ID: 321426
Cookbook: browseurl.jbs
Time: 02:37:38
Date: 22/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

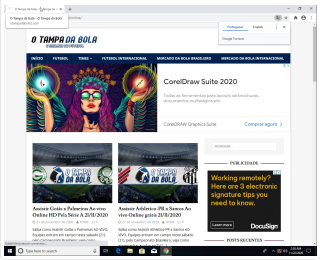
Analysis Report https://otampadabola2.com

Overview

General Information

Sample URL:	http://https://otampadabola2.com
Analysis ID:	321426

Most interesting Screenshot:



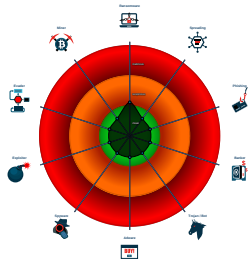
Detection

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

Signatures

No high impact signatures.

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 5128 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://otampadabola2.com' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 3980 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1564,10723194021886127913,5669998590995236100,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1756 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 6404 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1564,10723194021886127913,5669998590995236100,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=5960 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

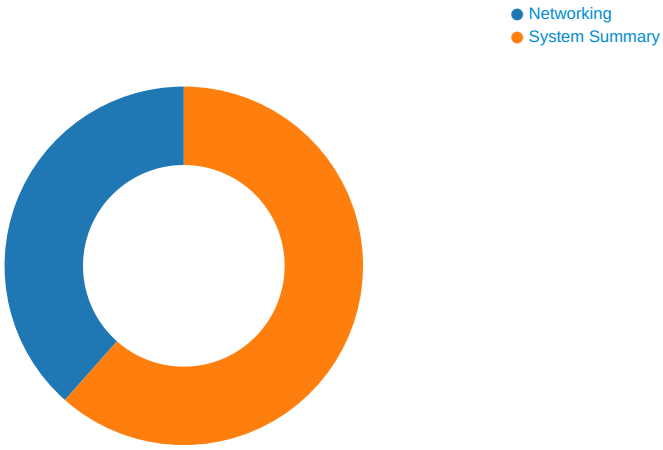
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



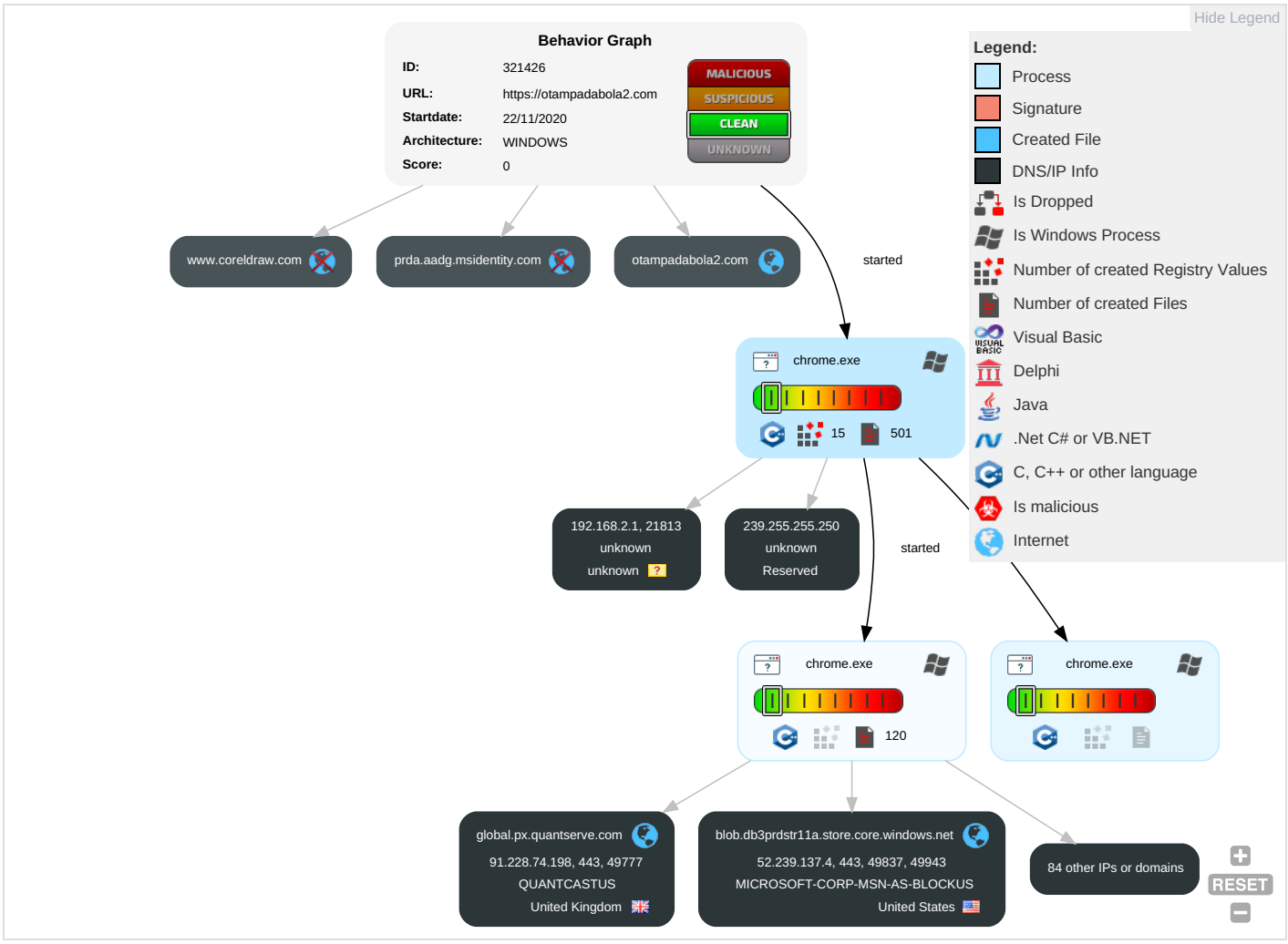
Click to jump to signature section

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

Mitre Att&ck Matrix

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

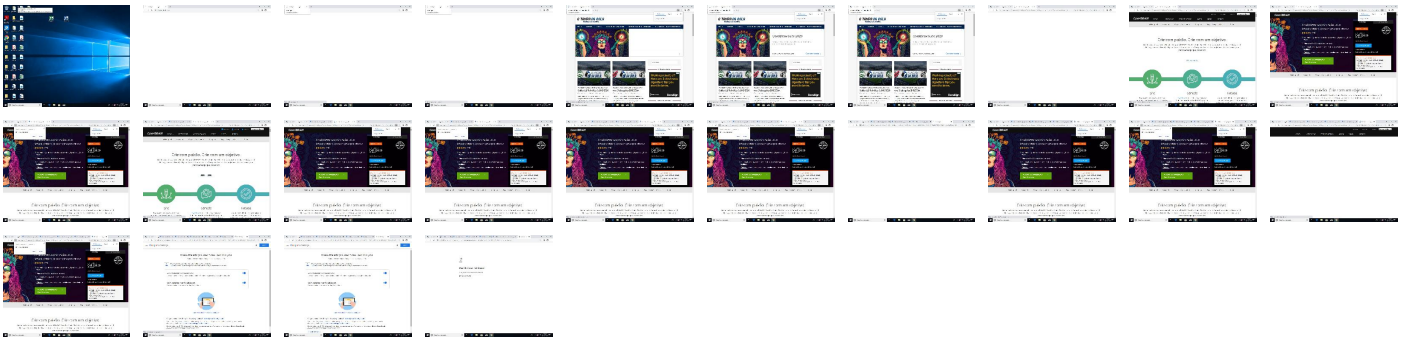
Behavior Graph

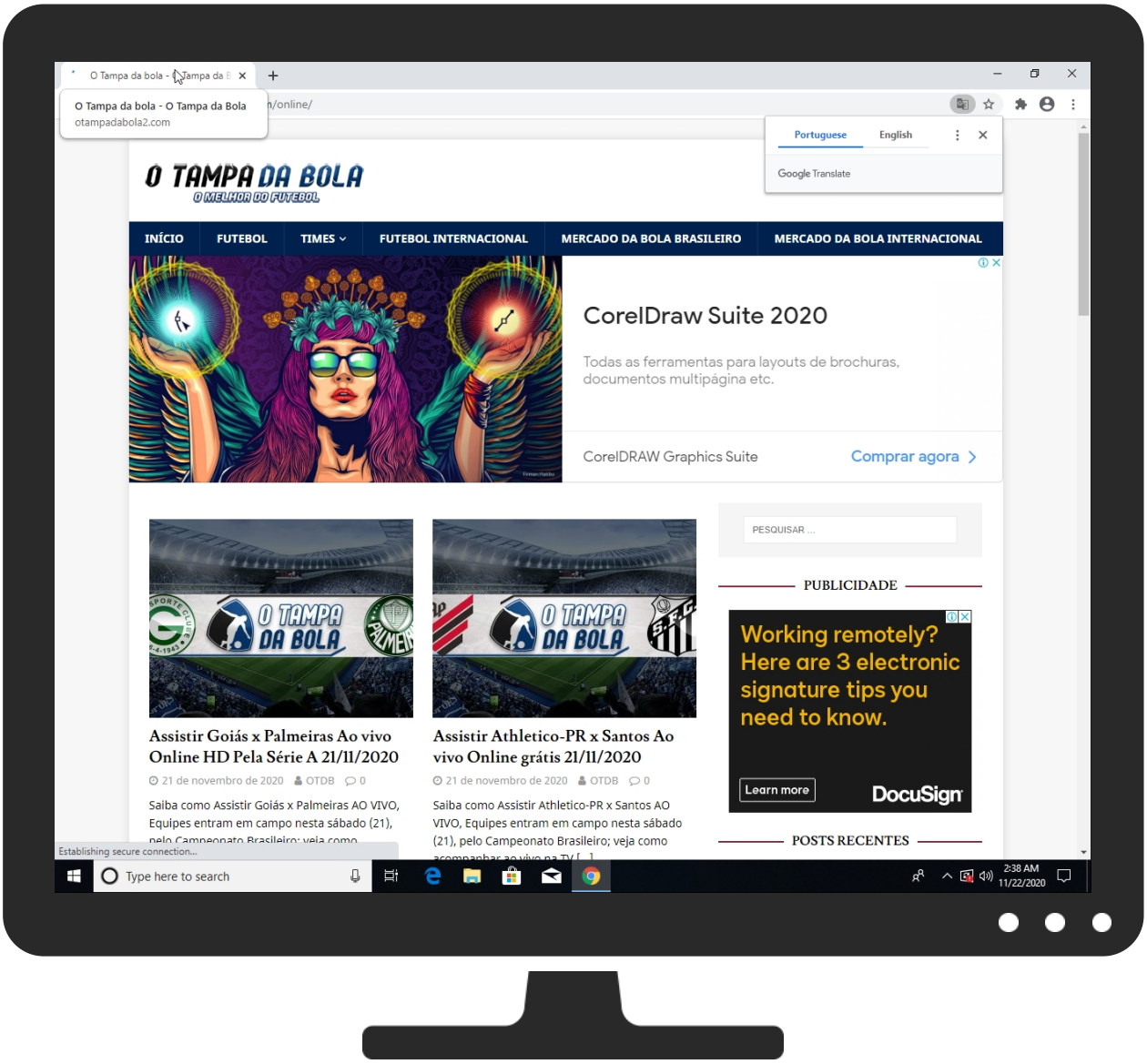


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://otampadabola2.com	0%	Virustotal		Browse
http://https://otampadabola2.com	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
otampadabola2.com	0%	Virustotal		Browse
280-qdk-215.mktoresp.com	0%	Virustotal		Browse
www.googleoptimize.com	0%	Virustotal		Browse
www.google.co.uk	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.aimtell.com/config/optin/	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/sv.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/sv.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/sv.html	0%	URL Reputation	safe	
http://https://dev.installer.public.corel.net/get_dwnld.cgi	0%	Avira URL Cloud	safe	
http://https://munchkin.marketo.net/munchkin.jsaD	0%	Avira URL Cloud	safe	
http://https://aimtell.com/jserror/manifestexists	0%	Avira URL Cloud	safe	
http://https://cdn.aimtell.com/sdk/aimtell-worker-sdk.jsaD	0%	Avira URL Cloud	safe	
http://https://network.aimtell.com/?u=	0%	Avira URL Cloud	safe	
http://https://munchkin.marketo.net/159/munchkin.jsa	0%	Avira URL Cloud	safe	
http://https://otampadabola2.com/wp-content/uploads/2020/10/cropped-Logo-O-Tampa-da-Bola-32x32.png	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/pl.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/pl.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/pl.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fr.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fr.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fr.html	0%	URL Reputation	safe	
http://https://otampadabola2.com/wp-includes/js/wp-emoji-release.min.js?ver=5.5.3	0%	Avira URL Cloud	safe	
http://https://munchkin.marketo.net/159/munchkin.js	0%	Avira URL Cloud	safe	
http://https://cdn.ywxi.net/js/1.js	0%	Avira URL Cloud	safe	
http://https://a.omappapi.com/app/js/webfont/1.5.18/webfont.js	0%	Avira URL Cloud	safe	
http://https://otampadabola2.com/wp-content/plugins/google-analytics-dashboard-for-wp/assets/js/frontend.mi	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/el.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/el.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/el.html	0%	URL Reputation	safe	
http://https://aimtell.com/developers	0%	Avira URL Cloud	safe	
http://https://otampadabola2.com/VG6gH89EbqAfs1RuoB5bYG9gHANIICQiA4YAQEAEYH5oJL2h0dHBzOi8vd3d3LmNvcmVsZHJhd	0%	Avira URL Cloud	safe	
http://https://otampadabola2.com/wp-includes/js/wp-embed.min.js?ver=5.5.3	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/zh.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/zh.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/zh.html	0%	URL Reputation	safe	
http://https://otampadabola2.com/online/O	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/fi.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fi.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/fi.html	0%	URL Reputation	safe	
http://https://otampadabola2.com/&	0%	Avira URL Cloud	safe	
http://https://www.coreldraw.comh	0%	Avira URL Cloud	safe	
http://https://otampadabola2.com/2	0%	Avira URL Cloud	safe	
http://https://otampadabola2.com/=m	0%	Avira URL Cloud	safe	
http://https://api.aimtell.com/prod/push/click/	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/sq.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/sq.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/sq.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/it.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/it.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/it.html	0%	URL Reputation	safe	
http://https://otampadabola2.com/wp-content/plugins/q2w3-fixed-widget/js/q2w3-fixed-widget.min.js?ver=5.1.9	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com	0%	URL Reputation	safe	
http://127.0.0.1/get_dwnld.cgi	0%	Avira URL Cloud	safe	
http://https://otampadabola2.com/O	0%	Avira URL Cloud	safe	
http://https://otampadabola2.com/p(T	0%	Avira URL Cloud	safe	
http://https://www.hotjarconsent.com/pt_br.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/pt_br.html	0%	URL Reputation	safe	
http://https://www.hotjarconsent.com/pt_br.html	0%	URL Reputation	safe	
http://https://otampadabola2.com/online/2	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
opmnstr.awesomemotive.netdna-cdn.com	23.111.11.182	true	false		high
global.px.quantserve.com	91.228.74.198	true	false		high
danv01ao0kdr2.cloudfront.net	13.224.89.212	true	false		high
cf.zdassets.com	104.18.70.113	true	false		high
rtb.openx.net	35.227.252.103	true	false		high
installer.corel.com	3.216.1.91	true	false		high
omappapi.awesomemotive.netdna-cdn.com	23.111.11.71	true	false		high
s3.amazonaws.com	52.216.147.61	true	false		high
script.hotjar.com	13.224.102.123	true	false		high
brandnode-1288026943.us-west-2.elb.amazonaws.com	52.42.117.229	true	false		high
otampadabola2.com	104.31.68.76	true	false	• 0%, Virustotal, Browse	unknown
pagead.l.doubleclick.net	216.58.205.226	true	false		high
tagr-gcp-odr-euw4.mookie1.com	34.98.67.61	true	false		high
d2bqow4fb67vs2.cloudfront.net	13.224.89.106	true	false		high
dkjrr5t9da86f.cloudfront.net	13.224.102.76	true	false		high
s3-us-west-2.amazonaws.com	52.218.248.16	true	false		high
static-cdn.hotjar.com	13.224.102.68	true	false		high
d1lpgznae1530s.cloudfront.net	13.224.102.10	true	false		high
pagead46.l.doubleclick.net	172.217.23.162	true	false		high
pugm22000nf.pubmatic.com	185.64.189.115	true	false		high
stats.l.doubleclick.net	74.125.140.157	true	false		high
280-qdk-215.mktoresp.com	192.28.147.68	true	false	• 0%, Virustotal, Browse	unknown
www.trustedsite.com	44.239.103.44	true	false		high
firewall-external-2134955858.eu-west-1.elb.amazonaws.com	108.128.94.32	true	false		high
d162h6x3rxav67.cloudfront.net	13.224.102.76	true	false		high
sjedt.adsafeprotected.com	104.244.38.20	true	false		high
insights-in-1202607485.eu-west-1.elb.amazonaws.com	52.31.241.82	true	false		high
www.googleoptimize.com	172.217.21.238	true	false	• 0%, Virustotal, Browse	unknown
vars.hotjar.com	13.224.102.94	true	false		high
partnerad.l.doubleclick.net	172.217.21.226	true	false		high
corel.zendesk.com	104.16.51.111	true	false		high
www.google.co.uk	172.217.21.195	true	false	• 0%, Virustotal, Browse	unknown
widget-mediator.zopim.com	18.194.82.2	true	false		high
dtx9pzf7ji0d9.cloudfront.net	13.224.102.99	true	false		high
blob.db3prdstr11a.store.core.windows.net	52.239.137.4	true	false		high
ib.anycast.adnxs.com	185.33.221.90	true	false		high
s.w.org	192.0.77.48	true	false		high
googlehosted.l.googleusercontent.com	172.217.16.193	true	false		high
geolocation.onetrust.com	104.20.184.68	true	false		high
pixel.everesttech.net	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
static.zdassets.com	unknown	unknown	false		high
static.hotjar.com	unknown	unknown	false		high
cm.g.doubleclick.net	unknown	unknown	false		high
ekr.zdassets.com	unknown	unknown	false		high
cdn.aimtell.com	unknown	unknown	false		unknown
ads.youtube.com	unknown	unknown	false		high
odr.mookie1.com	unknown	unknown	false		high
cdn.ywxi.net	unknown	unknown	false		unknown
portal.brandlock.io	unknown	unknown	false		unknown
pixel.rubiconproject.com	unknown	unknown	false		high
maxcdn.bootstrapcdn.com	unknown	unknown	false		high
munchkin.marketo.net	unknown	unknown	false		unknown
api.omappapi.com	unknown	unknown	false		unknown
ssum-sec.casalemedia.com	unknown	unknown	false		high
googleads.g.doubleclick.net	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
adclick.g.doubleclick.net	unknown	unknown	false		high
www.googletagservices.com	unknown	unknown	false		high
in.hotjar.com	unknown	unknown	false		high
image6.pubmatic.com	unknown	unknown	false		high
www.coreldraw.com	unknown	unknown	false		high
a.opmnstr.com	unknown	unknown	false		unknown
a.omappapi.com	unknown	unknown	false		unknown
ajax.aspnetcdn.com	unknown	unknown	false		high
adservice.google.co.uk	unknown	unknown	false		unknown
fw.adsafeprotected.com	unknown	unknown	false		high
dt.adsafeprotected.com	unknown	unknown	false		high
www.corel.com	unknown	unknown	false		high
optanon.blob.core.windows.net	unknown	unknown	false		high
dsum-sec.casalemedia.com	unknown	unknown	false		high
cms.quantserve.com	unknown	unknown	false		high
ib.adnxs.com	unknown	unknown	false		high
static.adsafeprotected.com	unknown	unknown	false		high

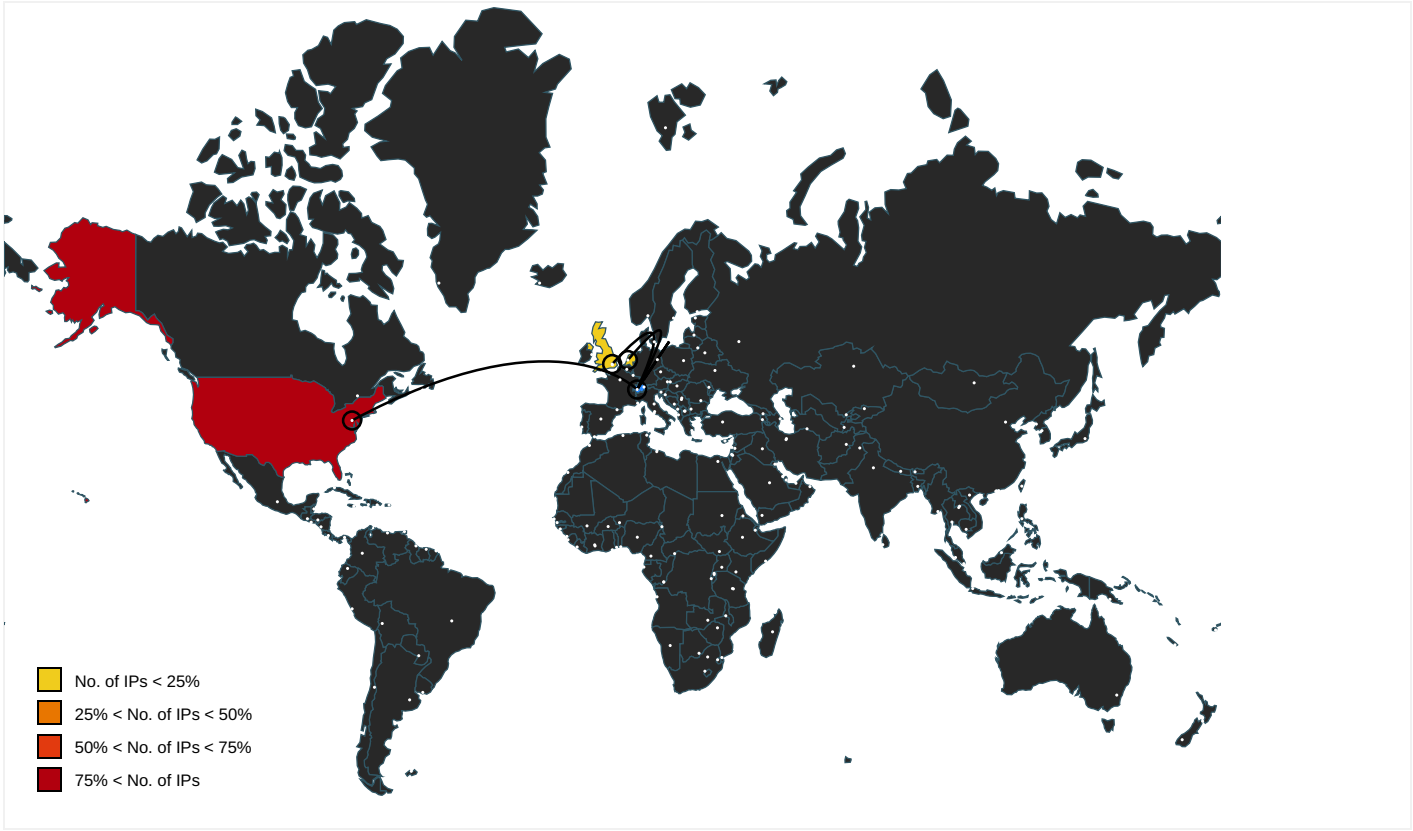
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.aimtell.com/config/optin/	84f9f4413dfeadac_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.hotjarconsent.com/sv.html	0710eb439444cf98_0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev.installer.public.corel.net/get_dwnld.cgi	ad5c3af72a4b1a91_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://munchkin.marketo.net/munchkin.jsaD	abcafd9c117cf694_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://aimtell.com/jserror/manifestexists	84f9f4413dfeadac_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://coreldraw.com/H%	4bf729f8a79cee0b_0.0.dr	false		high
http://https://www.coreldraw.com/static/common/scripts/omni-tracking/omni-tracking.min.jsaD	9f26e8b3e5102250_0.0.dr	false		high
http://https://cdn.aimtell.com/sdk/aimtell-worker-sdk.jsaD	4cb013792b196a35_1.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://network.aimtell.com/?u=	4cb013792b196a35_0.0.dr, 4cb013792b196a35_1.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://static.zdassets.com/web_widget/latest/	ce82ddef4d22607d_0.0.dr	false		high
http://https://www.corel.com/static/common/scripts/gtm/gtm-container.min.jsa	cd63cfd94ea6e329_0.0.dr	false		high
http://https://munchkin.marketo.net/159/munchkin.jsa	48f291afa9a147c0_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.coreldraw.com/static/common/scripts/gp/main.min.js	a40672e534fe8c73_0.0.dr	false		high
http://https://coreldraw.com/Wt	2d28c7d8ce7cd960_0.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/ads?guci=1.2.0.0.2.2.0.0&client=ca-pub-6297011322179391&o	Current Session.0.dr	false		high
http://https://static.zdassets.com/web_widget/latest/lazy/web_widget.ba9a857f2bb01785a8d1.chunk.jsaD	be0ecee0de7a754d_0.0.dr	false		high
http://https://www.coreldraw.com/static/common/scripts/omni-tracking/omni-tracking.min.js	9f26e8b3e5102250_0.0.dr	false		high
http://https://www.coreldraw.com/static/common/scripts/gp/main.min.jsaD	a40672e534fe8c73_0.0.dr	false		high
http://https://otampadabola2.com/wp-content/uploads/2020/10/cropped-Logo-O-Tampa-da-Bola-32x32.png	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.corel.com/static/common/scripts/gtm/gtm-container.min.jsaD	cd63cfd94ea6e329_0.0.dr	false		high
http://https://www.coreldraw.com/static/cdgs/js/trial-installer.js	ad5c3af72a4b1a91_0.0.dr	false		high
http://https://static.zdassets.com/web_widget/latest/web_widget.b8c69218285d2e8094b2.chunk.js	4fad52a0da7e4e43_0.0.dr, c4688328069dbc86_0.0.dr	false		high
http://https://www.corel.com/static/common/scripts/gtm/gtm-event-handlers.min.jsaD	e5ab37d46a06e4f2_0.0.dr	false		high
http://https://www.coreldraw.com/static/cdgs/js/owl.carousel.jsaD	6661e94a0ccb1861_0.0.dr	false		high
http://https://doubleclick.net/k	da62ad1aefac2632_0.0.dr	false		high
http://https://www.googletagservices.com/activeview/js/current/osd_listener.js?cache=r20110914aD	46db41e78b4307cf_0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.hotjarconsent.com/pl.html	0710eb439444cf98_0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.hotjarconsent.com/fr.html	0710eb439444cf98_0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://otampadabola2.com/wp-includes/js/wp-emoji-release.min.js?ver=5.5.3	94c05e03bdf09fdf_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://widget.manychat.com/	409d7183585b84f6_0.0.dr	false		high
http://https://maxcdn.bootstrapcdn.com/	Network Action Predictor.0.dr	false		high
http://https://www.coreldraw.com/	000003.log6.0.dr	false		high
http://https://www.coreldraw.com/static/common/scripts/css-phone.js	d010177029c605ae_0.0.dr	false		high
http://https://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.11.2.min.js	d7b107a561b4f0b9_0.0.dr, 996bdcade1a612cc_0.0.dr	false		high
http://https://munchkin.marketo.net/159/munchkin.js	48f291afa9a147c0_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.coreldraw.com/static/common/scripts/jquery.magnific-popup.min.jsa	6c66dcb53706dfab_0.0.dr	false		high
http://https://www.coreldraw.com/static/common/scripts/dynamic-pricing/dynamic-promotions.min.jsaD	7b9cd0a6e51ca8f1_0.0.dr	false		high
http://https://www.coreldraw.com/static/common/scripts/gp/function.min.js	bfb390eef3503cea_0.0.dr	false		high
http://https://github.com/webpack-contrib/style-loader#insertat)	409d7183585b84f6_0.0.dr	false		high
http://https://cdn.ywxi.net/js/1.js	a5908dada370f37f_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://doubleclick.net/I	91c56cc36baae634_0.0.dr	false		high
http://https://static.zdassets.com/web_widget/latest/lazy/web_widget.ba9a857f2bb01785a8d1.chunk.js	be0ecee0de7a754d_0.0.dr	false		high
http://https://www.coreldraw.com/static/common/scripts/gp/shadowbox.jsaD	e96bc7d59d385e1a_0.0.dr	false		high
http://https://www.coreldraw.com/static/common/scripts/jquery.magnific-popup.min.js	6c66dcb53706dfab_0.0.dr	false		high
http://www.coreldraw.com	2cc80dabc69f58b6_0.0.dr	false		high
http://https://danv01ao0kdr2.cloudfront.net/danv01ao0kdr.html	Current Session.0.dr	false		high
http://https://static.zdassets.com/	Network Action Predictor.0.dr	false		high
http://https://a.omappapi.com/app/js/webfont/1.5.18/webfont.js	7a7a3044cc4ae692_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://ajax.aspnetcdn.com/	Network Action Predictor.0.dr	false		high
http://https://identify.hotjar.com	0710eb439444cf98_0.0.dr	false		high
http://https://otampadabola2.com/wp-content/plugins/google-analytics-dashboard-for-wp/assets/js/frontend.mi	5e5984a807e18440_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.coreldraw.com/static/cdgs/js/trial-installer.jsaD	ad5c3af72a4b1a91_0.0.dr	false		high
http://https://www.hotjarconsent.com/el.html	0710eb439444cf98_0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://coreldraw.com/)B	be0ecee0de7a754d_0.0.dr	false		high
http://https://aimtell.com/developers	84f9f4413dfeadac_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://doubleclick.net/T	2a2a9a1a50374767_0.0.dr	false		high
http://https://www.coreldraw.com/static/common/scripts/dynamic-pricing/jquery.format-currency-1.4.0.min.js	4cf5a22a75d22bb9_0.0.dr	false		high
http://https://otampadabola2.com/VG6gH89EbqAfs1RuoB5bYG9gHANIICQiA4YAQEAEYH5oJL2h0dHBzOi8vd3d3LmNvcmVsZHJhd	History.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.hotjar.com/feedback-polls?utm_source=client&utm_medium=poll&utm_campaign=insights	0710eb439444cf98_0.0.dr	false		high
http://https://coreldraw.com/hXi	e80d5eb0d89256d9_0.0.dr	false		high
http://https://otampadabola2.com/wp-includes/js/wp-embed.min.js?ver=5.5.3	c7ad3049cf875f0e_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://www.hotjarconsent.com/zh.html	0710eb439444cf98_0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://doubleclick.net/G	160a04ebd7990d80_0.0.dr	false		high
http://https://a.nel.cloudflare.com/report?s=dUOZAN6rSHJ3kUITvTLALTkZY4OREDmi4Ed%2BiKbqzu17Qo%2FXucb%2F94A9	Reporting and NEL.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://otampadabola2.com/online/O	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.hotjarconsent.com/fi.html	0710eb439444cf98_0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.coreldraw.com/static/common/scripts/gp/shadowbox.js	e96bc7d59d385e1a_0.0.dr	false		high
http://https://doubleclick.net/	6019ad028452e15e_0.0.dr, f8f5f6d11b80e0de_0.0.dr, e91571dba04d49f6_0.0.dr	false		high
http://https://otampadabola2.com/&	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://googleads.g.doubleclick.net/	QuotaManager.0.dr, 000003.log0.0.dr	false		high
http://https://www.coreldraw.comh	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.corel.com/static/common/scripts/gtm/gtm-container.min.js	cd63cfd94ea6e329_0.0.dr	false		high
http://https://optinmonster.com/?utm_source=plugin&utm_medium=link&utm_campaign=powered-by-link	409d7183585b84f6_0.0.dr	false		high
http://https://otampadabola2.com/2	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://otampadabola2.com/=m	5e5984a807e18440_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://static.zdassets.com/web_widget/latest/preload.b134a3818b60177eac5c.jsaD	ce82ddef4d22607d_0.0.dr	false		high
http://https://api.aimtell.com/prod/push/click/	4cb013792b196a35_1.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.hotjarconsent.com/sq.html	0710eb439444cf98_0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.hotjarconsent.com/it.html	0710eb439444cf98_0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://otampadabola2.com/wp-content/plugins/q2w3-fixed-widget/js/q2w3-fixed-widget.min.js?ver=5.1.9	052494325eac1892_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.coreldraw.com/static/cdgs/js/imgslider-1.2.1-min.jsaD	99cf79b1ac0d33bd_0.0.dr	false		high
http://https://www.coreldraw.com/static/common/scripts/dynamic-pricing/dynamic-pricing.min.jsaD	20d600d5c3cfa464_0.0.dr	false		high
http://https://www.coreldraw.com/br/product/coreldraw/%3Ftopnav%3Dfalse%26trial%3Dbig%26sourceid%3Dcdgs2020	History.0.dr	false		high
http://https://www.hotjarconsent.com	0710eb439444cf98_0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://coreldraw.com/Kd	a5908dada370f37f_0.0.dr	false		high
http://https://script.hotjar.com/modules.ae930258b2386dc57451.js	b1eea72a9a753c29_0.0.dr	false		high
http://https://www.coreldraw.com/static/cdgs/js/jquery.main.jsaD	d4a518ee22c34ba0_0.0.dr	false		high
http://127.0.0.1/get_dwnld.cgi	ad5c3af72a4b1a91_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.coreldraw.com/aimtell-worker.js	000003.log6.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/956202557/?random=1606041553651&cv=	02da4a26b7e48bf2_0.0.dr	false		high
http://https://www.coreldraw.com/static/common/scripts/responsiveslides.min.js	5cc86c6607abbc80_0.0.dr	false		high
http://https://otampadabola2.com/O	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://otampadabola2.com/p(T	e58b157a3bf017dc_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://static.zdassets.com/web_widget/latest/web_widget.b8c69218285d2e8094b2.chunk.jsaD	4fad52a0da7e4e43_0.0.dr	false		high
http://https://googleads.g.doubleclick.net/ads/preferences/getcookie?sig=ACi0TCg_C7CUTj9C6KzIiY7rDWyks29Atw	History.0.dr	false		high
http://https://optanon.blob.core.windows.net/	Network Action Predictor.0.dr	false		high
http://https://www.hotjarconsent.com/pt_br.html	0710eb439444cf98_0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://static.zdassets.com/ekr/snippet.js?key=d3f88178-b699-4002-a1d6-f61fec7d4063	4bf729f8a79cee0b_0.0.dr	false		high
http://https://otampadabola2.com/online/2	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.33.221.90	unknown	Netherlands		29990	ASN-APPNEXUS	false
104.18.71.113	unknown	United States		13335	CLOUDFLARENETUS	false
216.58.208.34	unknown	United States		15169	GOOGLEUS	false
172.217.21.238	unknown	United States		15169	GOOGLEUS	false
216.58.205.226	unknown	United States		15169	GOOGLEUS	false
52.216.147.61	unknown	United States		16509	AMAZON-02US	false
104.20.184.68	unknown	United States		13335	CLOUDFLARENETUS	false
216.58.210.2	unknown	United States		15169	GOOGLEUS	false
13.224.102.68	unknown	United States		16509	AMAZON-02US	false
18.194.82.2	unknown	United States		16509	AMAZON-02US	false
52.31.241.82	unknown	United States		16509	AMAZON-02US	false
52.239.137.4	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
104.244.38.20	unknown	United States		7415	ADSAFE-1US	false
91.228.74.198	unknown	United Kingdom		27281	QUANTCASTUS	false
108.128.94.32	unknown	United States		16509	AMAZON-02US	false
74.125.140.157	unknown	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
104.18.70.113	unknown	United States		13335	CLOUDFLARENETUS	false
3.216.1.91	unknown	United States		14618	AMAZON-AESUS	false
172.217.21.195	unknown	United States		15169	GOOGLEUS	false
172.217.16.194	unknown	United States		15169	GOOGLEUS	false
13.224.102.99	unknown	United States		16509	AMAZON-02US	false
13.224.89.106	unknown	United States		16509	AMAZON-02US	false
172.217.16.193	unknown	United States		15169	GOOGLEUS	false
13.224.102.10	unknown	United States		16509	AMAZON-02US	false
34.98.67.61	unknown	United States		15169	GOOGLEUS	false
52.218.248.16	unknown	United States		16509	AMAZON-02US	false
13.224.89.212	unknown	United States		16509	AMAZON-02US	false
13.224.102.94	unknown	United States		16509	AMAZON-02US	false
104.31.68.76	unknown	United States		13335	CLOUDFLARENETUS	false
172.217.21.226	unknown	United States		15169	GOOGLEUS	false
192.28.147.68	unknown	United States		53580	MARKETOUS	false
172.217.23.98	unknown	United States		15169	GOOGLEUS	false
104.16.51.111	unknown	United States		13335	CLOUDFLARENETUS	false
52.42.117.229	unknown	United States		16509	AMAZON-02US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.224.102.123	unknown	United States		16509	AMAZON-02US	false
185.64.189.115	unknown	United Kingdom		62713	AS-PUBMATICUS	false
44.239.103.44	unknown	United States		16509	AMAZON-02US	false
23.111.11.71	unknown	United States		33438	HIGHWINDS2US	false
172.217.23.162	unknown	United States		15169	GOOGLEUS	false
35.227.252.103	unknown	United States		15169	GOOGLEUS	false
172.217.22.34	unknown	United States		15169	GOOGLEUS	false
13.224.102.76	unknown	United States		16509	AMAZON-02US	false
23.111.11.182	unknown	United States		33438	HIGHWINDS2US	false

Private

IP
192.168.2.1
192.168.2.3
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321426
Start date:	22.11.2020
Start time:	02:37:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://otampadabola2.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:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.win@50/302@54/47
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://adclick.g.doubleclick.net/aclk?sa=l&ai=CzIstF8G5X8rjNoGu3gPNj6-wD-DN6pNgz8DSx-wLnriItoMDEAEgq4qCJmC7BqAB9NbDvQPIAQmoAwHIA8sEqgTEAU_QGmYQJT_z1nSaqaGExbDL1MYM8kvXcSkj5GfrR3jWOe_VawECyTPPk_UUOEQf312KgAVjAD9-dT9G6dGf5tHOyKqKomcqscOS1g_cr9CFsse2ZDbf5bC9mCOFBrxozlXqJDHnS6xwdNpqQv_TS25xxqSpl5evCO1CsHOOO_9rJM_WuwZL6talhN8CoKkuCe61E_G9VKTFEdAb6cJRx2o4y1AhMGom2Apy7aSktK7kV6D_D9yyfskgkoC3y8_mJ9JNGV7ABJ_akafcAaAGLoAH9Ki8QqgH1ckbqAfw2RuoB_LZG6gHjs4bqAeT2BuoB7oGqAfulrECqAemvhuoB-zVG6gH89EbqAfs1RuoB5bYG9gHANIICQiA4YAQEAEYH7EJJ1y9IbcsoHuACgGYCwHICwGADAG4DAHYEw2IFAI&ae=1&num=1&sig=AOD64_24S7CJRXBcAhEC7NK-HzAO-GP4kQ&client=ca-pub-6297

011322179391&nb=9&adur
l=https://www.coreldraw.com/br
/product/coreldraw/%3Ftopnav%3
Dfalse%26trial%3Dbig%26sourceid%3Dcdgs2020-
xx-ppc_ron%26x-ve
hicle%3Dppc_ron%26gclid%3DEAIa
IQobChMIisv7lIKV7QIVAZd3Ch3Nxw
v2EAEYASAAEgI0ovD_BwE

- Browse: https://adclick.g.doubleclick.net/aclk?
sa=l&ai=CzIstF8G5X8rjNoGu3gPNj6-wD-
DN6pNgz8DSx-wLnriItoMDEAEgq4qCJmC7
BqAB9NbDvQPIAQmoAwHIA8sEqgTEAU
_QGmYQJT_z1nSaqaGExbDL1MYM8kvX
cSkj5GfrR3jWOe_VawECyTPPk_UUOE
Qf312KgAVjAD9-dT9G6dGf5tHOyKqK
omcqscOS1g_cr9CFsse2ZDbf5bC9mC
OFBrxozlXqJDHnS6xwdNpqQv_TS25x
xqSpl5evCO1CsHOOO_9rJM_WuwZL6t
alhN8CoKkuCe61E_G9VKTFEdAb6cJR
x2o4y1AhMGom2Apy7aSktK7kV6D_D9
yyfskgkoC3y8_mJ9JNGV7ABJ_akafc
AaAGLoAH9Ki8QqgH1ckbqAfw2RuoB_
LZG6gHjs4bqAeT2BuoB7oGqAfulrECqAemvhuoB-
zVG6gH89EbqAfs1RuoB5
bYG9gHANIICQiA4YAQEAEYH7EJJ1y9
IbcsoHuACgGYCwHICwGADAG4DAHYEw
2IFAI&ae=1&num=1&s
ig=AOD64_24S7CJRXBcAhEC7NK-HzAO-
GP4kQ&client=ca-pub-6297
011322179391&nb=0&adur
l=https://www.coreldraw.com/br
/product/coreldraw/%3Ftopnav%3
Dfalse%26trial%3Dbig%26sourceid%3Dcdgs2020-
xx-ppc_ron%26x-ve
hicle%3Dppc_ron%26gclid%3DEAIa
IQobChMIisv7lIKV7QIVAZd3Ch3Nxw
v2EAEYASAAEgI0ovD_BwE
- Browse: https://adclick.g.doubleclick.net/aclk?
sa=l&ai=CzIstF8G5X8rjNoGu3gPNj6-wD-
DN6pNgz8DSx-wLnriItoMDEAEgq4qCJmC7
BqAB9NbDvQPIAQmoAwHIA8sEqgTEAU
_QGmYQJT_z1nSaqaGExbDL1MYM8kvX
cSkj5GfrR3jWOe_VawECyTPPk_UUOE
Qf312KgAVjAD9-dT9G6dGf5tHOyKqK
omcqscOS1g_cr9CFsse2ZDbf5bC9mC
OFBrxozlXqJDHnS6xwdNpqQv_TS25x
xqSpl5evCO1CsHOOO_9rJM_WuwZL6t
alhN8CoKkuCe61E_G9VKTFEdAb6cJR
x2o4y1AhMGom2Apy7aSktK7kV6D_D9
yyfskgkoC3y8_mJ9JNGV7ABJ_akafc
AaAGLoAH9Ki8QqgH1ckbqAfw2RuoB_
LZG6gHjs4bqAeT2BuoB7oGqAfulrECqAemvhuoB-
zVG6gH89EbqAfs1RuoB5
bYG9gHANIICQiA4YAQEAEYH7EJJ1y9
IbcsoHuACgGYCwHICwGADAG4DAHYEw
2IFAI&ae=1&num=1&s
ig=AOD64_24S7CJRXBcAhEC7NK-HzAO-
GP4kQ&client=ca-pub-6297
011322179391&nb=9&adur
l=https://www.coreldraw.com/br
/product/coreldraw/%3Ftopnav%3
Dfalse%26trial%3Dbig%26sourceid%3Dcdgs2020-
xx-ppc_ron%26x-ve
hicle%3Dppc_ron%26gclid%3DEAIa
IQobChMIisv7lIKV7QIVAZd3Ch3Nxw
v2EAEYASAAEgI0ovD_BwE
- Browse: https://adclick.g.doubleclick.net/aclk?
sa=l&ai=CzIstF8G5X8rjNoGu3gPNj6-wD-
DN6pNgz8DSx-wLnriItoMDEAEgq4qCJmC7
BqAB9NbDvQPIAQmoAwHIA8sEqgTEAU
_QGmYQJT_z1nSaqaGExbDL1MYM8kvX
cSkj5GfrR3jWOe_VawECyTPPk_UUOE
Qf312KgAVjAD9-dT9G6dGf5tHOyKqK
omcqscOS1g_cr9CFsse2ZDbf5bC9mC
OFBrxozlXqJDHnS6xwdNpqQv_TS25x
xqSpl5evCO1CsHOOO_9rJM_WuwZL6t
alhN8CoKkuCe61E_G9VKTFEdAb6cJR
x2o4y1AhMGom2Apy7aSktK7kV6D_D9
yyfskgkoC3y8_mJ9JNGV7ABJ_akafc
AaAGLoAH9Ki8QqgH1ckbqAfw2RuoB_
LZG6gHjs4bqAeT2BuoB7oGqAfulrECqAemvhuoB-
zVG6gH89EbqAfs1RuoB5
bYG9gHANIICQiA4YAQEAEYH7EJJ1y9
IbcsoHuACgGYCwHICwGADAG4DAHYEw
2IFAI&ae=1&num=1&s
ig=AOD64_24S7CJRXBcAhEC7NK-HzAO-
GP4kQ&client=ca-pub-6297
011322179391&nb=7&adur
l=https://www.coreldraw.com/br
/product/coreldraw/%3Ftopnav%3
Dfalse%26trial%3Dbig%26sourceid%3Dcdgs2020-
xx-ppc_ron%26x-ve
hicle%3Dppc_ron%26gclid%3DEAIa
IQobChMIisv7lIKV7QIVAZd3Ch3Nxw
v2EAEYASAAEgI0ovD_BwE
- Browse: https://adclick.g.doubleclick.net/aclk?
sa=l&ai=CzIstF8G5X8rjNoGu3gPNj6-wD-
DN6pNgz8DSx-wLnriItoMDEAEgq4qCJmC7
BqAB9NbDvQPIAQmoAwHIA8sEqgTEAU
_QGmYQJT_z1nSaqaGExbDL1MYM8kvX
cSkj5GfrR3jWOe_VawECyTPPk_UUOE
Qf312KgAVjAD9-dT9G6dGf5tHOyKqK
omcqscOS1g_cr9CFsse2ZDbf5bC9mC
OFBrxozlXqJDHnS6xwdNpqQv_TS25x
xqSpl5evCO1CsHOOO_9rJM_WuwZL6t
alhN8CoKkuCe61E_G9VKTFEdAb6cJR
x2o4y1AhMGom2Apy7aSktK7kV6D_D9
yyfskgkoC3y8_mJ9JNGV7ABJ_akafc
AaAGLoAH9Ki8QqgH1ckbqAfw2RuoB_
LZG6gHjs4bqAeT2BuoB7oGqAfulrECqAemvhuoB-
zVG6gH89EbqAfs1RuoB5
bYG9gHANIICQiA4YAQEAEYH7EJJ1y9
IbcsoHuACgGYCwHICwGADAG4DAHYEw
2IFAI&ae=1&num=1&s
ig=AOD64_24S7CJRXBcAhEC7NK-HzAO-
GP4kQ&client=ca-pub-6297
011322179391&nb=1&adur
l=https://www.coreldraw.com/br
/product/coreldraw/%3Ftopnav%3
Dfalse%26trial%3Dbig%26sourceid%3Dcdgs2020-

xx-ppc_ron%26x-ve
hicle%3Dppc_ron%26gclid%3DEAIa
IQobChMIisv7lIKV7QIVAZd3Ch3Nxw
v2EAEYASAAEgI0ovD_BwE

- Browse: https://adclick.g.doubleclick.net/aclk?
sa=l&ai=CzIstF8G5X8rjNoGu3gPNj6-wD-
DN6pNgz8DSx-wLnriItoMDEAEgq4qCJmC7
BqAB9NbDvQPIAQmoAwHIA8sEqgTEAU
_QGmYQJT_z1nSaqaGExbDL1MYM8kvX
cSkj5GfrR3jWOe_VawECyTPPk_UUOE
Qf312KgAVjAD9-dT9G6dGf5tHOyKqK
omcqscOS1g_cr9CFsse2ZDbf5bC9mC
OFBrxozIXqJDHnS6xwdNpqQv_TS25x
xqSpI5evCO1CsHOOO_9rJM_WuwZL6t
alhN8CoKkuCe61E_G9VKTFEdAb6cJR
x2o4y1AhMGom2Apy7aSktK7kV6D_D9
yyfskgkoC3y8_mJ9JNGV7ABJ_akafc
AaAGLoAH9Ki8QqgH1ckbqAfw2RuoB_
LZG6gHjs4bqAeT2BuoB7oGqAfulrECqAemvhuoB-
zVG6gH89EbqAfs1RuoB5
bYG9gHANIICQiA4YAQEAEYH7EJJ1y9
IbcsoHuACgGYCwHICwGADAG4DAHYEw
2IFAI&ae=1&num=1&s
ig=AOD64_24S7CJRXBcAhEC7NK-HzAO-
GP4kQ&client=ca-pub-6297
011322179391&nb=8&adur
l=https://www.coreldraw.com/br
/product/coreldraw/%3Ftopnav%3
Dfalse%26trial%3Dbig%26sourceid%3Dcdgs2020-
xx-ppc_ron%26x-ve
hicle%3Dppc_ron%26gclid%3DEAIa
IQobChMIisv7lIKV7QIVAZd3Ch3Nxw
v2EAEYASAAEgI0ovD_BwE
- Browse: https://adssettings.google.com/whythisad?
reasons=AB3
afGEAAASPW1tbW251bGwsWzEwXSxud
WxsLG51bGwsbnVsbCxbljkyOTEzll1
dLFtudWxsLCJodHRwczovL2dvb2dsZ
WFkcy5nLmRvdWJsZWNsaWNrLm5ldC9
wYWdlYWQvY29udmVyc2lvbi8_YWk9Q
3pJc3RGOEc1WDhyak5vR3UzZ1BOajY
td0QtRE42cE5nejhEU3gtd0xucmlJd
G9NREVBRWdxNHFDSm1DN0JxQUI5TmJ
EdlFQSUFRbW9Bd0hJQThzRXFnVEVBV
V9RR21ZUUpUX3oxblNhcWFHRXhiREw
xTVlNOGt2WGNTa2o1R2ZyUjNqV09lX
1Zhd0VDeVRQUGtfVVVPRVFmMzEyS2d
BVmpBRDktZFQ5RzZkR2Y1dEhPeUtxS
29tY3FzY09TMWdfY3l5Q0Zzc2UyWkR
iZjViQzltQ09GQnJ4b3pJWHFKREhuU
zZ4d2ROcHFRdl9UUzI1eHhxU3BJNWV
2Q08xQ3NIT09PXzlySk1fV3V3Wkw2d
GFsaE44Q29La3VDZTYxRV9HOVZLVEZ
FZEFiNmNKUngybzR5MUFoTUdvbTJBc
Hk3YVNrdEs3a1Y2RF9EOXl5ZnNrZ2t
vQzN5OF9tSjlKTkdWN0FCSl9ha2FmY
0FhQUdMb0FIOUtpOFFxZ0gxY2ticUF
mdzJSdW9CX0xaRzZnSGpzNGJxQWVUM
kJ1b0l3b0dxQWZ1bHJFQ3FBZW12aHV
vQi16Vkc2Z0g4OUVicUFmczFSdW9CN
WJZRzlnSEFOSUlDUWlBNFlBUUVBRVl
IN0VKSjF5OUliY3NvSHVBQ2dHWUN3S
ElDd0dBREFHNERBSFlFdzJJRkFJXHU
wMDI2c2lnaD1Ja1R4TTVNSXI4SVx1M
DAyNmNpZD1DQVFTR3dDTklyTE03bWN
OVkFpWG9rU1NGNm5mS25GLVpKLTJQM
UNreEEiLFtudWxsLG51bGwsbnVsbCw
iaHR0cHM6Ly9kaXNwbGF5YWRzLWZvc
m1hdHMuZ29vZ2xldXNlcmNvbnRlbnQ
uY29tL2Fkcy9wcmV2aWV3L2NvbnRlb
nQuanM_Y2xpZW50PXd0YVx1MDAyNm9
iZnVzY2F0ZWRDdXN0b21lcklkPTkxN
TA3MTczNzJcdTAwMjZjcmVhdGl2ZUl
kPTQyNDY0MTgyMDQ3MFx1MDAyNnZlc
nNpb25JZD0yXHUwMDI2YWRHcm91cEN
yZWF0aXZlSWQ9NDA3MDk4NDAwODQ3X
HUwMDI2aHRtbFBhcmVudElkPXByZXY
tMFx1MDAyNmhlaWdodD0wXHUwMDI2d
2lkdGg9MFx1MDAyNnNpZz1BQ2lWQl9
5UTNvM2owdzE2bHVDVTRtX1lHUk5rT
3EzMEZnIl0sbnVsbCxudWxsLDEsIjA
xdll3emtCRUNZSXo4RFN4LXdMRU5MU
XNwOEZHSnl2dFVJaURXTnZjbVZzWkh
KaGR5NWpiMjB5Q0FnRkV4ajZud0VVU
WhkallTMXdkV0l0TmpJNU56QXhNVE1
5TWpFM09UTTVNVWdHV0M1Z2lDZHdBU
SIsIjE0MDgwMTg1MTQiXV1dLFsxLDE
sMV1de5BNuQ9C13GfbVmWpIV50NiMj
UeYwGraxhZEcyoTrGYd7NVDdOqvtxJ
dfJLt1RMeM4fusKZqp8WeeSUA5oWVa

	fy2MevAaK6LsV5uASIqU-vSZ1dMtFc E5w5M0JiikuXdzEcLaMjE6ygZSC-yCsKv7yo1Tvm- P5m3K_0qVnpG0DgQQ-j 5GaRvDUxDITOS0FvO6HP0gX1lxNYGS mmkkEl6UrUIdGiwUoOBB54i3UWq1Kc t6JtxOEe_v9zg6z8XgZ9WNwdhk9F_s 0IpwLQQb6WGa9cqcq4qFC8S7qczf14 ZF9RT8dt4mLvnPeAxk38L1jULwb1YE 5p1O_x0jHm7e39mZQ • Browse: pUS5kpEDBLtmZ3jjEPrjTw &source=display
Warnings:	Show All • Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 40.88.32.150, 172.217.18.173, 216.58.206.14, 216.58.212.163, 172.217.16.142, 173.194.187.8, 173.194.182.74, 172.217.18.106, 216.58.205.227, 172.217.23.142, 216.58.207.74, 216.58.205.234, 172.217.22.35, 172.217.23.97, 216.58.208.36, 2.20.85.164, 99.80.199.35, 34.246.227.69, 63.33.127.66, 69.173.144.139, 69.173.144.138, 69.173.144.165, 2.20.142.210, 2.20.142.209, 172.217.18.99, 2.20.84.134, 209.197.3.15, 152.199.19.160, 216.58.206.8, 204.79.197.200, 13.107.21.200, 2.21.60.250, 216.58.207.42, 172.217.16.202, 216.58.206.10, 172.217.22.10, 172.217.16.170, 216.58.208.42, 216.58.210.10, 172.217.23.106, 216.58.212.138, 172.217.22.42, 172.217.16.138, 172.217.22.106, 216.58.212.170, 142.250.74.202, 2.20.84.85, 51.104.139.180, 67.26.81.254, 8.248.131.254, 8.248.117.254, 67.26.83.254, 67.26.139.254, 172.217.16.174, 216.58.212.168, 172.217.18.14, 172.217.16.131, 173.194.182.233, 20.54.26.129, 40.126.1.130, 20.190.129.17, 40.126.1.145, 20.190.129.2, 40.126.1.166, 20.190.129.24, 20.190.129.19, 20.190.129.133, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, arc.msn.com.nsatc.net, r3---sn-4g5e6ns6.gvt1.com, partner.googleadservices.com, www.tm.lg.prod.aadmsa.akadns.net, clientservices.googleapis.com, e10776.b.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, e834.dscd.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, clients2.google.com, login.live.com, www.coreldraw.com.edgekey.net, audownload.windowsupdate.nsatc.net, update.googleapis.com, r4.sn-4g5e6nsz.gvt1.com, www.google.com, tp00.everesttech.net.akadns.net, ssl-google-analytics.l.google.com, watson.telemetry.microsoft.com, www.gstatic.com, au-bg-shim.trafficmanager.net, www.google-analytics.com, e834.d.akamaiedge.net, fonts.googleapis.com, fs.microsoft.com, content-autofill.googleapis.com, plus.l.google.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, www.tm.a.prd.aadg.akadns.net, pagead2.googlesyndication.com, www.googleapis.com, ris.api.iris.microsoft.com, www3.l.google.com, r4---sn-4g5e6nsz.gvt1.com, translate.googleapis.com, blobcollector.events.data.trafficmanager.net, dsum-sec.casalemedia.com.edgekey.net, clients.l.google.com, r5---sn-4g5e6ns7.gvt1.com, r3.sn-4g5e6ns6.gvt1.com, au.download.windowsupdate.com.edgesuite.net, www.googleadservices.com, pixel.rubiconproject.net.akadns.net, ogs.google.com, adservice.google.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wildcard.marketo.net.edgekey.net, arc.msn.com, e8037.g.akamaiedge.net, mscomajax.vo.msecnd.net, redirector.gvt1.com, www.googletagmanager.com, bat.bing.com, adssettings.google.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, accounts.google.com, www-google-

analytics.l.google.com, fonts.gstatic.com, cs22.wpc.v0cdn.net, www-googletagmanager.l.google.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, r5.sn-4g5e6ns7.gvt1.com, login.msa.msidentity.com, ssl.google-analytics.com, bat-bing-com.a-0001.a-msedge.net, play.google.com, tpc.googlesyndication.com, www-san.corel.com.edgekey.net, ssum-sec.casalemedia.com.edgekey.net, cds.j3z9t3p6.hwcdn.net, skypedataprdcolwus16.cloudapp.net, apis.google.com

- Report size exceeded maximum capacity and may have missing behavior 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
02:38:33	API Interceptor	2x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.... ....6...."..Z..4g....6.2...{/...3...5....AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GMDS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\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:	D9E03A617D1D9505D3ADA3C41FC8A53504F4F1C44F92AF00869F2FE150D6677FD4450E85EB1E3D920D32BA01F190E7F14BF130F8CC69EB47D834CCE43CAA760
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\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.118125015901308
Encrypted:	false
SSDEEP:	12:3rTkPlE99SNxAhUegeTQHkPlE99SNxAhUegeT2:nkPcUQU76SkPcUQU762
MD5:	C3FA7A17305E8A8F262422BFCFF39351
SHA1:	4F4BF6BF04B1731DA1CDC05D07794FD230DBADF2
SHA-256:	C83A82B58113FBFD58B05EF008A0894F49EF46E1BD0B0D99AFCCF906C9291508
SHA-512:	E7B9A66F411214FF747DB0AB22DC46C464D9CC5646B90F06A2FDF3C8F7649C617EB747AFC097C9ED0399A06E61CCCC562957D9BB41DDDFED03FA9739617075C
Malicious:	false
Reputation:	low
Preview:	p..... .....(..... .....Y.....$.....8...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...p..... .....a.....(..... .....Y.....$.....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\Local\Google\Chrome\User Data\60ab1266-68c1-41f0-bb06-0df981b46732.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	96744
Entropy (8bit):	3.751489796278514
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\60ab1266-68c1-41f0-bb06-0df981b46732.tmp	
SSDEEP:	384:uLn0EGpj1pNWQVhTQzNcrtvYk3nkSzHuzGj2rhWki1xHqi6FrxMmF5rlmUQ4DOGR:TualpamwHUe/bEIyUHPeAKWIQHx
MD5:	5713467D36B3C3599C2136648391B6EC
SHA1:	1F33C7F85930B3EA588DCB1F903E546EDBB0C38E
SHA-256:	B9E86C917E8208A39A47B0C35B86A84F6767ADE46E4A5F9B9847CF5168C74597
SHA-512:	921096DDB4C041AA7CEF18C69892863C90573A51D997C3E904429EE65ADFC507758782E8D8225A960CA6746E8280EB5C3F360C4C180291B4698712E92ECB965F
Malicious:	false
Reputation:	low
Preview:	.y.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....)8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\65bb24e1-cc2d-48e0-970b-c0737e14ba9f.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):	162688
Entropy (8bit):	6.083082841246901
Encrypted:	false
SSDEEP:	3072:ucA2NNCxQM9b0q+szv+tnMITFcbXafIB0u1GOJmA3iuRz:prExQM9b7fD+ZMWaqfIlUOoSiuRz
MD5:	F3E8EC06EC687399A4E3A9C1F3B28FCF
SHA1:	AB27113CD4007E593C8550D5D47D7F6A115E85DB
SHA-256:	27F5BF5BC66061A249F6C630205F1B8216656466EEC1ADB9FA62A08A9DC5D3EA
SHA-512:	64F2395F512EB67A23B2DA7F410C69F238112CC5DE25E4D626ABC1AA28308967EE586C9F333E1791B5AEF75699849A2ACFCFED7444F455956F73BEDBF66C932
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.606041508188736e+12,"network":1.60600911e+12,"ticks":96184659.0,"uncertainty":4476785.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016435097"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\6c027c38-049b-4804-b0bb-fc977bfc729e.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):	162439
Entropy (8bit):	6.082656117753312
Encrypted:	false
SSDEEP:	3072:TyIA2NNCxQM9b0q+szv+tnMITFcbXafIB0u1GOJmA3iuRz:eIrExQM9b7fD+ZMWaqfIlUOoSiuRz
MD5:	5A8936240ECC9E6E74149422F4F08D67
SHA1:	B98E1B07DEB7A3AB71A11B3F9FAD1DB1B18BA1F8
SHA-256:	B65E60FE167F44FFE8804131C811070CB17BBFC63B1BED7B4E5654B633FA9558
SHA-512:	873D98CBC9D1DB771BE569774C0B07537D693E5564A237E3696E74542905905F41B5D26DB9B0B8852113449F2A8193A295486E2C894FB805B83F0F6F02EF8024
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.606041508188736e+12,"network":1.60600911e+12,"ticks":96184659.0,"uncertainty":4476785.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displa

C:\Users\user\AppData\Local\Google\Chrome\User Data\812055ff-9ef4-4501-a0c6-a277c138257f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	96024
Entropy (8bit):	3.751875188879844
Encrypted:	false
SSDEEP:	384:dLn0EGpj1pNWQVhTQzNcrtvYk3nkSzHuzGj2rhWki1xHqi6FrxMmFSlmUQ4DOGaj:SualpamHHUe/bEIyUHPeAKWIQHW
MD5:	88E364A9998E5DED10111D4CEAA7CF96

C:\Users\user\AppData\Local\Google\Chrome\User Data\812055ff-9ef4-4501-a0c6-a277c138257f.tmp	
SHA1:	8E0D6CF286E091B19F91EACD82394AD25CFFC8F6
SHA-256:	66505B9A502B10B5A434D77C7947F5F0C6F223B87A6BD5F7BE16A79D1D0E4B40
SHA-512:	55D4C7FFAB0FC73B6A0F09E1D36D606ECF0BE3B6995DCF1A478ED937704DA737E72D6FA04C3F22DADD30E46AF5431383FC3A6F67CA56C6AD4616A98C8951AB5
Malicious:	false
Reputation:	low
Preview:	.w.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e .1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0 .0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....)8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\94b5e64a-71ff-4a08-bfe9-42eaae41a9fa.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):	162439
Entropy (8bit):	6.082653989695999
Encrypted:	false
SSDEEP:	3072:TDLA2NNCxQM9b0q+szv+tnMITFcbXafIB0u1GOJmA3iuRz:XLrExQM9b7fD+ZMWaqfIlUOoSiuRz
MD5:	C0D6A26F1479252C15B939068519BE1E
SHA1:	C08B5574CE9A7DD49640A421E0F030A7AF1F1EF8
SHA-256:	5DDDA1B72F169E12EAA6632911A7CC4896857A5A8E6227F0701E7D8B2F28CE1C
SHA-512:	3978AFA3391DA520BF6F8980B568CA566825DE2D133F1EC86EF7D089D2F1D8303EF2B8F7A6398B83CFCFC36BCFAB201DC17B01849D709788942FD939158545B
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.606041508188736e+12,"network":1.60600911e+12,"ticks":96184659.0,"uncertainty":4476785.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"displa

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):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftIE1G1mkftIE1G1mkftIE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Reputation:	low
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\055d6493-c82c-4766-9165-85e6491c28f9.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):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\055d6493-c82c-4766-9165-85e6491c28f9.tmp

Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\243c03ac-c6ca-4932-92bd-af60f5778949.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):	9818
Entropy (8bit):	4.875781157898667
Encrypted:	false
SSDEEP:	192:JOz6Gl1STF3DmZ9xe6reoP80bBFXMauZyA6EqySzIjs56/q6QQ3GtuAk+uJXC0EO:JOOGl1STF3DA9xe6reoP80bBFXMauZyw
MD5:	51804D658EBE5C4C4E677C8F8347182A
SHA1:	F361FB74E7A3D4063B281F878CEF2C3D2EFC385E
SHA-256:	06A74D214A6B821F7F527590D1EB02C02F4F775D41718980B958280089073F23
SHA-512:	70885660CD47F78053FEC08C4F4FAE5E03470038DF604A09B5E85C2A045D219A26E1E666F06700B4CAFC0634C9B24BFF65F6F0CFBA1C99629799C531EF522C78
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13253107109856579","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13253107109861610","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13253107109995697","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"expiration":"13253107109995701","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://r3---sn-4g5e6ns6.gvt1.com"},{"alternative_service":[{"advertised_versions":[50],"expiration":"13253107111429045","port":443,"protocol_str":"quic"}],"isolation":[],"server":"h

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2f56b7ea-4127-4685-aaa6-1250c86e93ed.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):	5755
Entropy (8bit):	5.1915899244804065
Encrypted:	false
SSDEEP:	96:nPSCJ44498qcV1ok0JCKL8tk418bOTcBVuwn:naw4xcG4Kgk4+n
MD5:	0917E67E11746D5A6AB136B420D2670A
SHA1:	999ACF29F9BD1F837352A349AC13EE60A191FE84
SHA-256:	9EA93598EAF739A3F9889AB0F5C491A92C9FBB1C787A759000190E0FF42845C4
SHA-512:	D3FBF16DDD431A5BE7D4CDD82B59864806993F4A66EAD827C8F3125DD5C694779C28B6E8037AFC32F6F0237F7B54DEC4D1EB6D57CBB326DE294C521D4319B EB
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13250515105624505","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\40319df7-5582-4b7c-8a2c-ebb21ef43479.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):	3462
Entropy (8bit):	5.6018389428446715
Encrypted:	false
SSDEEP:	96:1Mm2t/DeU2hieUEIUUeUzUoKUjcU1PeU1UUUEDdUEUAUD:1Mm2t/DeU2PUhUUeUzUoKUIU1WU1UUU5
MD5:	039F545FF33915F44F60D91BAB1EAB96
SHA1:	9ACE9AC6108DF1727DB14D706D886479CD893869
SHA-256:	4CE96A35BAAFF78DDDC3702DA1172B89C9B286766A3E8AA698022E1582E4160B
SHA-512:	F7226DA3217F70BB8FA0F78DFEA18DF9618E051B9CC828BB5B65DA010DFD32B20514DA4B7FCA89F487C1194403EA241B9D030B0BC22403C0B5F6A01BE27D19 8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\40319df7-5582-4b7c-8a2c-ebb21ef43479.tmp	
Preview:	{"expect_ct":[{"expect_ct_enforce":false,"expect_ct_expiry":1606646325.829882,"expect_ct_observed":1606041525.829882,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"MPw27WOO+zLwe1Gt06rSTpq4knWTDVfyKYc2mMHjUI8=","nik":[]},{"expect_ct_enforce":false,"expect_ct_expiry":1606646325.145557,"expect_ct_observed":1606041525.145557,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"Q2i8+5A3kREMoy37yPuUYKheqKsz3RQ2ENTog6mvPhc=","nik":[]},{"expect_ct_enforce":false,"expect_ct_expiry":1606646328.331666,"expect_ct_observed":1606041528.331666,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"SD/DkwsaWpqZqwVjO/rZ7aGScgQDfnTjSxuO8GEWU4w=","nik":[]},{"expect_ct_enforce":false,"expect_ct_expiry":1606646328.756928,"expect_ct_observed":1606041528.756928,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"Ulvztr58M3pa+KJMUamSWOmzTOculSFDNoO1yR

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\50c3e4ae-31fa-4f58-b3b6-274f149944fc.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):	5741
Entropy (8bit):	5.190733118998846
Encrypted:	false
SSDEEP:	96:nPSC044498qcV4ok0JCKL8tk418bOTcBVuwn:nah4xcB4Kgk4+n
MD5:	59679D16AE9EF1CEFEC511EB2453A58C
SHA1:	C1E9A9CA148170EAB5B04164E9EDB23BB52D8F56
SHA-256:	AB6A8D7D1F3614BD0BC36F21096212F577D1871E28400164ADA01432B4EF311A
SHA-512:	E7DC18698B1C7247EBC07147A9E8E75CBA123C7263E238E96F6939DEE02912CBFDAE470F47A60A213A5C6B0CDED7CADD4942A7988D4BFAB1FE9B74F99051F8 12
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13250515105624505","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"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","7355378"],"daily_received_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",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5d5e55a2-21e5-409b-9fc2-f431e7c3bf28.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):	5788
Entropy (8bit):	5.192746026960981
Encrypted:	false
SSDEEP:	96:nPS8JTg4498qcVsok0JCKL8tk418bOTcFVuwn:nacZ4xcp4Kgk4+z
MD5:	DC3C7B18BD18E6D38A5644987DF2280D
SHA1:	592FAE7BEBA30C084A37C0A4736351F45ABBBA7A
SHA-256:	E0A526C394C7B892279B58A23C4A3E36FE5EEC31DC48F044DA7D72CF1E119511
SHA-512:	6989630F45C99B93695EAEC90BE70132A3E2A1BC2E73B4E4DDB6F5D4DF50997039883BD6395DA368787AC194C449125323E82864C2C8F39A2AC6E5C9A4FE897
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13250515105624505","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"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","7355378"],"daily_received_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",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8c37d21e-0bf3-4b97-ac47-24277fe0db05.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):	3627
Entropy (8bit):	5.601473209463281
Encrypted:	false
SSDEEP:	96:JEtG/23/MGeUfieUGUURUCUoKUecU+PeU1UMeUXUEDdUr6UjkUi:JEu23/heURUGUURUCUoKUPU+WU1UMeUd
MD5:	7046DA8DA9E68406B8A291B495B379DF
SHA1:	91E83894142B2F1EF29D9BDBD9494734D10E8866
SHA-256:	01CAD0CFBE2D150AD4F8DF04FB32F908FFD09179AFF87B0223540A04020428EA
SHA-512:	6C438F285899C0FB61EE3C59527FFF2A96E6EE9EBD1C23D8A0A426109A57ECF5B8FC626C77DF96F01F98ACCDE36E741FE7210338A761F8A5E0597E3F76C8ED0 C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8c37d21e-0bf3-4b97-ac47-24277fe0db05.tmp

Preview:	{"expect_ct":[{"expect_ct_enforce":false,"expect_ct_expiry":1606646360.656083,"expect_ct_observed":1606041560.656083,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"MPw27WOO+zLwe1Gt06rSTpq4knWTDVfyKYc2mMHjUI8=","nik":[]},{"expect_ct_enforce":false,"expect_ct_expiry":1606646359.678883,"expect_ct_observed":1606041559.678883,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"Q2i8+5A3kREMoy37yPuUYKheqKsz3RQ2ENTog6mvPhc=","nik":[]},{"expect_ct_enforce":false,"expect_ct_expiry":1606646358.38642,"expect_ct_observed":1606041558.38642,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"SD/DkwsaWpqZqwVjO/rZ7aGScgQDfnTjSxuO8GEWU4w=","nik":[]},{"expect_ct_enforce":false,"expect_ct_expiry":1606646358.624254,"expect_ct_observed":1606041558.624254,"expect_ct_report_uri":"https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct","host":"Ulvztr58M3pa+KJMUamSWOmzTOculSFDNoO1yRLd

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8eb4a114-5270-4adf-b986-79b6f90c77df.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):	5082
Entropy (8bit):	4.973397988718611
Encrypted:	false
SSDEEP:	96:nPSc0RX4pcViMok0JCKL8tk418bOTQVuwn:naz4pcsb4Kgk44
MD5:	1BCE046A2337BBE398A508947DE537BA
SHA1:	C1D716230EF2EE21E754908F6633ED703665514D
SHA-256:	8CEADC003E60C63822A09AC1D31ED50276E7C1FE371E9831C62BD10EB3F8A77C
SHA-512:	6D1FB60E33FB53E00C3B76363E998CB3837E775E2C86954045AB60FD250C3122F265E05A0C74CA2DCCF4C6C98F84B3549F28E23EFF284A677D5A70FFAC3E107
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13250515105624505","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"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","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\93570e10-8aa8-4e68-9959-8d2eeea7452d.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):	22614
Entropy (8bit):	5.534924764567065
Encrypted:	false
SSDEEP:	384:qmDtCLl3DX+1kXqKf/pUZNCgVLH2HfD3rUIFHG5WnT9cox54V:ELl7+1kXqKf/pUZNCgVLH2Hf7rUIZG5D
MD5:	B9DF0186E9CFCADF794C4EF4EE4A943A
SHA1:	40FE6EBE9F721D576112D2A1806473F5CC1B0BCF
SHA-256:	0CE0E52D7D82AEDFF2CA0A6D4AA77432585DC07519B5D7B25518B7DD6BCCF68A
SHA-512:	558842BFC69A9C02C7381920D474802A66EBF3B0CA8059A9A8668B958236FD16B3A61EDED047E8852E019208ECA2926873BEF59395164C54AB2A1895F046C726
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":"13250515105396553","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\945099d8-59c0-4ae2-8cd4-f8a4c1a39f54.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):	5755
Entropy (8bit):	5.191560518833459
Encrypted:	false
SSDEEP:	96:nPSCJ44498qcVbok0JCKL8tk418bOTcfVuwn:naw4xck4Kgk4+R
MD5:	AFF38AFFDCC1515FE54775753CF1D42B
SHA1:	EFAA32D98E003D463EB7665F113C8AAEA35D7F4F
SHA-256:	A0C928ABCAF706E71AF66EBB5D716CA0365E38809AAEEC13518DC1E34506632A
SHA-512:	EF2290470F4D9BD9CA7789E2DCA29E536A6EE460B8E4EA0978C2728E2ABAD64B7B7B9BA161E8762ED53BA0F4101E2C148EC3CB8C08E3E52534581BCE1BF7BDBD
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\945099d8-59c0-4ae2-8cd4-f8a4c1a39f54.tmp	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13250515105624505","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"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","7355378"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.20804781630087
Encrypted:	false
SSDEEP:	6:+VF31L+q2PWXp+N23iKKdK9RXXTZIFUtwDFvM1ZmwyDFBlLVkwOWXp+N23iKKdKT:IjL+va5Kk7XT2FUtwZvy/yZBlLV5f5KU
MD5:	C571D4B03DF01A07FBF3C2E3F848590B
SHA1:	9ABA067F871B8D0AE309A12B58E6D933A8F5C706
SHA-256:	CC6560A263DC32A926E77632EC753E29505C2F2CEA81F54FA014BEFC23C6218C
SHA-512:	49EAAABF5A3186B8E421FC40CB15C748D23FCE7AAF8E0C9C8D4FF2D04263779399AC2E437DFE5FC9EB144DA789E2C641C206DD6E6A86A151509A7AEFDF7C9E89
Malicious:	false
Reputation:	low
Preview:	2020/11/22-02:38:43.199 17c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2020/11/22-02:38:43.200 17c Recovering log #3.2020/11/22-02:38:43.201 17c 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):	315
Entropy (8bit):	5.230641730480684
Encrypted:	false
SSDEEP:	6:+I1L+q2PWXp+N23iKKdKyDZIFUtwDz1ZmwyDpLVkwOWXp+N23iKKdKyJLJ:3L+va5Kk02FUtwN/yVLV5f5KkWJ
MD5:	E3110A95B99D79878BBE7F92B1824B44
SHA1:	48C7C09D406CE22D0B49A7DCD3A4720330809019
SHA-256:	EEFB817993838B5CE8A2158F5B953B339E8664118D3CA3A86881555137CBDF1F
SHA-512:	0C5F747AACE050A990136194D9602DBEB69ADAA963E5E5205BC3A1B859C2683C721306B234733B7BC250D6D11ADD6BFAD22E519BAF298C593E3419FFFE33A39A
Malicious:	false
Reputation:	low
Preview:	2020/11/22-02:38:43.189 17c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2020/11/22-02:38:43.191 17c Recovering log #3.2020/11/22-02:38:43.195 17c 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\000c0213cc64d062_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	181552
Entropy (8bit):	5.971807472730395
Encrypted:	false
SSDEEP:	3072:V4BMKm1uRbspYtL1Jt0vjqUWp69UihH72gKxUaekuDE:cTqvjqX66AsEI
MD5:	C5FE19C45B7035389923FDCF2AFA6B30
SHA1:	C4ACC4CBB8332D0B3750EE8BE7AD57438A8748F6
SHA-256:	9867674E99C4FD5416BE32520FF7A2C1E8188F4E7C257850599261C1FEAD44D8
SHA-512:	B0210AD4CD16F88957DB017C1BF3CE66C6809E9329BA573DD5BD5311582F981311971B395332B0FE40829BF7D0CDB60C30B9D5C45D70BAB2B658448B749B637
Malicious:	false
Reputation:	low
Preview:	0\r..m......@.....] ....20368C0857BC31A03E52E35B4D985E846731652D0AAC06BB709B9501D4CD90C0.............'.&.....O7.......E+..................2.. ....H...................#.............\...(S.<..`2.....L`.....(S....2.`je.....!.L`.........Rc................ ...QbN_>O....aa....Qb.......ba....Qbv.......da....Qb..h....ea....Qb^(......q.....Qb........fa....Qb.^......r.....Qb...e....ha....QbRR.....y.....Qbz.......ja....Qb.O.w....ka....Qb.A@.....pa.. ..Qb.......qa....Qb.......ra....Qbb.......sa....QbV.3.....ta....Qb.."u....ua....QbJNb.....A.....Qb.;.....va....Qb......za....QbJ..0....ya....Qb.......xa....Qb.0z.....Aa....Qb..O.....Da....Qbv.......Ea....Qb.^<9....Fa....Qbj..E....Ga....Qb..u....Ha....Qb.R?.....Ia....Qbz.......Ja....Qb.(......Ka....Qb6.......La....Qb.<q?....Ma....Qb:......Na....Qbj.?.....Oa....Qb.c......Pa....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\016ee97b796b7b8c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2428
Entropy (8bit):	5.739326111497214
Encrypted:	false
SSDEEP:	48:JZfttINpi/Y/F0hCU9oSj0Hqd41ord+9Hjyx1REEl+XziwPf:htINj/F0hZ9VgHEqjEl+XWk
MD5:	C9ACCC656A2A43C61E22A4EE54C02743
SHA1:	1D4FCE499007AA5849D79FBAFF251EB33180308E
SHA-256:	D21D14D0E130F607BDE6D9C28B95B049ACC0E6A5C0DEA2FBED9E83DCFC8595EA
SHA-512:	208BC7087C48A5F25D2A558B541A47900A868A002B8EA92C651FA37E212990CE5A6890A5F78C3923F273F9999A76CEEF458B8052428B4D646821BA9E3EBDC20A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....\...*....._keyhttps://www.coreldraw.com/static/common/scripts/css-phone-res.js .https://coreldraw.com/....E./.....~.X._..G|K.u.....7b..`e..P...A..Eo.....I?.. .....A..Eo.....E./.X.....'.....O.....p4.....(S.p..`....$L`.....(S.D.`>.....L`.....@Rc.....QeF..T....css_phoneInfo.....Qd^.2.....r eplaceTokenb.....I`....Da....'...(S.....IaD.....@.-....LP.!.....@...https://www.coreldraw.com/static/common/scripts/css-phone-res.jsa.....D`....D`N...D`.....`....&. ..&....&.(S.....5.a.....Q.Pz..q....cssPhoneInfo..Pc.....insert.aL...%...I....d.....&....&.(S.....Ia.....IE.d.....`....DI]d.....a...Qc...I....insert.....a>.... .....Qc.....en-US.....a.....Qd.....phonenumber...Qe...m....1-877-582-6735....Qc...W....hours....<Qm.}I.-...Mon-Fri: 9am-10pm EST Sat-Sun: 9am-6pm EST.....Qc 6.....en-CA..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\019ce20e3b1e34ef_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16045
Entropy (8bit):	5.980797417010146
Encrypted:	false
SSDEEP:	384:6rcywxsVqdq0QNzRlWtzLPYBGeN5JUBaCVU8:5d+w+NFlktm5ru
MD5:	FB5EAC83C050E176082EE345E50C81A8
SHA1:	C45A6C0487C71CF94D8057C7674747F4D912774A
SHA-256:	8DF6A96C293A48EE65E8EFC37227179334D80DD86F12ACC8134F032D5D90DE54
SHA-512:	D6C3AE2F263E1A49D0E446A0D91C6F71ABAAB099BB051EAAE184E60A3C01A18CED56D525506E20EE9FB4B02C9121BF6D813090A47919BE7282B11BECDD1129 38
Malicious:	false
Reputation:	low
Preview:	0\r..m.....u...?..n...._keyhttps://pagead2.googlesyndication.com/bg/7ACX1ll8pxmp-W5IFnwplmFbwq_vDvpxp5bFF4q7ftk.js .https://doubleclick.net/..].E./..... :..H.x...v...r...D..w[P..'Q..A..Eo.....!.....A..Eo.....'..6....O.....=..6.....D...@5.....(S.<..`2.....L`.....(S...`.....8L`.....\Rc*.....Qb...m ....Q.....Qb.....r.....Qbzv.....K.....f.....I`....Da.....m....Qb"M^.....self.(S...`.....4L`.....Qd^.M.....trustedTypes..Qd.N.....createPolicy..Qb&.....bg...$..a..... .Qd.....createHTML..C..Qd.(.D....createScriptC..QeV.=.....createScriptURL.C.....Q..... Rc.....Qb~.....O...`.....Qc.....console...Qcn$.....error....m...Kd .....E. ..9.....D.Q.(.....&...&.(...&...(.....%..'..(...&...&.}..)&.../...../...../...Z.....&..>&....&...%.....&.(....#....&.(..&.(...&...&.(...&.Y.....%...,Rc.....`.....aN.....e.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\02da4a26b7e48bf2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	801
Entropy (8bit):	5.919218079118529
Encrypted:	false
SSDEEP:	12:G2E3HypInxux2pHgyyyJ3CMxok04pAhiyt3EIdv5KEPCSVA3hCRUlFrC:dEipIxuyAyyASb9hdt3EyrP58CWU
MD5:	E50D1FE0F6AAEA265914A8C2B635F3C6
SHA1:	79C444FD6EB5F43F1D951740042A1EEED6230751
SHA-256:	1DD914C764241964DF9EB28BCB6D9CE5B081300FB4D29AEC7A87B8849DF95D6F
SHA-512:	374D0359E3CC663F15B32EC88FC30187C434306A64571AB99D68C8ADBCB097EF0B972F46234D05EF304102B7C79BD33B584E0E2314932D51ED916313F44AC269
Malicious:	false
Reputation:	low
Preview:	0\r..m.....,....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/956202557/?random=1606041553651&cv=9&fst=1606041553651&nu m=1&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-480&u_java=false&u_nplug=1&u_nmime=2& gtm=2wgb41&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fwww.coreldraw.com%2Fbr%2Fproduct%2Fcoreldraw%2F%3Ftopnav%3Dfalse%26trial%3Dbig%26s ourceid%3Dcdgs2020-xx-ppc_ron%26x-vehicle%3Dppc_ron%26gclid%3DEAIaIQobChMIisv7lIKV7QIVAZd3Ch3Nxwv2EAEYASAAEgI0ovD_BwE&tiba=Softwar e%20de%20design%20gr%C3%A1fico%20%E2%80%93%20CorelDRAW%20Graphics%20Suite%202020&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://coreldraw.com/....E./.....+.....s..''Z..bo..F.....H5B[<..8..A..Eo.....+.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\052494325eac1892_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\052494325eac1892_0	
Size (bytes):	264
Entropy (8bit):	5.642114977693371
Encrypted:	false
SSDEEP:	6:mVXYw1yGSVOlAsc8SD4QD4xTe51yGIg+ktpbuw+aGom45sol/lhK6t:g1yGSvmwPcTK1yGImE/oml4/N
MD5:	17505DC88461FA36A83623368B0BA073
SHA1:	3EC0DF1EB3106DC9B58700374BF15313DC3DC93B
SHA-256:	2981AE712EFCB5EC5CBE873BFA315E201C1013E8827CC68B47E5054EE12C24FE
SHA-512:	FE020262C05B3AE427946B46540CF989F66A590AD67DF00907D57DA589D0730C6F20BB458417B19A73B65DECD2B3D3DC7849E30B04F053BC6CAD53C342682D6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....(/....._keyhttps://otampadabola2.com/wp-content/plugins/q2w3-fixed-widget/js/q2w3-fixed-widget.min.js?ver=5.1.9 .https://otampadabola2.com/..B.E./..... .....-.q,... ...D.#..^h....D\}z...A..Eo.....p.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0710eb439444cf98_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	316600
Entropy (8bit):	6.073817156845698
Encrypted:	false
SSDEEP:	3072:4lFYWre84xyDZvmo484AIE/f08MlDUWeETk9xYd86NvKJSFAeqH3dSpBjUHAYh0R:y/A1On1QDULC86Nvceug2XZ6
MD5:	94BD502C9EAD4D9AAE719ED634C154AC
SHA1:	8C428CB84FDD40E6A0473131319ECCB89C1B9CFA
SHA-256:	5B6ED9AA249E57C747FC7235DC6074C995C954799FDEE8545475DC82FDF53228
SHA-512:	614136120964D702E801F8961F231F6D19EDF663AC72E81DE3C6589BFEF231CBB8FD05E6B1629B1529BB81A63F5193091A9A73FD32CD33D7D4A74301D03C7FD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....Vo....1C092C672D4F7D73670CE450F03197467DBDA211B5B33A350BE79B09F83935E9.....'.1W....O`...h.....As.....(...8.....x...x..... .....P.....8.....0..... .....D.....|.....(S.e...`.....L`~....(S...`.....LL`"....@Rc.....Qb..M[....e.....Qb.....t.....Qb.xY.....n...b$.....I`....Da.... ....(S...`.... ..L`.....Q.@>.....exports..$..a.....S.C..Qbv\(.....I...H.....a.....Qb.....call.....K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&.(...&...& .'..W.....-...(.....,Rc.....1.`....Da@...8.....e..... P.....@....@.-....HP.....9...https://script

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0bf3f108a330cf82_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.9260540023942445
Encrypted:	false
SSDEEP:	6:mOVYoDaZC1HEHlrDX+tJuKvX1yGCogSSaQBI4RK6trnlI0ccIGIIaQBI4sp//:P2ZCRLw1yGBxSaUd9ztISaUe
MD5:	3EBB9936BA1352AA378FA7437A49F922
SHA1:	F7CBA1D0595337D0B0107C109C4DBEDA06CFDE5C
SHA-256:	16C99AE9F33FC191F50C734F13472A9CD8661CBC85BC49F19D9F4290C4001C5A
SHA-512:	CBCC26FB4FA9C8C95BBD4BF67E1D56A46639EE65116D6AE258CD40A6E119D640A4C0D6272D369644EE2B4F1038D64CFA62EFC09E1841852D25D0FBC140B790 F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....^....._keyhttps://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js .https://otampadabola2.com/RWD.E./.....I...V6|O..M.....B..N....d.R.A..E o.....A..Eo.....RWD.E./.....20368C0857BC31A03E52E35B4D985E846731652D0AAC06BB709B9501D4CD90C0I...V6|O..M.....B..N....d.R.A..Eo.... ....J.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\132381413a5fb179_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5383
Entropy (8bit):	5.736145792418599
Encrypted:	false
SSDEEP:	96:GcpR0x3zWHYmqZjtkzhtlSU8EJ3RbheVD3kSS7A2SeAu+ACafgcvMJND2vvCTDfF:BRPy+VtYUz/leV7V92N7CwlaSh3gtw5i
MD5:	FFB6252066735F6946AAEDD42D3BB887
SHA1:	9206DE43EA29E48F472E44B56EE48EBC8B84E56D
SHA-256:	5308639FE485D80FF2174356A56AD183F4A1C6BFEE99EF3C10A74FE9CFAC37C8
SHA-512:	B46DA9551368DFEB2BB6C396E667019AD1AFB6FFAB410F416991827A6690AB33E8130C1C4A5FEDE0C0BB86835D201A4E1CC369BA59038E836D3BE96DFEC0AF 96

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\132381413a5fb179_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://www.coreldraw.com/static/common/scripts/dynamic-pricing/jquery.format-currency.corel.min.js .https://coreldraw.com/....E./.....k. \!~A.7\..m....,a.X.*..fg..r..A..Eo.....A..Eo.....'.....O....`...+..]..(S.8..`&.....L`.....(S....`.....9.L`.....Qe.\M.....formatCurrency....Qc 2.....regions..<..a.....U.bb.!v....K.....Qe..e.....positiveFormat....Qc.|".....%n %s.....Qe. k:....negativeFormat....QcRq.....-%n %s....Qe...l....decimalSymbol.....r....Qe..6.... digitGroupSymbol..Qb..W[.....Qd...H....groupDigits.G..Qc...x....cs-CZ....<.a.....Qb..A.....DKK...Q...Qc.0.....%s %n.....Qcz.....%s -%n.....A.....G..Qc...K....da-DK....<..a.....U.bF.!+..... ....Q.....r....A.....G..Qcb..&....de-DE....<..a.....Qb.s.....CHF...Q.....Qc6."....%s-%n.....A...Qb...>....'....G..Qc..l.....de-LI.... <.a.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\15e074aa4106d329_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1341
Entropy (8bit):	5.601877062659932
Encrypted:	false
SSDEEP:	24:GEGYjAngQPtDNKUunw1jIXSvZUyG4SHpNC4N8pirTlEX:8AKgOKUuwJIXyZGHLApirTG
MD5:	A6117D17418783B53E8E6F72B2CAFBB6
SHA1:	ACD674E1DC340D3F7B4F5169D50C7A48E130951A
SHA-256:	16B339901D1D7F60C332BE13EFC48013816E0B7C8060BD7D58351EE58494C108
SHA-512:	27A2B7A3FB3657BCB3E4683295A6DF20FBD1667A5EE67187702AEE92803DBFD359A640AAEF7768CB6279FBDE808702A89122E27B8794EF29FB7DD74479729407
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]...c.`....._keyhttps://www.coreldraw.com/static/common/scripts/x-clickref.min.js .https://coreldraw.com/.O..E./.....U...Y.}"...i.Uk)..../.u.R....(8..A..Eo.....>.. ~.....A..Eo.....O..E./.....'.W.....O.....s.....(S.H..`J.....L`.....,L`.....Qd.....constants....(S.....Ia..... QfV..L....setXClickRefCookie..E.@.- ....PP.1.....A...https://www.coreldraw.com/static/common/scripts/x-clickref.min.js...a.....D`....D`....D`.....$...`....&...&..A.&.(S...Ia..... Qf^..a....getXClickRefCookie..E....d .....&.(S...Ia.....(Qh.\|.....getXClickRefQueryStringParamE.d....%.....&.(S.....Ia....V.....d..... .... Qf~..B....updateXClickRefLinksE.d.....D&. (S...Ia`...U...IE.d.....`....DI]d.....`.....q.`.....`.....Q.`.....,..a.....$Qg.....xClickrefQueryStringName..Qd.2.....x-clickref... Qf.8....xClickRefCookieName

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\160a04ebd7990d80_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	243
Entropy (8bit):	5.631059934341791
Encrypted:	false
SSDEEP:	6:maPYGLKdfwM9OcoSY4jGtgCsEmYrFZwfIPjWGK6t:viylZ4qtiEmYrPP9
MD5:	F2DAA71C8C5E8E6AB9E44B3D3AA52BDB
SHA1:	E286235E8708DBD61815A48E43F6A30A1DFB55C2
SHA-256:	48FC1242DF6FB18FFDBB2F5645525CCB18AD57DCFCA309280D905E62790ACAE4
SHA-512:	5F9BCC8F21D826F1AA7E5008E00C1ED21F21616A11537CED0165AB0BEB43061AE398218D4C9B7B5DB59AF73906E7C12E41A2B55F76136A09945CC6622BF85D5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o...s....._keyhttps://www.gstatic.com/mysidia/dec8cae5017b94534ad9e9d42636c5f6.js?tag=text/ryuk .https://doubleclick.net/G.R.E./.....BZ.B= l&...3g.._0..=!.'llm..F<..A..Eo.....5..=.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1ffb2099678dcd07_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	24122
Entropy (8bit):	5.986284712633992
Encrypted:	false
SSDEEP:	384:JC1NndJi6uyiWfX1/8N/VO9r+9VtNpwntsN2iVwpDaZPnys:+YlW/18dVO9snpwnt8tVwA1L
MD5:	09A2BC4916BE7EA602F7534BE2E107D1
SHA1:	1793986B641A9FB2BC39E1E637B4B680C6337A90
SHA-256:	66061D3DB974A5857F908061BDADBDF27C784CCC02B105655544E77113F49341
SHA-512:	9E4B8587F475AB668E5E71073B5A90509A67DF7A73807341FDCACA75BBAA14321083B68C86C8FA213623B3FCDA01FA61E1CFB337995DE9D791923E3E71DE46FC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Y...._keyhttps://tpc.googlesyndication.com/pagead/js/r20201112/r20110914/client/qs_click_protection_fy2019.js .https://doubleclick.net/..S.E./..... ...N..wz.<.$h....)X.c.....{\|.A..Eo.....:.6x.....A..Eo.....N..wz.<.$h....)X.c.....{|.A..Eo.....3.....S.E./.....N..wz.<.$h....)X.c..... {|.A..Eo.....b+.....'.l4....O.....[...t.....4.....(S.<..`2....L`.....(S...`.....L`J....u.Rc6.....Qb..;V....h.....QbB.....aa....Qbf.....ba....Qb.... ....fa....Qb.....n.....Qb6V.....q.....Qb...P....t.....Qb.....ia....Qb.....r....R....Qb2nj.....ja....Qb*..6....y.....Qbf.....A.....Qb~t.....B.....Qb..|m....C.....Qb.....D.....Qb.....k a....Qb>..1....la....Qb..b.....F.....Qb.B.....ma....Qb.Eb.....na....Qb..%C....oa....Qb.y.E....pa....QbF.....qa....Qb.D.%....ra....Qb..Yc....sa....Qb"=.....G..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\20d600d5c3cfa464_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	14490
Entropy (8bit):	6.0086668057504165
Encrypted:	false
SSDEEP:	384:kVjWMjYVlDi9cFBSAB4pUz11KtZ5EHwwUSS:sjWXU9cF22JaJxX
MD5:	F921B995DE19B959F42B608DDD6ED61A
SHA1:	0B8FFF1534FB1593F2453CAC368DCDC74223DAEE
SHA-256:	659F88979A74FB9902A9CA214020AC55E8CA9BEDF9F090D030159284E51228AC
SHA-512:	4ACB0FC7AA5BABBF38B48129AE5D7FC38C26B0819AC449959ECC901830B36F8B988847308F4A566CCE59B85CF480A2D1CA2EABBEE4F7B84719F27941FBF66E15
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r.....Q^...._keyhttps://www.coreldraw.com/static/common/scripts/dynamic-pricing/dynamic-pricing.min.js .https://coreldraw.com/Uf..E./.....|y..rtFY%.c.$.R.....m.y.`.....A..Eo.....[.....A..Eo.....'..X....O.....6..?..P.....L.....(S....`.....4L`.....L`.....Q.@b*.....jQuery....QdjS.....noConflict....(S....`.....L`v.....Rc.....<.....Qbb..T....L.....Qb.....f.....QbJ..p....H.....Qb.C.z....B.....Qb".....z.....Qb^.....S.....Qb.K.~....T.....Qb.'.....V.....Qb.K.....M.....Qb..!.....N.....Qb6.h....O.....Qb..1.....P.....Qb:..A....C.....Qb.....t.....Qb...6....I.....Qb.e.....p.....Qb.;.....E.....Qb.Q.....K.....Qbf.....J.....Qb..PC....v.....Qb..f(....R.....QbJ..`....Q.....Qb..O]....F.....Qb.-`.....D.....Qb..47....x.....Qbr..R....X.....Qbb..E....U.....Qb.F&....G.....Qb..~.....h...}$.....$.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2195b3c8c040aad7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	801
Entropy (8bit):	5.9034074558245155
Encrypted:	false
SSDEEP:	12:5E3HypocQdnNcQqUPux2pHgyyyJ3CMxok04pAhiyt3EIdv5KEPCSVA3hCRUNXk7l:5EipeyUPuyAyyASb9hdt3EyrP58CZb
MD5:	5C780E90C4C80A19F90C0248803557A0
SHA1:	5FCC47FF1F049EA3D9A6C0461CC74A51B167ECA8
SHA-256:	B00886E33D342B4E82EEA3CA76DE0018ED32830401259ACFC60A8A9F6555FCC8
SHA-512:	D8429FF5F3BE23F9F7FB94E49457D64767013B78EB3210D122978F258065245EC9108EC5341D37083F5523A6AEBAA8E1BE7900F8D198186DCB93FFA013DD326A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X.`....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/956202557/?random=1606041547865&cv=9&fst=1606041547865&num=1&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-480&u_java=false&u_nplug=1&u_nmime=2&gtm=2wgb41&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fwww.coreldraw.com%2Fbr%2Fproduct%2Fcoreldraw%2F%3Ftopnav%3Dfalse%26trial%3Dbig%26sourceid%3Dcdgs2020-xx-ppc_ron%26x-vehicle%3Dppc_ron%26gclid%3DEAIaIQobChMIisv7IIKV7QIVAZd3Ch3Nxwv2EAEYASAAEgI0ovD_BwE&tiba=Software%20de%20design%20gr%C3%A1fico%20%E2%80%93%20CorelDRAW%20Graphics%20Suite%202020&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4.https://coreldraw.com/o.|.E./.....u.....i#-.6.Hs.[E...0...../B]....A..Eo.....7.H.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\22872dcab88d27a0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	279
Entropy (8bit):	5.671975556781316
Encrypted:	false
SSDEEP:	6:m4YoDaZC1HEHIrDXtGcNnU3DDz1yGCXuglKdPEm2wc+3///hK6t:h2ZCRwcRU33z1yGhIKdPEmcw//7
MD5:	73B4BA687262E7B11AF8FD466BD909B4
SHA1:	14B7ABAC2628D0BDC21CE131D2A393F16C0CE28E
SHA-256:	DF491DEDAE16C377E895C9EB7C1E6E0E5C7FD79A9C277FE5A47FF25DA1B32E62
SHA-512:	5CD49115EA93E0916C7DA12CF09106CA82059DCACE3B81F62993810A4863977F39E53C3A28083C04EBE0067B98AF6FCD986BA4B08CC7E67D0B45E37ABF3285C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z~. ...._keyhttps://pagead2.googlesyndication.com/pagead/js/r20201112/r20190131/show_ads_impl_exp_fy2019.js?bust=exp%3D21066652 .https://otampadabola2.com/.I.E./.....{6...B05.n..~:9....S.....G...A..Eo.....X.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2439443ce535a50e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7243
Entropy (8bit):	5.858856959337798
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2439443ce535a50e_0	
SSDEEP:	192:NkMn50NkMd8bcyyP6MOEkJobQpzT0EMJ2N5lJh3K8iQFh:NkA5Sk2+cd6tJnTf5lJ08xX
MD5:	CAF37F47EA84F468B7128A0BCF7FCEB2
SHA1:	2B191345AC7D77213232210CE6FCEBAE6E528DC6
SHA-256:	209727BF4CA2BB4031BE879AA18FEB89B0DD140139CEB607D5B7F1229F09C8DA
SHA-512:	2CA9DF302FEF32937480E483BB1696FC4B410DAB25413AF03282F13EE06D000647990FBABC2A28DE4D0746F6A251C8F0826E75EEEB00091A89FCE0ABAF32C3F4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....{.....4....._keyhttps://static.zdassets.com/web_widget/latest/lazy/framework-boot.b3e9cfaf9bf021f9aa72.chunk.js .https://coreldraw.com/....E./.....K.^. ...7Z.....p.m.)...1.G.[.A..Eo.....A..Eo.....'.....O.....Fh.....(S.t..`.....,L`.....Q.@..4.....window....Q.`.....zEWebpackJsonp. ...QbB.f.....push.....`.....L`.....`.....M`..... Qf:.J.....lazy/framework-boot.`.....a.....Qbb.....M9wyC..Qbr.2.....vRmCC.(S.d.`.....L`.....<Rc.....Qb.xY.....n.....Qb..... .t...b$.....`.....Pd.....push.M9wy...a.....Qb..> ....r....(S....`.....L`F.....Rcj.....,.....Qb..M[....e.....Qbn.....o.....S...R....Qb.?mx....s.....Qbv\(.....l....QbN..$....d.....Qb. .....f.....Qb.e.....p.....O.....Qb..~.....h.....Qb..N@....m.....Qb.FU|....w.....Qb..PC....v.....QbR!.i....y.....Qb.;.....E.....Qb..I.....k.....Qb".....z.....Qb.....A.....Qb6 .h...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\261a8518a8c62b69_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7094
Entropy (8bit):	5.526055590437725
Encrypted:	false
SSDEEP:	96:gOgeWjjMSvM4/cbXJTBkuZoPuMQeIA62NEZkebjI7YOaCOMmZnIDYBcJiqQemRWd:gOgdnMSkBQ/622vzCmgf9H
MD5:	DF42460F0D7523E99D972A11E10920E6
SHA1:	25FA7B231C3453363F55901298FEB32453890268
SHA-256:	632334183A93685D497FA4509DF2D09B9E58BF796848D08B67E5998F60E8B352
SHA-512:	E058882CAEAAE782392086766BCCD9ABB8D86C374E40C194D77FC3923FDE51703D058C936E7DEB5AB5A10D26A163CB76259B02EFF72108986109C0D3FAA7EE0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....^.....?E...._keyhttps://www.coreldraw.com/static/common/scripts/jquery.syotimer.js .https://coreldraw.com/DO..E./.....K...._..y./`...fsi..IVF.g....A..Eo....."e+.....A..Eo.....'..P....O....0...U.G.....(.....(S.4..`$.....L`.....(S....`.....L`z.....RcL.....Qb.^.....DAY...Qb^..U....HOUR..QcR;... ...MINUTE....Qcv..b....SECOND....Qd.Cw.....DAY_IN_SEC....Qd.k.....HOUR_IN_SEC...QeVdZt....MINUTE_IN_SEC.....Qd&z$5....LAYOUT_TYPES..Qe...Q....UNIT_LINKED_LIST..Qcn.5P....DEFAULTS. Qf.'T.....ITEMS_HAS_OPTIONS.....Qc.....SyoTimer..Qd6iyJ....staticMethod..Qc.i.w....methods.n$..... ....l`....Da.....Q.....I.,..a.....QbN..$....d...C..Qb..~.....h...C..Qb..N@....m...C..Qb.?mx....s...C.....A.....$.a.....C...C..Qb.1.....prevC.....`.....Ld.....(S..... .5.a.....Pc.....next...a....Q.....@.-

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\26d197d0a9d08372_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.737543496737773
Encrypted:	false
SSDEEP:	6:mI+YpLZuVvJGvhydwIYXc5nRbsV2dhKlu8tgPl4Fyy1/wnK6t:PLZ0vJrdwHc5psV2vXAECyy1I
MD5:	78A4B43BDA8AC945A73A10AEE2C795A3
SHA1:	AC5EDE9F3CCD4B5470878B5226F4E1BE122AE220
SHA-256:	5F34BAE05BF48BE91D3608EB1658B2BA34D16E1C02F6B789DA4C978DC9F61D69
SHA-512:	D3097A201CC248BC96369CBEE6AC78129E812809166526101F9BD16073B6F81C55589B0A1011DEF9902310798DF8BF49D7512118B0D7A789F43F80A64A070AA2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I.....keyhttps://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.uhBKOtz6fOw.O/m=gapi_iframes,googleapis_client/rt=j/sv=1/d=1/ed=1/rs=AHpOoo8GZHNTtpcfighnqAH0uUZTALLzrw/cb=gapi.loaded_0 .https://google.com/.._.E./.....mM.....$6.+..8/F)u...}.....|T...\.A..Eo.....fl.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2a2a9a1a50374767_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3726
Entropy (8bit):	6.164746131171846
Encrypted:	false
SSDEEP:	96:dLqZSh6QzMHnKv7HhoVlBNsrIYpVkeqd8:dLcSIfU7HVUYpVkZ8
MD5:	A1BCFF032516162BBEAAEC6EFA2FBAED
SHA1:	8DD0AC4F401D53EF1A6147C6115B97F2233ACDE2
SHA-256:	2D6357C54D19541B1D9B878D44542518EB541A357E3EA833F21152D22F864661
SHA-512:	DC69A6C2CEFFD7C7C7A112AEF957BDDCE789680F475A4092FA4A1D26D38FC64C499883D1CB748EF2DF640DEA5476187FD35B35A123CCB1F4AC78C0B5D2CB4EB7

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2a2a9a1a50374767_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T.w....._keyhttps://tpc.googlesyndication.com/pagead/js/r20201112/r20110914/client/load_preloaded_resource_fy2019.js .https://doubleclick.net/T.U.E./..... .....7.,L...E....CL..6..y.A..a...A..Eo.....A..Eo.....T.U.E./.@.....'.....O.....b..0.....(S.<..`2....L`.....(S....`.....XL`(....HRc ..... Qb.X:.....e.....Qb"..3....k.....QbBV.....l...c.....I`....Da.....(S.....Ia....%.....@.-....tP.....h...https://tpc.googlesyndication.com/pagead/js/r20201112/r2011091 4/client/load_preloaded_resource_fy2019.jsa.....D`....D`....D`..... ...`....&...&....&.(S..`d.... L`.....1.....u..... Rc....J.....Qb>T.....c...`.....)..8Kl`...+...l.....U...X..... .....D...p.....&.|.&.....%.....a...&.(...&..&.'...&.X...&..a....(....-(...&..&.'..'..%.'..\....&...&...%.....>...&.&..&..&...&.%..&'..(....&.X.....&.a.....&..m...%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2c4e23cad37709d9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	213
Entropy (8bit):	5.3715719688330426
Encrypted:	false
SSDEEP:	6:mRtVY71HEHINV01yG4gT2kt/clCi2PNf/0K6t:wt6Rly1yG4iawNHG
MD5:	93FF2D5CC6470A83E6F8D3B85A4F9EC4
SHA1:	8D4D8C813CB68DAF362FAD495335F17C9D00EDAB
SHA-256:	BABDDEF5CBD708BE0CE580D5E0159234BB756DE34A3634F147BFA51DEDE4D339
SHA-512:	A077D168DCB35456BE13B8EC55D6ED56A512AD5B615918AAA54B419D0812854FE6254A9D41D03DB211DC53895259F56C1F1114B46A540A0E036CF7F5C92CFA6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q.....B....._keyhttps://tpc.googlesyndication.com/sodar/sodar2.js .https://otampadabola2.com/....E./.....;..8eb.+A.W.."..P..h.R..>F+Jw..A..Eo.....b.:k. .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2d28c7d8ce7cd960_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1025
Entropy (8bit):	5.504331316269426
Encrypted:	false
SSDEEP:	24:v7IQSCl7IQ97pl7IQiNpl7IQ8Xl7IQol:DLvdLZpdLedLYdLL
MD5:	2B82F8632DA2A76F743E6748DFA0AC11
SHA1:	901A76BB929C691438E55E49A6DCB28E4E6F8795
SHA-256:	5C6111CF6C1C02A9FCE575E165CFC31AD9959113AF03A1E34B834B7624E31126
SHA-512:	9CFBA763FAFD0AC36F94B7D7A31893182122AC5682774E1C9DDAF6A2465F1D01585F6F4401DEC74ED2324561C00B482C7594377DDCB69FD0D5FE7FD2812CBE A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I.....Z...._keyhttps://www.google-analytics.com/analytics.js .https://coreldraw.com/....E./.....;.eK.....q.J.6..ng..1.</.ug.H}).A..Eo.....s.T.....A..Eo..... ...0\r..m.....I.....Z...._keyhttps://www.google-analytics.com/analytics.js .https://coreldraw.com/.w`.E./.....;.eK.....q.J.6..ng..1.</.ug.H}).A..Eo.....|.....A..Eo.. .....0\r..m.....I.....Z...._keyhttps://www.google-analytics.com/analytics.js .https://coreldraw.com/..u.E./.....I.....;.eK.....q.J.6..ng..1.</.ug.H}).A..Eo.....R,.H.....A.. Eo.....0\r..m.....I.....Z...._keyhttps://www.google-analytics.com/analytics.js .https://coreldraw.com/Wt..E./.....7).....;.eK.....q.J.6..ng..1.</.ug.H}).A..Eo.....6O .....A..Eo.....0\r..m.....I.....Z...._keyhttps://www.google-analytics.com/analytics.js .https://coreldraw.com/.l#.E./.....?.....;.eK.....q.J.6..ng..1.</.ug.H}).A..Eo..... .D.j.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\328d1a2fc68bd65c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1165
Entropy (8bit):	5.691267912843506
Encrypted:	false
SSDEEP:	24:4phWDq3cKphWDd3rKphWD+4Y33KphWDAI3rKphWDw53G:4XWDq3cKXWDd3rKXWD+33KXWDZ3rKXWt
MD5:	BAE0E0C7CF55D45D83B630955FD27677
SHA1:	C201B1798EADE1F3B7E8FDEEFF42574A64F23BDB
SHA-256:	4FB5A23A9F71463CA100C74D5551A0632534A02827226E764C852BBFAA79996D
SHA-512:	1B590EDAA9799AB44C8070C0105EC77E1551186889C6143FD39F07CA2A64659FF1BC707788DF8C0CA6DF6745043EBD870844CB12B8E3A9A11603199BC051B9C/
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\328d1a2fc68bd65c_0	
Preview:	0\r..m.....e.....)...._keyhttps://www.googletagmanager.com/gtag/js?id=G-QE2N8KSYQF&l=dataLayer&cx=c .https://coreldraw.com/.^..E./.....r.....aq...=.....A4.h...1.....8.<..A..Eo.....|.....A..Eo.....0\r..m.....e.....)...._keyhttps://www.googletagmanager.com/gtag/js?id=G-QE2N8KSYQF&l=dataLayer&cx=c .https://coreldraw.com/..q.E./.....aq...=.....A4.h...1.....8.<..A..Eo.....t.....A..Eo.....0\r..m.....e.....)...._keyhttps://www.googletagmanager.com/gtag/js?id=G-QE2N8KSYQF&l=dataLayer&cx=c .https://coreldraw.com/....E./.....aq...=.....A4.h...1.....8.<..A..Eo.....?..n.....A..Eo.....0\r..m.....e.....)...._keyhttps://www.googletagmanager.com/gtag/js?id=G-QE2N8KSYQF&l=dataLayer&cx=c .https://coreldraw.com/m...E./.....,.....aq...=.....A4.h...1.....8.<..A..Eo.....o.w!.....A..Eo.....0\r..m.....e.....)...._keyhttps://www.googletagmanager.com/gtag/js

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\33f13506b973ed55_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	35331
Entropy (8bit):	5.924411661523678
Encrypted:	false
SSDEEP:	768:WzYm5ar9ytlEB1TdrZ16625ASS0p0QeFsg:GYm84tG7TNZ1C5TVpFZg
MD5:	2D94BEE34D391DFBEB8B66A6921ED9B8
SHA1:	853D06547DE40FF35423604881E2B6ADA29FF879
SHA-256:	784FEA7782F53D7E7961D36D12314923462C936BD38179AC415500E97676504A
SHA-512:	F625CA2F226D0259F2EFA8C600E6FCF64988622D5163CA52EA52D14026E667B1B6F6FF59C1F4A758924C45E9139433A9C6F7C7F69218BDC28356D4619B6AA792
Malicious:	false
Reputation:	low
Preview:	0\r..m.....{....._keyhttps://pagead2.googlesyndication.com/bg/TBttBoAOV_9P70wCNe1Yb7YwaEpF9SEuHDe9V7wzOiY.js .https://googlesyndication.com/..f.E./.....n.!:w9G.L..[..FJD_P...9....?....A..Eo.....'RN.....A..Eo.....'.Q.....O....`.....F.....P.....(S.<..`2.....L`.....(S...`.....8L`.....\Rc*.....Qb..9.....P.....Qb.T.....W.....QbNb.....A.....f.....I`....Da.....Qbjb.....self.(S...`.....,L`.....Qd.i.....trustedTypes..Qd.|.....createPolicy.$..a.....QdzS.%..createHTML..C..Qd..K.....createScriptC..Qe.zyV....createScriptURL.C.....Q.. Rc.....Qb.....B...`.....Qc..1.....console..m...Kd .....C...).....D.Q.(...0.....&.(...&.'..%...(.....%..'..(...&.}..)&.../...../...../...Z.....&..?&....&...%.....&.(....$....&.(...&.%.*..&...&.(...&.Y.....%....,Rc.....`.....aR.....e.....0.....@.-....dP..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3895dcfb6d378811_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	935
Entropy (8bit):	5.44424274233681
Encrypted:	false
SSDEEP:	12:zXh9UF/F0jpXh9UUQlppXh9UxGXorpXh9UnYQGpXh9UrumF7Lmm:rh2OjthXapthcdthMYjth+P
MD5:	F394E5A35AA226FBBE102034CCAC421B
SHA1:	E0297D805177D8A203C4EFDD8DAA16C357C00C4A
SHA-256:	C326DDFE76AF47EB1F34B0A059EE301B23802C9DF06BFC93A07E52076A7C39FC
SHA-512:	E9831CAF4C29481AA09ED9BD63BCE94EB93C00388A5A9CBA1818DBABF3D8159489938C7AECFAC1F88B02B4283FD974A31125615A380F586B791CED9744EF753 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....7...LR.y...._keyhttps://bat.bing.com/bat.js .https://coreldraw.com/.@..E./.....wo.....jt.-....(ZQ..@..A..Eo.....ft.....A..Eo.....0\r..m.....7...LR.y...._keyhttps://bat.bing.com/bat.js .https://coreldraw.com/1...E./.....wo.....jt.-....(ZQ..@..A..Eo.....N.....A..Eo.....0\r..m.....7...LR.y...._keyhttps://bat.bing.com/bat.js .https://coreldraw.com/lwv.E./.....wo.....jt.-....(ZQ..@..A..Eo.....A..Eo.....0\r..m.....7...LR.y...._keyhttps://bat.bing.com/bat.js .https://coreldraw.com/....E./.....).....wo.....jt.-....(ZQ..@..A..Eo.....@'m(.....A..Eo.....0\r..m.....7...LR.y...._keyhttps://bat.bing.com/bat.js .https://coreldraw.com/.V$.E./.....?.....wo.....jt.-....(ZQ..@..A..Eo.....4&Cc.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3a429b03e7763408_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1085
Entropy (8bit):	5.644343673273055
Encrypted:	false
SSDEEP:	24:3yf8s3blhyQ3bnUhyi3bghySQ3blNhyeB3b5F:3yUsJhyQwhyishySQ3hyeBlF
MD5:	682E1A8CC3AB84E71C290CDE0914A1D3
SHA1:	320AF35EEF3629E99FC6A5AFF4321E5677E2F5FC
SHA-256:	D5CCC2EDB7324C9417F4AC87BCF9DFA3D2C29D2D4D8435D294030A4C4F31BDAA
SHA-512:	B6916A6F83C9B107B397C6890FFB1B88C1B76CA7180B37B03BE0DF80E25B53A218176839B770084C27E369B1CC3652F29FD2F3DE6FD3A482CF3BDCF7C7496FE
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3a429b03e7763408_0	
Preview:	0\r..m.....U.....d....._keyhttps://www.googleoptimize.com/optimize.js?id=OPT-PJJD4J3 .https://coreldraw.com/I...E./.....Q.....(...Tvi.3....$.G...s...T....C@.A..Eo..... 4?.....A..Eo.....0\r..m.....U.....d....._keyhttps://www.googleoptimize.com/optimize.js?id=OPT-PJJD4J3 .https://coreldraw.com/m.R.E./.....r.....(...Tvi.3....$.G... s...T....C@.A..Eo.....Pv.....A..Eo.....0\r..m.....U.....d....._keyhttps://www.googleoptimize.com/optimize.js?id=OPT-PJJD4J3 .https://coreldraw.com/V.d.E./..... .....(...Tvi.3....$.G...s...T....C@.A..Eo.....I.....A..Eo.....0\r..m.....U.....d....._keyhttps://www.googleoptimize.com/optimize.js?id=OPT-PJJD4J3 .https://co reldraw.com/]4..E./.....C&.....(...Tvi.3....$.G...s...T....C@.A..Eo.....W.....A..Eo.....0\r..m.....U.....d....._keyhttps://www.googleoptimize.com/optimize.js?i d=OPT-PJJD4J3 .https://coreldraw.com/C...E./.....=.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3bd902ca2fd015c3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.819753234838297
Encrypted:	false
SSDEEP:	6:mTYGLKdbVnIIf1lpiMvJNYG6RfaoG8aT76CeYCmoCbJxCAguOcXgH3CK3z+rvi+D:z7n/9l4MRKNCoG56rmocJx7xOcXIDkp
MD5:	FE2A7C641FEE37216E16AE43A87C755D
SHA1:	C0F85630691B024D935580D9BB137285E9A231E3
SHA-256:	47F236C6B4098C146A7E30370F8F4CF446B64B44A693709E808F2532A811DA5F
SHA-512:	F46D1784275C573747A815BC200EB9B4353C6ED7DAC586D1788AB3232CD7A73782DBE334600778C7116B0F9D62A5743D1CA34F8D942281337106D9E4A492F0D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....!....._keyhttps://www.gstatic.com/og/_/js/k=og.qtm.en_US.Uy00yW1PZ_k.O/rt=j/m=q_d,qmd,qcwid,qmutsd,qapid/exm=qaaw,qabr,qadd,qaid,qalo,qebr,qei n,qhaw,qhbr,qhch,qhga,qhid,qhin,qhlo,qhmn,qhpc,qhpr,qhsf,qhtb,qhtf/d=1/ed=1/rs=AA2YrTvqJb4fU1b04s4njDEmRjn4z7QgQw .https://google.com/?.[.E./.....L.... ....3.....`2....s..R.....@..A..Eo.....O.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\409d7183585b84f6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	181176
Entropy (8bit):	5.944802356248649
Encrypted:	false
SSDEEP:	3072:cvOkg22anYhN0ZL7zX3NPrLbvQo5B07cLLB:MOkUgY6FvzQg
MD5:	D62130824DA63F521A8EF1854F872768
SHA1:	5ED8777DFA0A4BB48C857B6592612671D971C818
SHA-256:	DA672ECBC838CD435B379CDE98B93C0E4131EEFB6CE2BF4606351F222F76DC20
SHA-512:	957BDD452B71F80491F9DF96CD320E6A5A1976EB7A25BCE5F59243525B61B6EC211B69A539D09373B2A7EB097FC9CAA50B090EB329F6301217EA4FC349BA37A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...V%.~....26F2672139B15616E1D29CCDDBB14265E2A74D618E5778476371FF186CF83A16.....'.HN....O4.....@..".....d...P..... .....x...,Y.....(,..$.....I.....X.....(S.i...`....!.L`.....(S...`.....LL`".....@Rc.....Qb.....t. ....Qb..M[....e.....Qb.xY.....n...b$.....I`....Da.....(S...`.....L`.....Q.@>.....exports..$..a.....S.C..Qbv\(.....I...H..!....a.....Qb.....call.....K`.....4KkT..... ... .\. . ....0.K.....}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&...&..'..W.....-...(.....,Rc.....`....Da.....!.....e..... P.....@....@.-....4P.. ....'...https://a.opmnstr.com/app/js/api.min.js.a.....D`....D`....D`.....Q....`$...&...&....&....&...(S.X..`l.....L`.....Qbn.....o.....e..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\46db41e78b4307cf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	150880
Entropy (8bit):	5.793453866708811
Encrypted:	false
SSDEEP:	3072:4INSB9SeinyvsxTCyHKUdGzlWdP5t1RGn2E:L29S5nyvmKUdWlMP5teZ
MD5:	82CDD741637BC1097916153E7A7CE18F
SHA1:	EC3F655DF891087A2F4E7D86ACE2F7ED15943B87
SHA-256:	A1425E731C43C2880C2C06078B482D2B8FEB398BC1A1A67C09303978CC827DA7
SHA-512:	20E5F43323FCEE5CF09618FFA5B7A1B9A02136D275AF19882F5909574D45C7C4F4472D52E51C061C1639C5E6145B1E31C9BDBFDB7B62B0A66BAF348A28193EF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....99863E64CBEF3FBFB3D7060B65F9858050548D8312E8BCC972BFA3F39E19EA6B.....'.,....O1....K..T....."..... ....$.....t...x.....8.....(S.L..`R....L`.....(S....".`jE.....L`f.....Rcb.....(.....Q.@Z.O.....doc ument..QcnY.....window....QbB.....aa....Qbf.....ba....Qb.2.*....da....Qb.....fa....Qb.....ha....Qb.....ia....Qb.Eb.....na....Qb..%C....oa....Qb...P....t.....QbF.....qa....Qb.D. %....ra....Qb..Yc....sa....Qb".....ta....QbB.N.....wa....QbjV.....xa....Qbb."l....v.....Qb^.....ya....Qb>.....za....Qb.....Aa....Qb...L....Ba....Qb.....Ca....Qb.t.....Da....Qb...8....Ea.. ..Qb...o....Fa....Qbr.Q....Ga....Qb.....Ia....Qb.J.....Ja....QbR..z....Ka....QbN.)7....La....Qb&d.....Na....Qb.....Oa....Qb..r5....Pa....Qbj.z.....Sa....QbJL.....Ua....Qb&C.h....Va.. ..Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4741b837184733aa_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4747
Entropy (8bit):	5.833923428761665
Encrypted:	false
SSDEEP:	48:ycf42+EfVCzJN9KBg+Oq2GfcuS9dYIJSNl6AOa+wE9TZFNhPnPNI5aRyfrTEnc1A:yc+LX9KXfEtJSv6DLzFzfPeAsfNvru
MD5:	E03747C79CD89143AD614D56B355123B
SHA1:	6859CFB1F88BEAB256FA07C9057955977708C6D9
SHA-256:	119194F9F884AC0835E8649332B51071B32AF89F11CB8ABA6520788C5A716558
SHA-512:	2684482607854EB78B9FB91B3FA9085F2DCB3985E7899B7EBBFE4F940FA6D822DC0BC12FBA1B92F1B43B1CEB6B9A52AF80ACF271278B7373314ECAAE48B7195A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....{....A....._keyhttps://tpc.googlesyndication.com/pagead/js/r20201112/r20110914/client/window_focus_fy2019.js .https://doubleclick.net/..S.E./.....kX.),.....U<...5...x....A..Eo.....<.H.....A..Eo.....S.E./.....kX.),.....U<...5...x....A..Eo.....<v.....S.E./.....kX.),.....U<...5...x....A..Eo.....B.....'.'.....O....@...R.....P.....(S.<..`2.....L`.....(S....`.....L`@.....Rc@.....Qbz.....f.....Qb..;V....h.....Qb"..3....k.....QbBV.....I.....Qbn.Do...m.....Qb.....n.....Qb...;...p.....Qb...P....t.....QbV.....w.....Qbb."l....v.....Qb*..6....y...k.....I`....Da....2....(S.D.`>.....L`.....Qe>..%....addEventListener..K`....Dk(... .....(.....(...&..&.'..'..'..W.....,Rc.....`....Da....f.....b.....@.-....lP.....]...https://tpc.g

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\48f291afa9a147c0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6744
Entropy (8bit):	5.749871674459042
Encrypted:	false
SSDEEP:	192:qu81YlDmLETT5aql4tvq0dSW7cPUg3uommz:R81YlegT5aR00D7O31Vz
MD5:	B8ED2C992F84C3DCBD42FCE1FBF9A5A9
SHA1:	CD448D004E79B4E68A54ABE851943F3A5F7A6E09
SHA-256:	659319063DC2F434204F252A23A2C02835167139271B37ACD2BF188FCC7C563E
SHA-512:	8DB2A2760E6F9B98091FD7EE503A0B274E0B32B5FE15C48A958599EE0DF6AC7F6FDB5CF11B5BD2B4E621BD3BEA82DFEAB597A62AD34B2011BE7F282B93EDE166
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H....._keyhttps://munchkin.marketo.net/159/munchkin.js .https://coreldraw.com/....E./.....p...T...3.....[...e-..z.D....A..Eo.....'.....A..Eo.....'.f+....O.....Y.....(S.4..`$.....L`.....(S.Y..`j.....L`x....q.Rc.....R.....Qb..~.....h.....Qbv\(.....l.....Qb*.....q.....Qb.-`.....D.....Qb.....A.....R....Qb.....t.....Qb.;.....E.....Qb..47....x.....Qb..O]....F.....Qb..PC....v.....Qb.'.....V.....Qb.....f.....Qb.F&....G.....Qb.....W.....Qb..> ....r.....QbJ..p....H.....Qb...6....I.....Qbf.....J....Qb.Q.....K.....Qbb..T....L.....QbR!.i....y.....Qb..M[....e.....Qb..N@....m.....Qb.e.....p.....Qbr..R....X.....Qb.C.z....B.....Qb:..A....C.....Qb.K.....M.....Qb.`9.....Y.....QbJ..`....Q....Qb.....Z.....Qb..f(....R.....Qb.FU|....w.....Qb^.....S.....Qb".....z.....Qb.K.~....T.....Qb..!.....N.....Qbb..E....U.....Qb6 .h....O.....$.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4a2181030e79f4da_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1225
Entropy (8bit):	5.683968380395454
Encrypted:	false
SSDEEP:	24:tEqt+5yFDMpfEqt+5yxTDMQ1fEqt+5y5rDMYfEqt+5yV5DMJfEqt+5yyGDMW1:tEqt+dpfEqt+Y8cfEqt+NYfEqt+HJfEw
MD5:	653457B25D8995AF69CA9CFB73B2818E
SHA1:	EE13D28147A5488B316DEB128B72814EBDC5D274
SHA-256:	AC74FF5282D1DC6577E8579964D667B6A6B7E01D5EA562EB16687DEB74E67F06
SHA-512:	89A4373DDCF02CA6403E79DA0307BBA68EDD922720B4BF318D21CB72FDF3E0F0233002746A275925603FFAD4BD941CDBE67755F31D9087E3805A2D8A86D502B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....q..... ...._keyhttps://optanon.blob.core.windows.net/consent/c619603a-836b-497d-858f-1d3e16886f07.js .https://coreldraw.com/....E./.....K.i<y..8....4.F..n.B....M,..A..Eo.....o..].....A..Eo.....0\r..m.....q..... ...._keyhttps://optanon.blob.core.windows.net/consent/c619603a-836b-497d-858f-1d3e16886f07.js .https://coreldraw.com/x.j.E./.....M.....K.i<y..8....4.F..n.B....M,..A..Eo...../..'.....A..Eo.....0\r..m.....q..... ...._keyhttps://optanon.blob.core.windows.net/consent/c619603a-836b-497d-858f-1d3e16886f07.js .https://coreldraw.com/.{.E./.....K.i<y..8....4.F..n.B....M,..A..Eo.....b.J.....A..Eo.....0\r..m.....q..... ..._keyhttps://optanon.blob.core.windows.net/consent/c619603a-836b-497d-858f-1d3e16886f07.js .https://coreldraw.com/.b..E./.....+.....K.i<y..8....4.F..n.B....M,..A..Eo.....A..Eo.....0\r..m.....q.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4bf729f8a79cee0b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4bf729f8a79cee0b_0	
Size (bytes):	1215
Entropy (8bit):	5.812476308006536
Encrypted:	false
SSDEEP:	24:fNka46QJ24phNka4tJYhNka4VyxJDhNka4BeJchNka4XJ4:FkaknkaTnkaEyfnkaK1nkaR
MD5:	D75DD6AFCBECFCB8062D60AC49A24DF7
SHA1:	576F025EEC0C5DFF7829F839888FA9F540F53ED0
SHA-256:	3FA4D6190F0ECF76B8DFCC74F1305813CA369D8C8FE6B0B75275329FF821E41F
SHA-512:	F483517B6B6B30396649B77FCCB2B041BC83E016E07AC68F1C94D658E0F27C017ABC620A91B380DCE615D25662378870C643F62FE5632ED75A493ED86EC44065
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o....._keyhttps://static.zdassets.com/ekr/snippet.js?key=d3f88178-b699-4002-a1d6-f61fec7d4063 .https://coreldraw.com/.@..E./.....RG.;E...`.m..I..Q..^|.L.|...).,.A..Eo.....&.....A..Eo.....0\r..m.....o....._keyhttps://static.zdassets.com/ekr/snippet.js?key=d3f88178-b699-4002-a1d6-f61fec7d4063 .https://coreldraw.com/u.P.E./.....RG.;E...`.m..I..Q..^|.L.|...).,.A..Eo.....l."......A..Eo.....0\r..m.....o....._keyhttps://static.zdassets.com/ekr/snippet.js?key=d3f88178-b699-4002-a1d6-f61fec7d4063 .https://coreldraw.com/-*d.E./.....@.....RG.;E...`.m..I..Q..^|.L.|...).,.A..Eo.....x.....A..Eo.....0\r..m.....o....._keyhttps://static.zdassets.com/ekr/snippet.js?key=d3f88178-b699-4002-a1d6-f61fec7d4063 .https://coreldraw.com/H%..E./.....p$.....RG.;E...`.m..I..Q..^|.L.|...).,.A..Eo.....A..Eo.....0\r..m.....o....._key

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4cf5a22a75d22bb9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1903
Entropy (8bit):	5.6194334486807005
Encrypted:	false
SSDEEP:	24:D+MZaxxIi/5UFfvSED+Je5lwOhMIgbBRa78tlSod/w+MiUy6M9IqcefoxuXF:SMZav355Je5b6IgbBRa7+lddYc4Ioy
MD5:	7BB6E639EA8B76994E837EC06DB490AC
SHA1:	762090DD7B8A4D35D8BD147F02A017F6C269BFFB
SHA-256:	0E39764693708EA45238D8B5EBFBBEF49B7D3E5D99BDE44E72EEBB89F4EB50C9
SHA-512:	3D3E79F000DEF0DBD7E0F1C2876823845D2FCF146171272F113AA4F37D32247D129F7536E16247E8A9C797DFFAC0D4626C33A58F508990A9AA4DD17CA6FBCCE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....5....._keyhttps://www.coreldraw.com/static/common/scripts/dynamic-pricing/jquery.format-currency-1.4.0.min.js .https://coreldraw.com/....E./.....s..>....R.".|M.....S1..s8.x...A..Eo.....Ymm.....A..Eo.....E./.(.....'.....O.....9:. .....(S.4..`$.....L`.....(S...`.....@L`.....HRc ..... Qf.....getRegionOrCulture... Qf.c. ....validateParseType.....Qezo/.....generateRegex...c$.....l`....Da.....!...(S....Iag...L.....@.-....pP.....c...https://www.coreldraw.com/static/common/scripts/dynamic-pricing/jquery.format-currency-1.4.0.min.js.a.....D`....D`....D`.....0...`....&...&....&.(S.....5.a.....a.....a.....Qb~.6v....fn.....a.....Qe.\M.....formatCurrency..a.....d.....=...l.....a.d.....D&.(S.....a.....Pd.....fn.toNumbera....q.....d.....0...I..d.....D&.(S..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4f11ebc47a2ae296_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	254
Entropy (8bit):	5.632567334404002
Encrypted:	false
SSDEEP:	6:mf//6EYk+tHzZ2HDFb7VPN9UugXWZ2hO4wtK6t:6+tHN81JN9UujZ26
MD5:	73074B01FA7377699735A239CFB835AF
SHA1:	1126E3E894CB765CF08EBC439121B4E206B03F7C
SHA-256:	E49374AA9F869DDAADA08B57377922203B0B9E3087A3BC4D18C0723C02717A24
SHA-512:	3230D6DED7F981BAC7DF6B0FAAEEF43B0B636C5D8B630B6B4A6F8CD2458D0534B627BF123D1C06C78085BD5B07BAA6732945C6BFA79E8EDE3231135CA7E776 1A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z.....X...._keyhttps://static.zdassets.com/web_widget/latest/locales/en-us-json.cc8e73e5fe307bb27426.chunk.js .https://coreldraw.com/....E./.....8....[...}....'.'..D>v.A..Eo.....h.L.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4fad52a0da7e4e43_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	72960
Entropy (8bit):	5.955223568758483
Encrypted:	false
SSDEEP:	1536:a2QhTJlkFtowF7xISUQwwQuav8nkXH8KdTEFve0b8RF8Lnbos:a2QhTAtokVw/ua0nkXH8KKJb7DD
MD5:	200336282938695AA33F8A4411CE4CB5
SHA1:	86741DF3B96012AB94454207895BD6EA4E421974

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4fad52a0da7e4e43_0	
SHA-256:	A92FD5A8C1A590E25D2FB270291B51759512C6DF980AD994D84C98346F8EC5D4
SHA-512:	A6BBB5555E25ED7D87414499FD350BBF9273BE6A9A698C84E4EBD37238A0680BD393A44A487B4E33F8844843DFFE4216BCAA220721DBE6BF3485A532D70ED8D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....9A609F29A7444ECFCE74F523CA64BD64D303D4AD65954DC364D20E44B2B0A4F8.....'..W....O.....^.....c.....|...P..... ..L.....(S.....`&....I.L` .....Q.@..G2....window....Q.`*.,.....zEWebpackJsonp....Qb..l.....push.....`.....L`.....`.....M`.....Q.P.....web_widget..`.... ...l...a .....QbR.*.....+/hVC..QbV.....+NxIC..Qb.LKV..../RGIC..Qbz...../lijC`....C`....C..Qb^.p.....1HBYC..Qb*E.F....1P4IC`....C..Qbj.....20s0C..Qb".....2GasC..Qb.O..... .2VHxC..Qb.p.....2Wy9C..Qb~..C....2bioC..Qbz.....2yNQC..Qbv/.(....3AXEC..Qb.7[.....3fg0C..QbZ.#.....4TMlC..Qb.B[.....4XLzC..Qb&.c.....4lRuC..QbZ.....4mM7C..Q b>.S.....4n1QC..Qb.....5/8DC..Qb.....53DGC..QbvR.7....54/XC..Qb..Q.....5CNoC..Qb.\.....5RgcC..QbJA.~....5c4VC..Qb2X.....5oQOC..Qb..1|....6HfxC..Qb..9..... 6dgFC..Qb.?.....6w4rC..Qb.o.....70GIC..Qb.....7BGfC..Qb.....7bIAC..Qb...Z....7lMtC..Qb.....7

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\51a146757e824d78_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1131
Entropy (8bit):	6.05648377215643
Encrypted:	false
SSDEEP:	24:34wwWR+XUWRKi56/X34fEIBBuTTkCXqsDwon7V6uzP4xRamJ:IN9XUDi2SEIDCXqhon7lzP4iO
MD5:	7DF245A47475296BCDA47AD4BD95B8E8
SHA1:	03A51684046FEBE33AC59CD5B249AB3BC89D8A3D
SHA-256:	1C0F8227939DAC48D855DDF9EA6B698D4EC2B48AEE1AD571A6D5E4AEABE79223
SHA-512:	3D3CFBF8A0A1BB4C52BC123708A974BD8158E92EF1254BBBE78986E2D89066151FBD7816D25332798E03E0B89F3936F3D9FCD2684EBD8B6C816197A88117E29
Malicious:	false
Reputation:	low
Preview:	0\r..m.....{VJ ...._keyhttps://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.AdsSettingsUi.en.54LqtFl99uk.es5.O/ck=boq-identity.AdsSettingsUi.afn1Y1t3DVA.L. B1.O/am=lA/d=1/exm=A4UTCb,A7fCU,BVgquf,CBlRxf,CG8cBd,COQbmf,EFQ78c,EcW08c,HDvRde,HLo3Ef,I6YDgd,IZT63,JNoxi,KG2eXe,KTWBP,KUM7Z,L1AA kb,LEikZe,LFMxUb,LGJfp,MdUzUe,MpJwZc,NpD4ec,NwH0H,O6y8ed,OgOVNe,OmgaI,PQaYAf,PrPYRd,PrUyhf,QlhFr,QLpTOd,QNqBAe,RMhBfe,RMwYNc,SF3gs d,SKhAfc,SM1lmd,SdcwHb,SpsfSb,U0aPgd,UUJqVe,Uas9Hd,UgAtXe,Ulmmrd,V3dDOb,VwDzFe,WCG2fe,WO9ee,WpP9Yc,XVMNvd,YLQSd,YTxL4,ZfAoz,ZwDk9d ,Zxe3i,_b,_tp,aW3pY,aurFic,bIf8i,bXpTS,blwjVc,byfTOb,doKs4c,duFQFc,e5qFLc,fKUV3e,fgj8Rb,gychg,hPtwLd,hc6Ubd,iBCuq,iTsyac,iWP1Yb,icmqKf,lPKSwe,lsjVmc,l wddkf,n73qwf,o02Jie,oWOlDb,pB6Zqd,pjICDe,pw70Gc,qfTGrb,qmdT9,rE6Mgd,rHjpXd,s39S4,tfTN8c,w9hDv,ws9Tlc,x60fie,xQtZb,xUdipf,xiqEse,yDVVkb,zbML3c,zk0ux,zy 0vNb/excm=_b,_tp,anonymousview/ed=1/wt=2/ct=zgms/rs=AOaEmlFEHEPDnnmKZbnTy6pY5x8uD7RFdQ/m=GILUZe,wGM7Jc,rGAWrf,VXdfxd,U7yoG,dTlQYe, mNyZub,Dkl

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\589df6f65d6011c3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1095
Entropy (8bit):	5.606070565609526
Encrypted:	false
SSDEEP:	12:OtnArRC7UBetmlUT4tnArRC7U1xmlDN4tnArRC7UZRlM4tnArRC7UTwcGol2i4tv:OSrwHT4Srw5N4Srw34SrwU4SrwmAz
MD5:	E53C48CC790539E3BD10E8602C4E4350
SHA1:	E675702D11D3D50BE1216301D8783625930EAF29
SHA-256:	09EF7D7105DF01AC7A566BF3B4D7129B06E3936A19294D9685EDFDA634203B87
SHA-512:	BE0A25BEDC6C931A0F21F9CFC244761C8A2CF022901274AB864742728643CC4B1CB6D2B6C4DA4BD09A3719DF2F2DEC26E17D71A862A45F6675D48179EF0F65 4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W...6..V...._keyhttps://www.googleadservices.com/pagead/conversion_async.js .https://coreldraw.com/!...E./.....'.....1..c|.....X<....R.....A..Eo.....%.~..... ....A..Eo.....0\r..m.....W...6..V...._keyhttps://www.googleadservices.com/pagead/conversion_async.js .https://coreldraw.com/.`.E./.....'.....1..c|.....X<....R. .....A..Eo.....L.....A..Eo.....0\r..m.....W...6..V...._keyhttps://www.googleadservices.com/pagead/conversion_async.js .https://coreldraw.com/$.v.E./..... .'.....1..c|.....X<....R.....A..Eo.....A..Eo.....0\r..m.....W...6..V...._keyhttps://www.googleadservices.com/pagead/conversion_async.js .https://coreldraw.com/] ...E./.....<).....'.....1..c|.....X<....R.....A..Eo....._.....A..Eo.....0\r..m.....W...6..V...._keyhttps://www.googleadservices.com/pagead/conversion_async.js .https://coreldraw.com/w.#.E./.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\58a27733a97c3858_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.430349596622268
Encrypted:	false
SSDEEP:	6:mYnYk+2iKxR9KYLoSYOgDrpwz934wtlhK6t:N+2iKxNLIOlFtN
MD5:	2AD6FCE90E25D418C7AA074C89EBF2E7
SHA1:	C2076B1B97541F092E4D531A73A84C4B220DDE29
SHA-256:	B60E077B384D08AA1FF466339550CF50DE4C4960FCDE601F3D188125CA5DA4A7

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\58a27733a97c3858_0	
SHA-512:	DF75F298DED47FDB5492685768C9A5AEA492A88D5AEC131BC9061402F02505E8BCC9FD4940ED3D9E65F18A9B473295454633B05C5E2E5A63DEDE11CF664211E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P.....8f...._keyhttps://static.adsafeprotected.com/sca.17.4.114.js .https://doubleclick.net/..d.E./.....cH.0..Or..Y....,..x.a...3...=0.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5cc86c6607abbc80_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1315
Entropy (8bit):	5.45246974988464
Encrypted:	false
SSDEEP:	24:65BY4AZKf9NHICxCu+gJpSvqkVvDQVZUIqwDo8Y8:Ai4tNoCx8Jyk00h8
MD5:	3481F9AD7CB5F2B9D0F8C61FAE00C3CB
SHA1:	529E4C3F52FC46CDF29AFE001B8746AA012CCD80
SHA-256:	DCECBE3DBAFC86DA61EC45C18FB2906E2B0577C69C98C49F4CF437F124A5C10C
SHA-512:	082AEA8E5C258F1A71306A0EFF3E04F5D927C2EA72DF7614A56E8F02FCE7C9EFFC46199377D394F7DBF15B5E3A8CFF59C93EB1132D7EAA073694CADB45F2F70
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c....@.a...._keyhttps://www.coreldraw.com/static/common/scripts/responsiveslides.min.js .https://coreldraw.com/cB..E./.....f..z..T.kQ..p$..<.T..a.\|YX..T .A..Eo.....?cp.....A..Eo.....cB..E./.....'.D.....O.....h.....(S.@..`6....L`.....(S.H.`J....L`.....@Rc.....Qb.C.z....B.....Qb...6....I.....Qbb.. .....c...bd.....$...I`....Da~...f.....Qb~.6v....fn...(S.....5.a.....a.....a.....a.....Qe~..s....responsiveSlidesae...2.....d.....(.....a..... ...../..*j.....$.g..... ....d.....I.....@.-....TP.A.....G...https://www.coreldraw.com/static/common/scripts/responsiveslides.min.js.a.....D`....D`$...D`.....t...`6...&...&....&.....D`....DI]d.....A...K`..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5e1c6b7527d473cf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	254
Entropy (8bit):	5.56254542100184
Encrypted:	false
SSDEEP:	6:mLzYk+tHzZ27tE41LRS9UtAgo/kUWX96rzK6t:6+tHNCth1LRS9UyP/rWXO
MD5:	18EC1C1770EB24521851E51840667AA5
SHA1:	57055DA1B4DDE56EEFD46B642B7E0EB6CA944343
SHA-256:	9ADACD688EB0C8BF3DD2AEB680E088FC267CC744049BD3EAB0F3B8B6C28FE87A
SHA-512:	CC5E0686F8EB700EB47CF6266CFDC11D1EC72DBCE4D5391062CBB935C0B62CBD4B50212A187F6E1F20651D62BB0C5ECA39448B4563E1891842533AF690D522E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z...A.c....._keyhttps://static.zdassets.com/web_widget/latest/locales/pt-br-json.b71a1a93f723f8a2873a.chunk.js .https://coreldraw.com/.;$.E./.....dw.`...b...c.7x4....Z.....%H..A..Eo.....\I.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5e5984a807e18440_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	278
Entropy (8bit):	5.554602398763908
Encrypted:	false
SSDEEP:	6:mlYw1yGSVOlAscQMk09fwyokPTInp1yGfKFgF4AST3N/PZK6t:E1yGSvLt9fVPTup1yGfuAnENHT
MD5:	92EA7224659035723884F324BEFCB093
SHA1:	3B0970F1F39A6982EC6CDF6F9DB8562F6B8BEA52
SHA-256:	9EA4ADDF9B958C66430B2FBD75E3B9A577DC94B84CBC88FCE001B863D43D024A
SHA-512:	315C8D0E00D558C146F6F11B9D6DFF5F65EA1C20B9889BD67533B52CB851C7E6C8B62D767D24F68D957AE3A4350503AD03D50BD770D4F3797EF9A8CB0BD5DA5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....(4v...._keyhttps://otampadabola2.com/wp-content/plugins/google-analytics-dashboard-for-wp/assets/js/frontend.min.js?ver=6.3.0 .https://otampadabola2.com/=m@.E./.....V.'@w=..~...d.]....h0.....A..Eo....."....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5e62bb69a9c4f59a_0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5e62bb69a9c4f59a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	257
Entropy (8bit):	5.67527953276257
Encrypted:	false
SSDEEP:	6:mOXYGLKdfw885TLOWAb3TSYIntgJlXNIivoPGBWk4PzK6t:iyrpLOWi3lIntg6itBzeI
MD5:	151FEC71D330EB5F447FD54AB7FDDFD3
SHA1:	9DEA4E9BCDFD7ECB9C5CCC8500B3C5D9588EEC9F
SHA-256:	66478626AE5D37E2CF12A79F4405AEB2144D8CD9035935E38C3EDEC6143C88E9
SHA-512:	1A79171CEA69116EB4909366D7A61BA3421498D0ED49B45B4E180EEC18AE63037B7D0B1E117C586EB1261DAF9BE36897F466217426AF9F5A89BF39D8747059AB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....}....:....._keyhttps://www.gstatic.com/mysidia/d3537bc478bfa26a2c6e70b12aa4d45c.js?tag=client_fast_engine_2019 .https://doubleclick.net/..R.E./..... .....v.....j.2D.2...)..9Q.0.d_..A..Eo.....(0D.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6019ad028452e15e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3412
Entropy (8bit):	6.166222811214663
Encrypted:	false
SSDEEP:	96:dMdWcu1t8uE4u0fKf2bD4BRxqx8+Jl7kZTjqM989:WdWcQ1if2bm8i+72Tj1989
MD5:	1AF9CD4F8107FA3E72264AE9311BED43
SHA1:	D91DB4612384BCE63175A91DA08F85D44F7183F6
SHA-256:	C6D84971A7B133FEB2EC030A8EAE1B5309FC10E4D906EF382E92AAA231945457
SHA-512:	C319B1436355BE1F7B3461CC518217254FACBCCDF77B00ED253EC3687C1A567BB44D0FE7757163212F9C2A06DA650A55B37BC0CB01EFE406118E3E91C8D7FB 8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U....._keyhttps://fw.adsafeprotected.com/rjss/bgd/178215/37126869/xbbe/creative/adj?p=APEucNVh-EuYoOfbKuO_1Ulx0ASq5LPnCCWy37NkOBVvGuR 3mTdBFnM&d=CnkAoCZ_4BpQ2PtK3nUCDlUQe7hPHJlVpg1jAIAMvLtLebbLTIe1lY1FRagWTrBTEBsqWUtTL2WyoX-yTIsEB4ubOcnrJqcNZRLeccPcJt0ytFpmDCalPw-bJ9K9IMxz-jUMtYu65kC3O-IKbDg8GP6_e4rQTNpXoRvHEokRAKAmf-Dm5noYPBdb3zU9FoxfhgLagvsE5FY6EGwsTp-LnjGo6bcGVY6U7yUgiF6woEhS1Ya5Wi6Zu4AVl 5Cpo1emKE3dEtU9-4eCebUNdzXE0s5WGDaPrWn-1QmWuGXiBnx04WaCXZmYsrJYPPjOvEK0PvXs4Xha70VCl-Utbvu3C5AnyNFYGtoegvNWPM8a2HakCCcNB LOkwETHSs7UVsqF2KZ6LWnPZKLl1-fLLw_GDRd_CyqwB3YeYm5U6FaYQDF7cuWUtjbetkIHRAFlUwXKxr_3cbcozHENacpr3Jrep6mBl_FOQ_xKceLwz2zLn SMwKrBtSEto1iNMPVHCm2kuVFUhCr9utGueAd-60VhAq1kuRSVfpjbLW9SxbSBj-giImloLSV-JKQfCL_Pmv5x6ucWbIsNwN8gzzRmcO-WuV0dfvR7Au4rlKmyc1xkHcTn G4wrd34urPr5J0PuI0gUGsIciFaTGInfCGmSe4qZIL_WSpd-AmtVxSdV4kPFCi3WrO5gfan55mAYnuLm8u4vxeBA595eGJpsW8E7GgiZAZ5OICM_Ulc3vx8Rb1S1qaXaOI U7eluXa1UXev2N9figulC32l2LJMNbnfEYMrzOL9DdFNik-KK85ZUqbGyp-n2V4sJmw2lRvL1tRH8MRikmOqmqozj

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6661e94a0ccb1861_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	23260
Entropy (8bit):	5.692400726351886
Encrypted:	false
SSDEEP:	384:b/ROxpoRvO1+g01ynMCLpzzzKpucK7OPmz09TOEXlEQ38SwZKk:jeoRW1i1ynMUpcK7PorlEQ3v4N
MD5:	0E99B295A4924433F7DC007B6A3F8F1A
SHA1:	C657197D39EA2C538A3113C56B0D7493CD7CDE83
SHA-256:	494FE0B564142AC1996B65006D2DED142939307DA70E74A2DE86540E3D6785BE
SHA-512:	701DF9C0B391A47D09E653D99F89585366EF355869BD2FE733D8AD440C64FB5913A8A45DF8373D35884BEA1D2F700DAE0EA289D932387946FE923ABDE4308F3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T....a`...._keyhttps://www.coreldraw.com/static/cdgs/js/owl.carousel.js .https://coreldraw.com/.B..E./.....V.[.~(.N9.\'..uI_.]Yz.p.1..K...A..Eo..... A..Eo.....'.._....O....PY.....,.....(S.....`b....@L`.....(S....`.....i.L`0....PRc$.....Qc.X.....document..Qc..4.....window..... Qb...r....Owl.d....$.....$.....I`....Da.....I...(S.....Ia...._....$..g.....+...*.@.-....DP.....8...https://www.coreldraw.com/static/cdgs/js/owl.carousel.jsa..... D`....D`:...D`.....M....`....&...&....&..!,.D&.(S.....5.a.....+..Pd.....Workers.runa....=.....Qb"..b....run....*...-d.....&.(S.....a.....Pd.....Workers.runa.....q>. .d.....&.(S.....a.....Pd.....Workers.runa....G.....d.....&.(S.....a.....Pd.....Workers.runa.....d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6838bc2f443ecd64_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	360
Entropy (8bit):	5.847045512389855

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6838bc2f443ecd64_0	
Encrypted:	false
SSDEEP:	6:m8YGLKdGMwjMGRRo+Al1cL1UYYVaEGCm9rzTYcuMwHgb/rMH+443XhK6t:w9wwWRonXxTam1YNPWTq+4E7
MD5:	79BBCE7E40B8FCAC53B8D8B057BB5A19
SHA1:	AC10F23934458ACC250E41C2B7A4405C235BECE6
SHA-256:	7D7616A95BC2672E9AEA846264B181BA201E2D1AD8B9F3339C8E95351BBF3B0F
SHA-512:	9FA33B00026547A2CDCC4E237E0556F84C25B4C0BD3E0CF1AA26DA15699C44A34C9688A8B227746E49514302AF6952C59C7935F718ED435DB0D8BE68BE51842
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V...._keyhttps://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.AdsSettingsUi.en.54LqtFl99uk.es5.O/am=lA/d=1/excm=_b,_tp,anonymousview/ed=1/dg=0/wt=2/ct=zgms/rs=AOaEmlHiCIRweGfSahRPlGKd4bV59xi-9A/m=_b,_tp .https://google.com/4.Y.E./.....PL.....F.%.xK.....s.i.....#..x.....A..Eo.....d.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6c66dcb53706dfab_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19320
Entropy (8bit):	5.736175899044815
Encrypted:	false
SSDEEP:	384:zGV1cMBTFUKSyZhwyaH/LAFo5BTItSwnRF8EM33:ENWyKAFo5qHF4
MD5:	7E8124D83114E394ED8D2D934171AA4A
SHA1:	31D9438CCD2E28B8138D86351DEF97D5575C9009
SHA-256:	FAA3549EF9071436F33B6D9964DB78E55B64E13516ECD5EAFE59F8D935A6EDE1
SHA-512:	2BEB843BDB5DC5932E1466114B81B927D673EC41C5B87F2A5CEF0B4F2FA7D830B3E5D239DF15E9A924B5E883C99B358751F97D07397E731C24D3F8912168E34
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....7....._keyhttps://www.coreldraw.com/static/common/scripts/jquery.magnific-popup.min.js .https://coreldraw.com/....E./.....d..%x.`.....o5a.....V>.....A..Eo.....]`.....A..Eo.....'.xR....O....I..^.....(S.X..`f.... L`.....(S.|.`.....,L`.....Q.@..oU....define....Qb..R.....amd.....`.....M`.....Qc.~.....jquery....Q.@>.....exports...Qc...X....require.....Qc..4.....window....Q.@b*.....jQuery....QcZ$=r....Zepto.....K`....Dy.....s.....&.(.....&.z..%&.^.....5...s.'.....&...&.].....&.(.....&.(...&.].....(Rc.....I`....Da....$.....e.....P.....@.-....XP.Q.....L...https://www.coreldraw.com/static/common/scripts/jquery.magnific-popup.min.jsa.....D`....D`@...D`.....`....&...&....&.(S....`.....q.L`4.....Rc.....^.....M....O...Qbb.....c.....QbN..$....d.....Qb..M[....e.....Qb.....f.....Qb..~....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7369f1b1520d379c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1160
Entropy (8bit):	6.053808267434334
Encrypted:	false
SSDEEP:	24:+wwWR+XUWRKGoK6/X34fEIBBuTTkvDLqsDwrw7V6szPsryAI:+N9XUDGodSEIDbLqhrw7LzPKyAI
MD5:	16896FBF6EDFD152250E0340A6ADC0B1
SHA1:	7259FB3BD1C319D6C1CD0E1F1895A56CA58DC592
SHA-256:	BFA93AC5A3BBF2E08B93577F3C356CBC9C9D3014CE6863655BA94C65779BBFF5
SHA-512:	90088DE84CD6BD0E21D04B1B7B632CBECC1BCD783A35477E9B7AA043E4672653CAC0AFA917D49C3963A919BD7AB42171036457E91A51485EC4BBCE2CFBEE36E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....8....._keyhttps://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.AdsSettingsUi.en.54LqtFl99uk.es5.O/ck=boq-identity.AdsSettingsUi.afn1Y1t3DVA.L.B1.O/am=lA/d=1/exm=A4UTCb,A7fCU,BVgquf,CBlRxf,CG8cBd,COQbmf,DkItH,EFQ78c,EcW08c,GILUZe,HDvRde,HLo3Ef,I6YDgd,IZT63,JNoxi,KG2eXe,KTWBP,KUM7Z,L1AAkb,LEikZe,LFMxUb,LGJfp,MdUzUe,MpJwZc,NpD4ec,NwH0H,O6y8ed,OgOVNe,OmgaI,PQaYAf,PrPYRd,PrUyhf,QIhFr,QLpTOd,QNqBAe,RMhBfe,RMwYNc,SF3gsd,SKhAfc,SM1lmd,SdcwHb,SpsfSb,U0aPgd,U7yoG,UUJqVe,Uas9Hd,UgAtXe,Ulmmrd,V3dDOb,VXdfxd,VwDzFe,WCG2fe,WO9ee,WpP9Yc,XVMNvd,YLQSd,YTxL4,ZfAoz,ZwDk9d,Zxe3i,_b,_tp,aW3pY,aurFic,blf8i,bXpTS,blwjVc,byfTOb,dTlQYe,doKs4c,duFQFc,e5qFLc,fKUV3e,fgj8Rb,gychg,hPtwLd,hc6Ubd,iBCuq,iTsyac,iWP1Yb,icmqKf,lPKSwe,lsjVmc,lwddkf,mNyZub,n73qwf,o02Jie,oWOlDb,pB6Zqd,pjICDe,pw70Gc,qfTGrb,qmdT9,rE6Mgd,rGAWrf,rHjpXd,s39S4,tfTN8c,w9hDv,wGM7Jc,ws9Tlc,x60fie,xQtZb,xUdipf,xiqEse,yDVVkb,zbML3c,zk0ux,zy0vNb/excm=_b,_tp,anonymousview/ed=1/wt=2/ct=zgms/rs=AOaEmlFEHEPDnnmKZbnTy6pY5x8uD7RFdQ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7595ebea1927a5a3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1077
Entropy (8bit):	6.062565804051903
Encrypted:	false
SSDEEP:	24:fAwwWR+XUWRgPObpuTpbbSMbQ8lK3rh0fP0bBMusNJvVRSllB:fAN9XUbPPxi8lKbZp4JvVoB
MD5:	B05DDDFC81ECDBF55712005557A1F5C6
SHA1:	7A6029CF8EBF3AE85DF0FD0A4CEE9454573BB0A0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7595ebea1927a5a3_0	
SHA-256:	5844B4406D81D6C0F89E5ED789534F31A90C7EA9CE363D847486CEFCA3E3B27A
SHA-512:	08BE43B5A9161DCC2C0A10ADDD29A276841C0587D362E2420A87B913511E6E9C75205D45053FFD20829897790ECC9C794B01A0AD7FF63C9FB3914B60F508F241
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<m...._keyhttps://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.AdsSettingsUi.en.54LqtFl99uk.es5.O/ck=boq-identity.AdsSettingsUi.afn1Y 1t3DVA.L.B1.O/am=lA/d=1/exm=LEikZe,_b,_tp,byfTOb,lsjVmc/excm=_b,_tp,anonymousview/ed=1/wt=2/ct=zgms/rs=AOaEmlFEHEPDnnmKZbnTy6pY5x8uD7RFdQ/m= n73qwf,ws9Tlc,IZT63,e5qFLc,UUJqVe,xUdipf,blwjVc,fKUV3e,aurFic,COQbmf,U0aPgd,ZwDk9d,V3dDOb,bXpTS,WCG2fe,WO9ee,A4UTCb,hPtwLd,O6y8ed,NpD4ec,PrP YRd,MpJwZc,NwH0H,OmgaI,HLo3Ef,x60fie,xiqEse,EcW08c,XVMNvd,L1AAkb,KUM7Z,rE6Mgd,WpP9Yc,duFQFc,s39S4,lwddkf,gychg,w9hDv,RMhBfe,SdcwHb ,aW3pY,YLQSd,PQaYAf,iWP1Yb,pw70Gc,EFQ78c,Ulmmrd,ZfAoz,CBlRxf,doKs4c,fgj8Rb,I6YDgd,xQtZb,lPKSwe,MdUzUe,QIhFr,JNoxi,CG8cBd,KTWBP,rHjpXd,yDVVkb ,pB6Zqd,SF3gsd,SM1lmd,iTsyac,hc6Ubd,SKhAfc,KG2eXe,SpsfSb,tfTN8c,o02Jie,VwDzFe,zbML3c,HDvRde,Uas9Hd,BVgquf,YTxL4,A7fCU,QLpTOd,UgAtXe,zy0vNb,i cmqKf,OgOVNe,RMwYNc,LGJfp,Zxe3i,qfTGrb,iBCuq,blf8i,PrUyhf,zk0ux,LFMxUb,QNqBAe,oWOlDb,qmdT9,pjICDe .https://google.com/(.].E./.....M.....O.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7a7a3044cc4ae692_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16891
Entropy (8bit):	5.968488609315371
Encrypted:	false
SSDEEP:	192:UGqpGAedsXE/mA/KlHggOA/mDG1vOCppgShskQPDD7zrBpvty3mvglaC9o6:EULsU+nlROCpvOCppYL3Bp1y3+glJo6
MD5:	2DD3A7C2D1B4C69993AC42F5BFF4DE17
SHA1:	8D1706C4FFE8DFBDB51075BDE24096B9ED644CD3
SHA-256:	FDDC7B636AB94B2DE4E3DC825E8152680C2A7B3F82EFE9661D4A4E83D38D54F3
SHA-512:	0825525B62622435B1CC2336AC74053833694E17FFEDA808885C94D9D0C9E4D651AA7C35A23601097B067F45A00D076181F1C1BBEC71825A8D2260C7A97CEA76
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S.....n3...._keyhttps://a.omappapi.com/app/js/webfont/1.5.18/webfont.js .https://coreldraw.com/cm..E./.....(uy..?]o.*v\>.u.Z..lc.K..p.....A..Eo....._..... .A..Eo.....'..@....O....p@.....(S.<..`0.....L`.....(S.q..`.....L`.....Rc.....v.....Qc.X.....document..Q.@..4.....window....QbJ.. .....aa....Qb~.....ba....Qb..I.....k.....Qb.xY.....n.....Qb*.....q.....Qb..> ....r.....Qb.....ca....Qb.?mx....s.....Qb.....t.....R....Qb..PC....v.....Qb.FU|....w.....Qb..47....x.....QbR!.i... .y.....Qb.....da....Qb".....z.....Qb.....A.....Qb.C.z....B.....Qb.....ea....Qb:..A....C.....Qb.-`.....D.....Qb..O]....F.....Qb.;.....E.....Qb.F&....G.....QbJ..p....H.....Qb...6....I.....Qb~?J B....ga....Qb..@.....ha....Qbf.....J.....Qb.Q.....K.....Qb.>w.....ia....Qbb..T....L.....Qb.K.....M.....Qb..!.....N.....Qb6 .h....O.....Qb..1.....P.....Qb..f(....R.....QbJ..`....Q

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7b33e1b314c92f93_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	271
Entropy (8bit):	5.580385883927089
Encrypted:	false
SSDEEP:	6:mU9PY71HEHIrDXtGUzfWNWLDhSYOmX1tg4hnvZMyJ16AD/hK6t:zIRwUTxDPHXRhnvZtJ16s/7
MD5:	E29CDA0A523D7418E0A293682AF6FA2E
SHA1:	05B376F0FDBA00BE1DD6FB1C014306D8DAEE3211
SHA-256:	2E0F3E4BEB9BABEFB5A0B3E16ED6630BC6FB8D95279C8BAF5CE6219CC0FDFA91
SHA-512:	77C432A7D6A127609FC8DFDFC859E88DE6B2E0B24A5E79B6AB30419A9EE820C0AA716009E5511FB47A75DD5BEE891464D18E252819888D10624584CB0CC7CD9 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R.Ok...._keyhttps://tpc.googlesyndication.com/pagead/js/r20201112/r20110914/elements/html/interstitial_ad_frame_fy2019.js .https://doubleclick.net/.iY.E./ .....b.....m..B..$..o...9.i.*.....v.....A..Eo.....9.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7b9cd0a6e51ca8f1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5069
Entropy (8bit):	5.969205080536246
Encrypted:	false
SSDEEP:	96:2sMjTeFSjatjSCG1VeaV4QH1IjCJ5EEu7AhJYCrnIA3TkTC2ZXoa:2PGSjatjSR1VFSe1IjwCvhTC2Z4a
MD5:	C898619CB615A2478019D5F138D85F30
SHA1:	1B8BAF02840F141F67A620D44C6A5A5C86FD05A6
SHA-256:	A68AEC39867FF9613B78638009300742D149736CDABA49DED780BD99EF4AB99F
SHA-512:	22419822FCF10D2AF1EE2EA92B171AFBA80B360B44EE4BE042549143A9C0701F94DE313A3C680DBCB644F5BD84F9CDBE7EF3906E4FC585006FE3A92C912946D 2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7b9cd0a6e51ca8f1_0	
Preview:	0\r..m.....u.....]...._keyhttps://www.coreldraw.com/static/common/scripts/dynamic-pricing/dynamic-promotions.min.js .https://coreldraw.com/....E./.....&|.ks[..hF...P.!O&.x...9.*..%.R.A..Eo.....I.....A..Eo.....'.."....O....0....H.....\.....(S.d..`..... L`.....(S...`.....@L`.....RcT....."....Qb.xY.....n.....Qb.....A.....Qb.C.z....B.....Qbf.....J.....Qb..O]....F.....Qb..~.....h.....Qb.-`.....D.....Qb.;.....E.....QbJ..p....H.....Qb.FU|....w.....Qb.Q.....K.....Qb.K.....M.....Qb..!.....N.....Qbb..T....L.....Qb:..A....C.....Qb...6....I.....O.p....$.....I`....Da.....D...(S.....Ia.....@.-....hP.....Y...https://www.coreldraw.com/static/common/scripts/dynamic-pricing/dynamic-promotions.min.js...a.....D`....D`....D`.....@...`....&...&....&....&.(S...Ia..../.....Q....q.d.....&.(S.....Ia9.....d.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\80b1748216058ce0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	22223
Entropy (8bit):	5.69162700680117
Encrypted:	false
SSDEEP:	384:4GHbeenbmDhTZGf3qtCfh4Sx4cW4LDbBMRiCKI4ZEJ4+u9:7TnEZztCJ4oTDZMRiA4Ks
MD5:	D64519359B2A8349F797A78D139F0034
SHA1:	3968D768894CDCE66E96EF265ABF41211EA03955
SHA-256:	417DE66221CB3F4FD76A35C02151D066DAAAFDC9321B62426EE78A52A5A33A00
SHA-512:	382635CB0E37F862602CD56EC5A14EBE19AC20EF3CD7C1EBBDBCD3DA6D683AA767ED625A04493CE304FDA04F779453DE9DE15C6EDB6022F9EF12383F57B21DE
Malicious:	false
Reputation:	low
Preview:	0\r..m....._.....o>...._keyhttps://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js .https://coreldraw.com/.L..E./..... R.S.....?.....4...x..*....?.A..Eo.....T.m.....A..Eo.....'.....O....8U.....|.....,.....(S.....`.....HL` .....Q.@b*....jQuery.....4Qk..!J&...Bootstrap's JavaScript requires jQuery...(S...`0....$L`.....Qb~.6v....fn....Qc.~.....jquery....Qc..wA....split.....K.....dQw..T.X...Bootstrap's JavaScript requires jQuery version 1.9.1 or higher, but lower than version 4..K`....D...(.....(...&.(...&.(...&...&.Y....&..*..&.(...&...&.Y....&..*..&...i.....*..&...i...8..&..*..g.....&...*..g.....*..&...i.....*..&...j..... &...&.%.e..."......(Rc.....I`....Da....t....$..g$.....P.. P.. ..."..."....@..@.-....PP.1.....C...https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js.a.....D`....D`6...D`.....`~...&...&..Q.&.(S.T..`b....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\831be288b6e21eaa_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	386
Entropy (8bit):	5.844469284350116
Encrypted:	false
SSDEEP:	6:mvEYk+tHzZCG6XLAGg0RS9U3RFgKTSPfOss4mYLRK6t4/awMSwcHPfOss4mYn:J+tHNyXngUS9U3RFhS3/G/bpH3
MD5:	C8DD19402204AE8BA91230FB7C03049E
SHA1:	4A426E3DAE1FA3A7BDC5CB9B17D3F5CE1BB33E44
SHA-256:	1A3C8BF499BA83EFB867E56AA1BB1C34AE1ADCB400BF4132C083A783591F6C73
SHA-512:	35ADC4EAFD671427D2F48A491DFCAE03C20C9DFE22E07C7E28F9F44506F86BEB408CBA9BE0BE04C570F56D5C496A9D2CEF14DFA65965C172E9B68DA0F99E1CE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....z...y....._keyhttps://static.zdassets.com/web_widget/latest/vendors~web_widget.ca239eb7094b76c34e1a.chunk.js .https://coreldraw.com/.<..E./.....#.....D..Q..t\..j.r .F60./k.A>Q.ut..7.A..Eo.....M~.....A..Eo.....<..E./.....5FA9900EAE98614DCA17D5EBE91D673C79F11948FB4808DBF7B9F16877AF5EA3D..Q..t\..j.r .F60./k.A>Q.ut..7.A..Eo.....X..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\84f9f4413dfeadac_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	20175
Entropy (8bit):	5.977277227728669
Encrypted:	false
SSDEEP:	384:v8TYr2TtV61aMpDqOnoDxMgTQFv4d9TS/iP:kT+2JMvsxfTSe9TN
MD5:	396C6175E8FD783CCCD278E498EA3CA6
SHA1:	39CA165CF035A7D1AFFFA5CB1143F1933FF475FF
SHA-256:	C01856E5CDDCB71F6A3BEF9F6C7637FC2552EE4CDCB656081F39863E050F0106
SHA-512:	C0DE1AE0A757294795B6E2EF724C4E7CF406FA003DB05AF85CC161900F0FAB991AB83C71FA8F35F07E600F54B156C8E7DB4D1CA9E2E587A230E216582D20457
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...r..X...._keyhttps://s3.amazonaws.com/cdn.aimtell.com/trackpush/trackpush.min.js .https://coreldraw.com/...E./.....(.+z...C'W5..`../.4..._.vmz...A..Eo.....E.....A..Eo.....'.....O....8M..c.FM.....4.....(S.....`n....M.L`.....e.L`..... Qf..p...._aimtellPushToken.... Qf..1b...._aimtellRanScript.... Qfri....._aimtellSubscriberID.$Qg..&2...._aimtellRefreshResult.....Qd.Kt.....trackData.... Qf6.bP...._aimtellTrackData.....QeB#....._aimtellDebug.....Qe./.c....aimtellDebugBox...Qd.*....._aimtellAPI.. Qf..w....._aimtellSWInitiated..$QgVK....._aimtellNewSubscriberID...QeJ.n....._aimtellVersion.. QfVcW....._aimtellDebugQueue...$QgV....._aimtellDebugQueueActive..Qe...f...._aimtellPrompted.(Qh...2...._aimtellUserDefinedWorker....(Qh..Y....._aimtellWebsiteConfiguration. QfR....._aimtellFunnelPixel..$Qg...Q...._aimtellUpdateViaCache... Qf....._aimtellWorkerScope..,Qi..#S...._a

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\86c674a180e61231_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1050
Entropy (8bit):	5.4965120903196985
Encrypted:	false
SSDEEP:	12:++xUT7WSm3E+xU4tF7ISmVTE+xUrSHFSmaE+xUVVtKYSmQlTE+xU/lHqSmg:+w/3Eata/lEu/aEaY/Q1ExY/g
MD5:	1314227FD3F022413F946FE7BD3229D8
SHA1:	02CAFA81849500647C79239F8339A7B535AD85B4
SHA-256:	6C5AAD575107DA9154F2518341800EC173AAA45C89D36E78D65E60E9F323EC4E
SHA-512:	CB1E06E13D8583D4F9629DF8A34743F059B047117D2A0CA57622E85BBD786F9E867CB1F37E8F1437C1841F25F15BA457D2065A268803D947542D046E9C6CAE3A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N.... .r...._keyhttps://static.hotjar.com/c/hotjar-1403528.js?sv=6 .https://coreldraw.com/]...E./.....j.....E..}{.B\.h.3R<..5h..e_.*|.@}..A..Eo.....A.. Eo.....0\r..m.....N.... .r...._keyhttps://static.hotjar.com/c/hotjar-1403528.js?sv=6 .https://coreldraw.com/.0a.E./.....E..}{.B\.h.3R<..5h..e_.*|.@}..A..Eo.. .....X.....A..Eo.....0\r..m.....N.... .r...._keyhttps://static.hotjar.com/c/hotjar-1403528.js?sv=6 .https://coreldraw.com/..w.E./.....E..}{.B\.h.3R<..5h. .e_.*|.@}..A..Eo.....u.....A..Eo.....0\r..m.....N.... .r...._keyhttps://static.hotjar.com/c/hotjar-1403528.js?sv=6 .https://coreldraw.com/....E./.....).....E..}{.B\. h.3R<..5h..e_.*|.@}..A..Eo.....E1t.....A..Eo.....0\r..m.....N.... .r...._keyhttps://static.hotjar.com/c/hotjar-1403528.js?sv=6 .https://coreldraw.com/..#.E./..... .?.....E..}{.B\.h.3R<..5h..e_.*|.@

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\88626338336e809f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	353
Entropy (8bit):	5.729996642090493
Encrypted:	false
SSDEEP:	6:mKdY71HEHIrDXtGUzXeCBFG3dhSY1tgLpMJtJmYszDK6thtgPYtpMJtJmYm:WRwUCCBFGtP1tQpMHJmpLt7pMHJm
MD5:	B26CE459CC37F33BA4CADB448747C95C
SHA1:	C3FA4B20FF84FFBE97238F7C4A4517C912EEAB44
SHA-256:	2ABF0A5C9225851D0F2979D641309A44F9F310303D62089F295FC71F18EE87E7
SHA-512:	AE5EC2BA29537CED0BAA20FD1B986378144165E350503A461E04A53A8C2F09E509B11E3786ED007B46B4405DCAF0AEBD4AF4C05F9A294AEB70645C9C0D815E 4
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://tpc.googlesyndication.com/pagead/js/r20201112/r20110914/client/one_click_handler_one_afma_fy2019.js .https://doubleclick.net/..R.E./.... .....W.:.7.....IR....."F....59..\.&..A..Eo.....}.....A..Eo.....R.E./.....W.:.7.....IR....."F....59..\.&..A..Eo.....P.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8c0eb26288a7740b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	369
Entropy (8bit):	5.837912100213622
Encrypted:	false
SSDEEP:	6:mgPYk+tHzZB2REJn9UdLFg4imf3rvTrZK6tM/M2eTbSxfh4UU9f3rvTD:pb+tHNB2Rm9UDzbvDi02MufhhUNv3
MD5:	B77F8C39A4AEB93D04DDAF496FFE4001
SHA1:	1D6C5A51668CC32C765A0A7C6041003F641BA76D
SHA-256:	B0C69A6ABB050AB7AA37984080A59C888AEB32CADBEAC3EB25D4810C6F63446E
SHA-512:	B66CC24097F6F7A93F14C1E7948C564B1675F141857E7367EAB4E2F05D57D9325E114A6358798659A54EC4801DD28610439F92A08F60AF62D0A3A64B6BED9024
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i.....dc...._keyhttps://static.zdassets.com/web_widget/latest/preload.b134a3818b60177eac5c.js .https://coreldraw.com/S>..E./.....8.>.[.c.i..Q.N.LyjA0fsL B.....A..Eo.....iRLI.....A..Eo.....S>..E./..(..B8F52DF74279547B66CE2C2B060D48FECA86A1C103C064924BC1DCA2944A79298.>.[.c.i..Q.N.LyjA0fsLB.....A. .Eo.....A..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\91c56cc36baae634_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.468203416863709
Encrypted:	false
SSDEEP:	6:mfYk+2iKxR9KuRHsAuSYQCg4lWyctWMcgr9qhZK6t:++2iKxxshAyctWMclp
MD5:	BFE2AB5A3569814FEF91A7D56C09D078

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\91c56cc36baae634_0	
SHA1:	8835372B84C72ED185304A6197EA6EDA2F92FCC0
SHA-256:	8FFF1348023F5E3EED018E7CE59B4FCEC26C9F6C73FB7409533258738DDB2488
SHA-512:	2ABB55FAB926EEEB6614B5B9B567DE8F04F3D2792519D2ABFA8B79372C1BDF1EDF27226E29C763D05A5B1C1A4F47F75E60187E16BCB46423338669E89345E09
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T.....|...._keyhttps://static.adsafeprotected.com/passback_300x250.js .https://doubleclick.net/l.d.E./.....f.M.(-..-y.Ob.H..Z..!k..P>...!..A..Eo..... .A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9434ea2adb137364_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	331
Entropy (8bit):	5.779770495263241
Encrypted:	false
SSDEEP:	6:m7vXYFxUKWKaUBTgEtQJ2vhR3UL446DK6tJXvR6m0p3pKovhR3UL4:MaxT/aUBTfQkhaH61jXkDprha
MD5:	CE7ABC294DAD2694C3EAE10D8E11BC5E
SHA1:	B25D8163CCF7067712D7AAB509854D29EADD6C93
SHA-256:	339E0212006C75CB8571D6A7D9E0DAC9C70EEC1BE44E7A1E3F98DF5661FCC13A
SHA-512:	9F5DD4942C4372FC2123AE646E8039D58694C34CE68B879739A07C350DEA16A46F5C149BE60D199E56EAE0E6BA65DA5B1BB39ED77D49D7EF769D65EAC6658D A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....C.....G...._keyhttps://a.opmnstr.com/app/js/api.min.js .https://coreldraw.com/....E./.....2R...3....$`..2w.4R.1..q..\|..A..Eo....._.....A..Eo.....E. /.....26F2672139B15616E1D29CCDDBB14265E2A74D618E5778476371FF186CF83A16.2R...3....$`..2w.4R.1..q..|..A..Eo....._Yl0L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\94c05e03bdf09fdf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	238
Entropy (8bit):	5.489632192026888
Encrypted:	false
SSDEEP:	6:muqg/VYw1yGSVUf4adTE51yGfHgZuS4qlWYAZK6t:Zqg51yGSKf4YTE51yGfH/SRloT
MD5:	E02DAB7667908417C03ED965F9467EA9
SHA1:	6D0A3049CCD09E5ADFEB167229C83F02BFDB34A2
SHA-256:	AE85C135BBA0FE6685C201D924BFC0E47BE33F1CDD767810730FD1177F327567
SHA-512:	A466659E3E4F21F8B3F3DDAC7FE975D71296B4C9DEEDBE360D64DA56A4BCD075B2569CC06FADBA8E647AD1817886BE684E5F5C365C7563FF67AEE113287D83 89
Malicious:	false
Reputation:	low
Preview:	0\r..m.....j...c(].....keyhttps://otampadabola2.com/wp-includes/js/wp-emoji-release.min.js?ver=5.5.3 .https://otampadabola2.com/.MC.E./.....C.....Eq.....i..W..... ....g.)]..A..Eo.....b.{.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\996bdcade1a612cc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	104456
Entropy (8bit):	5.794184290655512
Encrypted:	false
SSDEEP:	1536:pxPvvhepD7chfIJZxC5sJFeKxVOAJ74LAe7jPS5ebVwnGyOSj+qkqK:TP48InxtJsqVHOAEPSlhSXLj+D/
MD5:	5ADE7F3A38EFC6EB4D834533B2C932B4
SHA1:	ABD42803C8E756250C04C1F9A1C466957B5A1C26
SHA-256:	12108D36470742BA8C5A44E49CA664E9F1F5ABC80CD87DE3CAA9D46A8F0352B6
SHA-512:	8AC0B05395F46B926A505079D5FC9132C819070BD5EB5D7C5D610DE3E830673AE7676A0708A1B3C4B7B092E4CCDB91D0FB09E88CABD88BEA5B4F8A8BB1C7A8 C1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....G....B9007B2F10CB0052CAAF99534036C4DA4984A0D63F76BACE3352240373BEC22D.....'..v....O#.....2..(.....d....&.....`..... .....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....N.....Q.@.....module....Qc>.....exports...Q c.X.....document.(S.....5.a.....a.....a.....a.....a.....Pc.....exportsa....!...I.....@.-....HP.....;...https://ajax.aspnetcdn.com/ajax/jQuery/jquery- 1.11.2.min.js.a.....D`....D`....D`.....]....`....&...&..!.&....&.(S....&..`8M.....L`@.....Rc.....8.....M...Qbb.....c.....QbN..$....d.....Qb..M[....e.....Qb.....f.....Qb..~.....h.....S.. .Qb.0.p....j.....Qb..I.....k.....Qb..N@....m.....Qb.xY.....n.....Qbn.....o.....Qb.e.....p.....Qb*.....q.....Qb..> ....r.....Qb.....t.....R....Qb..PC....v.....Qb.FU|....w.....Qb..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\99cf79b1ac0d33bd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1227
Entropy (8bit):	5.516784030030112
Encrypted:	false
SSDEEP:	24:HB6qL9PLiVeo3Bl+QpRM9M0hANsIRxoPoEb:h6Y9zi8kAZ91gEb
MD5:	CF711A21A3AB1F0D8BF45ACF494E27C6
SHA1:	F85ECF4156D893677E2693BF1AFE27BCA85B3A02
SHA-256:	AC938455488575118A3386E43A647143135C5282EAF55FBBAD973ADE1E65AEB1
SHA-512:	C66A1AF9F0AD08A71EBB86299B7452A673338DC37214A3BD1754BB4A808089924983D6CF6C171AA8C0AD033D484518A9600B566419F16C0F8A997BC2199C63AE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....[....R)p...._keyhttps://www.coreldraw.com/static/cdgs/js/imgslider-1.2.1-min.js .https://coreldraw.com/]6..E./.....H.g....}..R....W.q.s.mZ..A..Eo.....E.!... .....A..Eo.....]6..E./.....'.M.....O....h.....i.....(S.8..`&.....L`.....(S.X.`j.... L`.....0Rc.....Qb.?mx....s...`$...I`....Da.....Qb~.6v....fn...(S. .....Pd.....s.fn.slider.a!.....4..k%...../.....I..A..@.-....LP.!.....?...https://www.coreldraw.com/static/cdgs/js/imgslider-1.2.1-min.js.a.....D`....D`v...D`..... (...`....&...&....&.....D`....DI]d.....Qcf.U.....slider...,..a.....Qe...$....triggerEvents.....Q.@.....click.....Qe&.#.....initialPosition...Xa.....?..Qe.....showInstructio n.G..Qe*.....instructionText....U.bB#.....!....Qe..j.....defaultOptions....K`....Dp.....%.....&.(...&.....-.....&.(...&.(...&.)..)-.....c.....P.S.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9bef09f720f32f4f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4970
Entropy (8bit):	5.800354365790938
Encrypted:	false
SSDEEP:	96:lxBu7LowmgIQ5PbNzQG/0dweS60/KprFrs:ljuguISPbNzQa0dwZvK7rs
MD5:	7743E08FDBF6700A3958D43D6215BDF2
SHA1:	E05ACB71FA55C4DF2985FE7072BA76A850F52F61
SHA-256:	AEFA198381D93565020051D7C48D561A035ACECC531314895CA5E54966385F38
SHA-512:	0A81086248D5655665594BCB50EF0F68432EA6F22C8719CF657CFB9C59A7438451E6791BEA13384ED65C5C3508134E643A4AAB1C6CAABC7D391F82524DEA7FE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....j....X&...._keyhttps://www.coreldraw.com/static/common/scripts/jquery.lazyloadxt.extra.min.js .https://coreldraw.com/A...E./.....~)L.$....FC=...P..... [E.c..A..Eo.....b.....A..Eo.....'.....O.....(S....`v....,L`.....(S....`.....L`L.....Rcx.....4.....Qbn.....o.....Qb..M[....e.....QbR!.i....y.. ...Qb..N@....m.....Qb.e.....p.....Qb.FU\|....w.....Qb:..A....C.....Qb".....z.....Qb.;.....E.....Qb.xY.....n.....M...Qb.K.~....T.....Qbb.....c.....O...Qbb..T....L.....Qb...6....I.....Qb..> ....r... ..QbN..$....d.....Qbr..R....X.....Qb.C.z....B.....Qb..I.....k.....S...Qbv\(.....I.....R....Qb.?mx....s.....Qb.....f...y....$.....$..... .....I`....Da....4....(S.....Ia.....a..@.-....\P.a.....N...https://www.coreldraw.com/static/common/scripts/jquery.lazyloadxt.extra.min.js..a.....D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9f26e8b3e5102250_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5206
Entropy (8bit):	5.73709542796014
Encrypted:	false
SSDEEP:	96:r2+/xdaNGW7h/jdkpJSaV3V9xQk+FPj0ejNJpOl7+YzR3aQG:rAZeSaV37Wku0ejNJpOlfz1XG
MD5:	BA5588327EB960800C3221C960A02BBB
SHA1:	0FB70F3CD6D675BF1B87FE90A34C1E4424CA8EAD
SHA-256:	533D92AD0ED9B9D5F1FC0CEB66C55518BC992862F629742D9F237C8046CAB570
SHA-512:	8359F1ABBA389C84120BA07CCC5809A888353D524060AC325D138251034B3F4CEBDE205AEAE114ACED20A9902DE9CC79155167AB4E78C850E0CD56E0D5B123 4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....n....._keyhttps://www.coreldraw.com/static/common/scripts/omni-tracking/omni-tracking.min.js .https://coreldraw.com/x...E./.....V?8..'..g.K..Jrcw ..P,...u...A..Eo.....O..N.....A..Eo.....'.H.....O.....L.....h.....(S.\..`t....L`.....L`.....(S.....Ia....8.....Qe>.y.....omni_trackEventsE.@.-....`P.q..... R...https://www.coreldraw.com/static/common/scripts/omni-tracking/omni-tracking.min.js..a.....D`....D`....D`.....T...`&...&...&....&.(S..`B.....L`@.....RcH.....Qb..> ....r.... ..S...Qbn.....o.....Qb.....t.....M...Qb.?mx....s.....Qbb.....c.....QbN..$....d.....Qbv\(.....I.....R....Qb.....f.....Qb.e.....p.....Qb.FU|....w.....Qb..N@....m...m..... .....I`....Da....F(...(S...IaS.....d.....(S.....Ia.... .....Q...d.....(S...Ia*.....d.....(S...Ia.....d..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a2c4f6175af1bd71_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	801
Entropy (8bit):	5.8732046232410005

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a2c4f6175af1bd71_0	
Encrypted:	false
SSDEEP:	12:xwE3HypZnuux2pHgyyyJ3CMxok04pAhiyt3EIdv5KEPCSVA3hCRUlTtcYD:xwEipZuuyAyyASb9hdt3EyrP58C87
MD5:	9990A522E1B769252271412264851A540
SHA1:	14D20B861B57B21CBE98E5DD9922883DBEF2D741
SHA-256:	7D51BC257E587E1FDD9669CC1981DC999FADFA332588E59FA610DEF37039BBBE
SHA-512:	916D3736DD9F37620E0764029D0D1E1DE33247B23595883FCF7CC99D8274E6D3F0E4C765654FB7F224CC54E8261EF7F8F777500637D18E0EE497CDC0ABE1505E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a..q...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/956202557/?random=1606041523893&cv=9&fst=1606041523893&num=1&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-480&u_java=false&u_nplug=1&u_nmime=2&gtm=2wgb41&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fwww.coreldraw.com%2Fbr%2Fproduct%2Fcoreldraw%2F%3Ftopnav%3Dfalse%26trial%3Dbig%26sourceid%3Dcdgs2020-xx-ppc_ron%26x-vehicle%3Dppc_ron%26gclid%3DEAIaIQobChMIisv7lIKV7QIVAZd3Ch3Nxwv2EAEYASAAEgI0ovD_BwE&tiba=Software%20de%20design%20gr%C3%A1fico%20%E2%80%93%20CorelDRAW%20Graphics%20Suite%202020&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://coreldraw.com/J...E./.....~.....*0...'O.I.i.O.U...4.q.....%.ft..A..Eo.....z.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a40672e534fe8c73_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1922
Entropy (8bit):	5.399575254250452
Encrypted:	false
SSDEEP:	48:An+IJn5LSy8DsZFIbrE1sF58r2GSCsiEfezjDRx9TJHQnHOL:AnzJnxS6FIF3bCsQFVwn8
MD5:	9CD6A1B3EE318E748452F42E6F965375
SHA1:	B3F6048C6E487E84B64C3EDC4585462CA6E0E3B2
SHA-256:	528C81D776CD4642F430E06BBCD91D404C5298BCBAD98B1A72BEDF4E237DDD64
SHA-512:	0C5CC63F8A5252B9175785F6410960D76226604B2F28EDB8C0F6808124AD79D1184C214DA7E9484C581D4FD97B7A45E3AD0AB4C3C26B36EC033D8465A22567F8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z....KX....._keyhttps://www.coreldraw.com/static/common/scripts/gp/main.min.js .https://coreldraw.com/.B..E./.....g..p..0...*.....h.....n.A..Eo.....:.....A..Eo.....B..E./.`.....'.2.....O.... ...L8!Y.....t.....(S....`.....$L`.....`L`,....(S.....Ia.....Qd.q.....initPopups..E.@.-....LP.!.....>...https://www.coreldraw.com/static/common/scripts/gp/main.min.js..a.....D`....D`"...D`.....t...`6...&...&....&.(S.....Ia....X....D..m.....(]@.....d..... .....d.....Qd.....initPopup...E....d.....D&.(S...Iao.....Qe..Q.....loadheaderonly..E.d.....&.(S...Ia4.....,Qi6|.j....getQueryStringParameterByName...E.d....&.....&.(S...Ia....N.....QeZ*u.....getCurrentRegionE.d.....&.(S...Iae.....Qe~?.;....getQueryString..E.d.....&.(S...Ia8.....Qe"2^.....set

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a5908dada370f37f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	940
Entropy (8bit):	5.470538454078259
Encrypted:	false
SSDEEP:	24:CHaWVkOgHabPzpgHal5gHaj2zgHaLTON:CXkOg2Lpg45gG2zg6q
MD5:	70C31F901A571491874D8D2D246FB85B
SHA1:	EDF6AEB197FCC414D463ED9C5C8E1D6CD38060E0
SHA-256:	A873474EC9F15525811E9CB4AAA65F933965930FBE91AB1A972CA13ABA14E470
SHA-512:	1A8BE5EC9FDB511180BB81258F901B65776AAFB23580C08FE98DB86D758EDFCA3EF7683A3060412062DBC5729F05241E74B59021083FD20EE8BD7594D43D59A2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....8.../..6...._keyhttps://cdn.ywxi.net/js/1.js .https://coreldraw.com/.6..E./.....d.....k.k.$.!..%.B..Y-.l.@...j6...A..Eo.....+`.....A..Eo.....0\r..m.....8.../..6...._keyhttps://cdn.ywxi.net/js/1.js .https://coreldraw.com/v.\.E./.....k.k.$.!..%.B..Y-.l.@...j6...A..Eo.....V.....A..Eo.....0\r..m.....8.../..6...._keyhttps://cdn.ywxi.net/js/1.js .https://coreldraw.com/.:n.E./.....4.....k.k.$.!..%.B..Y-.l.@...j6...A..Eo.....F.u.....A..Eo.....0\r..m.....8.../..6...._keyhttps://cdn.ywxi.net/js/1.js .https://coreldraw.com/....E./.....(.....k.k.$.!..%.B..Y-.l.@...j6...A..Eo.....)..q.....A..Eo.....0\r..m.....8.../..6...._keyhttps://cdn.ywxi.net/js/1.js .https://coreldraw.com/Kd".E./.....?.....k.k.$.!..%.B..Y-.l.@...j6...A..Eo.....k.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a7093c940d86fb27_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	801
Entropy (8bit):	5.891380067062155
Encrypted:	false
SSDEEP:	24:vhHEipi/uyAyyASb9hdt3EyrP58CBgEYC:5HEip6urxRh3l2C
MD5:	9E5D50739BC35DF9CA3031667699F694
SHA1:	9902C667F00FB0A1C4A1F4302A4D44D2FF675FC5
SHA-256:	51D77362D71E0976E1E1DA3E4AD77D4684750785896D3130B70811C8B6341BF5

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a7093c940d86fb27_0	
SHA-512:	E9656323FFB85E7E5D7B57B70E1DF3C4380DD9CA7D2A68D9C194D8869326FB23E60B5F758675D32C21926B61C33D6771D76624A92CD54A47877FDDC8750215A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/956202557/?random=1606041559417&cv=9&fst=1606041559417&num=1&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-480&u_java=false&u_nplug=1&u_nmime=2&gtm=2wgb41&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fwww.coreldraw.com%2Fbr%2Fproduct%2Fcoreldraw%2F%3Ftopnav%3Dfalse%26trial%3Dbig%26sourceid%3Dcdgs2020-xx-ppc_ron%26x-vehicle%3Dppc_ron%26gclid%3DEAIaIQobChMIisv7IIKV7QIVAZd3Ch3Nxwv2EAEYASAAEgI0ovD_BwE&tiba=Software%20de%20design%20gr%C3%A1fico%20%E2%80%93%20CorelDRAW%20Graphics%20Suite%202020&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://coreldraw.com/.h,.E./.....@.....&..._D.S.K.Xo..oj..-...P.-.AV..A..Eo.....T.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\aba8b2f5a80a0575_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	244
Entropy (8bit):	5.545090946892745
Encrypted:	false
SSDEEP:	6:mOXYk+tHzZM9voE7WS9U52ugk//eersry/m41hK6t:/z+tHNGvoJS9U5X3SId
MD5:	190394C9B0C9E730AA2C305BFD34D1DF
SHA1:	C414FC3ACA3DF5B17BE05DDB350F56AC2ABB415B
SHA-256:	1F1F817D45F090F0F751045D2A4A7939068FF6384EBC8D153BFEF791C80562B3
SHA-512:	64A69313D60BEE53D9E9C9010BBA9EA330F70C0440F0B1F1C1F79E9ADD125FC58C30DD8EEE34855E8721141510ED0E49AD0E50E66EF557FD463D2BED2C02659
Malicious:	false
Reputation:	low
Preview:	0\r..m.....p...Xn}....._keyhttps://static.zdassets.com/web_widget/latest/chat-sdk.cec40ba63b2a85de0a9c.chunk.js .https://coreldraw.com/...E./.....3...N.."Su..j%..RShL....}..P..A..Eo.....4w.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\abcafd9c117cf694_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1836
Entropy (8bit):	5.542946449053431
Encrypted:	false
SSDEEP:	48:qnQ7y+1d2T3qQ4wFtUD2uXH6dKB8fKo/O:U9fpFtUCuXH2i8fKMO
MD5:	E9F8AB5845EDAB9D016F2FBFF35EBA02
SHA1:	FC49D06D2A7EFC91C20F8D88AF2D4D3532352096
SHA-256:	34A16088BA2C0ACBF1BF72DA4B9B2C9BA0909D4CE67306B2A8AF988BDF9EE85A
SHA-512:	1B3E0B5C1421E322D5B7F03C336996B7165BBBA616F7CBF480802ED43145DB7E9A302EC149D9CC284808539F02F4121ED45FB66AB920D529FD807D006C27C3C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....D...ks.?..._keyhttps://munchkin.marketo.net/munchkin.js .https://coreldraw.com/....E./.....%.....V.p8a(h.....k.?2...r..^.d....A..Eo.....J.....A..Eo.....E./. .....'.....O.....5.....(S.4..`$.....L`.....(S...`.....@L`.....pRc4.....O...Qbb.....c.....Qb..M[....e.....Qb..I.....k.....Qbv\(.....I.....Qb..N@....m.....Qb.xY.....n.....Qb..~.....h...h$.....I`....Da.....Q.@.....Munchkin..Qc.X.....document....a.....y...Qb|.....159..(S.....a=.....@.-....4P.....(...https://munchkin.marketo.net/munchkin.jsa.....D`....D`....D`.....(...`....&...&....&....&.(S.....a.....d.....d.....D&.(S.....Pc.....h.init..a:...N.....Qb..%.....init..d.....&.(S.D..`@.....L`.....4Rc.....O.`$.....Qb.e.....p...`.....q.a.....(S.....Pd.....h.<computed>ar.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ad5c3af72a4b1a91_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	6695
Entropy (8bit):	6.376713436800273
Encrypted:	false
SSDEEP:	192:D472ovFEqCYd0VZDFTt1hob7AJ3B4FTj2lFT9m:Dx3K0DFp3ob7AAF3iNs
MD5:	625CF39837EC231F992AD0D45214E579
SHA1:	708E7712893A671531588CB46529DAA2881D47D6
SHA-256:	FB73D690DA1364EE4E7FD53A3B37695D304B418AFDDDF9398BDE6794EBD9636B
SHA-512:	0BD6E6A37C8A853D313E8CA88DEB29E41FB7E4E441374995D2C98FC3B7E320FB4A72FA08E3FCDC373282B425F4D24E4619F263980CA711AB3EE19E67B210139
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ad5c3af72a4b1a91_0	
Preview:	0\r..m.....W....Id*...._keyhttps://www.coreldraw.com/static/cdgs/js/trial-installer.js .https://coreldraw.com/...E./.....}.....0.....*.LM.q..s..7i.b...!...,.A..Eo.....8.SI.....A..Eo.....'.j.....O.....<.....(S.%...`.....L`.....tL`6.....Qc..n....urlQuery..Qb. A.....now...QbJ.....time..Qc.6H<....hostName..Qc.K.-....pathName..Qe~Q._....source_id_cdgs....Qc.. Q....cdgsId....Qc&.$.....cdstdId...Qd.-.....elementid.....Qd.....cookieName....Qc..?$....prodId....Qc&.....product...Qd.E.5....siteCookie....Qb6..1....ref...Qb.NZ^....req...Qd..|.....countryCode...Qd.....euCountries.. Qf.Jz.....installerServerPath...Qdr.X.....trialElement..Qe.....trialElementFlag..QdN.2.....sub_urlQuery....,(S.X.`j.... L`.....Q.@..O.....result....Qc..4.....window....Qd~.|.....navigator.....Qd.....userAgent.....Qc.}.....indexOf...Qb.>H.....Mac...K`....Dp.....&.(...&.(...&.(...&...&.Y....&...g.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\adba8338fc9be233_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	213
Entropy (8bit):	5.538339639021765
Encrypted:	false
SSDEEP:	6:m9tVY71HEHIN0ByjSYYugoXKHOzpYDDK6t:It6Rl0By1Yu3X0O41
MD5:	86CF4C9D9873C358ADA8EFEB68369D83
SHA1:	1CD86478561D58B62BBD8154C42835288EB4312D
SHA-256:	CC6D179BB84B157BF2FEABA745827510C355AF836661C19216A828CE7CF72C04
SHA-512:	8215E7360B08FFDA120C3C383A4416FD4856F0A114B72D5E485DD05768C3AB1FA1D8A4EA2381CD7CC7E527046EC160B3DA7275FAA01272BA7CAAAF6BB9F9411
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q.....M....._keyhttps://tpc.googlesyndication.com/sodar/UFYwWwmt.js .https://doubleclick.net/..].E./.....<..}..M.[.wE.i..1...p.?!^S.....A..Eo.....I.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b013e589bf9d74ca_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.924256824906119
Encrypted:	false
SSDEEP:	12:0v9wwWRonXP8WRo9AsMPCkvi7VXHtcmEaVGT:gwwWR+XUWRtsMPC4m6awT
MD5:	39C92D7AAA4129DAEDD4C6882119B529
SHA1:	6D617A25A396AA199287542C5709D06A106295AC
SHA-256:	63A150122D34F54E99990C4FB57099366BD6D6842E82F0BC4DF43BC94614FA8C
SHA-512:	0E5C376C6084CD600EE8DA9FF1134F72DCB00EE996583487B161493C78152DB760CCAA2C864AFA947DD14AB01D04F892240C31E6077C260C83E62706D9E24B6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....).....u...._keyhttps://www.gstatic.com/_/mss/boq-identity/_/js/k=boq-identity.AdsSettingsUi.en.54LqtFl99uk.es5.O/ck=boq-identity.AdsSettingsUi.afn1Y1t3DVA.L.B1.O/am=lA/d=1/exm=_b,_tp/excm=_b,_tp,anonymousview/ed=1/wt=2/ct=zgms/rs=AOaEmlFEHEPDnnmKZbnTy6pY5x8uD7RFdQ/m=byfTOb,lsjVmc,LEikZe .https://google.com/.X\.E./.....L.....Z.....J...Rk.j....Mp..!.....A..Eo.....+.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b1eea72a9a753c29_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	349
Entropy (8bit):	5.863596488606509
Encrypted:	false
SSDEEP:	6:mhkYMHAJnE5sT9U6gIIMj0Kp3T6ADSvDK6tdTpFjm2n0ScVd80j0Kp3T6A5plll:acO0shU6qjzhGWSv1jTnlII0jzhGYD
MD5:	F638B788B38DC27C84839656314CB5AA
SHA1:	C26C553BE14BA40440479F930885F186A4E627CF
SHA-256:	139D8E5F886F6EDF0D52EE7A453F57017762B19C6E0843088BB105218BF5B66D
SHA-512:	CCD028FA364C7FC191D675114B5B3A86E0EFC79A93F941EAB32E7650A5BBCFF12A2908719D1D813582B309A1F478FD06A2BAFCFE266C2F079028B8DE61C00F7C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U...b..m...._keyhttps://script.hotjar.com/modules.ae930258b2386dc57451.js .https://coreldraw.com/b...E./.....^.YQ.]...51.~g.d...9$..8....A..Eo.....A..Eo.....b...E./.....1C092C672D4F7D73670CE450F03197467DBDA211B5B33A350BE79B09F83935E9..^.YQ.]...51.~g.d...9$..8....A..Eo.....R..ZL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b4f06185546248b4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b4f06185546248b4_0	
Size (bytes):	801
Entropy (8bit):	5.910456602962065
Encrypted:	false
SSDEEP:	12:dqjE3HyprYKnCnux2pHgyyyJ3CMxok04pAhiyt3EIdv5KEPCSVA3hCRURkQp:+EiprdCnuyAyyASb9hdt3EyrP58Crw
MD5:	B0E59F0D2F938085F66938F688996DEE
SHA1:	425D78F814B5A878D2AD1BAA3DAC849A7A331A6D
SHA-256:	AB0B5916080B2F1AB55678F4512F3499012CCAAB618BCEFE72EB132F7C342047
SHA-512:	44053B0DA93C5F143B6901A68981EB74DE96CBCF07E7506FA49B6A8753F4997D57AD0C6435EDF23EA2490FDC9FCE1B70AA4AFC2E5AE1F09F806EC3AF4B48A123
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/956202557/?random=1606041529983&cv=9&fst=1606041529983&num=1&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-480&u_java=false&u_nplug=1&u_nmime=2&gtm=2wgb41&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fwww.coreldraw.com%2Fbr%2Fproduct%2Fcoreldraw%2F%3Ftopnav%3Dfalse%26trial%3Dbig%26sourceid%3Dcdgs2020-xx-ppc_ron%26x-vehicle%3Dppc_ron%26gclid%3DEAIaIQobChMIisv7lIKV7QIVAZd3Ch3Nxwv2EAEYASAAEgI0ovD_BwE&tiba=Software%20de%20design%20gr%C3%A1fico%20%E2%80%93%20CorelDRAW%20Graphics%20Suite%202020&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4.https://coreldraw.com/&zk.E./.....k.....7.....]N..*.|..Ei}5..Q..UW...A..Eo.....'.N.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b7ae806201a9b4a0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1065
Entropy (8bit):	5.680632202033243
Encrypted:	false
SSDEEP:	12:i/f3UB7Tn6s/f3UJHLnys/f3UAAnKs/f3UCEnhs/f3UMXV8nDp:iyX6sgys8Ks+hsj8d
MD5:	DD8ACF19CFBC3952A3BD5AA3DA95C776
SHA1:	305F31F6D1852DDBDD614E0690B14C502A5CF960
SHA-256:	D84BC18123E12C02F15229FB75C92A8D0DD94686E150B7E7C0CCFE029DD82743
SHA-512:	9D341E4FBB71195F2510FEAB3CD8CCE52B6BF4D4F6A719C7CEB2002768C26BF57D738878C60425CA105E980FE1D70C347CFAE081B10CEBAEE880F4C62FA185C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q...1..N...._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-5RC57S .https://coreldraw.com/.?..E./.....\.....%T...p..Df.X...!U>:.....A..Eo.....n.O~.....A..Eo.....0\r..m.....Q...1..N...._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-5RC57S .https://coreldraw.com/..S.E./.....%T...p..Df.X...!U>:.....A..Eo.....W.....A..Eo.....0\r..m.....Q...1..N...._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-5RC57S .https://coreldraw.com/.!f.E./.....%T...p..Df.X...!U>:.....A..Eo.....A..Eo.....0\r..m.....Q...1..N...._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-5RC57S .https://coreldraw.com/t...E./.....S&.....%T...p..Df.X...!U>:.....A..Eo.....A..Eo.....0\r..m.....Q...1..N...._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-5RC57S .https://coreldraw.com/....E./.....=.....%T...p..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\baf2fb638190cbf9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3588
Entropy (8bit):	5.391715726669494
Encrypted:	false
SSDEEP:	48:87er7MnEead7oEVMBdCqb495/yCAi9NE1CY8hPT5YdKEQuQBVSDqV2bRoFxquPgE:8lET7oSqCshCpuooQugSGVOR2qCl
MD5:	5DE1FAE4C9E4866065D568BED881A845
SHA1:	B4EBEEC79E5E0BC1D86B4792A1F8DE9DF119730F
SHA-256:	8F5FF2E89EFF2055530079853DB1C9F19BAF02D29A3034942B0CBA38ADF27286
SHA-512:	5CBC303A2D4960189E2B5FE3513B0694664C8BAB0D054D281495DEA0DC8F21952803FD0952A4CC6ED5B1FB62D37D8704DA258B8356203C6C22F1DF97EF9E7F4
Malicious:	false
Reputation:	low
Preview:	....E./.....'.z.....O....x...;.....@.....(S.8..`,.....L`.....Q.P.O.....setTimeout...(S.....Ia....v.....a.O..."....@.....@..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bc0307aec237d749_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.430876850084092
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bc0307aec237d749_0	
SSDEEP:	6:meAYGL+MIwJJm1yGyogiLgt7GhnLlZK6t:AIwvm1yGRi1GhRT
MD5:	C180A4E73147EF738FF651E9B0841D4E
SHA1:	63F36A59DAD253A029C7BC84FA8EEC7A1147CF20
SHA-256:	3C211155DC8726CEB3A03BCAB36B05C4AEAF725282A51C59D0A29F269C47840A
SHA-512:	854E3852C69BFCA1540B4AB5308F1A8D3FBC384AEEB4AF5F535809162DBC43878D57D34F41D053195D062734CB89E138A57EE642D523838FDDB9F539908FB3D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://www.google-analytics.com/analytics.js .https://otampadabola2.com/. D.E./.....Th..H.`.`.....S.F.Y.B.R..... .A..Eo.....r.....A..Eo.. .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bc2f3f3c4ccbc8ec_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.555564251287173
Encrypted:	false
SSDEEP:	6:mklVYw1yGSVUfIQKjWwpP1yGSr5ugeXe7fJWLk4/XhK6t:p1yGSKfIQKqm1yGSrM/ubYhX7
MD5:	E8135F912379F4EDFB9E7A1C76BB11FA
SHA1:	3854969839DF621EE7986E02CD5547ED8F4EA40E
SHA-256:	96A78EE6232F970AA0379473450E07494F5ED2DF160816BE86AE2745D332FE8D
SHA-512:	F1952F7EDC6B3BC301EA0A23B3E4B0AC3DAC249AD361EEF3D170A256645D88CBF3B8517117450C479518663385F30A882D638D935E74CFE47B7C3BB158E208C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g...d..$...._keyhttps://otampadabola2.com/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp .https://otampadabola2.com/w.@.E./.....J.k...}..T.a..g*XH.[.aq .0>....A..Eo.....n.....A..Eo.....

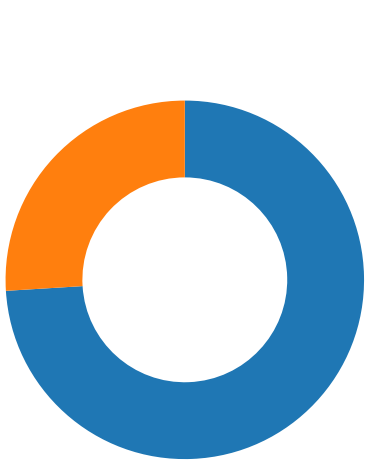
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bc8ac2c440ab98b5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	217
Entropy (8bit):	5.496793357320472
Encrypted:	false
SSDEEP:	6:meC//XYGL+MHMmb1yG/6tgDX5PRGANK6t:rCDHM61yGito04
MD5:	4FBA35D5C215FCC10F55DC034D27C2D8
SHA1:	A87B9AF17B6851728D234ABA825781801E45A627
SHA-256:	34F1474C75B4B598C2AA49E3CED770E17CC1313195B10560A5AF561C79926ED6
SHA-512:	FC2D525AF6BD6BA3E7535B93050DB93567DA7C607FC2F55B7FA4CE515D65A826801818696E48B3BA644DE9EB54374B2063CB9D1014E62FBD60189C44A6C2774
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U..."....._keyhttps://www.google-analytics.com/plugins/ua/linkid.js .https://otampadabola2.com/?cH.E./.....{.....z../...@\..(..I.!..6.A..Eo.....Z._..... ..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
Nov 22, 2020 02:38:30.128993034 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.130310059 CET	49726	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.155626059 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.155802965 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.156091928 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.156735897 CET	443	49726	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.156835079 CET	49726	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.157095909 CET	49726	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.182683945 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.183428049 CET	443	49726	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.185642004 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.185678005 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.185842037 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.186573982 CET	443	49726	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.186608076 CET	443	49726	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.186683893 CET	49726	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.388958931 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.389947891 CET	49726	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.391195059 CET	49726	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.391946077 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.394071102 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.415630102 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.415839911 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.416045904 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.416347980 CET	443	49726	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.416500092 CET	443	49726	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.416567087 CET	49726	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.417733908 CET	443	49726	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.417835951 CET	49726	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.418482065 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.418510914 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.442766905 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.459868908 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.737497091 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.749058962 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.816757917 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.844578028 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.844624996 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.844662905 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.844690084 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.844727039 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.844764948 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.844765902 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.844793081 CET	443	49723	104.31.68.76	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 02:38:30.844801903 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.844820976 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.844944000 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.844984055 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.845010996 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.845026016 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.845098972 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.934007883 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.934063911 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.934072018 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.934077024 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.934106112 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.934150934 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.934175014 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.934209108 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:30.961067915 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.961121082 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.961149931 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.961169958 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.961186886 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:30.961575031 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.016052961 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.016113997 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.016153097 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.016189098 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.016187906 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:31.016216040 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.016253948 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:31.016778946 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.016823053 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.016853094 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.016870975 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:31.016912937 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:31.017422915 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.021637917 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.021698952 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.021737099 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.021769047 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:31.021842957 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:31.021895885 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.022507906 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.022538900 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.022593975 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:31.022655010 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.022680998 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.022737026 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:31.022977114 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.023015976 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.023051023 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.023055077 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:31.023114920 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:31.023626089 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.023664951 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.023750067 CET	49723	443	192.168.2.3	104.31.68.76
Nov 22, 2020 02:38:31.024153948 CET	443	49723	104.31.68.76	192.168.2.3
Nov 22, 2020 02:38:31.024194956 CET	443	49723	104.31.68.76	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 02:38:22.085715055 CET	60831	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:22.123712063 CET	53	60831	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:23.352766037 CET	60100	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:23.380021095 CET	53	60100	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 02:38:24.152371883 CET	53195	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:24.190471888 CET	53	53195	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:25.182213068 CET	50141	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:25.218097925 CET	53	50141	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:26.607429028 CET	53023	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:26.647460938 CET	53	53023	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:27.941576004 CET	49563	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:27.968771935 CET	53	49563	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:28.972559929 CET	51352	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:29.000005960 CET	53	51352	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:29.704936981 CET	57568	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:29.740737915 CET	53	57568	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:30.078527927 CET	50540	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:30.080686092 CET	54366	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:30.083349943 CET	53034	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:30.090573072 CET	57762	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:30.091634989 CET	55435	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:30.116233110 CET	53	54366	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:30.118839025 CET	53	53034	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:30.118877888 CET	53	50540	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:30.125988007 CET	53	57762	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:30.137471914 CET	53	55435	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:30.404597998 CET	50713	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:30.460939884 CET	53	50713	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:30.529135942 CET	56132	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:30.572825909 CET	58987	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:30.573046923 CET	53	56132	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:30.599769115 CET	53	58987	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:30.936439037 CET	56579	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:30.972193956 CET	53	56579	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:31.113955975 CET	60633	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:31.114546061 CET	61292	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:31.132523060 CET	63619	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:31.133199930 CET	64938	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:31.140883923 CET	53	60633	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:31.160397053 CET	53	61292	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:31.168715000 CET	53	64938	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:31.188503981 CET	53	63619	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:31.367142916 CET	61946	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:31.406677008 CET	64910	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:31.412605047 CET	53	61946	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:31.450190067 CET	53	64910	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:31.541233063 CET	52123	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:31.584994078 CET	53	52123	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:31.596199036 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.619993925 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.620054007 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.621438026 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.621627092 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.631160975 CET	56130	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:31.645338058 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.645741940 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.658344984 CET	53	56130	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:31.668239117 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.668281078 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.668319941 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.668356895 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.668392897 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.668430090 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.668467045 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.668513060 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.668553114 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.668590069 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.668627024 CET	443	52124	216.58.208.34	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 02:38:31.668664932 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.669101000 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.669152975 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.669234991 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.669328928 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.669337988 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.669373035 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.669413090 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.679500103 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.679541111 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.679869890 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.680738926 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.680778027 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.680824995 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.680905104 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.681334019 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.682470083 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.682512045 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.682549000 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.682737112 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.684289932 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.684340954 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.684382915 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.684421062 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.684556007 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.684608936 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.685540915 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.685694933 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.696768999 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.696830988 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.697132111 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.697324038 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.697362900 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.697670937 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.697704077 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.697720051 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.697827101 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.699048996 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.699090004 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.699203968 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.700902939 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.700942993 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.700990915 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.701034069 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.701277018 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.701327085 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.701936007 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.717003107 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.717042923 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.717080116 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.717117071 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.717248917 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.717297077 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.717593908 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.717633963 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.717767954 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.718843937 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.718887091 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.718923092 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.718962908 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.719021082 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.719079018 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.720001936 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.720052958 CET	443	52124	216.58.208.34	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 02:38:31.720088005 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.720432043 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.720711946 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.737171888 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.737222910 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.737258911 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.737304926 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.737457991 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.737495899 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.739178896 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.739219904 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.739262104 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.739308119 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.739345074 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.739392042 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.739403963 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.739435911 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.739454031 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.739490032 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.739510059 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.739789963 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.740926981 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.750435114 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.750478983 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.750518084 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.750555992 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.750617027 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.750646114 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.752046108 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.752085924 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.752114058 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.752280951 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.752342939 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.782769918 CET	56338	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:31.788798094 CET	59420	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:31.791421890 CET	58784	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:31.802967072 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.807435989 CET	63978	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:31.826600075 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.826652050 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.827917099 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.828249931 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.832590103 CET	53	59420	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:31.834736109 CET	53	58784	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:31.839221954 CET	53	56338	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:31.850950956 CET	53	63978	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:31.858521938 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.859044075 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.877587080 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.878408909 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.878910065 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.880055904 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:31.883240938 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.895076990 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:31.896675110 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.037913084 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.056107044 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.056166887 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.056209087 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.056256056 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.056303978 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.056344986 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.056382895 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.056421041 CET	443	58785	216.58.208.34	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 02:38:32.056461096 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.056499004 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.056538105 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.056571007 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.056617022 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.056658983 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.057023048 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.057065964 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.057096958 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.057141066 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.057178974 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.057223082 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.057324886 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.057553053 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.057595968 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.057632923 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.057671070 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.057703972 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.057898045 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.057950020 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.057996035 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.079747915 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.079802036 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.079839945 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.079876900 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.079914093 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.079961061 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.080007076 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.080045938 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.080084085 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.080121040 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.080157042 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.080192089 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.080326080 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.080364943 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.080404043 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.080441952 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.081571102 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.085948944 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.085990906 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.086029053 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.086066961 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.087080002 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.087121964 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.087162018 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.087198973 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.087236881 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.087275028 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.088702917 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.088745117 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.088782072 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.088819981 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.089798927 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.089838982 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.089888096 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.089926004 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.089962959 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.090631962 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.090682983 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.090725899 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.090778112 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.090809107 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.090850115 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.090894938 CET	58785	443	192.168.2.3	216.58.208.34

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 02:38:32.090945959 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.091121912 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.091161966 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.091212988 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.091245890 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.091284037 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.091326952 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.091370106 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.091413021 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.092356920 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.092494011 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.093005896 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.093050003 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.093087912 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.093125105 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.093594074 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.093636990 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.094172001 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.094213009 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.094249964 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.094288111 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.094392061 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.094434023 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.095238924 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.095277071 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.095323086 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.095365047 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.097376108 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.097435951 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.097472906 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.097511053 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.097548962 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.097584963 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.097624063 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.097661018 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.097913027 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.097945929 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.097992897 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.098067045 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.098088026 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.098145008 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.098939896 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.098983049 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.099025965 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.099064112 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.099102020 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.099140882 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.100539923 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.100580931 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.100616932 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.100660086 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.102294922 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.102327108 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.102382898 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.102420092 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.102463007 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.106985092 CET	62938	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:32.108155012 CET	55708	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:32.108867884 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.118773937 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.133590937 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.133630037 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.133676052 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.133718967 CET	443	58785	216.58.208.34	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 02:38:32.133757114 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.133795977 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.133832932 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.133868933 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.133908033 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.133944988 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.134001017 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.134038925 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.134074926 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.134120941 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.134161949 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.134200096 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.134238005 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.134277105 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.134855032 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.134942055 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.135030985 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.135207891 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.135308981 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.135349989 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.135396004 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.135437012 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.135469913 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.142349958 CET	53	62938	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:32.143501997 CET	53	55708	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:32.157578945 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.172619104 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.192543983 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.192740917 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.192765951 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.194714069 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.197129011 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.197173119 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.209435940 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.213871002 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.218825102 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.218853951 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.220679045 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.220735073 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.221694946 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.226047993 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.226372957 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.230998039 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.246368885 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.246464014 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.251005888 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.320496082 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.354441881 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.354485035 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.354536057 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.354573011 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.354609966 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.354648113 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.354693890 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.354736090 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.354773045 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.354810953 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.354847908 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.354882956 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.355161905 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.355202913 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.355247974 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.355287075 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.355324984 CET	443	58785	216.58.208.34	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 02:38:32.355360985 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.357125044 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.357168913 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.357206106 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.357242107 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.357280016 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.357316971 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.357353926 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.357423067 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.357465029 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.357501984 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.359066963 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.359077930 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.359119892 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.359158039 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.359184027 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.359194994 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.359272003 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.359297037 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.359319925 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.359363079 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.359400034 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.360204935 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.360244989 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.360284090 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.360321999 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.360358000 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.362415075 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.367789030 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.419723034 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.419751883 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.437484980 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.448080063 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.448529959 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.448646069 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.453500986 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.464133978 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.481251955 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.498564005 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.515343904 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.521552086 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.526463985 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.528414011 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.543445110 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.543498993 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.543538094 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.543575048 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.545300007 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.549047947 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.605083942 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.605130911 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.609927893 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.639842987 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.639894962 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.639942884 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.639986992 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.640024900 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.640067101 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.640105009 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.640141964 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.640176058 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.640499115 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.640702009 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.733110905 CET	58785	443	192.168.2.3	216.58.208.34

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 02:38:32.733160973 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.733756065 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.733778954 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.735224009 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.744643927 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.748264074 CET	56803	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:32.749345064 CET	57145	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:32.749866009 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.750524044 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.760032892 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.760073900 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.760185957 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.760277033 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.765657902 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.768981934 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.769032955 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.773802042 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.776429892 CET	53	57145	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:32.778996944 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.779062033 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.779108047 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.779145956 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.779185057 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.779223919 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.779484034 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.783457994 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.786233902 CET	53	56803	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:32.975728989 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.976425886 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.984111071 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:32.986129045 CET	49361	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:32.986314058 CET	63150	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:32.988590002 CET	53279	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:32.992692947 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:32.998100042 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:33.000976086 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.001015902 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.001053095 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.001092911 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.001130104 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.002002954 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.002062082 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.006556988 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:33.010696888 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:33.015460014 CET	53	53279	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:33.025518894 CET	53	63150	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:33.029987097 CET	53	49361	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:33.035860062 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.035972118 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.043334961 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:33.071127892 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:33.092390060 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.096708059 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.096863031 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.102200031 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:33.323649883 CET	56881	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:33.347353935 CET	53642	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:33.363691092 CET	53	56881	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:33.372641087 CET	55667	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:33.382898092 CET	53	53642	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:33.389595985 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:33.399645090 CET	53	55667	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:33.410109043 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.417150021 CET	443	58785	216.58.208.34	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 02:38:33.417195082 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.421653986 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:33.542891979 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:33.553103924 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:33.563729048 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.569122076 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.569267035 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.569881916 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.569925070 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.569962978 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.570008993 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.570051908 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.570089102 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.570130110 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.570167065 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.570203066 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.570241928 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.570276976 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.571410894 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:33.576081038 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:33.616184950 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:33.636919022 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.644500017 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.645119905 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.650528908 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:33.654328108 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:33.671392918 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.677128077 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:33.679327965 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:33.700627089 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.789418936 CET	54833	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:33.792108059 CET	62476	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:33.793670893 CET	49705	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:33.794735909 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:33.815431118 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.819670916 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.820646048 CET	53	49705	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:33.824191093 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:33.831268072 CET	53	62476	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:33.833782911 CET	53	54833	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:33.904612064 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:33.904666901 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:33.910623074 CET	61477	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:33.912933111 CET	61633	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:33.915091991 CET	55949	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:33.925610065 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.931723118 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.931750059 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:33.937374115 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:33.937603951 CET	53	61477	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:33.939860106 CET	53	61633	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:33.960366964 CET	53	55949	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:33.990418911 CET	57601	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:34.027731895 CET	53	57601	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:34.189975977 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:34.210588932 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:34.211107969 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:34.217653036 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:34.217746973 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:34.222131968 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:34.231127024 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:34.237782001 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:34.237809896 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:34.243813038 CET	58785	443	192.168.2.3	216.58.208.34

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 02:38:34.250143051 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:34.271291018 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:34.277836084 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:34.277878046 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:34.283188105 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:34.303903103 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:34.324973106 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:34.331422091 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:34.331465960 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:34.337265015 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:34.347856045 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:34.357465982 CET	49342	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:34.368851900 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:34.375591993 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:34.375634909 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:34.377540112 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:34.394694090 CET	53	49342	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:34.398269892 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:34.403187990 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:34.407617092 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:35.208190918 CET	56253	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:35.251768112 CET	53	56253	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:35.717571020 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:35.717629910 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:35.738445044 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:35.744149923 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:35.744193077 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:35.750309944 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:35.895596027 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:35.925082922 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:35.925147057 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:35.925189018 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:35.925225973 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:35.925265074 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:35.925295115 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:35.925421000 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:35.925474882 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:35.925525904 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:36.310606003 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:36.331743956 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:36.336940050 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:36.336991072 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:36.342386007 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:36.501215935 CET	49667	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:36.544217110 CET	53	49667	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:39.395422935 CET	54717	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:39.431375980 CET	53	54717	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:39.467041016 CET	63975	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:39.510982990 CET	53	63975	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:39.942441940 CET	56639	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:39.979640007 CET	53	56639	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:40.836296082 CET	51856	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:40.837816000 CET	56546	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:40.841717005 CET	62152	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:40.843696117 CET	53470	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:40.864892960 CET	53	56546	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:40.870536089 CET	53	53470	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:40.873245955 CET	53	51856	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:40.880719900 CET	53	62152	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:42.141537905 CET	56446	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:42.200263023 CET	53	56446	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:42.348002911 CET	59631	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:42.391267061 CET	53	59631	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:42.476624966 CET	55515	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 02:38:42.476922035 CET	64547	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:42.504133940 CET	53	64547	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:42.514220953 CET	53	55515	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:42.653198957 CET	51759	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:42.680058002 CET	53	51759	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:43.846981049 CET	59207	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:43.884351969 CET	53	59207	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:44.201225996 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:44.222862005 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:44.228547096 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:44.228590965 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:44.228630066 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:44.228668928 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:44.228707075 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:44.228744984 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:44.228782892 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:44.228822947 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:44.228871107 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:44.228899956 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:44.231587887 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:44.252698898 CET	54269	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:44.254317999 CET	54856	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:44.256268978 CET	64140	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:44.257383108 CET	62271	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:44.280061007 CET	57404	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:44.280946970 CET	62997	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:44.288291931 CET	53	54269	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:44.291548014 CET	53	54856	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:44.291623116 CET	53	64140	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:44.294724941 CET	53	62271	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:44.311956882 CET	57712	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:44.314945936 CET	60065	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:44.317939997 CET	53	57404	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:44.318548918 CET	53	62997	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:44.347455025 CET	53	57712	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:44.350223064 CET	53	60065	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:44.475481987 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:44.496665955 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:44.629211903 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:44.629257917 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:44.629276037 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:44.654222012 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:44.665062904 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:44.666868925 CET	60066	443	192.168.2.3	74.125.140.157
Nov 22, 2020 02:38:44.669866085 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:44.694751024 CET	443	60066	74.125.140.157	192.168.2.3
Nov 22, 2020 02:38:44.694806099 CET	443	60066	74.125.140.157	192.168.2.3
Nov 22, 2020 02:38:44.696290970 CET	60066	443	192.168.2.3	74.125.140.157
Nov 22, 2020 02:38:44.724493027 CET	443	60066	74.125.140.157	192.168.2.3
Nov 22, 2020 02:38:44.733437061 CET	60066	443	192.168.2.3	74.125.140.157
Nov 22, 2020 02:38:44.743087053 CET	60066	443	192.168.2.3	74.125.140.157
Nov 22, 2020 02:38:44.743330956 CET	60066	443	192.168.2.3	74.125.140.157
Nov 22, 2020 02:38:44.745949030 CET	55068	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:44.750102043 CET	64700	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:44.751003981 CET	60066	443	192.168.2.3	74.125.140.157
Nov 22, 2020 02:38:44.771790981 CET	443	60066	74.125.140.157	192.168.2.3
Nov 22, 2020 02:38:44.771929026 CET	443	60066	74.125.140.157	192.168.2.3
Nov 22, 2020 02:38:44.772001982 CET	443	60066	74.125.140.157	192.168.2.3
Nov 22, 2020 02:38:44.773036957 CET	443	60066	74.125.140.157	192.168.2.3
Nov 22, 2020 02:38:44.773144960 CET	443	60066	74.125.140.157	192.168.2.3
Nov 22, 2020 02:38:44.779805899 CET	443	60066	74.125.140.157	192.168.2.3
Nov 22, 2020 02:38:44.779834032 CET	443	60066	74.125.140.157	192.168.2.3
Nov 22, 2020 02:38:44.787628889 CET	53	64700	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:44.789321899 CET	53	55068	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 02:38:44.818713903 CET	60066	443	192.168.2.3	74.125.140.157
Nov 22, 2020 02:38:44.818802118 CET	60066	443	192.168.2.3	74.125.140.157
Nov 22, 2020 02:38:44.818908930 CET	60066	443	192.168.2.3	74.125.140.157
Nov 22, 2020 02:38:44.840467930 CET	443	60066	74.125.140.157	192.168.2.3
Nov 22, 2020 02:38:44.857372046 CET	61998	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:44.866730928 CET	60066	443	192.168.2.3	74.125.140.157
Nov 22, 2020 02:38:44.901367903 CET	53	61998	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:45.309344053 CET	53724	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:45.310066938 CET	52328	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:45.310363054 CET	58051	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:45.346712112 CET	64130	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:45.347378016 CET	50491	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:45.347599030 CET	53	52328	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:45.347814083 CET	53	58051	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:45.352695942 CET	53	53724	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:45.382220030 CET	53	64130	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:45.396219969 CET	53	50491	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:45.401818037 CET	53004	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:45.403616905 CET	52529	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:45.441342115 CET	53	52529	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:45.442171097 CET	53	53004	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:45.498987913 CET	53656	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:45.499819040 CET	62724	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:45.525953054 CET	53	53656	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:45.537286043 CET	53	62724	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:46.128309011 CET	56059	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:46.163875103 CET	53	56059	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:46.338869095 CET	63060	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:46.382289886 CET	53	63060	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:47.333278894 CET	51498	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:47.372052908 CET	53	51498	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:47.566349983 CET	59943	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:47.601970911 CET	53	59943	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:47.821357965 CET	50118	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:47.857013941 CET	53	50118	8.8.8.8	192.168.2.3
Nov 22, 2020 02:38:48.434936047 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:48.455823898 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:48.460812092 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:48.460962057 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:48.464639902 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:48.485937119 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:48.497256041 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:48.497335911 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:48.501946926 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:48.916192055 CET	50120	443	192.168.2.3	172.217.21.238
Nov 22, 2020 02:38:48.939857960 CET	443	50120	172.217.21.238	192.168.2.3
Nov 22, 2020 02:38:48.939907074 CET	443	50120	172.217.21.238	192.168.2.3
Nov 22, 2020 02:38:48.953505993 CET	50120	443	192.168.2.3	172.217.21.238
Nov 22, 2020 02:38:48.954056025 CET	50120	443	192.168.2.3	172.217.21.238
Nov 22, 2020 02:38:48.983726025 CET	443	50120	172.217.21.238	192.168.2.3
Nov 22, 2020 02:38:48.987653971 CET	50120	443	192.168.2.3	172.217.21.238
Nov 22, 2020 02:38:48.992510080 CET	443	50120	172.217.21.238	192.168.2.3
Nov 22, 2020 02:38:48.992552042 CET	443	50120	172.217.21.238	192.168.2.3
Nov 22, 2020 02:38:48.994673967 CET	50120	443	192.168.2.3	172.217.21.238
Nov 22, 2020 02:38:49.922665119 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:49.943449020 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:49.947396040 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:49.947535992 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:49.952930927 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:49.961452961 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:49.982500076 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:50.520800114 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:50.541673899 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:50.659303904 CET	443	58785	216.58.208.34	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 02:38:50.659446955 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:50.663990974 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:50.897214890 CET	52124	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:38:50.938582897 CET	443	52124	216.58.208.34	192.168.2.3
Nov 22, 2020 02:38:50.939268112 CET	50123	443	192.168.2.3	172.217.21.195
Nov 22, 2020 02:38:50.962816954 CET	443	50123	172.217.21.195	192.168.2.3
Nov 22, 2020 02:38:50.962857962 CET	443	50123	172.217.21.195	192.168.2.3
Nov 22, 2020 02:38:50.963912964 CET	50123	443	192.168.2.3	172.217.21.195
Nov 22, 2020 02:38:50.977272034 CET	50123	443	192.168.2.3	172.217.21.195
Nov 22, 2020 02:38:50.977432966 CET	50123	443	192.168.2.3	172.217.21.195
Nov 22, 2020 02:38:51.000998974 CET	443	50123	172.217.21.195	192.168.2.3
Nov 22, 2020 02:38:51.001844883 CET	50123	443	192.168.2.3	172.217.21.195
Nov 22, 2020 02:38:51.015516043 CET	443	50123	172.217.21.195	192.168.2.3
Nov 22, 2020 02:38:51.041088104 CET	50123	443	192.168.2.3	172.217.21.195
Nov 22, 2020 02:38:54.698271990 CET	60066	443	192.168.2.3	74.125.140.157
Nov 22, 2020 02:38:54.727396965 CET	443	60066	74.125.140.157	192.168.2.3
Nov 22, 2020 02:38:54.727440119 CET	443	60066	74.125.140.157	192.168.2.3
Nov 22, 2020 02:38:54.728079081 CET	60066	443	192.168.2.3	74.125.140.157
Nov 22, 2020 02:38:54.732630014 CET	50123	443	192.168.2.3	172.217.21.195
Nov 22, 2020 02:38:54.760176897 CET	443	50123	172.217.21.195	192.168.2.3
Nov 22, 2020 02:38:54.760217905 CET	443	50123	172.217.21.195	192.168.2.3
Nov 22, 2020 02:38:54.760662079 CET	50123	443	192.168.2.3	172.217.21.195
Nov 22, 2020 02:38:56.182991028 CET	58357	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:38:56.222872972 CET	53	58357	8.8.8.8	192.168.2.3
Nov 22, 2020 02:39:02.520914078 CET	55804	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:39:02.548119068 CET	53	55804	8.8.8.8	192.168.2.3
Nov 22, 2020 02:39:03.956159115 CET	50120	443	192.168.2.3	172.217.21.238
Nov 22, 2020 02:39:03.997546911 CET	443	50120	172.217.21.238	192.168.2.3
Nov 22, 2020 02:39:05.522414923 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:39:05.543695927 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:06.531516075 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:39:06.552287102 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:06.556663036 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:06.556710958 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:06.556747913 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:06.560326099 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:39:06.580923080 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:06.594818115 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:06.594854116 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:06.599349022 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:39:06.972712040 CET	50120	443	192.168.2.3	172.217.21.238
Nov 22, 2020 02:39:06.997693062 CET	443	50120	172.217.21.238	192.168.2.3
Nov 22, 2020 02:39:06.997746944 CET	443	50120	172.217.21.238	192.168.2.3
Nov 22, 2020 02:39:06.999511957 CET	50120	443	192.168.2.3	172.217.21.238
Nov 22, 2020 02:39:08.081969023 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:39:08.102768898 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:08.106652021 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:08.106729031 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:08.113549948 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:39:08.406333923 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:39:08.427517891 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:08.536612988 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:08.536643982 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:08.536866903 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:08.542673111 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:39:09.126425982 CET	50123	443	192.168.2.3	172.217.21.195
Nov 22, 2020 02:39:09.156512022 CET	443	50123	172.217.21.195	192.168.2.3
Nov 22, 2020 02:39:09.156555891 CET	443	50123	172.217.21.195	192.168.2.3
Nov 22, 2020 02:39:09.157285929 CET	50123	443	192.168.2.3	172.217.21.195
Nov 22, 2020 02:39:09.701428890 CET	60066	443	192.168.2.3	74.125.140.157
Nov 22, 2020 02:39:09.754878044 CET	443	60066	74.125.140.157	192.168.2.3
Nov 22, 2020 02:39:10.774168968 CET	52080	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:39:10.801085949 CET	53	52080	8.8.8.8	192.168.2.3
Nov 22, 2020 02:39:12.526959896 CET	58785	443	192.168.2.3	216.58.208.34

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 02:39:12.548281908 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:12.552923918 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:12.552959919 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:12.556236029 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:39:12.577845097 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:12.588373899 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:12.588417053 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:12.593878984 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:39:12.954607010 CET	50120	443	192.168.2.3	172.217.21.238
Nov 22, 2020 02:39:12.979954958 CET	443	50120	172.217.21.238	192.168.2.3
Nov 22, 2020 02:39:12.979985952 CET	443	50120	172.217.21.238	192.168.2.3
Nov 22, 2020 02:39:12.980452061 CET	50120	443	192.168.2.3	172.217.21.238
Nov 22, 2020 02:39:13.873888016 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:39:13.894344091 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:13.898644924 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:13.898778915 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:13.904431105 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:39:14.195338011 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:39:14.216202021 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:14.327594995 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:14.327646017 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:14.327663898 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:14.333466053 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:39:14.847475052 CET	50123	443	192.168.2.3	172.217.21.195
Nov 22, 2020 02:39:14.876868963 CET	443	50123	172.217.21.195	192.168.2.3
Nov 22, 2020 02:39:14.877006054 CET	443	50123	172.217.21.195	192.168.2.3
Nov 22, 2020 02:39:14.877168894 CET	50123	443	192.168.2.3	172.217.21.195
Nov 22, 2020 02:39:18.561574936 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:39:18.582221985 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:18.587507963 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:18.587573051 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:18.590759039 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:39:18.611804008 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:18.625175953 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:18.625227928 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:18.629723072 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:39:18.949723959 CET	50120	443	192.168.2.3	172.217.21.238
Nov 22, 2020 02:39:18.974638939 CET	443	50120	172.217.21.238	192.168.2.3
Nov 22, 2020 02:39:18.974680901 CET	443	50120	172.217.21.238	192.168.2.3
Nov 22, 2020 02:39:18.976113081 CET	50120	443	192.168.2.3	172.217.21.238
Nov 22, 2020 02:39:19.450390100 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:39:19.471064091 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:19.475789070 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:19.475827932 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:19.480356932 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:39:19.958632946 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:39:19.980350018 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:20.090292931 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:20.090322971 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:20.090511084 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:20.096282959 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:39:20.248409033 CET	50123	443	192.168.2.3	172.217.21.195
Nov 22, 2020 02:39:20.278599977 CET	443	50123	172.217.21.195	192.168.2.3
Nov 22, 2020 02:39:20.278692007 CET	443	50123	172.217.21.195	192.168.2.3
Nov 22, 2020 02:39:20.279059887 CET	50123	443	192.168.2.3	172.217.21.195
Nov 22, 2020 02:39:21.637799025 CET	19794	21813	192.168.2.3	192.168.2.1
Nov 22, 2020 02:39:22.245691061 CET	55238	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:39:22.289999008 CET	53	55238	8.8.8.8	192.168.2.3
Nov 22, 2020 02:39:22.674380064 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:39:22.695322990 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:22.735990047 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:22.736031055 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:22.736742973 CET	58785	443	192.168.2.3	216.58.208.34
Nov 22, 2020 02:39:22.740205050 CET	49289	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 02:39:22.757601023 CET	443	58785	216.58.208.34	192.168.2.3
Nov 22, 2020 02:39:22.783267021 CET	53	49289	8.8.8.8	192.168.2.3
Nov 22, 2020 02:39:23.299388885 CET	61034	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:39:23.299725056 CET	51964	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:39:23.335372925 CET	53	51964	8.8.8.8	192.168.2.3
Nov 22, 2020 02:39:23.342753887 CET	53	61034	8.8.8.8	192.168.2.3
Nov 22, 2020 02:39:23.361659050 CET	58241	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:39:23.405313015 CET	53	58241	8.8.8.8	192.168.2.3
Nov 22, 2020 02:39:23.473645926 CET	59571	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:39:23.517209053 CET	53	59571	8.8.8.8	192.168.2.3
Nov 22, 2020 02:39:23.586268902 CET	60066	443	192.168.2.3	74.125.140.157
Nov 22, 2020 02:39:23.615603924 CET	443	60066	74.125.140.157	192.168.2.3
Nov 22, 2020 02:39:23.615643978 CET	443	60066	74.125.140.157	192.168.2.3
Nov 22, 2020 02:39:23.615885973 CET	60066	443	192.168.2.3	74.125.140.157
Nov 22, 2020 02:39:26.202455044 CET	51708	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:39:26.238161087 CET	53	51708	8.8.8.8	192.168.2.3
Nov 22, 2020 02:39:26.459889889 CET	63643	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:39:26.495579958 CET	53	63643	8.8.8.8	192.168.2.3
Nov 22, 2020 02:39:26.542308092 CET	62823	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:39:26.585721016 CET	53	62823	8.8.8.8	192.168.2.3
Nov 22, 2020 02:39:26.635173082 CET	63750	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:39:26.681130886 CET	53	63750	8.8.8.8	192.168.2.3
Nov 22, 2020 02:39:27.064893961 CET	61959	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:39:27.102686882 CET	53	61959	8.8.8.8	192.168.2.3
Nov 22, 2020 02:39:31.884704113 CET	63554	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:39:31.936434984 CET	53	63554	8.8.8.8	192.168.2.3
Nov 22, 2020 02:39:34.155231953 CET	50120	443	192.168.2.3	172.217.21.238
Nov 22, 2020 02:39:34.197278976 CET	443	50120	172.217.21.238	192.168.2.3
Nov 22, 2020 02:39:35.250157118 CET	50123	443	192.168.2.3	172.217.21.195
Nov 22, 2020 02:39:35.292702913 CET	443	50123	172.217.21.195	192.168.2.3
Nov 22, 2020 02:39:36.672513008 CET	57723	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:39:36.741090059 CET	53	57723	8.8.8.8	192.168.2.3
Nov 22, 2020 02:39:38.588341951 CET	60066	443	192.168.2.3	74.125.140.157
Nov 22, 2020 02:39:38.642004967 CET	443	60066	74.125.140.157	192.168.2.3
Nov 22, 2020 02:39:40.981722116 CET	58663	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:39:41.018939018 CET	53	58663	8.8.8.8	192.168.2.3
Nov 22, 2020 02:40:11.492623091 CET	50980	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:40:11.520034075 CET	53	50980	8.8.8.8	192.168.2.3
Nov 22, 2020 02:40:12.170663118 CET	50067	53	192.168.2.3	8.8.8.8
Nov 22, 2020 02:40:12.206136942 CET	53	50067	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 22, 2020 02:38:30.078527927 CET	192.168.2.3	8.8.8.8	0xd3a	Standard query (0)	otampadabo la2.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:31.113955975 CET	192.168.2.3	8.8.8.8	0x746c	Standard query (0)	s.w.org	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:31.541233063 CET	192.168.2.3	8.8.8.8	0xd6f5	Standard query (0)	googleads. g.doubleclick.net	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:31.631160975 CET	192.168.2.3	8.8.8.8	0xe7ad	Standard query (0)	stats.g.do ubleclick.net	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:31.788798094 CET	192.168.2.3	8.8.8.8	0xf94b	Standard query (0)	adservice. google.co.uk	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:31.807435989 CET	192.168.2.3	8.8.8.8	0x95c8	Standard query (0)	www.google tagservices.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:32.748264074 CET	192.168.2.3	8.8.8.8	0x1504	Standard query (0)	fw.adsafep rotected.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:32.986129045 CET	192.168.2.3	8.8.8.8	0xb834	Standard query (0)	cm.g.doubl eclick.net	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:32.986314058 CET	192.168.2.3	8.8.8.8	0xf0e9	Standard query (0)	dsum-sec.c asalemedia.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:32.988590002 CET	192.168.2.3	8.8.8.8	0x8bd5	Standard query (0)	ib.adnxs.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.323649883 CET	192.168.2.3	8.8.8.8	0x32f7	Standard query (0)	static.ads afeprotected.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 22, 2020 02:38:33.372641087 CET	192.168.2.3	8.8.8.8	0x6cc3	Standard query (0)	dt.adsafeprotected.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.789418936 CET	192.168.2.3	8.8.8.8	0x43e	Standard query (0)	cms.quantserve.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.792108059 CET	192.168.2.3	8.8.8.8	0x657d	Standard query (0)	pixel.everesttech.net	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.793670893 CET	192.168.2.3	8.8.8.8	0x2e94	Standard query (0)	odr.mookie1.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.910623074 CET	192.168.2.3	8.8.8.8	0xf8b6	Standard query (0)	rtb.openx.net	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.912933111 CET	192.168.2.3	8.8.8.8	0x9586	Standard query (0)	image6.pubmatic.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.915091991 CET	192.168.2.3	8.8.8.8	0x2874	Standard query (0)	pixel.rubiconproject.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.990418911 CET	192.168.2.3	8.8.8.8	0xed1b	Standard query (0)	ssum-sec.casalemedia.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:36.501215935 CET	192.168.2.3	8.8.8.8	0x26f6	Standard query (0)	otampadabola2.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:39.395422935 CET	192.168.2.3	8.8.8.8	0xa95a	Standard query (0)	adclick.g.doubleclick.net	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:39.942441940 CET	192.168.2.3	8.8.8.8	0xdad8	Standard query (0)	www.coreldraw.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:40.836296082 CET	192.168.2.3	8.8.8.8	0x1d1f	Standard query (0)	www.corel.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:40.837816000 CET	192.168.2.3	8.8.8.8	0x62bc	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:40.841717005 CET	192.168.2.3	8.8.8.8	0xb28e	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:40.843696117 CET	192.168.2.3	8.8.8.8	0xc5d6	Standard query (0)	static.zdassets.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:42.141537905 CET	192.168.2.3	8.8.8.8	0x2775	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:42.348002911 CET	192.168.2.3	8.8.8.8	0x3f16	Standard query (0)	www.googleoptimize.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:42.476624966 CET	192.168.2.3	8.8.8.8	0xcefb	Standard query (0)	cdn.ywxi.net	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:42.653198957 CET	192.168.2.3	8.8.8.8	0x69c1	Standard query (0)	ekr.zdassets.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:43.846981049 CET	192.168.2.3	8.8.8.8	0x8fac	Standard query (0)	installer.corel.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.254317999 CET	192.168.2.3	8.8.8.8	0xed3d	Standard query (0)	munchkin.marketo.net	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.256268978 CET	192.168.2.3	8.8.8.8	0xb746	Standard query (0)	optanon.blob.core.windows.net	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.257383108 CET	192.168.2.3	8.8.8.8	0x7c36	Standard query (0)	a.opmnstr.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.280061007 CET	192.168.2.3	8.8.8.8	0x9e32	Standard query (0)	static.hotjar.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.280946970 CET	192.168.2.3	8.8.8.8	0xc48b	Standard query (0)	d2bqow4fb67vs2.cloudfront.net	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.311956882 CET	192.168.2.3	8.8.8.8	0x5ac6	Standard query (0)	s3-us-west-2.amazonaws.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.314945936 CET	192.168.2.3	8.8.8.8	0xd409	Standard query (0)	s3.amazonaws.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.750102043 CET	192.168.2.3	8.8.8.8	0x3031	Standard query (0)	corel.zendesk.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.857372046 CET	192.168.2.3	8.8.8.8	0xe5bd	Standard query (0)	api.omappapi.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.309344053 CET	192.168.2.3	8.8.8.8	0xdd58	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.310066938 CET	192.168.2.3	8.8.8.8	0xf8cf	Standard query (0)	script.hotjar.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.310363054 CET	192.168.2.3	8.8.8.8	0xbd9e	Standard query (0)	www.trustedsite.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.346712112 CET	192.168.2.3	8.8.8.8	0xb87	Standard query (0)	280-qdk-215.mktoresp.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.347378016 CET	192.168.2.3	8.8.8.8	0xb12f	Standard query (0)	cdn.aimtell.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.401818037 CET	192.168.2.3	8.8.8.8	0x106b	Standard query (0)	danv01ao0kdr2.cloudfront.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 22, 2020 02:38:45.403616905 CET	192.168.2.3	8.8.8.8	0x133e	Standard query (0)	vars.hotjar.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.498987913 CET	192.168.2.3	8.8.8.8	0x92c7	Standard query (0)	geolocation.onetrust.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.499819040 CET	192.168.2.3	8.8.8.8	0x3e65	Standard query (0)	a.omappapi.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:46.128309011 CET	192.168.2.3	8.8.8.8	0x1c26	Standard query (0)	widget-mediator.zopim.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:46.338869095 CET	192.168.2.3	8.8.8.8	0xa637	Standard query (0)	portal.brandlock.io	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:47.333278894 CET	192.168.2.3	8.8.8.8	0xd600	Standard query (0)	www.coreldraw.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:47.821357965 CET	192.168.2.3	8.8.8.8	0x1b2b	Standard query (0)	in.hotjar.com	A (IP address)	IN (0x0001)
Nov 22, 2020 02:39:22.740205050 CET	192.168.2.3	8.8.8.8	0x7658	Standard query (0)	ads.youtube.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 02:38:30.118877888 CET	8.8.8.8	192.168.2.3	0xd3a	No error (0)	otampadabola2.com		104.31.68.76	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:30.118877888 CET	8.8.8.8	192.168.2.3	0xd3a	No error (0)	otampadabola2.com		172.67.209.57	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:30.118877888 CET	8.8.8.8	192.168.2.3	0xd3a	No error (0)	otampadabola2.com		104.31.69.76	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:31.140883923 CET	8.8.8.8	192.168.2.3	0x746c	No error (0)	s.w.org		192.0.77.48	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:31.188503981 CET	8.8.8.8	192.168.2.3	0x2522	No error (0)	pagead46.l.doubleclick.net		172.217.23.162	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:31.584994078 CET	8.8.8.8	192.168.2.3	0xd6f5	No error (0)	googleads.g.doubleclick.net	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:31.584994078 CET	8.8.8.8	192.168.2.3	0xd6f5	No error (0)	pagead46.l.doubleclick.net		216.58.208.34	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:31.658344984 CET	8.8.8.8	192.168.2.3	0xe7ad	No error (0)	stats.g.doubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:31.658344984 CET	8.8.8.8	192.168.2.3	0xe7ad	No error (0)	stats.l.doubleclick.net		74.125.140.157	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:31.658344984 CET	8.8.8.8	192.168.2.3	0xe7ad	No error (0)	stats.l.doubleclick.net		74.125.140.156	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:31.658344984 CET	8.8.8.8	192.168.2.3	0xe7ad	No error (0)	stats.l.doubleclick.net		74.125.140.155	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:31.658344984 CET	8.8.8.8	192.168.2.3	0xe7ad	No error (0)	stats.l.doubleclick.net		74.125.140.154	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:31.832590103 CET	8.8.8.8	192.168.2.3	0xf94b	No error (0)	adservice.google.co.uk	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:31.832590103 CET	8.8.8.8	192.168.2.3	0xf94b	No error (0)	pagead46.l.doubleclick.net		172.217.22.34	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:31.834736109 CET	8.8.8.8	192.168.2.3	0x4971	No error (0)	pagead46.l.doubleclick.net		216.58.210.2	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:31.839221954 CET	8.8.8.8	192.168.2.3	0x3cf8	No error (0)	partnerad.l.doubleclick.net		172.217.21.226	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:31.850950956 CET	8.8.8.8	192.168.2.3	0x95c8	No error (0)	www.googletagservices.com	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:31.850950956 CET	8.8.8.8	192.168.2.3	0x95c8	No error (0)	pagead46.l.doubleclick.net		172.217.23.98	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:32.786233902 CET	8.8.8.8	192.168.2.3	0x1504	No error (0)	fw.adsafeprotected.com	iefw.adsafeprotected.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 02:38:32.786233902 CET	8.8.8.8	192.168.2.3	0x1504	No error (0)	iefw.adsafeprotected.com	firewall-external-2134955858.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:32.786233902 CET	8.8.8.8	192.168.2.3	0x1504	No error (0)	firewall-external-2134955858.eu-west-1.elb.amazonaws.com		108.128.94.32	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:32.786233902 CET	8.8.8.8	192.168.2.3	0x1504	No error (0)	firewall-external-2134955858.eu-west-1.elb.amazonaws.com		52.50.154.233	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:32.786233902 CET	8.8.8.8	192.168.2.3	0x1504	No error (0)	firewall-external-2134955858.eu-west-1.elb.amazonaws.com		54.76.15.48	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:32.786233902 CET	8.8.8.8	192.168.2.3	0x1504	No error (0)	firewall-external-2134955858.eu-west-1.elb.amazonaws.com		52.211.241.80	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:32.786233902 CET	8.8.8.8	192.168.2.3	0x1504	No error (0)	firewall-external-2134955858.eu-west-1.elb.amazonaws.com		54.171.14.14	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:32.786233902 CET	8.8.8.8	192.168.2.3	0x1504	No error (0)	firewall-external-2134955858.eu-west-1.elb.amazonaws.com		52.213.83.3	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:32.786233902 CET	8.8.8.8	192.168.2.3	0x1504	No error (0)	firewall-external-2134955858.eu-west-1.elb.amazonaws.com		63.32.41.216	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:32.786233902 CET	8.8.8.8	192.168.2.3	0x1504	No error (0)	firewall-external-2134955858.eu-west-1.elb.amazonaws.com		52.18.153.122	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.015460014 CET	8.8.8.8	192.168.2.3	0x8bd5	No error (0)	ib.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:33.015460014 CET	8.8.8.8	192.168.2.3	0x8bd5	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:33.015460014 CET	8.8.8.8	192.168.2.3	0x8bd5	No error (0)	ib.anycast.adnxs.com		185.33.221.90	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.015460014 CET	8.8.8.8	192.168.2.3	0x8bd5	No error (0)	ib.anycast.adnxs.com		185.33.220.145	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.015460014 CET	8.8.8.8	192.168.2.3	0x8bd5	No error (0)	ib.anycast.adnxs.com		185.33.221.91	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.015460014 CET	8.8.8.8	192.168.2.3	0x8bd5	No error (0)	ib.anycast.adnxs.com		185.33.220.240	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.015460014 CET	8.8.8.8	192.168.2.3	0x8bd5	No error (0)	ib.anycast.adnxs.com		185.33.220.243	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.015460014 CET	8.8.8.8	192.168.2.3	0x8bd5	No error (0)	ib.anycast.adnxs.com		185.33.220.241	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.015460014 CET	8.8.8.8	192.168.2.3	0x8bd5	No error (0)	ib.anycast.adnxs.com		185.33.221.53	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.015460014 CET	8.8.8.8	192.168.2.3	0x8bd5	No error (0)	ib.anycast.adnxs.com		185.33.221.13	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.025518894 CET	8.8.8.8	192.168.2.3	0xf0e9	No error (0)	dsum-sec.casalemedia.com	dsum-sec.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:33.029987097 CET	8.8.8.8	192.168.2.3	0xb834	No error (0)	cm.g.doubleclick.net	pagead.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 02:38:33.029987097 CET	8.8.8.8	192.168.2.3	0xb834	No error (0)	pagead.l.doubleclick.net		216.58.205.226	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.363691092 CET	8.8.8.8	192.168.2.3	0x32f7	No error (0)	static.adsafeprotected.com	d162h6x3rxav67.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:33.363691092 CET	8.8.8.8	192.168.2.3	0x32f7	No error (0)	d162h6x3rxav67.cloudfront.net		13.224.102.76	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.363691092 CET	8.8.8.8	192.168.2.3	0x32f7	No error (0)	d162h6x3rxav67.cloudfront.net		13.224.102.64	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.363691092 CET	8.8.8.8	192.168.2.3	0x32f7	No error (0)	d162h6x3rxav67.cloudfront.net		13.224.102.90	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.363691092 CET	8.8.8.8	192.168.2.3	0x32f7	No error (0)	d162h6x3rxav67.cloudfront.net		13.224.102.65	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.399645090 CET	8.8.8.8	192.168.2.3	0x6cc3	No error (0)	dt.adsafeprotected.com	sjedt.adsafeprotected.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:33.399645090 CET	8.8.8.8	192.168.2.3	0x6cc3	No error (0)	sjedt.adsafeprotected.com		104.244.38.20	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.820646048 CET	8.8.8.8	192.168.2.3	0x2e94	No error (0)	odr.mookie1.com	tagr-gcp-odr-euw4.mookie1.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:33.820646048 CET	8.8.8.8	192.168.2.3	0x2e94	No error (0)	tagr-gcp-odr-euw4.mookie1.com		34.98.67.61	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.831268072 CET	8.8.8.8	192.168.2.3	0x657d	No error (0)	pixel.everesttech.net	tp00.everesttech.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:33.833782911 CET	8.8.8.8	192.168.2.3	0x43e	No error (0)	cms.quantserve.com	2kpixel.quantserve.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:33.833782911 CET	8.8.8.8	192.168.2.3	0x43e	No error (0)	2kpixel.quantserve.com	global.px.quantserve.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:33.833782911 CET	8.8.8.8	192.168.2.3	0x43e	No error (0)	global.px.quantserve.com		91.228.74.198	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.833782911 CET	8.8.8.8	192.168.2.3	0x43e	No error (0)	global.px.quantserve.com		91.228.74.133	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.833782911 CET	8.8.8.8	192.168.2.3	0x43e	No error (0)	global.px.quantserve.com		91.228.74.189	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.833782911 CET	8.8.8.8	192.168.2.3	0x43e	No error (0)	global.px.quantserve.com		91.228.74.134	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.833782911 CET	8.8.8.8	192.168.2.3	0x43e	No error (0)	global.px.quantserve.com		91.228.74.226	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.937603951 CET	8.8.8.8	192.168.2.3	0xf8b6	No error (0)	rtb.openx.net		35.227.252.103	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.937603951 CET	8.8.8.8	192.168.2.3	0xf8b6	No error (0)	rtb.openx.net		35.186.253.211	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.939860106 CET	8.8.8.8	192.168.2.3	0x9586	No error (0)	image6.pubmatic.com	pugm22000nfc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:33.939860106 CET	8.8.8.8	192.168.2.3	0x9586	No error (0)	pugm22000nfc.pubmatic.com	pugm22000nf.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:33.939860106 CET	8.8.8.8	192.168.2.3	0x9586	No error (0)	pugm22000nf.pubmatic.com		185.64.189.115	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:33.960366964 CET	8.8.8.8	192.168.2.3	0x2874	No error (0)	pixel.rubiconproject.com	pixel.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:34.027731895 CET	8.8.8.8	192.168.2.3	0xed1b	No error (0)	ssum-sec.casalemedia.com	ssum-sec.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:36.544217110 CET	8.8.8.8	192.168.2.3	0x26f6	No error (0)	otampadabola2.com		104.31.68.76	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 02:38:36.544217110 CET	8.8.8.8	192.168.2.3	0x26f6	No error (0)	otampadabola2.com		104.31.69.76	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:36.544217110 CET	8.8.8.8	192.168.2.3	0x26f6	No error (0)	otampadabola2.com		172.67.209.57	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:39.431375980 CET	8.8.8.8	192.168.2.3	0xa95a	No error (0)	adclick.g.doubleclick.net	pagead.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:39.431375980 CET	8.8.8.8	192.168.2.3	0xa95a	No error (0)	pagead.l.doubleclick.net		216.58.205.226	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:39.510982990 CET	8.8.8.8	192.168.2.3	0xefd4	No error (0)	pagead.l.doubleclick.net		172.217.16.194	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:39.979640007 CET	8.8.8.8	192.168.2.3	0xdad8	No error (0)	www.coreldraw.com	www.coreldraw.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:40.864892960 CET	8.8.8.8	192.168.2.3	0x62bc	No error (0)	maxcdn.bootstrapcdn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:40.870536089 CET	8.8.8.8	192.168.2.3	0xc5d6	No error (0)	static.zdassets.com	cf.zdassets.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:40.870536089 CET	8.8.8.8	192.168.2.3	0xc5d6	No error (0)	cf.zdassets.com		104.18.70.113	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:40.870536089 CET	8.8.8.8	192.168.2.3	0xc5d6	No error (0)	cf.zdassets.com		104.18.71.113	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:40.873245955 CET	8.8.8.8	192.168.2.3	0x1d1f	No error (0)	www.corel.com	www-san.corel.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:40.880719900 CET	8.8.8.8	192.168.2.3	0xb28e	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:42.200263023 CET	8.8.8.8	192.168.2.3	0x2775	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:42.200263023 CET	8.8.8.8	192.168.2.3	0x2775	No error (0)	googlehosted.l.googleusercontent.com		172.217.16.193	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:42.391267061 CET	8.8.8.8	192.168.2.3	0x3f16	No error (0)	www.googleoptimize.com		172.217.21.238	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:42.514220953 CET	8.8.8.8	192.168.2.3	0xcefb	No error (0)	cdn.ywxi.net	dtx9pzf7ji0d9.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:42.514220953 CET	8.8.8.8	192.168.2.3	0xcefb	No error (0)	dtx9pzf7ji0d9.cloudfront.net		13.224.102.99	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:42.514220953 CET	8.8.8.8	192.168.2.3	0xcefb	No error (0)	dtx9pzf7ji0d9.cloudfront.net		13.224.102.90	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:42.514220953 CET	8.8.8.8	192.168.2.3	0xcefb	No error (0)	dtx9pzf7ji0d9.cloudfront.net		13.224.102.26	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:42.514220953 CET	8.8.8.8	192.168.2.3	0xcefb	No error (0)	dtx9pzf7ji0d9.cloudfront.net		13.224.102.63	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:42.680058002 CET	8.8.8.8	192.168.2.3	0x69c1	No error (0)	ekr.zdassets.com	cf.zdassets.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:42.680058002 CET	8.8.8.8	192.168.2.3	0x69c1	No error (0)	cf.zdassets.com		104.18.71.113	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:42.680058002 CET	8.8.8.8	192.168.2.3	0x69c1	No error (0)	cf.zdassets.com		104.18.70.113	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:43.884351969 CET	8.8.8.8	192.168.2.3	0x8fac	No error (0)	installer.corel.com		3.216.1.91	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:43.884351969 CET	8.8.8.8	192.168.2.3	0x8fac	No error (0)	installer.corel.com		34.192.198.140	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.291548014 CET	8.8.8.8	192.168.2.3	0xed3d	No error (0)	munchkin.marketo.net	wildcard.marketo.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 02:38:44.291623116 CET	8.8.8.8	192.168.2.3	0xb746	No error (0)	optanon.blob.core.windows.net	blob.db3prdstr11a.store.core.windows.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:44.291623116 CET	8.8.8.8	192.168.2.3	0xb746	No error (0)	blob.db3prdstr11a.store.core.windows.net		52.239.137.4	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.294724941 CET	8.8.8.8	192.168.2.3	0x7c36	No error (0)	a.opmnstr.com	opmnstr.awesomemotive.netdna-cdn.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:44.294724941 CET	8.8.8.8	192.168.2.3	0x7c36	No error (0)	opmnstr.awesomemotive.netdna-cdn.com		23.111.11.182	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.317939997 CET	8.8.8.8	192.168.2.3	0x9e32	No error (0)	static.hotjar.com	static-cdn.hotjar.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:44.317939997 CET	8.8.8.8	192.168.2.3	0x9e32	No error (0)	static-cdn.hotjar.com		13.224.102.68	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.317939997 CET	8.8.8.8	192.168.2.3	0x9e32	No error (0)	static-cdn.hotjar.com		13.224.102.14	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.317939997 CET	8.8.8.8	192.168.2.3	0x9e32	No error (0)	static-cdn.hotjar.com		13.224.102.20	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.317939997 CET	8.8.8.8	192.168.2.3	0x9e32	No error (0)	static-cdn.hotjar.com		13.224.102.53	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.318548918 CET	8.8.8.8	192.168.2.3	0xc48b	No error (0)	d2bqow4fb67vs2.cloudfront.net		13.224.89.106	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.318548918 CET	8.8.8.8	192.168.2.3	0xc48b	No error (0)	d2bqow4fb67vs2.cloudfront.net		13.224.89.166	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.318548918 CET	8.8.8.8	192.168.2.3	0xc48b	No error (0)	d2bqow4fb67vs2.cloudfront.net		13.224.89.215	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.318548918 CET	8.8.8.8	192.168.2.3	0xc48b	No error (0)	d2bqow4fb67vs2.cloudfront.net		13.224.89.10	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.347455025 CET	8.8.8.8	192.168.2.3	0x5ac6	No error (0)	s3-us-west-2.amazonaws.com		52.218.248.16	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.350223064 CET	8.8.8.8	192.168.2.3	0xd409	No error (0)	s3.amazonaws.com		52.216.147.61	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.787628889 CET	8.8.8.8	192.168.2.3	0x3031	No error (0)	corel.zendesk.com		104.16.51.111	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.787628889 CET	8.8.8.8	192.168.2.3	0x3031	No error (0)	corel.zendesk.com		104.16.53.111	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.901367903 CET	8.8.8.8	192.168.2.3	0xe5bd	No error (0)	api.omappapi.com	d1lpgznae1530s.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:44.901367903 CET	8.8.8.8	192.168.2.3	0xe5bd	No error (0)	d1lpgznae1530s.cloudfront.net		13.224.102.10	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.901367903 CET	8.8.8.8	192.168.2.3	0xe5bd	No error (0)	d1lpgznae1530s.cloudfront.net		13.224.102.46	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.901367903 CET	8.8.8.8	192.168.2.3	0xe5bd	No error (0)	d1lpgznae1530s.cloudfront.net		13.224.102.94	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:44.901367903 CET	8.8.8.8	192.168.2.3	0xe5bd	No error (0)	d1lpgznae1530s.cloudfront.net		13.224.102.47	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.347599030 CET	8.8.8.8	192.168.2.3	0xf8cf	No error (0)	script.hotjar.com		13.224.102.123	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.347599030 CET	8.8.8.8	192.168.2.3	0xf8cf	No error (0)	script.hotjar.com		13.224.102.122	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.347599030 CET	8.8.8.8	192.168.2.3	0xf8cf	No error (0)	script.hotjar.com		13.224.102.55	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 02:38:45.347599030 CET	8.8.8.8	192.168.2.3	0xf8cf	No error (0)	script.hotjar.com		13.224.102.49	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.347814083 CET	8.8.8.8	192.168.2.3	0xbd9e	No error (0)	www.trustedsite.com		44.239.103.44	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.347814083 CET	8.8.8.8	192.168.2.3	0xbd9e	No error (0)	www.trustedsite.com		44.240.129.90	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.352695942 CET	8.8.8.8	192.168.2.3	0xdd58	No error (0)	www.google.co.uk		172.217.21.195	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.382220030 CET	8.8.8.8	192.168.2.3	0xb87	No error (0)	280-qdk-215.mktoresp.com		192.28.147.68	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.396219969 CET	8.8.8.8	192.168.2.3	0xb12f	No error (0)	cdn.aimtell.com	dkjrr5t9da86f.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:45.396219969 CET	8.8.8.8	192.168.2.3	0xb12f	No error (0)	dkjrr5t9da86f.cloudfront.net		13.224.102.76	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.396219969 CET	8.8.8.8	192.168.2.3	0xb12f	No error (0)	dkjrr5t9da86f.cloudfront.net		13.224.102.109	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.396219969 CET	8.8.8.8	192.168.2.3	0xb12f	No error (0)	dkjrr5t9da86f.cloudfront.net		13.224.102.121	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.396219969 CET	8.8.8.8	192.168.2.3	0xb12f	No error (0)	dkjrr5t9da86f.cloudfront.net		13.224.102.57	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.441342115 CET	8.8.8.8	192.168.2.3	0x133e	No error (0)	vars.hotjar.com		13.224.102.94	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.441342115 CET	8.8.8.8	192.168.2.3	0x133e	No error (0)	vars.hotjar.com		13.224.102.47	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.441342115 CET	8.8.8.8	192.168.2.3	0x133e	No error (0)	vars.hotjar.com		13.224.102.36	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.441342115 CET	8.8.8.8	192.168.2.3	0x133e	No error (0)	vars.hotjar.com		13.224.102.79	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.442171097 CET	8.8.8.8	192.168.2.3	0x106b	No error (0)	danv01ao0kdr2.cloudfront.net		13.224.89.212	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.442171097 CET	8.8.8.8	192.168.2.3	0x106b	No error (0)	danv01ao0kdr2.cloudfront.net		13.224.89.133	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.442171097 CET	8.8.8.8	192.168.2.3	0x106b	No error (0)	danv01ao0kdr2.cloudfront.net		13.224.89.58	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.442171097 CET	8.8.8.8	192.168.2.3	0x106b	No error (0)	danv01ao0kdr2.cloudfront.net		13.224.89.63	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.525953054 CET	8.8.8.8	192.168.2.3	0x92c7	No error (0)	geolocation.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.525953054 CET	8.8.8.8	192.168.2.3	0x92c7	No error (0)	geolocation.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:45.537286043 CET	8.8.8.8	192.168.2.3	0x3e65	No error (0)	a.omappapi.com	omappapi.awesomemotive.netdna-cdn.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:45.537286043 CET	8.8.8.8	192.168.2.3	0x3e65	No error (0)	omappapi.awesomemotive.netdna-cdn.com		23.111.11.71	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:46.163875103 CET	8.8.8.8	192.168.2.3	0x1c26	No error (0)	widget-mediator.zopim.com		18.194.82.2	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:46.163875103 CET	8.8.8.8	192.168.2.3	0x1c26	No error (0)	widget-mediator.zopim.com		54.93.73.12	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:46.163875103 CET	8.8.8.8	192.168.2.3	0x1c26	No error (0)	widget-mediator.zopim.com		18.196.16.101	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:46.163875103 CET	8.8.8.8	192.168.2.3	0x1c26	No error (0)	widget-mediator.zopim.com		18.195.130.25	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 02:38:46.163875103 CET	8.8.8.8	192.168.2.3	0x1c26	No error (0)	widget-mediator.zopim.com		18.197.87.213	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:46.163875103 CET	8.8.8.8	192.168.2.3	0x1c26	No error (0)	widget-mediator.zopim.com		35.158.236.168	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:46.163875103 CET	8.8.8.8	192.168.2.3	0x1c26	No error (0)	widget-mediator.zopim.com		18.196.236.175	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:46.163875103 CET	8.8.8.8	192.168.2.3	0x1c26	No error (0)	widget-mediator.zopim.com		18.194.133.116	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:46.382289886 CET	8.8.8.8	192.168.2.3	0xa637	No error (0)	portal.brandlock.io	brandnode-1288026943.us-west-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:46.382289886 CET	8.8.8.8	192.168.2.3	0xa637	No error (0)	brandnode-1288026943.us-west-2.elb.amazonaws.com		52.42.117.229	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:46.382289886 CET	8.8.8.8	192.168.2.3	0xa637	No error (0)	brandnode-1288026943.us-west-2.elb.amazonaws.com		34.210.118.39	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:47.372052908 CET	8.8.8.8	192.168.2.3	0xd600	No error (0)	www.coreldraw.com	www.coreldraw.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:47.857013941 CET	8.8.8.8	192.168.2.3	0x1b2b	No error (0)	in.hotjar.com	insights-in-1202607485.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:38:47.857013941 CET	8.8.8.8	192.168.2.3	0x1b2b	No error (0)	insights-in-1202607485.eu-west-1.elb.amazonaws.com		52.31.241.82	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:47.857013941 CET	8.8.8.8	192.168.2.3	0x1b2b	No error (0)	insights-in-1202607485.eu-west-1.elb.amazonaws.com		34.252.252.123	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:47.857013941 CET	8.8.8.8	192.168.2.3	0x1b2b	No error (0)	insights-in-1202607485.eu-west-1.elb.amazonaws.com		34.255.46.51	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:47.857013941 CET	8.8.8.8	192.168.2.3	0x1b2b	No error (0)	insights-in-1202607485.eu-west-1.elb.amazonaws.com		54.246.211.3	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:47.857013941 CET	8.8.8.8	192.168.2.3	0x1b2b	No error (0)	insights-in-1202607485.eu-west-1.elb.amazonaws.com		52.208.77.122	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:47.857013941 CET	8.8.8.8	192.168.2.3	0x1b2b	No error (0)	insights-in-1202607485.eu-west-1.elb.amazonaws.com		54.74.233.68	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:47.857013941 CET	8.8.8.8	192.168.2.3	0x1b2b	No error (0)	insights-in-1202607485.eu-west-1.elb.amazonaws.com		52.31.127.7	A (IP address)	IN (0x0001)
Nov 22, 2020 02:38:47.857013941 CET	8.8.8.8	192.168.2.3	0x1b2b	No error (0)	insights-in-1202607485.eu-west-1.elb.amazonaws.com		99.80.174.18	A (IP address)	IN (0x0001)
Nov 22, 2020 02:39:22.783267021 CET	8.8.8.8	192.168.2.3	0x7658	No error (0)	ads.youtube.com	www3.l.google.com		CNAME (Canonical name)	IN (0x0001)
Nov 22, 2020 02:39:36.741090059 CET	8.8.8.8	192.168.2.3	0xacb5	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 22, 2020 02:38:32.886800051 CET	108.128.94.32	443	192.168.2.3	49755	CN=fw.adsafeprotected.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 09 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Sat Oct 09 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		
Nov 22, 2020 02:38:33.086117029 CET	185.33.221.90	443	192.168.2.3	49756	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		
Nov 22, 2020 02:38:33.765818119 CET	104.244.38.20	443	192.168.2.3	49768	CN=*.adsafeprotected.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Jun 17 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Fri Jun 18 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Nov 22, 2020 02:38:33.765896082 CET	104.244.38.20	443	192.168.2.3	49767	CN=*.adsafeprotected.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Jun 17 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Fri Jun 18 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Nov 22, 2020 02:38:33.766027927 CET	104.244.38.20	443	192.168.2.3	49769	CN=*.adsafeprotected.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Jun 17 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Fri Jun 18 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 22, 2020 02:38:33.957057953 CET	91.228.74.198	443	192.168.2.3	49777	CN=*.quantserve.com, O=Quantcast Corporation, L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Oct 02 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Thu Oct 07 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Nov 22, 2020 02:38:33.986129999 CET	185.64.189.115	443	192.168.2.3	49778	CN=*.pubmatic.com, OU=Enterprise SSL Pro Wildcard, OU=PubMatic, O="PubMatic, Inc.", STREET=305 Main St, L=Redwood City, ST=CA, OID.2.5.4.17=94063, C=US CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Feb 22 01:00:00 CET 2019 Fri Nov 02 01:00:00 CET 2018	Mon Feb 22 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Sectigo RSA Organization Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
Nov 22, 2020 02:38:34.395817041 CET	104.244.38.20	443	192.168.2.3	49781	CN=*.adsafeprotected.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Jun 17 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Fri Jun 18 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Nov 22, 2020 02:38:36.612529993 CET	104.31.68.76	443	192.168.2.3	49798	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	Sat Oct 10 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sun Oct 10 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		
Nov 22, 2020 02:38:36.653139114 CET	104.31.68.76	443	192.168.2.3	49799	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	Sat Oct 10 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Sun Oct 10 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
					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		
Nov 22, 2020 02:38:44.105783939 CET	3.216.1.91	443	192.168.2.3	49834	CN=installer.corel.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 Apr 13 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Thu May 13 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		
Nov 22, 2020 02:38:44.361434937 CET	23.111.11.182	443	192.168.2.3	49838	CN=*.opmnstr.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Thu Apr 11 15:22:21 CEST 2019 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Sun Apr 11 15:22:21 CEST 2021 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Nov 22, 2020 02:38:44.610063076 CET	52.216.147.61	443	192.168.2.3	49843	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Nov 22, 2020 02:38:44.714050055 CET	52.216.147.61	443	192.168.2.3	49844	CN=s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Aug 04 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Mon Aug 09 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Nov 22, 2020 02:38:44.774375916 CET	52.218.248.16	443	192.168.2.3	49842	CN=*.s3-us-west-2.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 30 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Wed Aug 04 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Nov 22, 2020 02:38:44.782222986 CET	52.218.248.16	443	192.168.2.3	49841	CN=*.s3-us-west-2.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 30 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Wed Aug 04 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Nov 22, 2020 02:38:44.874686003 CET	104.16.51.111	443	192.168.2.3	49846	CN=corel.zendesk.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	Sun Jul 19 02:00:00 CEST 2020 Mon Jan 27 13:48:08 CET 2020	Mon Jul 19 14:00:00 CEST 2021 Wed Jan 01 00:59:59 CET 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b

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		
Nov 22, 2020 02:38:44.943931103 CET	52.218.248.16	443	192.168.2.3	49845	CN=*.s3-us-west-2.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 30 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Wed Aug 04 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Nov 22, 2020 02:38:45.611809969 CET	23.111.11.71	443	192.168.2.3	49859	CN=*.omappapi.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Mon Mar 16 17:48:27 CET 2020 Tue May 03 09:00:00 CEST 2011 Wed Jan 01 08:00:00 CET 2014 Tue Jun 29 19:06:20 CEST 2004	Wed Mar 16 17:48:27 CET 2022 Sat May 03 09:00:00 CEST 2031 Fri May 30 09:00:00 CEST 2031 Thu Jun 29 19:06:20 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
					CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Wed Jan 01 08:00:00 CET 2014	Fri May 30 09:00:00 CEST 2031		
					OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=US	Tue Jun 29 19:06:20 CEST 2004	Thu Jun 29 19:06:20 CEST 2034		
Nov 22, 2020 02:38:45.745716095 CET	44.239.103.44	443	192.168.2.3	49849	CN=*.trustedsite.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 Mar 09 01:00:00 CET 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	Fri Apr 09 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Nov 22, 2020 02:38:45.746829033 CET	192.28.147.68	443	192.168.2.3	49854	CN=*.mktoresp.com, OU=IT, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jan 17 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013 Fri Nov 10 01:00:00 CET 2006	Fri Jan 21 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023 Mon Nov 10 01:00:00 CET 2031	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
Nov 22, 2020 02:38:46.202047110 CET	18.194.82.2	443	192.168.2.3	49862	CN=*.zopim.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Sat May 30 02:00:00 CEST 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Mon May 31 01:59:59 CEST 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-5-13-18-51-45-43-27-21,29-23-24,0	74ad8ec6876e2e3366bfd566581ca7e8
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Nov 22, 2020 02:38:46.802881002 CET	52.42.117.229	443	192.168.2.3	49866	CN=*.brandlock.io CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu May 28 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jun 28 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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Nov 22, 2020 02:38:46.967089891 CET	52.42.117.229	443	192.168.2.3	49867	CN=*.brandlock.io CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Thu May 28 02:00:00 CEST 2020 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Jun 28 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		
Nov 22, 2020 02:38:47.941705942 CET	52.31.241.82	443	192.168.2.3	49875	CN=*.hotjar.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sat Aug 29 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 Sep 28 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
Nov 22, 2020 02:39:08.684052944 CET	52.218.248.16	443	192.168.2.3	49957	CN=*.s3-us-west-2.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 30 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Wed Aug 04 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Nov 22, 2020 02:39:08.689809084 CET	52.218.248.16	443	192.168.2.3	49958	CN=*.s3-us-west-2.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 30 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Wed Aug 04 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Nov 22, 2020 02:39:14.508841038 CET	52.218.248.16	443	192.168.2.3	50003	CN=*.s3-us-west-2.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 30 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Wed Aug 04 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Nov 22, 2020 02:39:14.510879040 CET	52.218.248.16	443	192.168.2.3	50002	CN=*.s3-us-west-2.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 30 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Wed Aug 04 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		
Nov 22, 2020 02:39:20.269526005 CET	52.218.248.16	443	192.168.2.3	50016	CN=*.s3-us-west-2.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 30 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Wed Aug 04 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 22, 2020 02:39:20.272449017 CET	52.218.248.16	443	192.168.2.3	50017	CN=*.s3-us-west-2.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Jul 30 02:00:00 CEST 2020 Tue Dec 08 13:05:07 CET 2015	Wed Aug 04 14:00:00 CEST 2021 Sat May 10 14:00:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		

Code Manipulations

Statistics

Behavior

chrome.exe
chrome.exe
chrome.exe

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 5128 Parent PID: 996

General

Start time:	02:38:24
Start date:	22/11/2020
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://otampadabola2.com'
Imagebase:	0x7ff77b960000
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

Analysis Process: chrome.exe PID: 3980 Parent PID: 5128

General

Start time:	02:38:25
Start date:	22/11/2020
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=1564,10723194021886127913,5669998590995236100,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1756 /prefetch:8
Imagebase:	0x7ff77b960000
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	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: 6404 Parent PID: 5128

General

Start time:	02:38:34
Start date:	22/11/2020
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=audio.mojom.AudioService --field-trial-handle=1564,10723194021886127913,5669998590995236100,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=5960 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly