)	oeu.vap.lijit.com		216.52.2.30	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:29.833322048 CET	8.8.8.8	192.168.2.4	0xbfbd	No error (0)	oeu.vap.lijit.com		216.52.2.19	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.833322048 CET	8.8.8.8	192.168.2.4	0xbfbd	No error (0)	oeu.vap.lijit.com		216.52.2.39	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.833322048 CET	8.8.8.8	192.168.2.4	0xbfbd	No error (0)	oeu.vap.lijit.com		72.251.249.14	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.927848101 CET	8.8.8.8	192.168.2.4	0x72cd	No error (0)	googleads.g.doubleclick.net	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:29.927848101 CET	8.8.8.8	192.168.2.4	0x72cd	No error (0)	pagead46.l.doubleclick.net		172.217.23.162	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.950113058 CET	8.8.8.8	192.168.2.4	0x6cbf	No error (0)	eb2.3lift.com	eu-eb2.3lift.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:29.950113058 CET	8.8.8.8	192.168.2.4	0x6cbf	No error (0)	eu-eb2.3lift.com	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:29.950113058 CET	8.8.8.8	192.168.2.4	0x6cbf	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.185.170.181	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.950113058 CET	8.8.8.8	192.168.2.4	0x6cbf	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		52.57.162.23	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.950113058 CET	8.8.8.8	192.168.2.4	0x6cbf	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.158.81.184	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.950113058 CET	8.8.8.8	192.168.2.4	0x6cbf	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.184.39.197	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.950113058 CET	8.8.8.8	192.168.2.4	0x6cbf	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		35.158.4.230	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.950113058 CET	8.8.8.8	192.168.2.4	0x6cbf	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.157.239.120	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.950113058 CET	8.8.8.8	192.168.2.4	0x6cbf	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		18.159.63.118	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:29.950113058 CET	8.8.8.8	192.168.2.4	0x6cbf	No error (0)	dualstack.engagement-bus-prod-641612343.eu-central-1.elb.amazonaws.com		52.58.68.181	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.146634102 CET	8.8.8.8	192.168.2.4	0xda65	No error (0)	x.bidswitch.net	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:30.146634102 CET	8.8.8.8	192.168.2.4	0xda65	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		35.156.245.144	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.146634102 CET	8.8.8.8	192.168.2.4	0xda65	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		35.156.19.236	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.146634102 CET	8.8.8.8	192.168.2.4	0xda65	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		52.58.102.227	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.146634102 CET	8.8.8.8	192.168.2.4	0xda65	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		35.157.13.124	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.146634102 CET	8.8.8.8	192.168.2.4	0xda65	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		35.157.252.59	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.146634102 CET	8.8.8.8	192.168.2.4	0xda65	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		18.195.193.185	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.146634102 CET	8.8.8.8	192.168.2.4	0xda65	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		52.57.230.211	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.146634102 CET	8.8.8.8	192.168.2.4	0xda65	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		52.28.88.30	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.189182043 CET	8.8.8.8	192.168.2.4	0x8a50	No error (0)	cm.g.doubleclick.net	pagead.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:30.189182043 CET	8.8.8.8	192.168.2.4	0x8a50	No error (0)	pagead.l.doubleclick.net		172.217.21.226	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.190382957 CET	8.8.8.8	192.168.2.4	0x5e9a	No error (0)	pixel.quantserve.com	global.px.quantserve.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:30.190382957 CET	8.8.8.8	192.168.2.4	0x5e9a	No error (0)	global.px.quantserve.com		91.228.74.189	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.190382957 CET	8.8.8.8	192.168.2.4	0x5e9a	No error (0)	global.px.quantserve.com		91.228.74.134	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.190382957 CET	8.8.8.8	192.168.2.4	0x5e9a	No error (0)	global.px.quantserve.com		91.228.74.133	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.190382957 CET	8.8.8.8	192.168.2.4	0x5e9a	No error (0)	global.px.quantserve.com		91.228.74.198	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.190382957 CET	8.8.8.8	192.168.2.4	0x5e9a	No error (0)	global.px.quantserve.com		91.228.74.226	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.190975904 CET	8.8.8.8	192.168.2.4	0x520c	No error (0)	c1.adform.net	track.adformnet.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:30.272983074 CET	8.8.8.8	192.168.2.4	0x6949	No error (0)	image6.pubmatic.com	pugm-lhrc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:30.272983074 CET	8.8.8.8	192.168.2.4	0x6949	No error (0)	pugm-lhrc.pubmatic.com	pugm-lhr.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:30.272983074 CET	8.8.8.8	192.168.2.4	0x6949	No error (0)	pugm-lhr.pubmatic.com		185.64.190.78	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.276062012 CET	8.8.8.8	192.168.2.4	0x79ed	No error (0)	sync.mathtag.com	pixel-origin.mathtag.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:30.276062012 CET	8.8.8.8	192.168.2.4	0x79ed	No error (0)	pixel-orig in.mathtag.com		185.29.132.30	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.276062012 CET	8.8.8.8	192.168.2.4	0x79ed	No error (0)	pixel-orig in.mathtag.com		185.29.135.190	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.276062012 CET	8.8.8.8	192.168.2.4	0x79ed	No error (0)	pixel-orig in.mathtag.com		185.29.135.42	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.276062012 CET	8.8.8.8	192.168.2.4	0x79ed	No error (0)	pixel-orig in.mathtag.com		185.29.135.227	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.277926922 CET	8.8.8.8	192.168.2.4	0x4d5d	No error (0)	bh.context web.com	lga-bh.contextweb.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:30.277926922 CET	8.8.8.8	192.168.2.4	0x4d5d	No error (0)	lga-bh.con textweb.com	lga-bh-bgp.contextweb.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:30.277926922 CET	8.8.8.8	192.168.2.4	0x4d5d	No error (0)	lga-bh-bgp .contextweb.com		198.148.27.140	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.277926922 CET	8.8.8.8	192.168.2.4	0x4d5d	No error (0)	lga-bh-bgp .contextweb.com		198.148.27.139	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.344809055 CET	8.8.8.8	192.168.2.4	0xab86	No error (0)	aorta.clic kagy.com		52.22.205.135	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.344809055 CET	8.8.8.8	192.168.2.4	0xab86	No error (0)	aorta.clic kagy.com		52.205.157.124	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.344809055 CET	8.8.8.8	192.168.2.4	0xab86	No error (0)	aorta.clic kagy.com		54.161.205.16	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.344809055 CET	8.8.8.8	192.168.2.4	0xab86	No error (0)	aorta.clic kagy.com		50.17.97.172	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.344809055 CET	8.8.8.8	192.168.2.4	0xab86	No error (0)	aorta.clic kagy.com		35.169.105.118	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.344809055 CET	8.8.8.8	192.168.2.4	0xab86	No error (0)	aorta.clic kagy.com		52.71.232.242	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.344809055 CET	8.8.8.8	192.168.2.4	0xab86	No error (0)	aorta.clic kagy.com		54.165.189.199	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.344809055 CET	8.8.8.8	192.168.2.4	0xab86	No error (0)	aorta.clic kagy.com		34.200.74.1	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.458209991 CET	8.8.8.8	192.168.2.4	0xe067	No error (0)	match.prod .bidr.io		54.171.14.147	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.458209991 CET	8.8.8.8	192.168.2.4	0xe067	No error (0)	match.prod .bidr.io		52.31.242.159	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.458209991 CET	8.8.8.8	192.168.2.4	0xe067	No error (0)	match.prod .bidr.io		52.214.70.9	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.458209991 CET	8.8.8.8	192.168.2.4	0xe067	No error (0)	match.prod .bidr.io		52.49.193.31	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.458209991 CET	8.8.8.8	192.168.2.4	0xe067	No error (0)	match.prod .bidr.io		54.72.203.0	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.458209991 CET	8.8.8.8	192.168.2.4	0xe067	No error (0)	match.prod .bidr.io		54.228.192.197	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.462146044 CET	8.8.8.8	192.168.2.4	0x70f3	No error (0)	bcp.crwdcntrl.net		52.48.137.92	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.462146044 CET	8.8.8.8	192.168.2.4	0x70f3	No error (0)	bcp.crwdcntrl.net		52.30.140.199	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.462146044 CET	8.8.8.8	192.168.2.4	0x70f3	No error (0)	bcp.crwdcntrl.net		52.48.248.240	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.462146044 CET	8.8.8.8	192.168.2.4	0x70f3	No error (0)	bcp.crwdcntrl.net		52.30.234.204	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:30.462146044 CET	8.8.8.8	192.168.2.4	0x70f3	No error (0)	bcp.crwdcntrl.net		34.245.253.34	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.462146044 CET	8.8.8.8	192.168.2.4	0x70f3	No error (0)	bcp.crwdcntrl.net		52.210.253.186	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.462146044 CET	8.8.8.8	192.168.2.4	0x70f3	No error (0)	bcp.crwdcntrl.net		54.171.173.220	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.462146044 CET	8.8.8.8	192.168.2.4	0x70f3	No error (0)	bcp.crwdcntrl.net		99.80.128.92	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.600167036 CET	8.8.8.8	192.168.2.4	0xcfa8	No error (0)	ce.lijit.com	vap.lijit.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:30.600167036 CET	8.8.8.8	192.168.2.4	0xcfa8	No error (0)	vap.lijit.com	emeas.vap.lijit.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:30.600167036 CET	8.8.8.8	192.168.2.4	0xcfa8	No error (0)	emeas.vap.lijit.com	oeu.vap.lijit.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:30.600167036 CET	8.8.8.8	192.168.2.4	0xcfa8	No error (0)	oeu.vap.lijit.com		216.52.2.30	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.600167036 CET	8.8.8.8	192.168.2.4	0xcfa8	No error (0)	oeu.vap.lijit.com		72.251.249.9	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.600167036 CET	8.8.8.8	192.168.2.4	0xcfa8	No error (0)	oeu.vap.lijit.com		216.52.2.39	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.600167036 CET	8.8.8.8	192.168.2.4	0xcfa8	No error (0)	oeu.vap.lijit.com		72.251.249.13	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.600167036 CET	8.8.8.8	192.168.2.4	0xcfa8	No error (0)	oeu.vap.lijit.com		72.251.249.14	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.600167036 CET	8.8.8.8	192.168.2.4	0xcfa8	No error (0)	oeu.vap.lijit.com		216.52.2.19	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.600167036 CET	8.8.8.8	192.168.2.4	0xcfa8	No error (0)	oeu.vap.lijit.com		216.52.2.48	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.675499916 CET	8.8.8.8	192.168.2.4	0xa897	No error (0)	static.criteo.net	static.par.vip.prod.criteo.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:30.675499916 CET	8.8.8.8	192.168.2.4	0xa897	No error (0)	static.par.vip.prod.criteo.net		178.250.0.130	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.738059044 CET	8.8.8.8	192.168.2.4	0x2878	No error (0)	d5p.de17a.com		213.155.156.164	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.738059044 CET	8.8.8.8	192.168.2.4	0x2878	No error (0)	d5p.de17a.com		213.155.156.167	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.738059044 CET	8.8.8.8	192.168.2.4	0x2878	No error (0)	d5p.de17a.com		213.155.156.185	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.738059044 CET	8.8.8.8	192.168.2.4	0x2878	No error (0)	d5p.de17a.com		213.155.156.165	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.738059044 CET	8.8.8.8	192.168.2.4	0x2878	No error (0)	d5p.de17a.com		213.155.156.181	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.738059044 CET	8.8.8.8	192.168.2.4	0x2878	No error (0)	d5p.de17a.com		213.155.156.182	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.738059044 CET	8.8.8.8	192.168.2.4	0x2878	No error (0)	d5p.de17a.com		213.155.156.180	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.738059044 CET	8.8.8.8	192.168.2.4	0x2878	No error (0)	d5p.de17a.com		213.155.156.184	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.738059044 CET	8.8.8.8	192.168.2.4	0x2878	No error (0)	d5p.de17a.com		213.155.156.183	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.738059044 CET	8.8.8.8	192.168.2.4	0x2878	No error (0)	d5p.de17a.com		213.155.156.166	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:30.738059044 CET	8.8.8.8	192.168.2.4	0x2878	No error (0)	d5p.de17a.com		213.155.156.169	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.738059044 CET	8.8.8.8	192.168.2.4	0x2878	No error (0)	d5p.de17a.com		213.155.156.168	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.797924042 CET	8.8.8.8	192.168.2.4	0x786	No error (0)	dis.criteo.com	widget.am5.vip.prod.criteo.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:30.797924042 CET	8.8.8.8	192.168.2.4	0x786	No error (0)	widget.am5.vip.prod.criteo.com		178.250.2.151	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.916914940 CET	8.8.8.8	192.168.2.4	0x7ad6	No error (0)	dsp.adfarm1.adition.com		85.114.159.93	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:30.916914940 CET	8.8.8.8	192.168.2.4	0x7ad6	No error (0)	dsp.adfarm1.adition.com		85.114.159.118	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.007373095 CET	8.8.8.8	192.168.2.4	0x2ff2	No error (0)	image2.pubmatic.com	pug22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:31.007373095 CET	8.8.8.8	192.168.2.4	0x2ff2	No error (0)	pug22000nfc.pubmatic.com	pug22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:31.007373095 CET	8.8.8.8	192.168.2.4	0x2ff2	No error (0)	pug22000nf.pubmatic.com		185.64.189.110	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.097199917 CET	8.8.8.8	192.168.2.4	0x62d0	No error (0)	simage2.pubmatic.com	pug-lhrc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:31.097199917 CET	8.8.8.8	192.168.2.4	0x62d0	No error (0)	pug-lhrc.pubmatic.com	pug-lhr.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:31.097199917 CET	8.8.8.8	192.168.2.4	0x62d0	No error (0)	pug-lhr.pubmatic.com		185.64.190.80	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.291832924 CET	8.8.8.8	192.168.2.4	0xee78	No error (0)	green.erne.co		87.98.252.5	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.291832924 CET	8.8.8.8	192.168.2.4	0xee78	No error (0)	green.erne.co		94.23.73.243	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.291832924 CET	8.8.8.8	192.168.2.4	0xee78	No error (0)	green.erne.co		87.98.128.108	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.291832924 CET	8.8.8.8	192.168.2.4	0xee78	No error (0)	green.erne.co		87.98.228.78	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.291832924 CET	8.8.8.8	192.168.2.4	0xee78	No error (0)	green.erne.co		188.165.4.142	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.291832924 CET	8.8.8.8	192.168.2.4	0xee78	No error (0)	green.erne.co		188.165.27.173	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.291832924 CET	8.8.8.8	192.168.2.4	0xee78	No error (0)	green.erne.co		87.98.242.60	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.291832924 CET	8.8.8.8	192.168.2.4	0xee78	No error (0)	green.erne.co		94.23.171.206	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.291832924 CET	8.8.8.8	192.168.2.4	0xee78	No error (0)	green.erne.co		188.165.137.78	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.291832924 CET	8.8.8.8	192.168.2.4	0xee78	No error (0)	green.erne.co		94.23.144.220	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.449318886 CET	8.8.8.8	192.168.2.4	0x6803	No error (0)	sync.targeting.unrulymedia.com	sync.1rx.io		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:31.449318886 CET	8.8.8.8	192.168.2.4	0x6803	No error (0)	sync.1rx.io		213.19.147.151	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.498030901 CET	8.8.8.8	192.168.2.4	0xa2d5	No error (0)	uipglob.semasio.net	uipglob.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:31.498030901 CET	8.8.8.8	192.168.2.4	0xa2d5	No error (0)	uip.semasio.net		77.243.60.138	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:31.546766996 CET	8.8.8.8	192.168.2.4	0x94f2	No error (0)	visitor.fiftyt.com		104.26.13.50	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.546766996 CET	8.8.8.8	192.168.2.4	0x94f2	No error (0)	visitor.fiftyt.com		104.26.12.50	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.546766996 CET	8.8.8.8	192.168.2.4	0x94f2	No error (0)	visitor.fiftyt.com		172.67.73.8	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.557796955 CET	8.8.8.8	192.168.2.4	0xc173	No error (0)	pixel.onaudience.com		51.210.112.63	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.557796955 CET	8.8.8.8	192.168.2.4	0xc173	No error (0)	pixel.onaudience.com		51.210.112.236	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.557796955 CET	8.8.8.8	192.168.2.4	0xc173	No error (0)	pixel.onaudience.com		51.210.112.64	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.557796955 CET	8.8.8.8	192.168.2.4	0xc173	No error (0)	pixel.onaudience.com		51.210.112.66	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.769035101 CET	8.8.8.8	192.168.2.4	0x10eb	No error (0)	ad.turn.com	ad.turn.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:31.799555063 CET	8.8.8.8	192.168.2.4	0x78d3	No error (0)	pr-bh.ybp.yahoo.com	ds-pr-bh.ybp.gysm.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:31.799555063 CET	8.8.8.8	192.168.2.4	0x78d3	No error (0)	ds-pr-bh.ybp.gysm.yahoodns.net		212.82.100.176	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.803966045 CET	8.8.8.8	192.168.2.4	0x342d	No error (0)	ups.analytics.yahoo.com	prod.ups-ats.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:31.803966045 CET	8.8.8.8	192.168.2.4	0x342d	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)
Dec 3, 2020 10:12:31.803966045 CET	8.8.8.8	192.168.2.4	0x342d	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		3.126.56.137	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.803966045 CET	8.8.8.8	192.168.2.4	0x342d	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		18.156.0.31	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.812740088 CET	8.8.8.8	192.168.2.4	0xb339	No error (0)	sync-tm.everesttech.net	sync.tubemogul.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:31.812740088 CET	8.8.8.8	192.168.2.4	0xb339	No error (0)	sync.tubemogul.com	syncf.tubemogul.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:31.812740088 CET	8.8.8.8	192.168.2.4	0xb339	No error (0)	syncf.tubemogul.com	h2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:31.812983036 CET	8.8.8.8	192.168.2.4	0xcfb	No error (0)	pubmatic-match.dotomi.com	afp.dotomi.weighted.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:31.812983036 CET	8.8.8.8	192.168.2.4	0xcfb	No error (0)	ams02-usadmm-ds.dotomi.com		64.158.223.137	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.824805021 CET	8.8.8.8	192.168.2.4	0x3d02	No error (0)	us-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:31.824805021 CET	8.8.8.8	192.168.2.4	0x3d02	No error (0)	us-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.024908066 CET	8.8.8.8	192.168.2.4	0x3cf5	No error (0)	eu-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.024908066 CET	8.8.8.8	192.168.2.4	0x3cf5	No error (0)	eu-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.073081017 CET	8.8.8.8	192.168.2.4	0x71d2	No error (0)	pixel-sync.sitescout.com	pixel-a.sitescout.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:32.073081017 CET	8.8.8.8	192.168.2.4	0x71d2	No error (0)	pixel-a.sitescout.com		66.155.71.149	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:32.201543093 CET	8.8.8.8	192.168.2.4	0x7bec	No error (0)	rtb.4finance.com	pool.4finance.iponweb.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:32.201543093 CET	8.8.8.8	192.168.2.4	0x7bec	No error (0)	pool.4finance.iponweb.net		35.210.181.65	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.201543093 CET	8.8.8.8	192.168.2.4	0x7bec	No error (0)	pool.4finance.iponweb.net		35.206.141.96	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.404186010 CET	8.8.8.8	192.168.2.4	0x9bd0	No error (0)	ads.betweendigital.com	ssp.ads.betweendigital.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:32.404186010 CET	8.8.8.8	192.168.2.4	0x9bd0	No error (0)	ssp.ads.betweendigital.com		96.46.183.20	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.404186010 CET	8.8.8.8	192.168.2.4	0x9bd0	No error (0)	ssp.ads.betweendigital.com		96.46.186.57	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.417644024 CET	8.8.8.8	192.168.2.4	0x74e6	No error (0)	match.adsby.bidtheatre.com		174.138.12.104	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.417644024 CET	8.8.8.8	192.168.2.4	0x74e6	No error (0)	match.adsby.bidtheatre.com		167.99.220.155	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.444205999 CET	8.8.8.8	192.168.2.4	0x363a	No error (0)	um.simpli.fi		159.253.128.183	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.444205999 CET	8.8.8.8	192.168.2.4	0x363a	No error (0)	um.simpli.fi		169.50.137.190	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.444205999 CET	8.8.8.8	192.168.2.4	0x363a	No error (0)	um.simpli.fi		159.253.128.188	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.491159916 CET	8.8.8.8	192.168.2.4	0x642d	No error (0)	image4.pubmatic.com	spug22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:32.491159916 CET	8.8.8.8	192.168.2.4	0x642d	No error (0)	spug22000nfc.pubmatic.com	spug22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:32.491159916 CET	8.8.8.8	192.168.2.4	0x642d	No error (0)	spug22000nf.pubmatic.com		185.64.189.114	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.556216002 CET	8.8.8.8	192.168.2.4	0x5fc7	No error (0)	loada.exelator.com	eu-west.load.exelator.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:32.556216002 CET	8.8.8.8	192.168.2.4	0x5fc7	No error (0)	eu-west.load.exelator.com	load-ams1.exelator.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:32.556216002 CET	8.8.8.8	192.168.2.4	0x5fc7	No error (0)	load-ams1.exelator.com		147.75.102.200	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.731950998 CET	8.8.8.8	192.168.2.4	0xced2	No error (0)	cdn.connectad.io		172.67.8.174	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.731950998 CET	8.8.8.8	192.168.2.4	0xced2	No error (0)	cdn.connectad.io		104.22.54.206	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.731950998 CET	8.8.8.8	192.168.2.4	0xced2	No error (0)	cdn.connectad.io		104.22.55.206	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.745358944 CET	8.8.8.8	192.168.2.4	0x73cb	No error (0)	acdn.adnxs.com	secure-adnxs.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:32.856019974 CET	8.8.8.8	192.168.2.4	0xb300	No error (0)	aax-eu.amazon-adsystem.com		52.95.123.167	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.872056007 CET	8.8.8.8	192.168.2.4	0x9981	No error (0)	match.adsrvr.org	match-1943069928.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:32.872056007 CET	8.8.8.8	192.168.2.4	0x9981	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.17.171.52	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.872056007 CET	8.8.8.8	192.168.2.4	0x9981	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		54.72.52.19	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:32.872056007 CET	8.8.8.8	192.168.2.4	0x9981	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		99.80.71.186	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.872056007 CET	8.8.8.8	192.168.2.4	0x9981	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.210.128.165	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.872056007 CET	8.8.8.8	192.168.2.4	0x9981	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		34.246.149.44	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.872056007 CET	8.8.8.8	192.168.2.4	0x9981	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		54.154.164.132	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.872056007 CET	8.8.8.8	192.168.2.4	0x9981	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		54.216.123.169	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.872056007 CET	8.8.8.8	192.168.2.4	0x9981	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.49.114.167	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.876769066 CET	8.8.8.8	192.168.2.4	0x328e	No error (0)	pixel.quantserve.com	global.px.quantserve.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:32.876769066 CET	8.8.8.8	192.168.2.4	0x328e	No error (0)	global.px.quantserve.com		91.228.74.189	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.876769066 CET	8.8.8.8	192.168.2.4	0x328e	No error (0)	global.px.quantserve.com		91.228.74.134	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.876769066 CET	8.8.8.8	192.168.2.4	0x328e	No error (0)	global.px.quantserve.com		91.228.74.133	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.876769066 CET	8.8.8.8	192.168.2.4	0x328e	No error (0)	global.px.quantserve.com		91.228.74.198	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.876769066 CET	8.8.8.8	192.168.2.4	0x328e	No error (0)	global.px.quantserve.com		91.228.74.226	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:32.877597094 CET	8.8.8.8	192.168.2.4	0x6e6b	No error (0)	c1.adform.net	track.adformnet.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:32.884644985 CET	8.8.8.8	192.168.2.4	0x9798	No error (0)	cm.g.doubleclick.net	pagead.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:32.884644985 CET	8.8.8.8	192.168.2.4	0x9798	No error (0)	pagead.l.doubleclick.net		172.217.21.226	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.015130997 CET	8.8.8.8	192.168.2.4	0xaab3	No error (0)	us-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.015130997 CET	8.8.8.8	192.168.2.4	0xaab3	No error (0)	us-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.149255991 CET	8.8.8.8	192.168.2.4	0x6268	No error (0)	bh.contextweb.com	lga-bh.contextweb.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:33.149255991 CET	8.8.8.8	192.168.2.4	0x6268	No error (0)	lga-bh.contextweb.com	lga-bh-bgp.contextweb.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:33.149255991 CET	8.8.8.8	192.168.2.4	0x6268	No error (0)	lga-bh-bgp.contextweb.com		198.148.27.140	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.149255991 CET	8.8.8.8	192.168.2.4	0x6268	No error (0)	lga-bh-bgp.contextweb.com		198.148.27.139	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.168677092 CET	8.8.8.8	192.168.2.4	0x25b8	No error (0)	aorta.clickagy.com		52.22.205.135	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:33.168677092 CET	8.8.8.8	192.168.2.4	0x25b8	No error (0)	aorta.clickagy.com		52.205.157.124	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.168677092 CET	8.8.8.8	192.168.2.4	0x25b8	No error (0)	aorta.clickagy.com		54.161.205.16	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.168677092 CET	8.8.8.8	192.168.2.4	0x25b8	No error (0)	aorta.clickagy.com		50.17.97.172	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.168677092 CET	8.8.8.8	192.168.2.4	0x25b8	No error (0)	aorta.clickagy.com		35.169.105.118	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.168677092 CET	8.8.8.8	192.168.2.4	0x25b8	No error (0)	aorta.clickagy.com		52.71.232.242	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.168677092 CET	8.8.8.8	192.168.2.4	0x25b8	No error (0)	aorta.clickagy.com		54.165.189.199	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.168677092 CET	8.8.8.8	192.168.2.4	0x25b8	No error (0)	aorta.clickagy.com		34.200.74.1	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.174869061 CET	8.8.8.8	192.168.2.4	0x669	No error (0)	bcp.crwdcntrl.net		52.48.248.240	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.174869061 CET	8.8.8.8	192.168.2.4	0x669	No error (0)	bcp.crwdcntrl.net		52.48.137.92	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.174869061 CET	8.8.8.8	192.168.2.4	0x669	No error (0)	bcp.crwdcntrl.net		34.253.109.165	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.174869061 CET	8.8.8.8	192.168.2.4	0x669	No error (0)	bcp.crwdcntrl.net		34.245.253.34	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.174869061 CET	8.8.8.8	192.168.2.4	0x669	No error (0)	bcp.crwdcntrl.net		52.49.190.28	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.174869061 CET	8.8.8.8	192.168.2.4	0x669	No error (0)	bcp.crwdcntrl.net		52.30.234.204	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.174869061 CET	8.8.8.8	192.168.2.4	0x669	No error (0)	bcp.crwdcntrl.net		52.30.140.199	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.174869061 CET	8.8.8.8	192.168.2.4	0x669	No error (0)	bcp.crwdcntrl.net		99.80.128.92	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.177757978 CET	8.8.8.8	192.168.2.4	0xfaf8	No error (0)	match.prod.bidr.io		54.171.14.147	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.177757978 CET	8.8.8.8	192.168.2.4	0xfaf8	No error (0)	match.prod.bidr.io		52.31.242.159	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.177757978 CET	8.8.8.8	192.168.2.4	0xfaf8	No error (0)	match.prod.bidr.io		52.214.70.9	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.177757978 CET	8.8.8.8	192.168.2.4	0xfaf8	No error (0)	match.prod.bidr.io		52.49.193.31	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.177757978 CET	8.8.8.8	192.168.2.4	0xfaf8	No error (0)	match.prod.bidr.io		54.72.203.0	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.177757978 CET	8.8.8.8	192.168.2.4	0xfaf8	No error (0)	match.prod.bidr.io		54.228.192.197	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.220918894 CET	8.8.8.8	192.168.2.4	0x587	No error (0)	sync-eu.connectad.io		104.22.54.206	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.220918894 CET	8.8.8.8	192.168.2.4	0x587	No error (0)	sync-eu.connectad.io		172.67.8.174	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.220918894 CET	8.8.8.8	192.168.2.4	0x587	No error (0)	sync-eu.connectad.io		104.22.55.206	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.303751945 CET	8.8.8.8	192.168.2.4	0x5310	No error (0)	ce.lijit.com	vap.lijit.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:33.303751945 CET	8.8.8.8	192.168.2.4	0x5310	No error (0)	vap.lijit.com	emeas.vap.lijit.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:33.303751945 CET	8.8.8.8	192.168.2.4	0x5310	No error (0)	emeas.vap.lijit.com	oeu.vap.lijit.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:33.303751945 CET	8.8.8.8	192.168.2.4	0x5310	No error (0)	oeu.vap.lijit.com		216.52.2.48	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.303751945 CET	8.8.8.8	192.168.2.4	0x5310	No error (0)	oeu.vap.lijit.com		216.52.2.19	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.303751945 CET	8.8.8.8	192.168.2.4	0x5310	No error (0)	oeu.vap.lijit.com		72.251.249.13	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.303751945 CET	8.8.8.8	192.168.2.4	0x5310	No error (0)	oeu.vap.lijit.com		216.52.2.39	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.303751945 CET	8.8.8.8	192.168.2.4	0x5310	No error (0)	oeu.vap.lijit.com		216.52.2.30	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.303751945 CET	8.8.8.8	192.168.2.4	0x5310	No error (0)	oeu.vap.lijit.com		72.251.249.9	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.303751945 CET	8.8.8.8	192.168.2.4	0x5310	No error (0)	oeu.vap.lijit.com		72.251.249.14	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.452867031 CET	8.8.8.8	192.168.2.4	0xb5da	No error (0)	simage4.pubmatic.com	spug22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:33.452867031 CET	8.8.8.8	192.168.2.4	0xb5da	No error (0)	spug22000nfc.pubmatic.com	spug22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:33.452867031 CET	8.8.8.8	192.168.2.4	0xb5da	No error (0)	spug22000nf.pubmatic.com		185.64.189.114	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.465816021 CET	8.8.8.8	192.168.2.4	0xc0d6	No error (0)	ads.creative-serving.com	elb-aws-fr-clickdistrict-1651093077.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:33.465816021 CET	8.8.8.8	192.168.2.4	0xc0d6	No error (0)	elb-aws-fr-clickdistrict-1651093077.eu-central-1.elb.amazonaws.com		18.195.7.149	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.465816021 CET	8.8.8.8	192.168.2.4	0xc0d6	No error (0)	elb-aws-fr-clickdistrict-1651093077.eu-central-1.elb.amazonaws.com		3.127.51.194	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.465816021 CET	8.8.8.8	192.168.2.4	0xc0d6	No error (0)	elb-aws-fr-clickdistrict-1651093077.eu-central-1.elb.amazonaws.com		18.196.214.144	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.465816021 CET	8.8.8.8	192.168.2.4	0xc0d6	No error (0)	elb-aws-fr-clickdistrict-1651093077.eu-central-1.elb.amazonaws.com		3.123.96.39	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.488857031 CET	8.8.8.8	192.168.2.4	0x3ac	No error (0)	cm.adform.net	track-eu.adformnet.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:33.522258997 CET	8.8.8.8	192.168.2.4	0xe20e	No error (0)	rtb.openx.net		35.186.253.211	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.522258997 CET	8.8.8.8	192.168.2.4	0xe20e	No error (0)	rtb.openx.net		35.227.252.103	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.650801897 CET	8.8.8.8	192.168.2.4	0xa3ba	No error (0)	sync.connectad.io		104.22.55.206	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.650801897 CET	8.8.8.8	192.168.2.4	0xa3ba	No error (0)	sync.connectad.io		172.67.8.174	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:33.650801897 CET	8.8.8.8	192.168.2.4	0xa3ba	No error (0)	sync.connectad.io		104.22.54.206	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:33.910077095 CET	8.8.8.8	192.168.2.4	0xa739	No error (0)	ssum.casalemedia.com	ssum.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:35.200778961 CET	8.8.8.8	192.168.2.4	0x1298	No error (0)	cs.emxdgt.com		18.195.155.181	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:35.218913078 CET	8.8.8.8	192.168.2.4	0x20f0	No error (0)	sync.1rx.io		213.19.147.150	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:35.385051012 CET	8.8.8.8	192.168.2.4	0xb607	No error (0)	ib.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:35.385051012 CET	8.8.8.8	192.168.2.4	0xb607	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:35.385051012 CET	8.8.8.8	192.168.2.4	0xb607	No error (0)	ib.anycast.adnxs.com		185.33.220.244	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:35.385051012 CET	8.8.8.8	192.168.2.4	0xb607	No error (0)	ib.anycast.adnxs.com		185.33.220.241	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:35.385051012 CET	8.8.8.8	192.168.2.4	0xb607	No error (0)	ib.anycast.adnxs.com		185.33.220.240	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:35.385051012 CET	8.8.8.8	192.168.2.4	0xb607	No error (0)	ib.anycast.adnxs.com		185.33.221.14	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:35.385051012 CET	8.8.8.8	192.168.2.4	0xb607	No error (0)	ib.anycast.adnxs.com		185.33.221.13	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:35.385051012 CET	8.8.8.8	192.168.2.4	0xb607	No error (0)	ib.anycast.adnxs.com		185.33.220.145	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:35.385051012 CET	8.8.8.8	192.168.2.4	0xb607	No error (0)	ib.anycast.adnxs.com		185.33.221.53	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:35.385051012 CET	8.8.8.8	192.168.2.4	0xb607	No error (0)	ib.anycast.adnxs.com		185.33.221.88	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:35.568140030 CET	8.8.8.8	192.168.2.4	0xf5b5	No error (0)	sync.targeting.unrulymedia.com	sync.1rx.io		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:35.568140030 CET	8.8.8.8	192.168.2.4	0xf5b5	No error (0)	sync.1rx.io		213.19.147.151	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:36.370603085 CET	8.8.8.8	192.168.2.4	0x4621	No error (0)	ads.pubmatic.com	pubmatic.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:36.405549049 CET	8.8.8.8	192.168.2.4	0xe08e	No error (0)	uipglob.semasio.net	uipglob.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:36.405549049 CET	8.8.8.8	192.168.2.4	0xe08e	No error (0)	uip.semasio.net		77.243.60.138	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:36.430538893 CET	8.8.8.8	192.168.2.4	0x5b7a	No error (0)	visitor.fiftyt.com		172.67.73.8	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:36.430538893 CET	8.8.8.8	192.168.2.4	0x5b7a	No error (0)	visitor.fiftyt.com		104.26.12.50	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:36.430538893 CET	8.8.8.8	192.168.2.4	0x5b7a	No error (0)	visitor.fiftyt.com		104.26.13.50	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:36.450054884 CET	8.8.8.8	192.168.2.4	0x5743	No error (0)	pixel.onaudience.com		51.210.112.64	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:36.450054884 CET	8.8.8.8	192.168.2.4	0x5743	No error (0)	pixel.onaudience.com		51.210.112.66	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:36.450054884 CET	8.8.8.8	192.168.2.4	0x5743	No error (0)	pixel.onaudience.com		51.210.112.236	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:36.450054884 CET	8.8.8.8	192.168.2.4	0x5743	No error (0)	pixel.onaudience.com		51.210.112.63	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:36.578702927 CET	8.8.8.8	192.168.2.4	0x446b	No error (0)	sync.mathtag.com	pixel-origin.mathtag.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:36.578702927 CET	8.8.8.8	192.168.2.4	0x446b	No error (0)	pixel-orig in.mathtag.com		185.29.133.52	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:36.578702927 CET	8.8.8.8	192.168.2.4	0x446b	No error (0)	pixel-orig in.mathtag.com		185.29.135.234	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:36.578702927 CET	8.8.8.8	192.168.2.4	0x446b	No error (0)	pixel-orig in.mathtag.com		185.29.133.208	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:36.578702927 CET	8.8.8.8	192.168.2.4	0x446b	No error (0)	pixel-orig in.mathtag.com		185.29.135.42	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:36.592196941 CET	8.8.8.8	192.168.2.4	0x6f1d	No error (0)	image2.pub matic.com	pug22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:36.592196941 CET	8.8.8.8	192.168.2.4	0x6f1d	No error (0)	pug22000nf c.pubmatic.com	pug22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:36.592196941 CET	8.8.8.8	192.168.2.4	0x6f1d	No error (0)	pug22000nf .pubmatic.com		185.64.189.110	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:36.607680082 CET	8.8.8.8	192.168.2.4	0x5b5f	No error (0)	loada.exel ator.com	eu-west.load.exelator.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:36.607680082 CET	8.8.8.8	192.168.2.4	0x5b5f	No error (0)	eu-west.lo ad.exelator.com	load-ams1.exelator.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:36.607680082 CET	8.8.8.8	192.168.2.4	0x5b5f	No error (0)	load-ams1. exelator.com		147.75.102.200	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:36.627707005 CET	8.8.8.8	192.168.2.4	0x65fe	No error (0)	ad.turn.com	ad.turn.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:37.028755903 CET	8.8.8.8	192.168.2.4	0xf6e0	No error (0)	simage2.pu bmatic.com	pug-lhrc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:37.028755903 CET	8.8.8.8	192.168.2.4	0xf6e0	No error (0)	pug-lhrc.p ubmatic.com	pug-lhr.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:37.028755903 CET	8.8.8.8	192.168.2.4	0xf6e0	No error (0)	pug-lhr.pu bmatic.com		185.64.190.80	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.340480089 CET	8.8.8.8	192.168.2.4	0x5552	No error (0)	x.bidswitch.net	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:38.340480089 CET	8.8.8.8	192.168.2.4	0x5552	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1 .elb.amazo naws.com		35.156.245.144	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.340480089 CET	8.8.8.8	192.168.2.4	0x5552	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1 .elb.amazo naws.com		35.156.19.236	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.340480089 CET	8.8.8.8	192.168.2.4	0x5552	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1 .elb.amazo naws.com		52.58.102.227	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.340480089 CET	8.8.8.8	192.168.2.4	0x5552	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1 .elb.amazo naws.com		35.157.13.124	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.340480089 CET	8.8.8.8	192.168.2.4	0x5552	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1 .elb.amazo naws.com		35.157.252.59	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.340480089 CET	8.8.8.8	192.168.2.4	0x5552	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1 .elb.amazo naws.com		18.195.193.185	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.340480089 CET	8.8.8.8	192.168.2.4	0x5552	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1 .elb.amazo naws.com		52.57.230.211	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:38.340480089 CET	8.8.8.8	192.168.2.4	0x5552	No error (0)	alb-aws-fr-bswx-1-445786803.eu-central-1.elb.amazonaws.com		52.28.88.30	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.470942974 CET	8.8.8.8	192.168.2.4	0xb5d2	No error (0)	ups.analytics.yahoo.com	prod.ups-ats.aolp-ds-prd.aws.oath.cloud		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:38.470942974 CET	8.8.8.8	192.168.2.4	0xb5d2	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)
Dec 3, 2020 10:12:38.470942974 CET	8.8.8.8	192.168.2.4	0xb5d2	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		18.156.0.31	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.470942974 CET	8.8.8.8	192.168.2.4	0xb5d2	No error (0)	prod.ups-ats.eu-central-1.aolp-ds-prd.aws.oath.cloud		3.126.56.137	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.486473083 CET	8.8.8.8	192.168.2.4	0xc339	No error (0)	pr-bh.ybp.yahoo.com	ds-pr-bh.ybp.gysm.yahoodns.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:38.486473083 CET	8.8.8.8	192.168.2.4	0xc339	No error (0)	ds-pr-bh.ybp.gysm.yahoodns.net		212.82.100.176	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.529767990 CET	8.8.8.8	192.168.2.4	0x64ac	No error (0)	a.volvelle.tech	pool.optomaton.iponweb.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:38.529767990 CET	8.8.8.8	192.168.2.4	0x64ac	No error (0)	pool.optomaton.iponweb.net	optomaton.geo.iponweb.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:38.529767990 CET	8.8.8.8	192.168.2.4	0x64ac	No error (0)	optomaton.geo.iponweb.net		35.210.178.101	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.535257101 CET	8.8.8.8	192.168.2.4	0x36d1	No error (0)	sync-tm.everesttech.net	sync.tubemogul.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:38.535257101 CET	8.8.8.8	192.168.2.4	0x36d1	No error (0)	sync.tubemogul.com	syncf.tubemogul.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:38.535257101 CET	8.8.8.8	192.168.2.4	0x36d1	No error (0)	syncf.tubemogul.com	h2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:38.540898085 CET	8.8.8.8	192.168.2.4	0xd73c	No error (0)	pubmatic-match.dotomi.com	afp.dotomi.weighted.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:38.540898085 CET	8.8.8.8	192.168.2.4	0xd73c	No error (0)	ams01-login-ds.dotomi.com		63.215.202.140	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.562277079 CET	8.8.8.8	192.168.2.4	0xf001	No error (0)	pixel-sync.sitescout.com	pixel-a.sitescout.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:38.562277079 CET	8.8.8.8	192.168.2.4	0xf001	No error (0)	pixel-a.sitescout.com		66.155.71.25	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.563225985 CET	8.8.8.8	192.168.2.4	0x8124	No error (0)	match.adsby.bidtheatre.com		174.138.12.104	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.563225985 CET	8.8.8.8	192.168.2.4	0x8124	No error (0)	match.adsby.bidtheatre.com		167.99.220.155	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.582454920 CET	8.8.8.8	192.168.2.4	0x8e7a	No error (0)	um.simpli.fi		159.253.128.183	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.582454920 CET	8.8.8.8	192.168.2.4	0x8e7a	No error (0)	um.simpli.fi		169.50.137.190	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.582454920 CET	8.8.8.8	192.168.2.4	0x8e7a	No error (0)	um.simpli.fi		159.253.128.188	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:38.612987041 CET	8.8.8.8	192.168.2.4	0x450b	No error (0)	image4.pubmatic.com	spug22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:38.612987041 CET	8.8.8.8	192.168.2.4	0x450b	No error (0)	spug22000nfc.pubmatic.com	spug22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:38.612987041 CET	8.8.8.8	192.168.2.4	0x450b	No error (0)	spug22000nf.pubmatic.com		185.64.189.114	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.736223936 CET	8.8.8.8	192.168.2.4	0x4dad	No error (0)	cm.adgrx.com	rtb.adgrx.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:39.736223936 CET	8.8.8.8	192.168.2.4	0x4dad	No error (0)	rtb.adgrx.com		173.231.180.197	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.737694979 CET	8.8.8.8	192.168.2.4	0x8ab1	No error (0)	a.tribalfusion.com		104.18.12.5	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.737694979 CET	8.8.8.8	192.168.2.4	0x8ab1	No error (0)	a.tribalfusion.com		104.18.13.5	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.747378111 CET	8.8.8.8	192.168.2.4	0x35e9	No error (0)	trc.taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:39.747378111 CET	8.8.8.8	192.168.2.4	0x35e9	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.747378111 CET	8.8.8.8	192.168.2.4	0x35e9	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.747378111 CET	8.8.8.8	192.168.2.4	0x35e9	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.747378111 CET	8.8.8.8	192.168.2.4	0x35e9	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.758143902 CET	8.8.8.8	192.168.2.4	0xeed1	No error (0)	pm.w55c.net	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:39.758143902 CET	8.8.8.8	192.168.2.4	0xeed1	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		52.59.61.242	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.758143902 CET	8.8.8.8	192.168.2.4	0xeed1	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		3.127.88.255	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.758143902 CET	8.8.8.8	192.168.2.4	0xeed1	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		35.158.49.68	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.758143902 CET	8.8.8.8	192.168.2.4	0xeed1	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		3.123.192.108	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.758143902 CET	8.8.8.8	192.168.2.4	0xeed1	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		18.185.167.52	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.758143902 CET	8.8.8.8	192.168.2.4	0xeed1	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		35.157.48.14	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.758143902 CET	8.8.8.8	192.168.2.4	0xeed1	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		18.157.138.23	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.758143902 CET	8.8.8.8	192.168.2.4	0xeed1	No error (0)	dxedge-prod-lb-404808087.eu-central-1.elb.amazonaws.com		18.185.192.106	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.765779972 CET	8.8.8.8	192.168.2.4	0x78cc	No error (0)	cm.smadex.com		65.9.86.12	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.765779972 CET	8.8.8.8	192.168.2.4	0x78cc	No error (0)	cm.smadex.com		65.9.86.7	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:39.765779972 CET	8.8.8.8	192.168.2.4	0x78cc	No error (0)	cm.smadex.com		65.9.86.20	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.765779972 CET	8.8.8.8	192.168.2.4	0x78cc	No error (0)	cm.smadex.com		65.9.86.41	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.814460039 CET	8.8.8.8	192.168.2.4	0x488e	No error (0)	mwzeom.zeotap.com		172.67.13.182	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.814460039 CET	8.8.8.8	192.168.2.4	0x488e	No error (0)	mwzeom.zeotap.com		104.22.25.87	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.814460039 CET	8.8.8.8	192.168.2.4	0x488e	No error (0)	mwzeom.zeotap.com		104.22.24.87	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:39.907367945 CET	8.8.8.8	192.168.2.4	0x240a	No error (0)	pixel.tapad.com		35.227.248.159	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:40.142749071 CET	8.8.8.8	192.168.2.4	0xe1cf	No error (0)	match.taboola.com	tls13.taboola.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:40.142749071 CET	8.8.8.8	192.168.2.4	0xe1cf	No error (0)	tls13.taboola.map.fastly.net		151.101.1.44	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:40.142749071 CET	8.8.8.8	192.168.2.4	0xe1cf	No error (0)	tls13.taboola.map.fastly.net		151.101.65.44	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:40.142749071 CET	8.8.8.8	192.168.2.4	0xe1cf	No error (0)	tls13.taboola.map.fastly.net		151.101.129.44	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:40.142749071 CET	8.8.8.8	192.168.2.4	0xe1cf	No error (0)	tls13.taboola.map.fastly.net		151.101.193.44	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:40.185560942 CET	8.8.8.8	192.168.2.4	0x408a	No error (0)	s.tribalfusion.com		104.18.13.5	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:40.185560942 CET	8.8.8.8	192.168.2.4	0x408a	No error (0)	s.tribalfusion.com		104.18.12.5	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:41.910768986 CET	8.8.8.8	192.168.2.4	0xc525	No error (0)	loadm.exelator.com	loadus.tm.ssl.exelator.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:41.910768986 CET	8.8.8.8	192.168.2.4	0xc525	No error (0)	loadus.tm.ssl.exelator.com	eu-west.load.exelator.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:41.910768986 CET	8.8.8.8	192.168.2.4	0xc525	No error (0)	eu-west.load.exelator.com	load-ams1.exelator.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:41.910768986 CET	8.8.8.8	192.168.2.4	0xc525	No error (0)	load-ams1.exelator.com		147.75.102.200	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:42.034549952 CET	8.8.8.8	192.168.2.4	0xc671	No error (0)	secure.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:42.034549952 CET	8.8.8.8	192.168.2.4	0xc671	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:42.034549952 CET	8.8.8.8	192.168.2.4	0xc671	No error (0)	ib.anycast.adnxs.com		185.33.220.241	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:42.034549952 CET	8.8.8.8	192.168.2.4	0xc671	No error (0)	ib.anycast.adnxs.com		185.33.221.50	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:42.034549952 CET	8.8.8.8	192.168.2.4	0xc671	No error (0)	ib.anycast.adnxs.com		185.33.220.242	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:42.034549952 CET	8.8.8.8	192.168.2.4	0xc671	No error (0)	ib.anycast.adnxs.com		185.33.221.15	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:42.034549952 CET	8.8.8.8	192.168.2.4	0xc671	No error (0)	ib.anycast.adnxs.com		185.33.221.87	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:42.034549952 CET	8.8.8.8	192.168.2.4	0xc671	No error (0)	ib.anycast.adnxs.com		185.33.221.14	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:42.034549952 CET	8.8.8.8	192.168.2.4	0xc671	No error (0)	ib.anycast.adnxs.com		185.33.221.52	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:42.034549952 CET	8.8.8.8	192.168.2.4	0xc671	No error (0)	ib.anycast.adnxs.com		185.33.220.240	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:42.148340940 CET	8.8.8.8	192.168.2.4	0x364c	No error (0)	um2.eqads.com	um3.eqads.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:42.148340940 CET	8.8.8.8	192.168.2.4	0x364c	No error (0)	um3.eqads.com		54.85.167.1	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:42.148340940 CET	8.8.8.8	192.168.2.4	0x364c	No error (0)	um3.eqads.com		54.204.142.198	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:42.163594961 CET	8.8.8.8	192.168.2.4	0x53f1	No error (0)	ssum-sec.casalemedia.com	ssum-sec.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:42.167993069 CET	8.8.8.8	192.168.2.4	0xcb68	No error (0)	dsum-sec.casalemedia.com	dsum-sec.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:42.414362907 CET	8.8.8.8	192.168.2.4	0xb9ad	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:42.414362907 CET	8.8.8.8	192.168.2.4	0xb9ad	No error (0)	googlehosted.l.googleusercontent.com		172.217.16.193	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:42.462907076 CET	8.8.8.8	192.168.2.4	0x9fa2	No error (0)	s.amazon-adsystem.com		72.21.206.140	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:43.669836044 CET	8.8.8.8	192.168.2.4	0xcb88	No error (0)	rtb.gumgum.com		54.154.144.178	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:43.669836044 CET	8.8.8.8	192.168.2.4	0xcb88	No error (0)	rtb.gumgum.com		54.171.43.242	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:43.669836044 CET	8.8.8.8	192.168.2.4	0xcb88	No error (0)	rtb.gumgum.com		108.129.8.178	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:43.669836044 CET	8.8.8.8	192.168.2.4	0xcb88	No error (0)	rtb.gumgum.com		18.200.32.70	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:43.669836044 CET	8.8.8.8	192.168.2.4	0xcb88	No error (0)	rtb.gumgum.com		52.51.206.28	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:43.669836044 CET	8.8.8.8	192.168.2.4	0xcb88	No error (0)	rtb.gumgum.com		34.250.108.63	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:43.669836044 CET	8.8.8.8	192.168.2.4	0xcb88	No error (0)	rtb.gumgum.com		63.33.123.138	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:43.669836044 CET	8.8.8.8	192.168.2.4	0xcb88	No error (0)	rtb.gumgum.com		34.250.244.32	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:44.358285904 CET	8.8.8.8	192.168.2.4	0xffa9	No error (0)	bttrack.com		192.132.33.46	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:44.442217112 CET	8.8.8.8	192.168.2.4	0x8407	No error (0)	rtb.adentifi.com		52.4.242.89	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:44.442217112 CET	8.8.8.8	192.168.2.4	0x8407	No error (0)	rtb.adentifi.com		52.44.132.4	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:44.442217112 CET	8.8.8.8	192.168.2.4	0x8407	No error (0)	rtb.adentifi.com		52.45.126.152	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:44.442217112 CET	8.8.8.8	192.168.2.4	0x8407	No error (0)	rtb.adentifi.com		52.4.245.32	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:44.442217112 CET	8.8.8.8	192.168.2.4	0x8407	No error (0)	rtb.adentifi.com		52.44.79.149	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:44.442217112 CET	8.8.8.8	192.168.2.4	0x8407	No error (0)	rtb.adentifi.com		52.45.148.83	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:44.442217112 CET	8.8.8.8	192.168.2.4	0x8407	No error (0)	rtb.adentifi.com		52.44.83.58	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:44.442217112 CET	8.8.8.8	192.168.2.4	0x8407	No error (0)	rtb.adentifi.com		52.44.166.129	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:44.501203060 CET	8.8.8.8	192.168.2.4	0x4e6	No error (0)	ads.avct.cloud	eventd-eu.avct.cloud		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:44.501203060 CET	8.8.8.8	192.168.2.4	0x4e6	No error (0)	eventd-eu.avct.cloud		54.194.211.3	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:44.501203060 CET	8.8.8.8	192.168.2.4	0x4e6	No error (0)	eventd-eu.avct.cloud		34.240.2.137	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:44.501203060 CET	8.8.8.8	192.168.2.4	0x4e6	No error (0)	eventd-eu.avct.cloud		3.250.166.134	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:44.787878036 CET	8.8.8.8	192.168.2.4	0x2258	No error (0)	d.adroll.com	adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:44.787878036 CET	8.8.8.8	192.168.2.4	0x2258	No error (0)	adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com		54.77.74.200	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:44.787878036 CET	8.8.8.8	192.168.2.4	0x2258	No error (0)	adserver-vpc-alb-3-890571764.eu-west-1.elb.amazonaws.com		3.248.28.111	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:45.588421106 CET	8.8.8.8	192.168.2.4	0x87b	No error (0)	sync.srv.stackadapt.com		52.202.170.46	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:45.588421106 CET	8.8.8.8	192.168.2.4	0x87b	No error (0)	sync.srv.stackadapt.com		52.55.4.67	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:45.588421106 CET	8.8.8.8	192.168.2.4	0x87b	No error (0)	sync.srv.stackadapt.com		50.16.38.94	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:45.588421106 CET	8.8.8.8	192.168.2.4	0x87b	No error (0)	sync.srv.stackadapt.com		52.44.53.247	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:45.588421106 CET	8.8.8.8	192.168.2.4	0x87b	No error (0)	sync.srv.stackadapt.com		52.22.254.90	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:45.588421106 CET	8.8.8.8	192.168.2.4	0x87b	No error (0)	sync.srv.stackadapt.com		52.45.203.131	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:45.588421106 CET	8.8.8.8	192.168.2.4	0x87b	No error (0)	sync.srv.stackadapt.com		34.192.210.97	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:45.588421106 CET	8.8.8.8	192.168.2.4	0x87b	No error (0)	sync.srv.stackadapt.com		52.1.18.121	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:45.614321947 CET	8.8.8.8	192.168.2.4	0xadc	No error (0)	sync.ipredictive.com		35.169.194.138	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:45.614321947 CET	8.8.8.8	192.168.2.4	0xadc	No error (0)	sync.ipredictive.com		35.174.108.79	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:45.614321947 CET	8.8.8.8	192.168.2.4	0xadc	No error (0)	sync.ipredictive.com		35.172.126.30	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:45.614321947 CET	8.8.8.8	192.168.2.4	0xadc	No error (0)	sync.ipredictive.com		35.173.30.247	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:45.614321947 CET	8.8.8.8	192.168.2.4	0xadc	No error (0)	sync.ipredictive.com		52.200.246.203	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:45.614321947 CET	8.8.8.8	192.168.2.4	0xadc	No error (0)	sync.ipredictive.com		52.0.84.81	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:45.614321947 CET	8.8.8.8	192.168.2.4	0xadc	No error (0)	sync.ipredictive.com		35.169.45.106	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:45.614321947 CET	8.8.8.8	192.168.2.4	0xadc	No error (0)	sync.ipredictive.com		52.20.14.141	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:45.618840933 CET	8.8.8.8	192.168.2.4	0xfa7c	No error (0)	dsum.casalemedia.com	dsum.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:47.744323015 CET	8.8.8.8	192.168.2.4	0x7b1	No error (0)	s.amazon-adsystem.com		72.21.206.140	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.747181892 CET	8.8.8.8	192.168.2.4	0x97e0	No error (0)	dsum-sec.casalemedia.com	dsum-sec.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:47.747236013 CET	8.8.8.8	192.168.2.4	0x74b0	No error (0)	nep.advangelists.com		18.204.112.31	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.747236013 CET	8.8.8.8	192.168.2.4	0x74b0	No error (0)	nep.advangelists.com		34.238.66.169	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.747236013 CET	8.8.8.8	192.168.2.4	0x74b0	No error (0)	nep.advangelists.com		54.84.123.42	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.747236013 CET	8.8.8.8	192.168.2.4	0x74b0	No error (0)	nep.advangelists.com		23.23.32.252	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.747236013 CET	8.8.8.8	192.168.2.4	0x74b0	No error (0)	nep.advangelists.com		34.203.107.157	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.747236013 CET	8.8.8.8	192.168.2.4	0x74b0	No error (0)	nep.advangelists.com		23.22.52.122	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.747236013 CET	8.8.8.8	192.168.2.4	0x74b0	No error (0)	nep.advangelists.com		18.208.69.188	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.747236013 CET	8.8.8.8	192.168.2.4	0x74b0	No error (0)	nep.advangelists.com		52.55.177.181	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.758385897 CET	8.8.8.8	192.168.2.4	0x2d01	No error (0)	bttrack.com		192.132.33.46	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.775279045 CET	8.8.8.8	192.168.2.4	0xe09e	No error (0)	rtb.adentifi.com		52.4.51.239	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.775279045 CET	8.8.8.8	192.168.2.4	0xe09e	No error (0)	rtb.adentifi.com		52.44.83.58	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.775279045 CET	8.8.8.8	192.168.2.4	0xe09e	No error (0)	rtb.adentifi.com		52.45.11.130	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.775279045 CET	8.8.8.8	192.168.2.4	0xe09e	No error (0)	rtb.adentifi.com		52.44.214.200	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.775279045 CET	8.8.8.8	192.168.2.4	0xe09e	No error (0)	rtb.adentifi.com		52.44.64.106	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.775279045 CET	8.8.8.8	192.168.2.4	0xe09e	No error (0)	rtb.adentifi.com		52.45.16.192	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.775279045 CET	8.8.8.8	192.168.2.4	0xe09e	No error (0)	rtb.adentifi.com		52.45.155.24	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.775279045 CET	8.8.8.8	192.168.2.4	0xe09e	No error (0)	rtb.adentifi.com		52.207.62.93	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.800344944 CET	8.8.8.8	192.168.2.4	0x6e6b	No error (0)	sync.srv.stackadapt.com		54.205.191.176	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.800344944 CET	8.8.8.8	192.168.2.4	0x6e6b	No error (0)	sync.srv.stackadapt.com		52.45.203.131	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.800344944 CET	8.8.8.8	192.168.2.4	0x6e6b	No error (0)	sync.srv.stackadapt.com		50.16.38.94	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.800344944 CET	8.8.8.8	192.168.2.4	0x6e6b	No error (0)	sync.srv.stackadapt.com		52.22.254.90	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.800344944 CET	8.8.8.8	192.168.2.4	0x6e6b	No error (0)	sync.srv.stackadapt.com		52.1.18.121	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.800344944 CET	8.8.8.8	192.168.2.4	0x6e6b	No error (0)	sync.srv.stackadapt.com		52.44.53.247	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.800344944 CET	8.8.8.8	192.168.2.4	0x6e6b	No error (0)	sync.srv.stackadapt.com		52.202.170.46	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:47.800344944 CET	8.8.8.8	192.168.2.4	0x6e6b	No error (0)	sync.srv.stackadapt.com		34.192.210.97	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.814398050 CET	8.8.8.8	192.168.2.4	0xaa8a	No error (0)	sync.connectad.io		104.22.55.206	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.814398050 CET	8.8.8.8	192.168.2.4	0xaa8a	No error (0)	sync.connectad.io		172.67.8.174	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.814398050 CET	8.8.8.8	192.168.2.4	0xaa8a	No error (0)	sync.connectad.io		104.22.54.206	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:47.826941967 CET	8.8.8.8	192.168.2.4	0xfbc5	No error (0)	ssum-sec.casalemedia.com	ssum-sec.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:49.399090052 CET	8.8.8.8	192.168.2.4	0x27b3	No error (0)	secure.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:49.399090052 CET	8.8.8.8	192.168.2.4	0x27b3	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:49.399090052 CET	8.8.8.8	192.168.2.4	0x27b3	No error (0)	ib.anycast.adnxs.com		185.33.221.15	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:49.399090052 CET	8.8.8.8	192.168.2.4	0x27b3	No error (0)	ib.anycast.adnxs.com		185.33.221.53	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:49.399090052 CET	8.8.8.8	192.168.2.4	0x27b3	No error (0)	ib.anycast.adnxs.com		185.33.221.50	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:49.399090052 CET	8.8.8.8	192.168.2.4	0x27b3	No error (0)	ib.anycast.adnxs.com		185.33.220.242	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:49.399090052 CET	8.8.8.8	192.168.2.4	0x27b3	No error (0)	ib.anycast.adnxs.com		185.33.221.88	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:49.399090052 CET	8.8.8.8	192.168.2.4	0x27b3	No error (0)	ib.anycast.adnxs.com		185.33.220.145	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:49.399090052 CET	8.8.8.8	192.168.2.4	0x27b3	No error (0)	ib.anycast.adnxs.com		185.33.221.13	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:49.399090052 CET	8.8.8.8	192.168.2.4	0x27b3	No error (0)	ib.anycast.adnxs.com		185.33.220.241	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:49.432542086 CET	8.8.8.8	192.168.2.4	0xd53d	No error (0)	d.adroll.com	adserver-vpc-alb-0-1578609942.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:49.432542086 CET	8.8.8.8	192.168.2.4	0xd53d	No error (0)	adserver-vpc-alb-0-1578609942.eu-west-1.elb.amazonaws.com		63.35.200.21	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:49.432542086 CET	8.8.8.8	192.168.2.4	0xd53d	No error (0)	adserver-vpc-alb-0-1578609942.eu-west-1.elb.amazonaws.com		54.77.187.185	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:49.484996080 CET	8.8.8.8	192.168.2.4	0xaa06	No error (0)	ads.avct.cloud	eventd-eu.avct.cloud		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:49.484996080 CET	8.8.8.8	192.168.2.4	0xaa06	No error (0)	eventd-eu.avct.cloud		54.194.211.3	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:49.484996080 CET	8.8.8.8	192.168.2.4	0xaa06	No error (0)	eventd-eu.avct.cloud		3.250.166.134	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:49.484996080 CET	8.8.8.8	192.168.2.4	0xaa06	No error (0)	eventd-eu.avct.cloud		34.240.2.137	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:49.755558014 CET	8.8.8.8	192.168.2.4	0x78ec	No error (0)	dsum.casalemedia.com	dsum.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:50.511682034 CET	8.8.8.8	192.168.2.4	0xbfb4	No error (0)	mwzeom.zeotap.com		172.67.13.182	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:50.511682034 CET	8.8.8.8	192.168.2.4	0xbfb4	No error (0)	mwzeom.zeotap.com		104.22.25.87	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.511682034 CET	8.8.8.8	192.168.2.4	0xbfb4	No error (0)	mwzeom.zeotap.com		104.22.24.87	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.533435106 CET	8.8.8.8	192.168.2.4	0x1e1f	No error (0)	ads.playground.xyz		3.121.163.163	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.533435106 CET	8.8.8.8	192.168.2.4	0x1e1f	No error (0)	ads.playground.xyz		3.125.132.240	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.533435106 CET	8.8.8.8	192.168.2.4	0x1e1f	No error (0)	ads.playground.xyz		52.57.47.66	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.533998013 CET	8.8.8.8	192.168.2.4	0xd054	No error (0)	rtb.gumgum.com		63.33.123.138	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.533998013 CET	8.8.8.8	192.168.2.4	0xd054	No error (0)	rtb.gumgum.com		54.154.144.178	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.533998013 CET	8.8.8.8	192.168.2.4	0xd054	No error (0)	rtb.gumgum.com		108.128.209.152	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.533998013 CET	8.8.8.8	192.168.2.4	0xd054	No error (0)	rtb.gumgum.com		52.51.206.28	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.533998013 CET	8.8.8.8	192.168.2.4	0xd054	No error (0)	rtb.gumgum.com		52.215.241.211	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.533998013 CET	8.8.8.8	192.168.2.4	0xd054	No error (0)	rtb.gumgum.com		52.19.189.90	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.533998013 CET	8.8.8.8	192.168.2.4	0xd054	No error (0)	rtb.gumgum.com		34.250.108.63	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.533998013 CET	8.8.8.8	192.168.2.4	0xd054	No error (0)	rtb.gumgum.com		52.31.234.119	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.534235954 CET	8.8.8.8	192.168.2.4	0xf31e	No error (0)	sync.ipredictive.com		52.20.14.141	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.534235954 CET	8.8.8.8	192.168.2.4	0xf31e	No error (0)	sync.ipredictive.com		35.173.30.247	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.534235954 CET	8.8.8.8	192.168.2.4	0xf31e	No error (0)	sync.ipredictive.com		52.1.128.202	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.534235954 CET	8.8.8.8	192.168.2.4	0xf31e	No error (0)	sync.ipredictive.com		34.226.8.26	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.534235954 CET	8.8.8.8	192.168.2.4	0xf31e	No error (0)	sync.ipredictive.com		35.169.45.106	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.534235954 CET	8.8.8.8	192.168.2.4	0xf31e	No error (0)	sync.ipredictive.com		52.202.125.251	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.534235954 CET	8.8.8.8	192.168.2.4	0xf31e	No error (0)	sync.ipredictive.com		34.225.95.133	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:50.534235954 CET	8.8.8.8	192.168.2.4	0xf31e	No error (0)	sync.ipredictive.com		52.20.127.209	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:57.967593908 CET	8.8.8.8	192.168.2.4	0xf3b5	No error (0)	ad.360yield.com	ice.360yield.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:57.967593908 CET	8.8.8.8	192.168.2.4	0xf3b5	No error (0)	ice.360yield.com	eu2-ice.360yield.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:12:57.967593908 CET	8.8.8.8	192.168.2.4	0xf3b5	No error (0)	eu2-ice.360yield.com		54.93.141.230	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:57.967593908 CET	8.8.8.8	192.168.2.4	0xf3b5	No error (0)	eu2-ice.360yield.com		35.156.198.184	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:57.967593908 CET	8.8.8.8	192.168.2.4	0xf3b5	No error (0)	eu2-ice.360yield.com		52.57.38.160	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:57.967593908 CET	8.8.8.8	192.168.2.4	0xf3b5	No error (0)	eu2-ice.360yield.com		18.185.245.187	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:57.967593908 CET	8.8.8.8	192.168.2.4	0xf3b5	No error (0)	eu2-ice.360yield.com		52.58.124.95	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:57.967593908 CET	8.8.8.8	192.168.2.4	0xf3b5	No error (0)	eu2-ice.360yield.com		52.58.206.142	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:57.967593908 CET	8.8.8.8	192.168.2.4	0xf3b5	No error (0)	eu2-ice.360yield.com		52.59.73.29	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:57.967593908 CET	8.8.8.8	192.168.2.4	0xf3b5	No error (0)	eu2-ice.360yield.com		52.57.193.99	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:04.726794004 CET	8.8.8.8	192.168.2.4	0x6c3c	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:13:04.726794004 CET	8.8.8.8	192.168.2.4	0x6c3c	No error (0)	star-mini.c10r.facebook.com		31.13.92.36	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:05.272008896 CET	8.8.8.8	192.168.2.4	0x25fd	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:13:05.272008896 CET	8.8.8.8	192.168.2.4	0x25fd	No error (0)	scontent.xx.fbcdn.net		31.13.81.13	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:05.765806913 CET	8.8.8.8	192.168.2.4	0x9124	No error (0)	facebook.com		31.13.92.36	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:07.878066063 CET	8.8.8.8	192.168.2.4	0x6a3e	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:13:07.878066063 CET	8.8.8.8	192.168.2.4	0x6a3e	No error (0)	scontent.xx.fbcdn.net		31.13.81.13	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:09.260493994 CET	8.8.8.8	192.168.2.4	0xfe0	No error (0)	api.twitter.com	tpop-api.twitter.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:13:09.260493994 CET	8.8.8.8	192.168.2.4	0xfe0	No error (0)	tpop-api.twitter.com		104.244.42.2	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:09.260493994 CET	8.8.8.8	192.168.2.4	0xfe0	No error (0)	tpop-api.twitter.com		104.244.42.66	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:09.260493994 CET	8.8.8.8	192.168.2.4	0xfe0	No error (0)	tpop-api.twitter.com		104.244.42.130	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:09.260493994 CET	8.8.8.8	192.168.2.4	0xfe0	No error (0)	tpop-api.twitter.com		104.244.42.194	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:09.577992916 CET	8.8.8.8	192.168.2.4	0x1298	No error (0)	abs-0.twimg.com	abs-zero.twimg.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:13:09.577992916 CET	8.8.8.8	192.168.2.4	0x1298	No error (0)	abs-zero.twimg.com		104.244.43.131	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:09.702414989 CET	8.8.8.8	192.168.2.4	0x48d6	No error (0)	pbs.twimg.com	cs196.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:13:09.702414989 CET	8.8.8.8	192.168.2.4	0x48d6	No error (0)	cs196.wac.edgecastcdn.net	cs2-wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:13:09.702414989 CET	8.8.8.8	192.168.2.4	0x48d6	No error (0)	cs2-wac-eu.8315.ecdns.net	cs45.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:13:09.702414989 CET	8.8.8.8	192.168.2.4	0x48d6	No error (0)	cs45.wac.edgecastcdn.net		93.184.220.70	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:09.716006994 CET	8.8.8.8	192.168.2.4	0x83b8	No error (0)	twitter.com		104.244.42.193	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:09.716006994 CET	8.8.8.8	192.168.2.4	0x83b8	No error (0)	twitter.com		104.244.42.1	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:13.121139050 CET	8.8.8.8	192.168.2.4	0x6178	No error (0)	accounts.youtube.com	www3.l.google.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:13:23.829029083 CET	8.8.8.8	192.168.2.4	0x7f8a	No error (0)	pixel.facebook.com	z-m.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:13:23.829029083 CET	8.8.8.8	192.168.2.4	0x7f8a	No error (0)	z-m.c10r.facebook.com		31.13.92.37	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:29.040354013 CET	8.8.8.8	192.168.2.4	0x3fc	No error (0)	pastebin.com		104.23.98.190	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:29.040354013 CET	8.8.8.8	192.168.2.4	0x3fc	No error (0)	pastebin.com		104.23.99.190	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:30.506563902 CET	8.8.8.8	192.168.2.4	0x8558	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:13:30.506563902 CET	8.8.8.8	192.168.2.4	0x8558	No error (0)	stats.l.doubleclick.net		108.177.15.155	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:30.506563902 CET	8.8.8.8	192.168.2.4	0x8558	No error (0)	stats.l.doubleclick.net		108.177.15.156	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:30.506563902 CET	8.8.8.8	192.168.2.4	0x8558	No error (0)	stats.l.doubleclick.net		108.177.15.157	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:30.506563902 CET	8.8.8.8	192.168.2.4	0x8558	No error (0)	stats.l.doubleclick.net		108.177.15.154	A (IP address)	IN (0x0001)
Dec 3, 2020 10:13:31.597203016 CET	8.8.8.8	192.168.2.4	0x4720	No error (0)	sync.go.sonobi.com	ams-1-sync.go.sonobi.com		CNAME (Canonical name)	IN (0x0001)
Dec 3, 2020 10:13:31.597203016 CET	8.8.8.8	192.168.2.4	0x4720	No error (0)	ams-1-sync.go.sonobi.com		178.162.133.149	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- pastebin.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49742	104.23.98.190	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:12:26.353768110 CET	91	OUT	GET / HTTP/1.1 Host: pastebin.com Connection: keep-alive Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Accept-Encoding: gzip, deflate Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Dec 3, 2020 10:12:26.379285097 CET	97	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 03 Dec 2020 09:12:26 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Thu, 03 Dec 2020 10:12:26 GMT Location: https://pastebin.com/ cf-request-id: 06c978e1fb00001f1d1f956000000001 Vary: Accept-Encoding Server: cloudflare CF-RAY: 5fbc2a7cb8cd1f1d-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

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

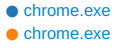
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Dec 3, 2020 10:12:28.344305992 CET	51.89.20.86	443	192.168.2.4	49770	CN=*.id5-sync.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Sep 27 20:07:21 CEST 2020 Thu Mar 17 17:40:46 CET 2016	Sat Dec 26 19:07:21 CET 2020 Wed Mar 17 17:40:46 CET 2021	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=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Dec 3, 2020 10:12:28.371737957 CET	52.17.171.52	443	192.168.2.4	49771	C=US, ST=California, L=Ventura, O=The Trade Desk Inc, CN=*.adsrvr.org EMAILADDRESS=ca@trustwave.com, CN="Trustwave Organization Validation SHA256 CA, Level 1", O="Trustwave Holdings, Inc.", L=Chicago, ST=Illinois, C=US	EMAILADDRESS=ca@trustwave.com, CN="Trustwave Organization Validation SHA256 CA, Level 1", O="Trustwave Holdings, Inc.", L=Chicago, ST=Illinois, C=US CN=SecureTrust CA, O=SecureTrust Corporation, C=US	Thu Mar 07 11:41:08 CET 2019 Thu Sep 01 16:35:35 CEST 2016	Mon Apr 19 18:41:08 CEST 2021 Sun Sep 29 16:35:35 CEST 2024	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
					EMAILADDRESS=ca@trustwave.com, CN="Trustwave Organization Validation SHA256 CA, Level 1", O="Trustwave Holdings, Inc.", L=Chicago, ST=Illinois, C=US	CN=SecureTrust CA, O=SecureTrust Corporation, C=US	Thu Sep 01 16:35:35 CEST 2016	Sun Sep 29 16:35:35 CEST 2024		
Dec 3, 2020 10:12:28.461308002 CET	52.95.116.38	443	192.168.2.4	49774	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	Mon Jun 15 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 Jun 15 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		
Dec 3, 2020 10:12:29.099725008 CET	104.23.99.190	443	192.168.2.4	49781	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Aug 17 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Tue Aug 17 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 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

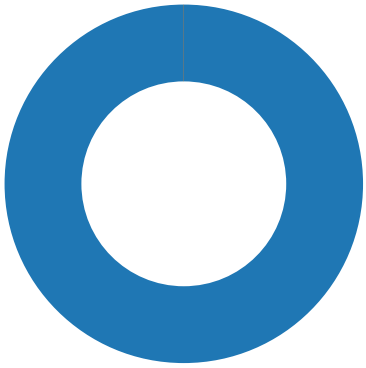
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Dec 3, 2020 10:12:29.215336084 CET	51.89.9.253	443	192.168.2.4	49785	CN=onetag-sys.com CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=Let's Encrypt Authority X3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Nov 02 16:01:23 CET 2020 Thu Mar 17 17:40:46 CET 2016	Sun Jan 31 16:01:23 CET 2021 Wed Mar 17 17:40:46 CET 2021	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=Let's Encrypt Authority X3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Mar 17 17:40:46 CET 2016	Wed Mar 17 17:40:46 CET 2021		
Dec 3, 2020 10:12:29.235512972 CET	185.33.221.11	443	192.168.2.4	49786	CN=*.adnxs.com, O="AppNexus, Inc.", L=New York, ST=New York, C=US CN=DigiCert ECC Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert ECC Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Jan 23 01:00:00 CET 2019 Fri Mar 08 13:00:00 CET 2013	Mon Mar 08 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
					CN=DigiCert ECC 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		
Dec 3, 2020 10:12:29.271390915 CET	172.217.18.102	443	192.168.2.4	49796	CN=*.doubleclick.net, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Nov 03 08:33:39 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Jan 26 08:33:39 CET 2021 Wed Dec 15 01:00:42 CET 2021	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 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Code Manipulations

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6972 Parent PID: 1476

General

Start time:	10:12:20
Start date:	03/12/2020
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'http://pastebin.com'
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF609CBFC4B	RegSetValueExW

Analysis Process: chrome.exe PID: 5484 Parent PID: 6972

General

Start time:	10:12:21
Start date:	03/12/2020
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=1500,13364953271334854619,5261983793971551056,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1672 /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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly