ID: 404015
Cookbook: browseurl.jbs
Time: 16:34:28
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Analysis Report https://protect-us.mimecast.com/s/HvV…

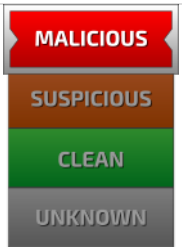
Overview

General Information

Sample URL:	http://https://protect-us.mimecast.com/s/HvV0Cn58k7CA73Ec9v4Fg?domain=lnkd.in
Analysis ID:	404015
Infos:	

Most interesting Screenshot:

Detection



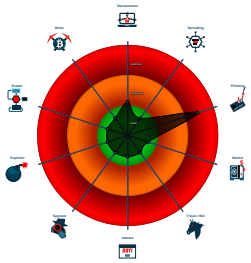
HTMLPhisher

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Yara detected HtmlPhish10
- Yara detected HtmlPhish7
- HTML body contains low number of …
- HTML title does not match URL
- Suspicious form URL found

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 2576 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://protect-us.mimecast.com/s/HvV0Cn58k7CA73Ec9v4Fg?domain=lnkd.in' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5208 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1564,2383217152926214841,1807454043240481656,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1772 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

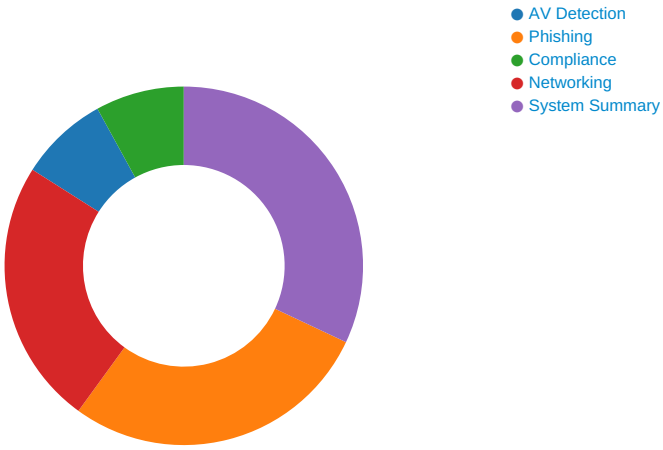
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:

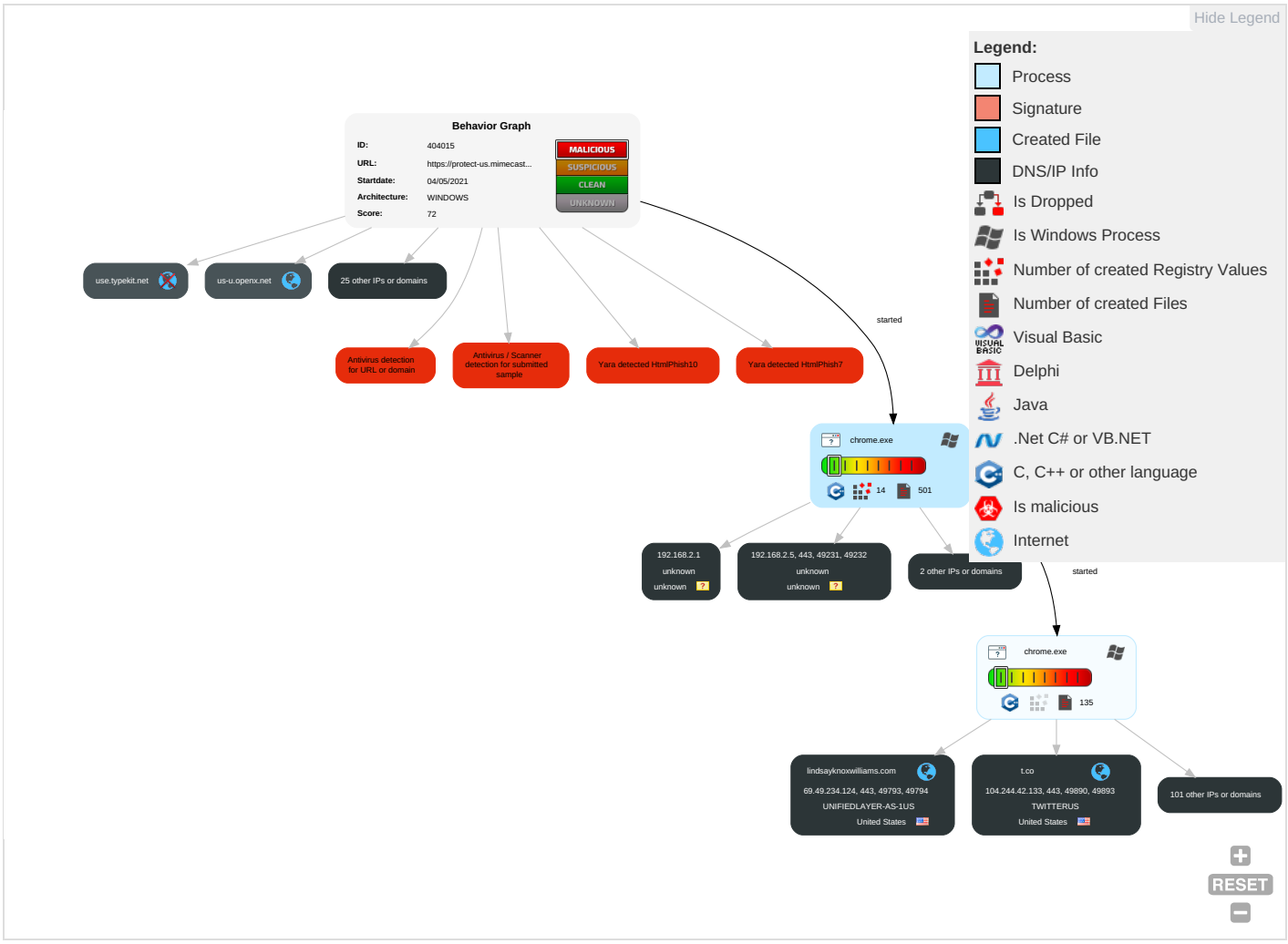
Yara detected HtmlPhish10

Yara detected HtmlPhish7

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 1	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

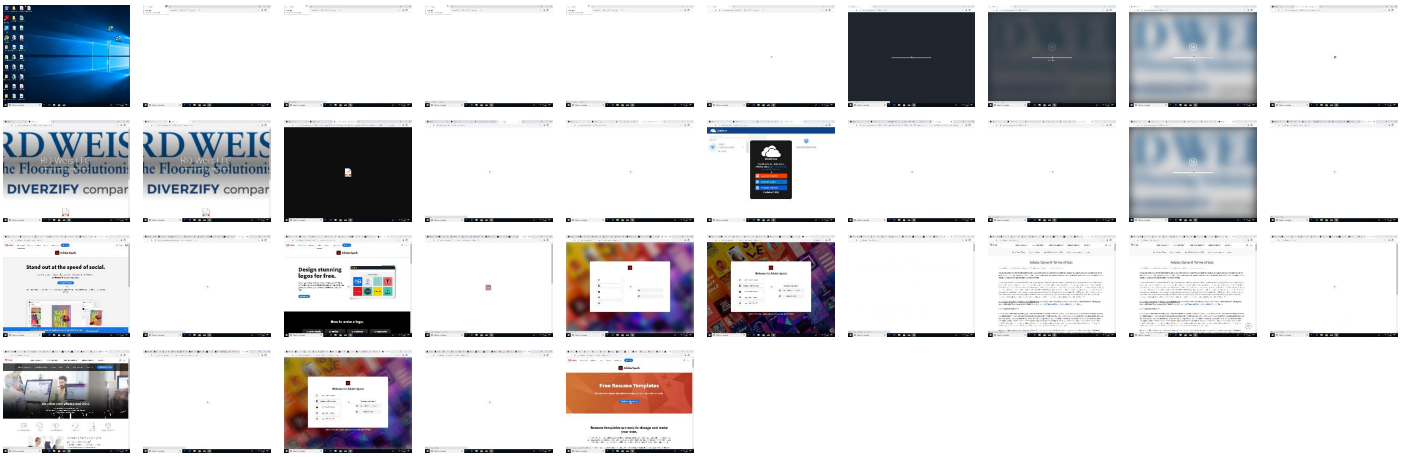
Behavior Graph



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://protect-us.mimecast.com/s/HvV0Cn58k7CA73Ec9v4Fg?domain=lnkd.in	0%	Avira URL Cloud	safe	
http://https://protect-us.mimecast.com/s/HvV0Cn58k7CA73Ec9v4Fg?domain=lnkd.in	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://lindsayknoxwilliams.com/Bernard/Vargas/	100%	UrlScan	phishing brand: onedrive generic	Browse

Source	Detection	Scanner	Label	Link
http://https://lindsayknoxwilliams.com/Bernard/Vargas/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://lindsayknoxwilliams.com/	0%	Avira URL Cloud	safe	
http://https://9212252.fls.doubleclick.net)	0%	Avira URL Cloud	safe	
http://https://lindsayknoxwilliams.com/Bernard/Vargas	0%	Avira URL Cloud	safe	
http://https://lindsayknoxwilliams.com/Bernard/Vargas/Share	0%	Avira URL Cloud	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://prod.adobeccstatic.com/utilnav/8.2/utilitynav.css	0%	Avira URL Cloud	safe	
http://https://blog.adobespark.com/wp-json/wp/v2/	0%	Avira URL Cloud	safe	
http://https://static.ads-twitter.com/uwt.js	0%	URL Reputation	safe	
http://https://static.ads-twitter.com/uwt.js	0%	URL Reputation	safe	
http://https://static.ads-twitter.com/uwt.js	0%	URL Reputation	safe	
http://https://lnkd.in/erSai7KR	0%	Avira URL Cloud	safe	
http://https://cookiepedia.co.uk/host/.app.onetrust.com?_ga=2.157675898.1572084395.1556120090-1266459230.15	0%	Avira URL Cloud	safe	
http://https://www.cookiepro.com/products/cookie-consent/	0%	Avira URL Cloud	safe	
http://https://lnkd.in/erSai7K2	0%	Avira URL Cloud	safe	
http://https://sc-static.net/scevent.min.js	0%	Avira URL Cloud	safe	
http://https://lindsayknoxwilliams.com/rU	0%	Avira URL Cloud	safe	
http://https://lnkd.in/erSai7KRD	0%	Avira URL Cloud	safe	
http://https://lindsayknoxwilliams.com/P	0%	Avira URL Cloud	safe	
http://https://page.adobespark-assets.com/runtime/1.22/images/favicon.ico	0%	Avira URL Cloud	safe	
http://https://spark.adobe.com/page/Eo8M9TkyXs7ta/?page-mode=static	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://https://spark.adobe.com/page/Eo8M9TkyXs7ta/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
protect-us.mimecast.com	205.139.111.113	true	false		high
pug-lhr.pubmatic.com	185.64.190.80	true	false		high
px2.px.quantserve.com	91.228.74.189	true	false		high
segments.company-target.com	13.225.74.27	true	false		unknown
tr.snapchat.com	35.186.226.184	true	false		high
tag.device9.com	34.251.104.84	true	false		unknown
platform.twitter.map.fastly.net	199.232.136.157	true	false		unknown
bttrack.com	192.132.33.46	true	false		unknown
s3.amazonaws.com	52.216.79.14	true	false		high
t.co	104.244.42.133	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
api.demandbase.com	13.225.74.124	true	false		high
cm.g.doubleclick.net	142.250.186.98	true	false		high
id.rlcdn.com	35.244.174.68	true	false		high
page.adobespark-assets.com	13.224.193.29	true	false		unknown
star-mini.c10r.facebook.com	31.13.92.36	true	false		high
match.prod.bidr.io	52.19.106.86	true	false		unknown
lindsayknoxwilliams.com	69.49.234.124	true	false		unknown
pix-us.revjet.com	51.81.46.161	true	false		high
us-u.openx.net	35.244.159.8	true	false		high
s.twitter.com	104.244.42.195	true	false		high
services.prod.ims.adobejanus.com	63.32.113.5	true	false		unknown
sc-static.net	13.225.74.126	true	false		unknown
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
bam.nr-data.net	162.247.242.19	true	false		unknown
googleads.g.doubleclick.net	142.250.185.130	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ams01.sync.search.spotxchange.com	185.94.180.125	true	false		high
a.tribalfusion.com	104.18.12.5	true	false		high
aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com	52.58.248.2	true	false		high
ml314.com	52.31.168.5	true	false		unknown
googlehosted.l.googleusercontent.com	216.58.212.129	true	false		high
cdn.cookielaw.org	104.16.148.64	true	false		high
dart.l.doubleclick.net	142.250.185.102	true	false		high
pixel-origin.mathtag.com	185.29.133.199	true	false		high
s.tribalfusion.com	104.18.12.5	true	false		high
g2.gumgum.com	54.247.114.64	true	false		high
pop-eda6.mix.linkedin.com	108.174.11.69	true	false		high
dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com	18.200.233.208	true	false		high
spark.adobeprojectm.com	143.204.98.51	true	false		unknown
scontent.xx.fbcdn.net	31.13.92.14	true	false		high
idsync.rlcdn.com	35.244.174.68	true	false		high
adobe.com.ssl.d1.sc.omtrdc.net	35.181.18.61	true	false		unknown
demdex.net.ssl.sc.omtrdc.net	35.181.18.61	true	false		unknown
adobe.tt.omtrdc.net	54.75.9.158	true	false		unknown
prod.adobeccstatic.com	13.224.193.51	true	false		unknown
mwsyncpixel.eu-west-1.elasticbeanstalk.com	34.240.86.127	true	false		high
stackpath.bootstrapcdn.com	104.18.11.207	true	false		high
dd20fzx9mj46f.cloudfront.net	13.224.187.69	true	false		high
www.google.de	142.250.184.195	true	false		high
pixel.tapad.com	35.227.248.159	true	false		high
pagead46.l.doubleclick.net	142.250.186.162	true	false		high
iad06-usadmm-ds.dotomi.com	205.180.85.201	true	false		high
adobelogin-origin.prod.ims.adobejanus.com	54.73.76.208	true	false		unknown
ethos51-prod-va6-k8s-pub2-0-dd4b5c1747f92a5e.elb.us-east-1.amazonaws.com	3.223.65.39	true	false		high
s.thebrighttag.com	34.248.208.147	true	false		high
lnkd.in	108.174.10.10	true	false		unknown
api.company-target.com	143.204.98.86	true	false		unknown
ib.anycast.adnxs.com	37.252.173.38	true	false		high
geolocation.onetrust.com	104.20.185.68	true	false		high
scripts.demandbase.com	13.224.193.78	true	false		high
static.ads-twitter.com	unknown	unknown	false		unknown
ka-f.fontawesome.com	unknown	unknown	false		high
ims-na1.adobelogin.com	unknown	unknown	false		high
pixel.everesttech.net	unknown	unknown	false		high
adservice.google.de	unknown	unknown	false		high
cm.everesttech.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
adobedc.demdex.net	unknown	unknown	false		high
static.adobelogin.com	unknown	unknown	false		high
adobe.demdex.net	unknown	unknown	false		high
use.typekit.net	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
assets.adobedtm.com	unknown	unknown	false		high
rtd.tubemogul.com	unknown	unknown	false		high
pixel.rubiconproject.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
px.ads.linkedin.com	unknown	unknown	false		high
d.turn.com	unknown	unknown	false		high
p.typekit.net	unknown	unknown	false		high
sync.mathtag.com	unknown	unknown	false		high
sync-tm.everesttech.net	unknown	unknown	false		high
p.rfihub.com	unknown	unknown	false		high
image2.pubmatic.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
dpm.demdex.net	unknown	unknown	false		high
aa.agkn.com	unknown	unknown	false		high
servedby.flashtalking.com	unknown	unknown	false		high
rtd-tm.everesttech.net	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.facebook.com	unknown	unknown	false		high
bumper.adobeprojectm.com	unknown	unknown	false		unknown
www.linkedin.com	unknown	unknown	false		high
js-agent.newrelic.com	unknown	unknown	false		high
pixel.quantserve.com	unknown	unknown	false		high
adobe-sync.dotomi.com	unknown	unknown	false		high
lasteventf-tm.everesttech.net	unknown	unknown	false		high
www.everestjs.net	unknown	unknown	false		high
analytics.twitter.com	unknown	unknown	false		high
dsum-sec.casalemedia.com	unknown	unknown	false		high
snap.licdn.com	unknown	unknown	false		high
9212252.fls.doubleclick.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://9212252.fls.doubleclick.net/activityi;dc_pre=CPvRwoegsPACFcSAewodM-4LsA;src=9212252;type=invmedia;cat=japan000;dc_lat=;dc_rdid=;tag_for_child_directed_treatment=;tfua=;npa=;ord=9744082147173.045?	false		high
http://https://lindsayknoxwilliams.com/Bernard/Vargas/	true	• 100%, UrlScan, Browse • SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://https://9212252.fls.doubleclick.net/activityi;dc_pre=CJbe3oCgsPACFVqTewod6-MF_g;src=9212252;type=invmedia;cat=japan000;dc_lat=;dc_rdid=;tag_for_child_directed_treatment=;tfua=;npa=;ord=2783188260717.3774?	false		high
http://https://9212252.fls.doubleclick.net/activityi;dc_pre=CKLMwI-gsPACFYW8ewodSPUDog;src=9212252;type=invmedia;cat=japan000;dc_lat=;dc_rdid=;tag_for_child_directed_treatment=;tfua=;npa=;ord=1813091254297.3433?	false		high

URLs from Memory and Binaries

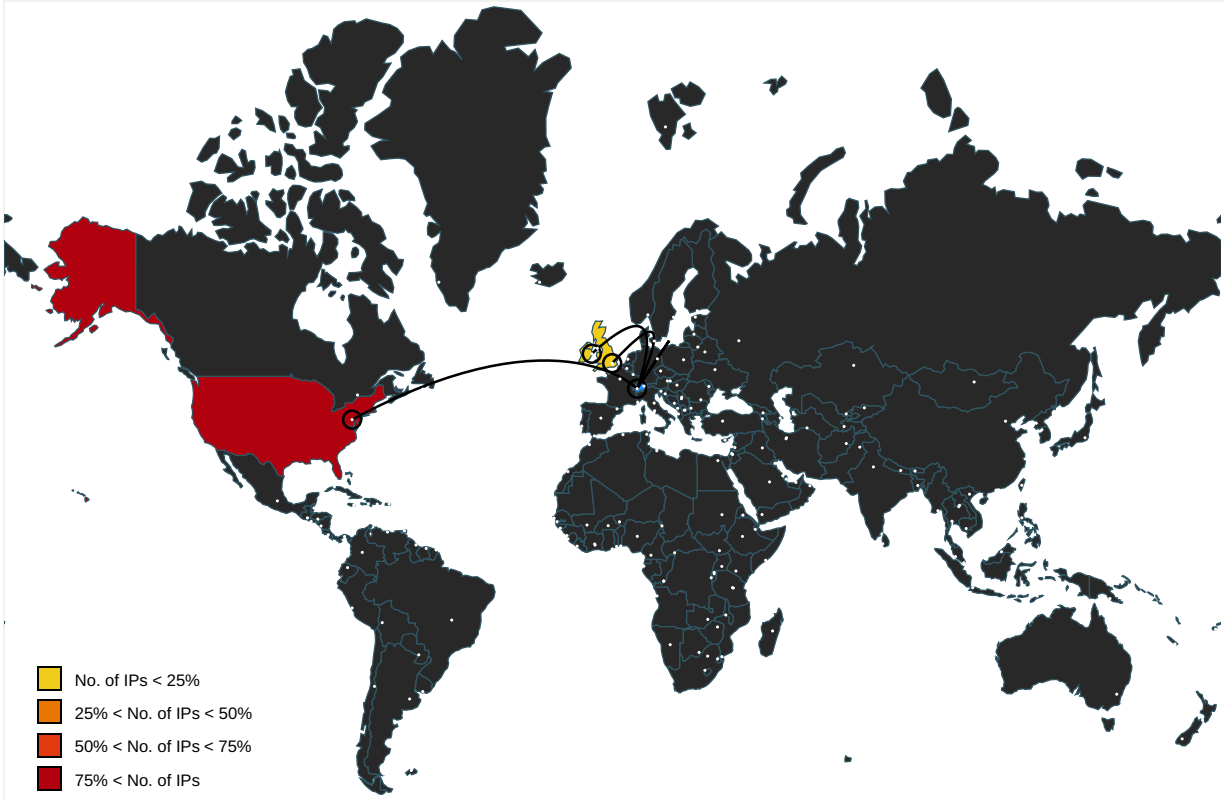
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.linkedin.com/slink?code=erSai7KRD	History-journal.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/951622910/?random=1620171405914&cv=	d9cf9443d75c501a_0.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/983956512/?random=1620171405792&cv=	4f3af61e14a7c13e_0.0.dr	false		high
http://https://www.linkedin.com/li/repC	Reporting and NEL.1.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/983956512/?random=1620171389474&cv=	fb1bf3e12ee62174_0.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/1004494713/?random=1620171376026&cv	7ad07de8579b1fd1_0.0.dr	false		high
http://https://code.jquery.com/jquery-3.2.1.slim.min.js	2bec0e299b9329e1_0.0.dr	false		high
http://https://lindsayknoxwilliams.com/	Network Action Predictor-journal.0.dr, 2bec0e299b9329e1_0.0.dr, 6a11233d0598b9fe_0.0.dr, 5db8039e291244de_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://9212252.fls.doubleclick.net)	Current Session.0.dr	false	• Avira URL Cloud: safe	low
http://https://9212252.fls.doubleclick.net/activityi;dc_pre=CPmLtYagsPACFcDZEQgdtAEEjQ;src=9212252;type=inv	Current Session.0.dr	false		high
http://https://assets.adobedtm.com/launch-EN919758db9a654a17bac7d184b99c4820.min.js	a6942155eb9698ff_0.0.dr	false		high
http://https://use.typekit.net/af/97fbd1/00000000000000003b9b3f88/27/	36d0235949f31082_0.0.dr	false		high
http://https://a.nel.cloudflare.com/report?s=9hucRgVLLNNGXxcPklvVsC4i%2BFw%2FGaRq5lGeqQIZeCangNl8WGb0XaAGs7	Reporting and NEL.1.dr	false		high
http://https://json-schema.org/draft/2019-09/vocab/	af374cb4784ea935_0.0.dr	false		high
http://https://9212252.fls.doubleclick.net/activityi;dc_pre=CJbe3oCgsPACFVqTewod6-MF_g;src=9212252;type=inv	Current Session.0.dr	false		high
http://https://giphy.com/	ba23d8ecda68de77_1.0.dr	false		high
http://https://www.linkedin.com/li/repY	Reporting and NEL.1.dr	false		high
http://https://9212252.fls.doubleclick.net	Current Session.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/951622910/?random=1620171405787&cv=	0a2d93a31980ff5d_0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://px.ads.linkedin.com/collect?	c1edc6da6ebfc6d9_0.0.dr	false		high
http://https://static.adobelogin.com/imslib/imslib.min.js	a8448f8e0f201664_0.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/951622910/?random=1620171375999&cv=	8f03a761ab0a7cc9_0.0.dr	false		high
http://https://protect-us.mimecast.com/s/HvV0Cn58k7CA73Ec9v4Fg?domain=lnkd.in0	History-journal.0.dr	false		high
http://https://connect.facebook.net/en_US/fbevents.js	d6595452d2846755_0.0.dr	false		high
http://https://9212252.fls.doubleclick.net/activityi;dc_pre=CPvRwoegsPACFcSAewodM-4LsA;src=9212252;type=inv	Current Session.0.dr	false		high
http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f675e54cc6b6/RCbbd93c1920fd422b84787f67ddbfbe5	022f580e45e66582_0.0.dr	false		high
http://https://kit.fontawesome.com/585b051251.js	e15c9c6281009a1f_0.0.dr	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	5f9866b4455c9fbb_0.0.dr	false		high
http://https://protect-us.mimecast.com/s/HvV0Cn58k7CA73Ec9v4Fg?domain=lnkd.in2	History Provider Cache.0.dr	false		high
http://https://use.typekit.net/onz5gap.js	36d0235949f31082_0.0.dr	false		high
http://https://use.typekit.net/af/3d913c/00000000000000000000017709/26/	04e3f25e64ef23bc_0.0.dr	false		high
http://https://adobesparkpost.app.link/qtResize	ba23d8ecda68de77_1.0.dr	false		high
http://https://servedby.flashtalking.com	Current Session.0.dr	false		high
http://https://lindsayknoxwilliams.com/Bernard/Vargas	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://lindsayknoxwilliams.com/Bernard/Vargas/Share	History-journal.0.dr	true	• Avira URL Cloud: safe	unknown
http://https://protect-us.mimecast.com/s/HvV0Cn58k7CA73Ec9v4Fg?domain=lnkd.in&w	History-journal.0.dr	false		high
http://https://dns.google	0e35d00b-e134-4ac4-837e-1017474e3718.tmp.1.dr, 94756ca2-525b-4394-88c6-953a1b662453.tmp.1.dr, da9b0a4d-8f97-4264-8c82-840a340a81f4.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn.cookielaw.org/scripttemplates/6.9.0/otBannerSdk.js	7a906a6be84e1af0_0.0.dr, 2354abbff3a2b46a_0.0.dr	false		high
http://https://use.typekit.net/	Network Action Predictor-journal.0.dr	false		high
http://https://prod.adobeccstatic.com/utilnav/8.2/utilitynav.css	ba23d8ecda68de77_1.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://maxcdn.bootstrapcdn.com/	Network Action Predictor-journal.0.dr	false		high
http://https://fb.me/react-async-component-lifecycle-hooks	f2045d66a6ee901f_0.0.dr	false		high
http://https://use.typekit.net/af/edcf1e/00000000000000000000158d9/26/	04e3f25e64ef23bc_0.0.dr	false		high
http://https://blog.adobespark.com/wp-json/wp/v2/	ba23d8ecda68de77_1.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js	5f6f8ddc9b9453d5_0.0.dr	false		high
http://https://kit.fontawesome.com/	Network Action Predictor-journal.0.dr	false		high
http://https://use.typekit.net/rbi5aua.js	04e3f25e64ef23bc_0.0.dr	false		high
http://https://9212252.fls.doubleclick.net/activityi;dc_pre=CKLMwI-gsPACFYW8ewodSPUDog;src=9212252;type=inv	Current Session.0.dr	false		high
http://https://servedby.flashtalking.com/container/13539;99030;10307;iframe/?ftXRef=&ftXValue=&ftXType=&ftX	Current Session.0.dr	false		high
http://https://static.ads-twitter.com/uwt.js	528df7fa00e0aa0d_0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/webpack-contrib/style-loader#insertat)	af374cb4784ea935_0.0.dr	false		high
http://https://9212252.fls.doubleclick.net/activityi;dc_pre=CNaX9oygsPACFZTeEQgdW9AM8Q;src=9212252;type=inv	Current Session.0.dr	false		high
http://https://d9.flashtalking.com/d9core	9f7e885e8c444e3d_0.0.dr	false		high
http://https://lnkd.in/erSai7KR	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://static.adobelogin.com/	Network Action Predictor.0.dr	false		high
http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f675e54cc6b6/RC1a83c357d323419db9d2ba211efeeaa	67b7e7530ed32021_0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://protect-us.mimecast.com/s/HvV0Cn58k7CA73Ec9v4Fg?domain=lnkd.inRD	History-journal.0.dr	false		high
http://https://protect-us.mimecast.com/s/HvV0Cn58k7CA73Ec9v4Fg?domain=lnkd.in	Current Session.0.dr, History-journal.0.dr	false		high
http://crl.godaddy.com/repository/gdroot.crl0J	EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D0.1.dr	false		high
http://https://adobespark.zendesk.com/hc/en-us/articles/219243657	9d8177d41f917273_0.0.dr	false		high
http://https://cdn.cookielaw.org/	Network Action Predictor-journal.0.dr	false		high
http://https://flashtalking.com/	9f7e885e8c444e3d_0.0.dr	false		high
http://https://cookiepedia.co.uk/host/.app.onetrust.com?_ga=2.157675898.1572084395.1556120090-1266459230.15	7a906a6be84e1af0_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://tr.snapchat.com/p	Current Session.0.dr	false		high
http://https://use.typekit.net/onz5gap.jsaD	36d0235949f31082_0.0.dr	false		high
http://https://www.cookiepro.com/products/cookie-consent/	8ea8fd6251ae6b4d_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://ims-na1.adobelogin.com	ba23d8ecda68de77_1.0.dr	false		high
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://use.typekit.net/af/9951d2/00000000000000000000158d7/26/	04e3f25e64ef23bc_0.0.dr	false		high
http://https://cdn.cookielaw.org/scripttemplates/otSDKStub.js	0ba91aa6ae29d08a_0.0.dr	false		high
http://braze.com	67a473248953641b_0.0.dr	false		high
http://https://adobespark.zendesk.com/hc/en-us/articles/218956027	9d8177d41f917273_0.0.dr	false		high
http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f675e54cc6b6/RCcb1611437f6c42849c41ffe54a71d59	9efdd4a8d8632664_0.0.dr	false		high
http://https://lnkd.in/erSai7K2	History Provider Cache.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://npms.io/search?q=ponyfill.	7451b1541ed8a461_0.0.dr	false		high
http://https://protect-us.mimecast.com/s/HvV0Cn58k7CA73Ec9v4Fg?domain=lnkd.inSQLite	History.0.dr	false		high
http://https://sc-static.net/scevent.min.js	7812293e5d091f0b_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/983956512/?random=1620171405910&cv=	0cba5b2c919929e8_0.0.dr	false		high
http://https://lindsayknoxwilliams.com/rU	082f28e6a371a71f_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://lnkd.in/erSai7KRD	History-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://use.typekit.net/af/9d1933/00000000000000000001705b/26/	04e3f25e64ef23bc_0.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/987390658/?random=1620171389276&cv=	f5d20470cbe29465_0.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/983956512/?random=1620171376030&cv=	8c42284ea9fac8ba_0.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/987390658/?random=1620171405675&cv=	bd72fd9df2e083f3_0.0.dr	false		high
http://https://opsparc.gsfc.nasa.gov/?sdid=MC95SNMJ&mv=social	9d8177d41f917273_0.0.dr	false		high
http://https://protect-us.mimecast.com/redirect/eNqtlttu20YQhl_FYG8tec8Hoygin4C0jRHYDVKgKoTZ3VmJjSiqJGXXDfz	Favicons-journal.0.dr	false		high
http://https://a.nel.cloudflare.com/report?s=ZgdWosJxMeM7Y5Ps3aWTo3PIlZ9bz3QuVP5Z%2BEMJMNEDszuWbap3ARUEXKuM	Reporting and NEL.1.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/1004494713/?random=1620171386749&cv	dd2b34ebf898b0c6_0.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/983956512/?random=1620171386740&cv=	2d7f286d74a18ae7_0.0.dr	false		high
http://https://servedby.flashtalking.com/	000003.log0.0.dr	false		high
http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f675e54cc6b6/RC6f46e43fa6d44dbeb45cc5801ffded0	4e4147266d5a1b82_0.0.dr	false		high
http://https://lindsayknoxwilliams.com/P	e15c9c6281009a1f_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://page.adobespark-assets.com/runtime/1.22/images/favicon.ico	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://adservice.google.de/ddm/fls/i/dc_pre=CJbe3oCgsPACFVqTewod6-MF_g;src=9212252;type=invmedia;ca	Current Session.0.dr	false		high
http://https://js-agent.newrelic.com/nr-1177.min.js	d1e9bca73e9ccebd_0.0.dr	false		high
http://https://use.typekit.net/af/180c9d/00000000000000003b9b3f8a/27/	36d0235949f31082_0.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.225.74.126	sc-static.net	United States		16509	AMAZON-02US	false
31.13.92.36	star-mini.c10r.facebook.com	Ireland		32934	FACEBOOKUS	false
13.225.74.124	api.demandbase.com	United States		16509	AMAZON-02US	false
142.250.185.102	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false
52.216.79.14	s3.amazonaws.com	United States		16509	AMAZON-02US	false
13.224.193.78	scripts.demandbase.com	United States		16509	AMAZON-02US	false
205.180.85.201	iad06-usadmm-ds.dotomi.com	United States		26762	CNVR-US-EASTUS	false
104.16.148.64	cdn.cookielaw.org	United States		13335	CLOUDFLARENETUS	false
13.225.74.27	segments.company-target.com	United States		16509	AMAZON-02US	false
143.204.98.51	spark.adobeprojectm.com	United States		16509	AMAZON-02US	false
63.32.113.5	services.prod.ims.adobejanus.com	United States		16509	AMAZON-02US	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
35.227.248.159	pixel.tapad.com	United States		15169	GOOGLEUS	false
192.132.33.46	bttrack.com	United States		18568	BIDTELLECTUS	false
69.49.234.124	lindsayknoxwilliams.com	United States		46606	UNIFIEDLAYER-AS-1US	false
13.224.187.69	dd20fzx9mj46f.cloudfront.net	United States		16509	AMAZON-02US	false
104.244.42.133	t.co	United States		13414	TWITTERUS	false
13.224.193.29	page.adobespark-assets.com	United States		16509	AMAZON-02US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.223.65.39	ethos51-prod-va6-k8s-pub2-0-dd4b5c1747f92a5e.elb.us-east-1.amazonaws.com	United States		14618	AMAZON-AESUS	false
35.186.226.184	tr.snapchat.com	United States		15169	GOOGLEUS	false
35.244.174.68	id.rlcdn.com	United States		15169	GOOGLEUS	false
104.18.12.5	a.tribalfusion.com	United States		13335	CLOUDFLARENETUS	false
104.18.10.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
162.247.242.19	bam.nr-data.net	United States		23467	NEWRELIC-AS-1US	false
91.228.74.189	px2.px.quantserve.com	United Kingdom		27281	QUANTCASTUS	false
31.13.92.14	scontent.xx.fbcdn.net	Ireland		32934	FACEBOOKUS	false
185.29.133.199	pixel-origin.mathtag.com	United Kingdom		30419	MEDIAMATH-INCUS	false
216.58.212.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
52.19.106.86	match.prod.bidr.io	United States		16509	AMAZON-02US	false
18.200.157.96	unknown	United States		16509	AMAZON-02US	false
108.174.10.10	lnkd.in	United States		14413	LINKEDINUS	false
108.174.11.69	pop-eda6.mix.linkedin.com	United States		14413	LINKEDINUS	false
13.224.193.51	prod.adobeccstatic.com	United States		16509	AMAZON-02US	false
142.250.186.98	cm.g.doubleclick.net	United States		15169	GOOGLEUS	false
205.139.111.113	protect-us.mimecast.com	United States		30031	MIMECAST-US	false
142.250.186.162	pagead46.l.doubleclick.net	United States		15169	GOOGLEUS	false
54.75.9.158	adobe.tt.omtrdc.net	United States		16509	AMAZON-02US	false
104.244.42.195	s.twitter.com	United States		13414	TWITTERUS	false
52.31.168.5	ml314.com	United States		16509	AMAZON-02US	false
104.18.11.207	stackpath.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
52.58.248.2	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
104.20.185.68	geolocation.onetrust.com	United States		13335	CLOUDFLARENETUS	false
142.250.185.130	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
35.181.18.61	adobe.com.ssl.d1.sc.omtrdc.net	United States		16509	AMAZON-02US	false
143.204.98.86	api.company-target.com	United States		16509	AMAZON-02US	false
18.200.233.208	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
199.232.136.157	platform.twitter.map.fastly.net	United States		54113	FASTLYUS	false
34.251.104.84	tag.device9.com	United States		16509	AMAZON-02US	false

Private

IP
192.168.2.1
192.168.2.7
192.168.2.5
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404015
Start date:	04.05.2021
Start time:	16:34:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs

Sample URL:	http://https://protect-us.mimecast.com/s/HvV0Cn58k7CA73Ec9v4Fg?domain=lnkd.in
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:	10
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:	MAL
Classification:	mal72.phis.win@51/309@86/53
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://spark.adobe.com/page/Eo8M9TkyXs7ta/?page-mode=static • Browse: https://spark.adobe.com/page/Eo8M9TkyXs7ta/images/6064272a-2f19-415b-a277-ddfca1a623bc.png?asset_id=f43008a8-a1f1-45e8-bbd4-44b1887775c4&img_etag=%220x8D90ECCBEFBAA75%22&size=1024 • Browse: https://lindsayknoxwilliams.com/Bernard/Vargas • Browse: https://spark.adobe.com/page/Eo8M9TkyXs7ta/images/e9072759-ba5d-4fcf-98a2-f56dfa6b4923.png?asset_id=539231b7-6c0a-4efa-a8ab-e78efa3957de&img_etag=%220x8D90ECCD704924A%22&size=1024 • Browse: https://spark.adobe.com/page/Eo8M9TkyXs7ta • Browse: https://spark.adobe.com/about?r=reader_page_logo • Browse: https://spark.adobe.com/make/logo-maker?r=reader_page_learnmore • Browse: https://spark.adobe.com/login?r=reader_page_bumper_createyourown • Browse: http://www.adobe.com/legal/terms.html • Browse: http://www.adobe.com/go/privacy • Browse: https://spark.adobe.com/login?r=reader_page_topbar_createyourown • Browse: https://spark.adobe.com/templates/resumes/
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 168.61.161.212, 52.255.188.83, 13.64.90.137, 92.122.145.220, 104.42.151.234, 142.250.185.206, 142.250.185.78, 216.58.212.173, 95.168.222.146, 34.104.35.123, 142.250.184.195, 184.30.24.56, 13.107.42.14, 23.32.238.192, 23.32.238.210, 23.37.33.211, 142.250.185.106, 142.250.185.138, 142.250.185.170, 142.250.185.202, 142.250.185.234, 142.250.181.234, 216.58.212.170, 142.250.74.202, 142.250.186.42, 142.250.186.74, 142.250.186.106, 142.250.186.138, 142.250.186.170, 142.250.184.202, 142.250.184.234, 172.217.18.106, 172.217.23.106, 2.20.142.210, 2.20.142.209, 69.16.175.42, 69.16.175.10, 172.217.16.138, 104.18.22.52, 104.18.23.52, 142.250.185.227, 172.64.101.17, 172.64.100.17, 95.101.22.203, 95.101.22.195, 23.57.80.54, 23.57.81.34, 192.124.249.36, 192.124.249.22, 192.124.249.41, 192.124.249.24, 192.124.249.23, 23.37.44.206, 142.250.185.136, 204.79.197.200, 13.107.21.200, 23.57.82.43, 63.33.127.66, 34.246.227.69, 99.80.199.35, 205.185.216.10, 205.185.216.42, 151.101.2.49, 151.101.66.49, 151.101.130.49, 151.101.194.49, 142.250.184.194, 13.225.74.13, 13.225.74.74, 13.225.74.111, 13.225.74.48, 142.250.185.162, 142.250.184.196, 142.250.186.80, 142.250.186.112, 142.250.186.144, 142.250.186.176, 142.250.184.208, 142.250.184.240, 172.217.18.112, 172.217.23.112, 216.58.212.144, 142.250.185.80, 172.217.16.144, 142.250.185.112, 142.250.185.144, 142.250.185.176, 142.250.185.208, 142.250.185.240, 151.101.2.110, 151.101.66.110, 151.101.130.110,

151.101.194.110, 34.253.145.149, 34.250.153.194, 99.81.11.244, 34.255.166.243, 54.171.42.33, 54.194.191.134, 13.224.193.34, 13.224.193.52, 13.224.193.115, 13.224.193.82, 3.251.13.136, 54.217.37.194, 52.87.45.233, 52.3.102.249, 46.228.164.13, 193.0.160.129, 172.217.23.99, 69.173.144.165, 69.173.144.138, 69.173.144.139, 23.57.81.215, 142.250.185.67, 20.82.210.154, 2.20.84.251

- TCP Packets have been reduced to 100
- Created / dropped Files have been reduced to 100
- Excluded domains from analysis (whitelisted): gstaticadssl.l.google.com, d.turn.com.akadns.net, ka-f.fontawesome.com.cdn.cloudflare.net, storage.googleapis.com, www.everestjs.net.edgekey.net, cn-assets.adobedtm.com.edgekey.net, clientservices.googleapis.com, fs-wildcard.microsoft.com.edgekey.net, server.messaging.adobe.com, l-0005.l-msedge.net, clients2.google.com, use-stls.adobe.com.edgesuite.net, ssl-delivery.adobe.com.edgekey.net, afp.dotomi.weighted.com.akadns.net, www.google.com, au-bg-shim.trafficmanager.net, dual-a-0001.a-msedge.net, cm.everesttech.net.akadns.net, a-emea.rfihub.com.akadns.net, edgedl.me.gvt1.com, c.bing.com, dsum-sec.casalemedia.com.edgekey.net, clients.l.google.com, geo2.adobe.com, e4578.a.akamaiedge.net, h2.shared.global.fastly.net, cds.f7f2q8c3.hwcdn.net, e4578.dscg.akamaiedge.net, c-bing-com.a-0001.a-msedge.net, adservice.google.com, e9706.dscg.akamaiedge.net, e12564.dspb.akamaiedge.net, www.googletagmanager.com, arc.trafficmanager.net, prod.fs.microsoft.com.akadns.net, client.messaging.adobe.com, skypedataprdcolwus17.cloudapp.net, accounts.google.com, fonts.gstatic.com, a767.dscg3.akamai.net, cc-api-data.adobe.io, stls.adobe.com-cn.edgesuite.net, adobeid-na1.services.adobe.com, e7808.dscg.akamaiedge.net, wildcard.licdn.com.edgekey.net, cdn.cp.adobe.io, r7---sn-n02xgoxufvg3-2gbs.gvt1.com, e6653.dscf.akamaiedge.net, cds.s5x3j6q5.hwcdn.net, arc.msn.com.nsatc.net, commerce.adobe.com, spark.adobe.com, audownload.windowsupdate.nsatc.net, update.googleapis.com, tp00.everesttech.net.akadns.net, watson.telemetry.microsoft.com, www.gstatic.com, ocsp.godaddy.com.akadns.net, e9518.c.akamaiedge.net, fonts.googleapis.com, fs.microsoft.com, content-autofill.googleapis.com, stls.adobe.com-cn.edgesuite.net.globalredir.akadns.net, ajax.googleapis.com, sparkbumper-production1-va6.cloud.adobe.io, commerce.adobe.com.edgekey.net, skypedataprdcolcus17.cloudapp.net, www.googleapis.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, a1815.dscr.akamai.net, au.download.windowsupdate.com.edgesuite.net, www.googleadservices.com, pixel.rubiconproject.net.akadns.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, e8037.g.akamaiedge.net, redirector.gvt1.com, bat.bing.com, a.rfihub.com.akadns.net, www-linkedin-com.l-0005.l-msedge.net, kit.fontawesome.com.cdn.cloudflare.net, sstats.adobe.com, p.typekit.net-v3.edgekey.net, www-googletagmanager.l.google.com, f4.shared.global.fastly.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, sync.search-gtm.spotxchange.com.akadns.net, skypedataprdcoleus17.cloudapp.net, r7.sn-n02xgoxufvg3-2gbs.gvt1.com, bat-bing-com.a-0001.a-msedge.net, ocsp.godaddy.com, skypedataprdcolwus16.cloudapp.net, a1988.dscg1.akamai.net, www.adobe.com

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

Simulations

Behavior and APIs

Time	Type	Description
16:35:56	API Interceptor	3x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
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\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1731
Entropy (8bit):	7.318888900464152
Encrypted:	false
SSDEEP:	48:panitqGVRfanGnita8lnitq1+Zvl3oXS9As5RmEWqu5H99:pWoMndz1+boavLJpu5
MD5:	8CEA9D9ED7168F33CBFBE1C0B4C00D5B
SHA1:	AD5B642EA39022F2F4EB2570A4AADF58E9E7F3D2
SHA-256:	5A0181CD13E0AFF2D43A58B023F3E4D5E6DCAF7293082102FCED6194C534200E
SHA-512:	BA8A7A2B8ED3C4BDF30A888BA86DAEFB8FCA869116A602D00C980662B78731B118E74CCE1B0E9D57B3675CF75CC40B7C3C3828515D577E1C62186D4DC7BA775
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0.....0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U...'Go Daddy Root Validation Authority - G2..20210503204504Z0d0b0:0...+.....#o..K.....#....+...:....g(.....An .....20210503204504Z....20210505084504Z0...*.H.....z.....'$.....2.xq..@x...P?...:a.g.v.N.T....7J.,I.0p..c..d=...t..R.8.d..;i...AZ.#...x[BE.M.=.`&.$zmL.2....`....M.P4.DB*.m..#JC...H/.\...G5i..a>.uj.i.H...?.....O..ZY.n}$..).0kZ<..[...H..=q.....s"..z{.T|/.C...:....iO.0.)...f.;..o..W.X.(...h....0...0...0..g.....f...p.t0...*.H.....0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.110/..U...(Go Daddy Root Certificate Authority - G20...200909070000Z..210909070000Z0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U...'Go Daddy Root Validation Authority - G20.."0...*.H.....0.....'....^Y.u..U.qU..."......-]XG(qk#.+....J...G.3

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Reputation:	low
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-J...."Y...$E.KB..D...D.....3.n..u.....|..=H4..c&.....f.,..=..-....p2.:..`HX.....b.....Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..|0.+?.`-../.xvy..e.....w.+^...w|.Q.k.9&.Q.EzS.f.....>?w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_..).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s...,f`D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.I....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1697
Entropy (8bit):	7.313644488434989
Encrypted:	false
SSDEEP:	48:snitqJCLoo5nruVnitqsXA49e5REMeZ6+23wQ:UJfo5wsw49eEMeZ6+Y
MD5:	6D5131A0D3B08AF0F2789ABE2C7A03D6
SHA1:	6D566FC1046E91F9BC857047A2CA925D09519BB4
SHA-256:	2D569EE91CFBCAA016601EEBE10DA3572EEBA739AB4D5D651205251E37C0EDB2

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D	
SHA-512:	1914B7DA4862B28BB1C3529F85072EDDC5889B3D4964113347F3B8FD3757BAD9AC055209E79FF94821A43D0A402890C7A9BE0FF27F4D246643023495DD5D0D7C
Malicious:	false
Reputation:	low
Preview:	0.....0.....+.....0.....0...0.....0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U...'Go Daddy Root Validation Authority - G1..20210503153653Z0f0d0<0...+..... .....]..J^.y_..F<.....L.q.a.=...j.....20210503153653Z....2021050503033653Z0...*.H.....px....B...../.`..}.T+.<....AO[.)P.Jm....'..@.....v..K-.g...w.....mL.>.H.bZ<.irv..$.....O.[l..l3&k.@.g..ZK.9K...I)..j..oZ...u&v.....Y1...W.....8....oL.=-..][.ku...u[....@%*...T..}..o.8.J....k.2VD..v..Y..w..b.....0...?Z.....f...%.. ...-...b0..^0..Z0..B.....1g...r.0...*.H.....0c1.0...U....US1!0...U....The Go Daddy Group, Inc.110/..U...(Go Daddy Class 2 Certification Authority0...161213070000Z..211213070000Z0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U...'Go Daddy Root Validation Authority - G10.."0...*.H.....0.....}...@.H.....j.b.2.c....'eSA...6""2.hf.m.m9....._N."gV..{.J"{..0f.W$.X

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\223DE96EE265046957A660ED7C9DD9E7_EFF9B9BA98DEAA773F261FA85A0B1771	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	900
Entropy (8bit):	3.6974322360913887
Encrypted:	false
SSDEEP:	24:B3wyPV13MhmyFqPvNpgwyPV13MhmyFqPvr:B3wkV1XyFCpgwkV1XyFE
MD5:	D713315BB86CB8197B6A7450EE96DF0E
SHA1:	879B359018E1180BDA29C174F55A6A7A4C8182E0
SHA-256:	FFC1CDC6EF58A32A3372416E88CB7E3AB7D1259C72864F7C178B89A73E4B8BFC
SHA-512:	4D26036E36157FDD47CF412C804BD34650D55EF5FD02F7A55B0AABE70D18292858873ECEC5A4BADE6B1B0B3D57336260884F3EF6EC0F6A2796244EA822C53F5
Malicious:	false
Reputation:	low
Preview:	p..... .....e.jh>A..(..... .....1]@.....V.....h.t.t.p.:././.o.c.s.p...g.o.d.a.d.d.y...c.o.m././.M.E.I.w.Q.D.A.%.2.B.M.D.w.w.O.j.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.Q.d.I.2.%.2.B.O.B.k.u.X.H.9.3.f.o.R.U.j.4.a.7.l.A.r.4.r.G.w.Q.U.O.p.q.F.B.x.B.n.K.L.b.v.9.r.0.F.Q.W.4.g.w.Z.T.a.D.9.4.C.A.Q.c.%.3.D...".a.d.5.b.6.4.2.e.a.3.9.0.2.2.f.2.f.4.e.b.2.5.7.0.a.4.a.a.d.f.5.8.e.9.e.7.f.3.d.2."...p..... .....e.jh>A..(.....1]@...hG.A.....hG.A.. .....1]@.....V.....h.t.t.p.:././.o.c.s.p...g.o.d.a.d.d.y...c.o.m././.M.E.I.w.Q.D.A.%.2.B.M.D.w.w.O.j.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.Q.d.I.2.%.2.B.O.B.k.u.X.H.9.3.f.o.R.U.j.4.a.7.l.A.r.4.r.G.w.Q.U.O.p.q.F.B.x.B.n.K.L.b.v.9.r.0.F.Q.W.4.g.w.Z.T.a.D.9.4.C.A.Q.c.%.3.D...".a.d.5.b.6.4.2.e.a.3.9.0.2.2.f.2.f.4.e.b.2.5.7.0.a.4.a.a.d.f.5.8.e.9.e.7.f.3.d.2."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.129251112301174
Encrypted:	false
SSDEEP:	6:kKs2wTJ0N+SkQlPlEGYRMY9z+4KlDA3RUe0ht:nwTJrkPlE99SNxAhUe0ht
MD5:	A01347EA697182CD3E8B57C5195EAB7D
SHA1:	3E813768006776BE1CDE03DB9CA1084F9DD5950F
SHA-256:	4613236CD1B7A4C2168481C04EA547C6A34C11AC62B40E8928C81D9EA48D8F31
SHA-512:	7977E6F649B29EC7343043BD483CA9681E8D5714EC94CDBEF5B37461C4C60988FDD90C4750702C8320917035F2E33DA36A30FA5EAE1C3DBF89AD442ABF93E53
Malicious:	false
Reputation:	low
Preview:	p..... .....;>A..(..... .....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."..0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	916
Entropy (8bit):	3.78902069774868
Encrypted:	false
SSDEEP:	12:THmzrQEFDsFrvgxE0P6GANMjOpuZUQOlUHd0cNzrQEFDsFrvgxE0P6GANMjOpuZV:yzV4xaVSGAmqpuEuzV4xaVSGAmqpuL
MD5:	CF0D40989E4B4334E4A16F0F7EF4EF2F
SHA1:	A1D987D19A6572915648432C8C98FA198118FEF2
SHA-256:	68C3B716E47711E3F3C3133C8C803DC4DD2E4C67AB94EC3C46CBDB70AC110281
SHA-512:	3BC29AEAAD4ABECD2A781960BD0A6A4504A81BB55C3B381E5894B5E324BBE2C7D38E57989F6C5BC8AFE430A56F0F8C9AC61AFBE909F7CC8B5ECADCDB2431C008
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D	
Preview:	p..... .....jV>A..(..... .....*$2@.....V.....h.t.t.p.:././.o.c.s.p...g.o.d.a.d.d.y...c.o.m././.M.E.Q.w.Q.j.B.A.M.D.4.w.P.D.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.k.I.I.n.K.B.A.z.X.k.F.0.Q.h.0.p.e.l.3.l.f.H.J.9.G.P.A.Q.U.0.s.S.w.0.p.H.U.T.B.F.x.s.2.H.L.P.a.H.%.2.B.3.a.h.q.1.O.M.C.A.x.v.n.F.Q.%.3.D.%.3.D...".6.d.5.6.6.f.c.1.0.4.6.e.9.1.f.9.b.c.8.5.7.0.4.7.a.2.c.a.9.2.5.d.0.9.5.1.9.b.b.4."...p..... .....jV>A..(.....*$2@....._A..... ._A.. .....*$2@.....V.....h.t.t.p.:././.o.c.s.p...g.o.d.a.d.d.y...c.o.m././.M.E.Q.w.Q.j.B.A.M.D.4.w.P.D.A.J.B.g.U.r.D.g.M.C.G.g.U.A.B.B.T.k.I.I.n.K.B.A.z.X.k.F.0.Q.h.0.p.e.l.3.l.f.H.J.9.G.P.A.Q.U.0.s.S.w.0.p.H.U.T.B.F.x.s.2.H.L.P.a.H.%.2.B.3.a.h.q.1.O.M.C.A.x.v.n.F.Q.%.3.D.%.3.D...".6.d.5.6.6.f.c.1.0.4.6.e.9.1.f.9.b.c.8.5.7.0.4.7.a.2.c.a.9.2.5.d.0.9.5.1.9.b.b.4."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\3977a942-715b-4166-a0f2-acbea28ee790.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94772
Entropy (8bit):	3.749187897346947
Encrypted:	false
SSDEEP:	384:Wbgf/FCsZGdRVOUD+NrrwvHN3Afl8H18GcLr2hbHxwRx1ArqnmiG4iNzTTsO5RLb:YWalFCZEs8ebXZJHQ3v+FKn9DwY
MD5:	379952D0B8D9C3CAF38AC9CB33575DC3
SHA1:	B2B9920789AE692A61BFB9C4C26EB26F1F240FEF
SHA-256:	D8381F8AEE02C1F379DD9947F9E1521FBF812E3722D747E69E80F633A2BCB7DD
SHA-512:	64F97E466C7FBDDAB2AE766E7AA4A0A8BABBDC7AFAA0CF5673034ECC7A235991BC1481E6307F265640D9E7691DA2844F92F3B86389710A07920918CA3C19F25E
Malicious:	false
Reputation:	low
Preview:	0r.....*...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....98.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\44e89e7f-3234-4a78-8309-c5fd5d24a710.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):	361356
Entropy (8bit):	6.022417974365728
Encrypted:	false
SSDEEP:	6144:kuhZZ4/fHwt8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBA:xvg/nxzurRDn9nfNxF4ijZVtilBA
MD5:	2731AA000E85C64ECA6BEE0DC2C024B8
SHA1:	73ABDF6EAE0A8E4C63529A31AF2564CC91113169
SHA-256:	720F2BAECD9DF209AF263CC174FECF24056D446F3AAE256A6D0C781A0DBD8E92
SHA-512:	6FEC5EA32C3C4F43FE8246296FED5FB52E8DFCD49C7EC5104BC39C10C70E4B050E5D7FDCD4C9C6E160DCD825E0FDB1C12426C230B095961EDE19565BA6AACB9
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":1.620171333790254e+12,"network":1.620138935e+12,"ticks":120758603.0,"uncertainty":4579143.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxlY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075330779"},"policy":{"last_statistics_update":"13264644928802

C:\Users\user\AppData\Local\Google\Chrome\User Data\568764d5-e503-4764-982a-7e7e5b51ed43.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):	359252
Entropy (8bit):	6.015404067964013
Encrypted:	false
SSDEEP:	6144:2uhZZ4/fHwt8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBA:vvg/nxzurRDn9nfNxF4ijZVtilBA
MD5:	582CC06BE90878304AA33CF93BD105BD
SHA1:	CC6166174818E185F4601D5E8EA2BEBD9DE260F3
SHA-256:	B825AA64E62F751E46A28D1B648810072179B99288BA9E7531E3D0F8A77CAFAA
SHA-512:	5B5D89AA727ECEE0F604745EDF83A5A24B615B713D1D3E21B65718154343D081823BC8378C7E9A743596D314867BC977082D13DD6ED64ADF30651C80B63F3B4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\568764d5-e503-4764-982a-7e7e5b51ed43.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.620171333790254e+12,"network":1.620138935e+12,"ticks":120758603.0,"uncertainty":4579143.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13264644928802

C:\Users\user\AppData\Local\Google\Chrome\User Data\5c46785d-732a-426b-a667-b6407df8455a.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):	362826
Entropy (8bit):	6.027966015706294
Encrypted:	false
SSDEEP:	6144:LuhZZ4/fHwt8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBA:8vg/nxzurRDn9nfNxF4ijZVtilBA
MD5:	2CD06349DD314B25BCD64CC7D557B131
SHA1:	04A4FD7AC80971BDF1D2F0545EE1E972D8467963
SHA-256:	B19DF4F81DDDA69EA5E0820FCFEA0BA57150A92FBC9CD6E6ED050D14A14258E9
SHA-512:	EB7332D957F73485BE2AD642E233BEB81283225F0962A8DA0828438BCECFA2DB692A142ED2992483657AF7FD29BDAA15250F6EC117491B39B1A5BD3F64922D1
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":1.620171333790254e+12,"network":1.620138935e+12,"ticks":120758603.0,"uncertainty":4579143.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075330779"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\6861407b-ccc3-41e3-98ff-31441736264e.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):	359253
Entropy (8bit):	6.015403295097497
Encrypted:	false
SSDEEP:	6144:yuhZZ4/fHwt8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBA:jvg/nxzurRDn9nfNxF4ijZVtilBA
MD5:	D21AF192B50F973D0282CC4202A94A7E
SHA1:	C87535354A474955A2EF2F8A02A567758E09C502
SHA-256:	F751DFFD5DDE328A072B4550B9856918D0AA2697FB8A781184DB920EE58301E8
SHA-512:	5CEBF82B02E4D152A4B49ECB9AF067D1943D099C9BAF41EC0DB0B906B09D6C0078C347D4F4633B1848856F957599AFF188DBFF7103B1497FD5F22EE369C1308
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":1.620171333790254e+12,"network":1.620138935e+12,"ticks":120758603.0,"uncertainty":4579143.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075330779"},"policy":{"last_statistics_update":"13264644928802

C:\Users\user\AppData\Local\Google\Chrome\User Data\834d546e-3f60-4074-bca8-335f509852d8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94052
Entropy (8bit):	3.7490924715525886
Encrypted:	false
SSDEEP:	384:obgf/FCsZGdRVOUD+NrrwvHN3Afl8H18GcLr2hbHxwRx1ArqnmiliNzTTsO5RLNu:2WalFCZMs8ebXZJHQ3v+FKn9Dwf
MD5:	883BE96A489A7332DAFEB200DB821B2B
SHA1:	663B2ACBB241D9038D3C98386456C97DA0192D55
SHA-256:	D7EEA33B9AE3B50A5D29C639B798814E95122906B6D2EDCD5EB394AEEAA45222
SHA-512:	355B7010F8638A30584777940B52E74B5998A9A430083865DA0CE07950D823CAA5486316C51B933C4405A28A992C080263D7C83D6379CDA29B673D171254E530
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\834d546e-3f60-4074-bca8-335f509852d8.tmp	
Preview:	`o.............*...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....98.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o .m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f .f.i.c.e.1.6.\.......m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.......1.6...0...4.2.6.6...1.0.0.1.....D...C .:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXYDu6cR9iTXYDu6cR9iTXYDu6cR9n:+Y66cR4TXY66cR4TXY66cR9
MD5:	569FA64ACAA310B1DE1A6250CC7356B0
SHA1:	14251450C245F8612958BF94779E8B72AE6D6213
SHA-256:	AEE20ADEBF2D35EB8A39BE2DC391B0E5966EFCB4AFDC971BB3A18115C929F563
SHA-512:	850914A053EF541046B29260266C17FEFF2466A87784394F9AB3B565D2EA1E656F61F02BDB78F9F9676E90365F837F3709BCC0856B3B844256848F477250E0C7
Malicious:	false
Reputation:	low
Preview:	sdPC....................8...?E."..N_.sdPC....................8...?E."..N_.sdPC....................8...?E."..N_.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\24e6b832-965c-4ffa-961e-619677f6364c.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):	5624
Entropy (8bit):	5.181846515828031
Encrypted:	false
SSDEEP:	96:nIFGsgOfHG8OSVe+OIk0JCKL8kRkEx111ltbOTQVuwn:nIXfHG9SAhC4K3kQ1P
MD5:	D6850925BFEF394EB694CAC7FC507CED
SHA1:	F9CF7C5B83636C0668BBD7B9EF7CF7457C84FE13
SHA-256:	532C22333699010C7727EA6FAD17BFAEEE683880B5BC185ADCCAFFDA24593C52
SHA-512:	C92A49840E8FF1CB102156AA1D8FF902D7ABD0B119D2BB1AF1720703AAE04EA2A32C00B6C30449B2EBDC28CEF0D1CF1B34E7D416D42DEED4F9F6F24EA921FE88
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13264644929852012","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","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","1538886"],"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","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4ec8b620-bc9e-48af-83a0-dbee3f276a14.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):	1543
Entropy (8bit):	5.583526745172804
Encrypted:	false
SSDEEP:	48:YGEUW6UUh5rgUDwUDDKUeyBsmUJUeCmTwU6UUeh:eULUUfrgUsUDDKUZFUJUHVUDUc
MD5:	AB2E674D4065748AB47AC7FF18955515
SHA1:	8BF27D87A7BEE5C94567F550840AA1E62DB9EEC2
SHA-256:	3D99EF067E87BF87F7A8CDB33A6C8FB225D8F275684BF2A9D61A4922243DF19F
SHA-512:	56E71F3B5525A9981D0E4A355C08594211C41E51C30EAC013F4751E0D54104E9A300C7BDBE167FB76B230165B4E770253504DD7E801C5F8714664B8C626AEE60
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1651707340.919093,"host":"OJAwwDug+gPr+xWjx2kFIFhHDQULu5ljftVMMZ74I4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620171340.919097},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1651707338.638194,"host":"Qea0mu+MIu3KJ6YK35cSVLSQk3FGOPYjdJApFsmQfDA=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620171338.638199},{"expiry":1651707341.385815,"host":"YBf+o277nAvW3A1uFG7ThwT6zuF7asaeDH6RPNOXinc=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620171341.385821},{"expiry":1633013028.743725,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601477028.743728},{"expiry":1651707339.566534,"host":"tXjOdUMSBgtiUbrbGkl6XP80fiDB8uXOkUbnCf0IKvw=","mode":"force-https","sts_include_subdomains":false,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\544fa77b-91fb-4338-9d27-aaac5f75b413.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):	4714
Entropy (8bit):	5.596934441619867
Encrypted:	false
SSDEEP:	96:FRUX8sUVULUfRieUZU2UUTUNrgUHUujUJ1U7Uh1UZUXTUntU7UiU6KUNUeFUJUH3:bUX8sUVULUffUZU2UUTUFgUHUujUDU7S
MD5:	F013FB97A61B4B3E126FDD177624AF8D
SHA1:	D2F72D789F5E8F45D7EF1C1D790758CED316DB97
SHA-256:	63FA5AC249CDFD6C124DF5B8A0373DEBBB8791B80018E45270AB4BD1D75CA743
SHA-512:	1FBD7BFB888CBF3CCBE6FEEAF7D3A198575E35FA0F059DEDEC6F772B75D2F15795CE8DF63543D4955DF09A9AAE56C98809B45E544ED7CCFBA11D2BB6CE725 0B3
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1651707359.683095,"host":"AKBA0EXj1W1QmJumkxUOTpibikAwoUEp1CDrh5UFWY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620171359.683099},{"expiry":1651707467.179606,"host":"CJ6kx0n19VtUkGfz4J6tLFRfDatw73CAqzbGpnezKw0=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620171467.179611},{"expiry":1622763465.384606,"host":"Dg14flaciUHGX6Lc+OnYmaNiAA/ADiwumtIyPrC3d6U=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620171465.384611},{"expiry":1635951359.681047,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620171359.681051},{"expiry":1651707432.752908,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620171432.752911},{"expiry":1651707467.107785,"host":"OJAwwDug+gPr+xWjx2kFIFhHDQULu5ljftVMMZ74l4o=","mode":"force-https","sts_include_subdomains":true,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\545e668a-f2cd-4dff-898b-3a39ddb76845.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):	5221
Entropy (8bit):	5.59914790482545
Encrypted:	false
SSDEEP:	96:FRU18sUqvSUIBUfqULjfieUuU6UUTUNrgURUNUJUKUAUriUTTUYtU/UpUqULxKUb:bU18sUHUIBUfqULdUuU6UUTUFgURUNUx
MD5:	77D2286279A7F170E8908AD66A669CA9
SHA1:	8D95735A2E3BA3ADE14CD3DC645AF4A6E8EAD963
SHA-256:	50111533B31F4F2A230F04CD57FCB094B1F78B78AB8A1A3AE8DAE58DFF07216D
SHA-512:	C61C92F7A83AB6C135A5AD999698C34AC3AD2B4573807837A856200F2EC5D981C880F7B5260AE4093FDAE87C669E97024C4BCA2392DC5881C338DBBDEDDF3C 7
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1651707359.683095,"host":"AKBA0EXj1W1QmJumkxUOTpibikAwoUEp1CDrh5UFWY=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620171359.683099},{"expiry":1651707487.735411,"host":"CJ6kx0n19VtUkGfz4J6tLFRfDatw73CAqzbGpnezKw0=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620171487.735415},{"expiry":1622763478.645158,"host":"Dg14flaciUHGX6Lc+OnYmaNiAA/ADiwumtIyPrC3d6U=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620171478.645164},{"expiry":1635951359.681047,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620171359.681051},{"expiry":1651707478.095279,"host":"Hi4bEdMq563Qsqn4sVyUls/uVk7U80lxMa3wyWVUqWU=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620171478.095283},{"expiry":1651707485.539699,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7cb497c4-3e7f-4cac-b3c4-423691b20b16.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):	8726
Entropy (8bit):	4.828400077313548
Encrypted:	false
SSDEEP:	192:JOTXDHzY2u6gvKaRl5+xGC5C6N66YyZCzM7Ji6LP0M/kyzL+684t5SF/je4umGoy:JOTX7U2u6gvKaRl5+xGC5C6N66YyZCoZ
MD5:	DB25E8ABD93250270F84E56FA080B72C
SHA1:	7267C827E3A3AFD6EE26C1B56362F24D74C99D71
SHA-256:	067A637A6D6CFA388EB06684A96C099CFA6AE1342C36A41D970FF23E6D6A97ED
SHA-512:	73DBEA53BF4F9868BB2DDEC3F168C6AC36B61C6E52552D99C78FD8E33092B487E9C83F1A5DFA19B8CD23ABEFB7FEE69D90A1DB03C2F9D992A21A4558A0C99 A22
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"isolation":[],"server":"https://ssl.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://www.gstatic.com","supports_spdy":true},{"isolation":[],"server":"https://apis.google.com","supports_spdy":true},{"isolation":[],"server":"https://ogs.google.com","supports_spdy":true},{"isolation":[],"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13267236934242174","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://accounts.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13267236934250773","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://redirector.gvt1.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[50],"expiration":"13267236934630395","port":443,"protocol_str":"quic"},{"advertised_versions":[50],"expiration":"13267236934630398","port":443,"protocol_str

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7f4e61d1-360f-4c8e-94c2-2e0dbba8119d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.535690946625806
Encrypted:	false
SSDEEP:	384:JbItzLlMPXt1kXqKf/pUZNCgVLH2HfDmrU5HGvnTiMyo49:oLlKt1kXqKf/pUZNCgVLH2HfKrUdGvnC
MD5:	55D3BE1C20F2652B68B8E3A45A360F80
SHA1:	EE358FB7DFF3CCFDD4A541743225F3AB3FDF2622
SHA-256:	F9A2D90119852B1DB9A819B9F9D396431435481A7B039484F95B8D1D4E45A5F2
SHA-512:	7E401C7633F01D87F31DA9A80C5AF3C0B4F22861C271F96A49734C8965BF6E098A9B1F902BB7E334427D28CCBF3D61671808FCD3EDEDF5DAB305C3FB6689FE7
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":"13264644929346166","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\94756ca2-525b-4394-88c6-953a1b662453.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):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DBCAA
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9bdc9ce7-0606-448f-bbc8-7e5f33cdfd82.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22595
Entropy (8bit):	5.535780829614333
Encrypted:	false
SSDEEP:	384:JbItzLlMPXt1kXqKf/pUZNCgVLH2HfDmrU5HGknTiOyo4Ha:oLlKt1kXqKf/pUZNCgVLH2HfKrUdGknP
MD5:	38B9913ABFB6F1DB7455DA53F8102E1A
SHA1:	A1ECCA9328D51DBD67702EECCF224C125D130DA2
SHA-256:	D3DA0E657B0B029E992199AFB5B71E3927FC0720E4F94AD55E47755176D0E579
SHA-512:	91F3D2167003FF31508982F99381E7F9829F7C149F360A46C1A86BF715F3D35D0F16015B1B644468FFD6D021AA68EAAC934618D34EC0271CDD864A9BF10FF5FD
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":"13264644929346166","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
File Type:	ASCII text
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.185328992352869
Encrypted:	false
SSDEEP:	6:msTt+q2P923iKKdK9RXXTZIFUtpdToHZZmwPdToHNVkwO923iKKdK9RXX5LJ:t8v45Kk7XT2FUtpdw/Pd45L5Kk7XVJ
MD5:	3314ACFA0F7B837DA7E7B249725338B5
SHA1:	78329427BF010D4FF015E9017DA3E6CCE71C385E
SHA-256:	32D651788578580CD923D784D3A295C8136CA18E025B0233432E8A16A7173A53
SHA-512:	A99AD2F5CDF3C3819011B21EF6DDC6E63EC43D9267CDAB93B5C42306D333C0330CAB0C45AFA729F32AACDD2EE705BE0F2DAC06A60512A7F608B771F5740CA D97
Malicious:	false
Reputation:	low
Preview:	2021/05/04-16:35:50.529 1158 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/ 05/04-16:35:50.531 1158 Recovering log #3.2021/05/04-16:35:50.531 1158 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrik eDatabase/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):	320
Entropy (8bit):	5.211152371921958
Encrypted:	false
SSDEEP:	6:msTzSQ+q2P923iKKdKyDZIFUtpdTzckXZmwPdTzck3VkwO923iKKdKyJLJ:tqVv45Kk02FUtpdFX/PdFF5L5KkWJ
MD5:	593D233D928DC5080D33786C70A05AE5
SHA1:	7B53C7771C799CA04BE23DD83E3A3AF3C670FC21
SHA-256:	51121722BC966D8B380E82D497DBB1E5F4CECFAB813D3C44262F8AA3691150C0
SHA-512:	4773F1BF04EB27974079822427CF02E5193F26B7857435FB01F30954E0B1AD3D5EE93CB95B57467DE3A64D89A4403D4BBBD99EEB1D68269304AFC06A5D365B29
Malicious:	false
Reputation:	low
Preview:	2021/05/04-16:35:50.417 1158 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/05/04-16 :35:50.419 1158 Recovering log #3.2021/05/04-16:35:50.419 1158 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatab ase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\00a73600649a63ce_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1145
Entropy (8bit):	5.695722525580215
Encrypted:	false
SSDEEP:	12:Q/GpDd/V3m/GpDx/VENm/GpDgP8/Vhpm/GpDoz7/Vzm/GpDA2t/Vf:bDd/pFDx/SNFDgP8/tFDa/VFDl/9
MD5:	BCD66C43F76EBF637A9EBD84F22A400D
SHA1:	E40FAFF5869E87C701DC8ADB86D8609A0D3C6A30
SHA-256:	4CCC5715E3ACCAC0655EE146CC5A16546ABE103658B74F0FE65FE658990C9DE9
SHA-512:	B20598E0482EE51F4A166EE900A048FC431B6844B0D3913CFB18223F333D252BCB5CF8310FD364171EAF39B3E1C8CCC7C56B6064B3C54DCF055905D93204905A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a...&[....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-951622910&l=dataLayer&cx=c .https://adobe.com/.C?.. /.....y.....q...|.K...y.....YL...;..>J.. A..Eo.....bt.....A..Eo.....0\r..m.....a...&[....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-951622910&l=dataLayer&cx=c .https://adobe.com/r.... /..... .....q...|.K...y.....YL...;..>J..A..Eo.....*.....A..Eo.....0\r..m.....a...&[....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-951622910&l=dataLaye r&cx=c .https://adobe.com/..... /.....q...|.K...y.....YL...;..>J..A..Eo.....A..Eo.....0\r..m.....a...&[....._keyhttps://www.googletagmanager.com/gtag/j s?id=AW-951622910&l=dataLayer&cx=c .https://adobe.com/..... /.....].....q...|.K...y.....YL...;..>J..A..Eo.....A..Eo.....0\r..m.....a...&[....._keyh ttps://www.googletagmanager.com/gtag/js?id=AW-951622910

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\022f580e45e66582_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	538
Entropy (8bit):	5.660402235822865
Encrypted:	false
SSDEEP:	6:mK8Ycv0KgiSP8AlZtA4lsuIatrd6oLbQYEK6tWK8Ycv0KgiSP8AlZtA4lsuIa7kN:3ASPRNX3vbQB5ASPRNXVkPbQqN
MD5:	646C2B82A8559539829F5E92CC6819AB

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\022f580e45e66582_0	
SHA1:	60047863EB83B0824F69A8CF86885D30170D898B
SHA-256:	87AD68BB68076EF9064DD2317A70ED66007354D94C1EC6348E1CEE65757769EF
SHA-512:	2F0FF3F961FDA1AD68E23A9714625406781A3110F7F3702C9062A4A4CDD372122600971689457FE2E4D177349FA176960AE90FBCCFCF093D702461A397284529
Malicious:	false
Reputation:	low
Preview:	0\r..m.....:+K;...._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f675e54cc6b6/RCbbd93c1920fd422b84787f67ddbfbe55-file.min.js .https://adobe.com/.c... /.....t.....Z..d.z...0o..['.....}..xu.A..Eo.....Iza.....A..Eo.....0\r..m.....:+K;...._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f675e54cc6b6/RCbbd93c1920fd422b84787f67ddbfbe55-file.min.js .https://adobe.com/.9.. /.....Z..d.z...0o..['.....}..xu.A..Eo.....$`.A.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\04e3f25e64ef23bc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	13832
Entropy (8bit):	5.853853476768403
Encrypted:	false
SSDEEP:	192:NBcu6ntDtHBgPEhuhmuCWqoBsnADQdUo5bNrxmJR86QqhGvSb+kK2ZTVUw4:N7sRYdhmxWHqaExz6NhGnkKaTVUw4
MD5:	294C1E92E5700379414ED93F3869D022
SHA1:	5B4BBC61B8A9E571FBE9C4B6C6D9C3BD7DBDBCCD
SHA-256:	329A2821114984D4C5DFB30EADA107BD5C49052A1ABF52822A016470DDF7B77D
SHA-512:	88FE67D82BB8AD2114533E67B7861BB4508A91818ECDF9E76098BAF4EFE720929F93465B848609B97EE98272DC77603A752DE12454529CBE19A8C6BA260805F0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....:.....{....._keyhttps://use.typekit.net/rbi5aua.js .https://adobe.com/=o... /.....9...:'T4".y.a..z.~.Xey....1..A..Eo.....vv.....A..Eo.....'..J....O.....3..2y.1.....H.....(S.d..`.....$L`.....Qc*g.....window....Q.@.`_,....Typekit.....a>.....M...QcD.e.....1655249...Qb.....c.....`.....M`.....Qe./i.....tk-proxima-nova.(Qh.v....."proxima-nova",sans-serif....(Qh.....tk-proxima-nova-condensed...0Qj^m55#..."proxima-nova-condensed",sans-serif...Qbf.It....fi.....`.....,Mi....V...X...Z...\...^...`....*...*..$.....QbFm.Z....fc.....`.....,L`.....,a.....Qb.....id..`V.....Qc.....family....Qdb..d....proxima-nova..Qb.!.-....src..lQy...a_...https://use.typekit.net/af/e030d3/00000000000000000000158d3/26/{format}{?primer,subset_id,fvd,v}...Qd.....descriptors...,a.....Qc.4r.....weight....Qb.....100..q..!...Qc.>.o....display.....Qd...6....subset_id...`.....,a.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\082f28e6a371a71f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	366
Entropy (8bit):	5.944622171788523
Encrypted:	false
SSDEEP:	6:mAYSHT8NWQAlKPUQyTJAyFBtnXYfYkH4VFK6trzMOT2ueEnCXYfYkH4:nz8NWQCUUhJAyX5EwFzMi7eECE
MD5:	42D5CCE1F2169A1277573F756D8325A3
SHA1:	8519C1119087A172D4895891EDF8642B13AED7B8
SHA-256:	1C7B4BBD954EF9EBFF8AD4DA9DB4BD3ABDD2D970547E5055548767E2C5F1D968
SHA-512:	64979625B20356D71186D2A877ED43C1BB936F560152B955634BE57AB49117D1C862A7A1490C4E45E0B8965AAE244C5C2C872B61D6E8715879FD09ED760CDDC4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f...H.r....._keyhttps://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js .https://lindsayknoxwilliams.com/rU... /.....9.....I....^2.9..f.H...=..].(.....A..Eo.....8h.....A..Eo.....rU... /.Po..A20E39BA81960CF84FE4CF8C4114910A068DC3C9B72527BAB0025D9BA4A4BB0E.I....^2.9..f.H...=..].(.....A..Eo.....1.@L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0a2d93a31980ff5d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.810468609311142
Encrypted:	false
SSDEEP:	12:pE3GQFmoux2peyye3CMx0DPViH2NRmxACc0ey5UGyCd1:pEWQluyeyyeSVDN/OxACp5UG71
MD5:	2B648BAFAEFDAB3133DE5993D9308E37
SHA1:	6E06F9998A88CE74369D1CBA1C2D620FD029BF2A
SHA-256:	A1822699B5E44B459D825D59B6D85B065D2A11F44370B2F23C49AFEBAE0BE6FC
SHA-512:	1544266DBEA700F66D50ABB0CAA13BD5F071C1ED02C7B50A920DEB0F8C5DCAAF7F27219F24A1A0D8C4303193C61D1CD883169C3E4D022772D44101E1441088C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0a2d93a31980ff5d_0	
Preview:	0\r..m.....L&....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/951622910/?random=1620171405787&cv=9&fst=1620171405787&num=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&eid=2505059650&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa4l3&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fwww.adobe.com%2Fexpress%2Fdiscover%2Ftemplates%2Fresume&tiba=Free%20Resume%20Templates%20%7C%20Adobe%20Spark&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://adobe.com/q.... /.....$.....+3n..z....L^.N.....]..7.....A..Eo..... Z'd.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0b5f56a615420e43_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	336352
Entropy (8bit):	5.7473477396971555
Encrypted:	false
SSDEEP:	3072:M8FWoR0OQ0drN9WvM0yf3wYqB7GvRZAA7kW7A2lorJQMGUYPZaza:M8FRR0O/N96M0T47l7ploK3
MD5:	F25688C76794C28566DAA6843313959B
SHA1:	FEB7BC329586B1BC04D9A37066BCDAFD44F84EB5
SHA-256:	7B2E42BEB400D457C3111E2CEC1CCEE966922E60F31EA4E27CD5399931AB52FA
SHA-512:	7418416BF185089E9B6E5507387B65BC1D58658A17901E7B0FF089A87AC39508808745F516A4C54B56D4DEF1CAC3A93BFDFC8BDC0E801AA27CB036DD9CC81E03
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...9.^(....7A1551EAE279D3967EC7691F686D0C93827AC7A866D9991161502F899FED97D3.....'..;....Oh...p.....'&.....X'.....<.....H.....p.....p.....`.....`.....(S....`.....M.L`.....(S.`.`z.... L`.....@Rc.....M....O...Qbj.5.....c...b$.....I`....Da....~....(S...`.....L`.....Qc&.7:....exports..$..a.....a.....Qb..N.....id..C..Qc.}.R....loaded..H.....Qb:f.....call.....K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&.(...&...&.'..W.....-...(.....,Rc.....`....Da....<.....!.....e..... P.....@....@.-....PP.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0ba91aa6ae29d08a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	52062
Entropy (8bit):	6.190865479825867
Encrypted:	false
SSDEEP:	768:9PUpktV0xBN3EVUGhMq+7iH/NFZh/S5KeXmQQ60PnZRx//i7jihLkCO/F:pcB3oUGyqYQ/eaxRh/i72hkN/F
MD5:	79FE3935D9E9F207555870610C8F82DE
SHA1:	1CC15CA9AFA75A37933D90FE1B592A0224F866E2
SHA-256:	5C2EDF81969D07274697C00459FC500A174157DFD635A6D78CD643DA4FEF2861
SHA-512:	C052EE92A1EA930D64B6A954C07EDA8CE2301BAEE32B591AD6F44032D07144856893B3823FED04F79B25D2EF314D3D2B3B8425ABA4EC0F51C0705FE2A1C8FE2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N...f.n...._keyhttps://cdn.cookielaw.org/scripttemplates/otSDKStub.js .https://adobe.com/{AK.. /.....e.....^...T.Q..'nm..;...m'..E...r.4.^..A..Eo.....Y.....A..Eo.....'..C....O.....a..e.).....4.....(S.@..`<....L`.....L`.....Qd...K....OneTrustStub.(S....`:.....L`J....@Rc.....Qb"P.....ee....Qb..^....te....Qb.D.....oe..b.....I`....Da2.....(S...`.....L`B....8Rc.....Qb.b.....c...a.....Qb^W%.....ae..`....Da&a..J.....(..Qc.>*.....iabType...Qd.Z.....iabTypeAdded..Qd.....crossOrigin...Qc.....isAmp...I..Qc..J.....domainId..QcZ.....isReset...Qd.2.....isPreview.....Qd.z.....geoFromUrl...(S...E..`B.....L`b....4Rc.....QbF..r....o...`....I`.....Qf...t....addBannerSDKScript..a.b...m.....0...1..Qb.....IAB...Qd..}.....getRegionSet..Qb".AC....Type..Qb:.....IAB2..q1..QeJ.CF....intializeIabStub..Qd.....removeTcf.... Qf...L..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0cba5b2c919929e8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	613
Entropy (8bit):	5.8194697862864375
Encrypted:	false
SSDEEP:	12:mME3xj9UfcUUoux2pmYyye3CMx0DPV2myYJyCSLhra/eDb:mMEt2fltuyRyyeSVDN2myY4CSLhO2P
MD5:	970E4A00A11319E1B59196EB2E31C69B
SHA1:	2F94E19877E9481BF552016788140C7CB292D63F
SHA-256:	C340ABC80F8F7113423987BA17FD49BF83620AA156E74C922BB6D11FED287E78
SHA-512:	980F07A491E5FFD17A04FDCECF4932C0D9AACD519AA18183825B37BBFAE62F3D61A465BDB3BFA9F66EBAD576A0347A91C948B31DB25E7E09D253F91711AB28C5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0cba5b2c919929e8_0	
Preview:	0\r..m...../.T...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/983956512/?random=1620171405910&cv=9&fst=1620171405910&num=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&eid=2505059651&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa4l3&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fwww.adobe.com%2Fprivacy.html&tiba=Adobe%20Privacy%20Center&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://adobe.com/.... /.....,...&.Lz....U...&...b-;&m.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1aed6b6619289abf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3408
Entropy (8bit):	5.4296460319608775
Encrypted:	false
SSDEEP:	96:FJ1zo/SicNCDyRbJqwJycAzOBk7hkhnnmuyWwl2NMZ:T1hlBUwJyJO67ChmlJlJZ
MD5:	F27BB87927511CD613D4BA451C7879A5
SHA1:	07DCA258F0A11B4550EB8CFB178650B7BA6C121E
SHA-256:	1B6E3171AC970B1BB58E922725AC24AD535CFD280A885A2B1DAA8E4605D06E87
SHA-512:	378DDA394C0EC3463C4B776B8BC4DAD9CF4AEB41FBB5B9F330BA5011EF1BAF64F6D01D6255DE1F169A6D40F7CB60D7E4B1B3F26EBED4A7D0C99BC79B3541B11B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X..../...../...._keyhttps://www.everestjs.net/static/le/last-event-tag-latest.min.js .https://adobe.com/npp.. /.....Yo.....d....hbo)&.-.d..B..U..l....c.9}.A..Eo.....A..Eo.....npp.. /.0.....'.h.....O.....[.....(.....(S....`d....<L`.....(S.x.`.....L`.....PRc$.....Qb6..n....d.....Qb.[l....s.....M...R....Qb.....I...d $.....$.....Qb...y....r..`....Da....X....(S....`.....4L`.....4Rc.....Qbv(.....t...`$....`....Da:.....Q.@..$....require..... Qf.I.....Cannot find module '..QbR)K.....'....Qe.o.5....MODULE_NOT_FOUND.9.....a.....Q.@..?.....exports....a.....Qb.....call.....(S.L.`T...]..K`....Dm.....&.....&...*..&...*..&.%.*....%.&.].....,Rc.....I`....Da(...`.....c..... .....@.-....LP.!.....@...https://www.everestjs.net/static/le/last-event-tag-latest.min.jsa.....D`....D`X...D`.....`H...&....&....&....&....&.(S.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2354abbff3a2b46a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2190
Entropy (8bit):	5.802048972132222
Encrypted:	false
SSDEEP:	24:eHAeulkxSHTIH47TIHfxuBIHfymW7O7IHOcTIHoxIHnIHhYqtDsj7N:eRTszI0TI/xwI/yf7mIVTIIxIHIx6N
MD5:	428DCD261FF9C8CD4C4F7E2C452888B3
SHA1:	876326464F5FA51B9C848ECB0E49AB6BE1CEC966
SHA-256:	6841647327ED4273AB43F5D172C8E60778CC3D57F7D81564979DB1EA6559E257
SHA-512:	4705331534BC853E9946ECC13A92A7727A59678E2CD259BD54B8B95D5FCFCE9D9832C4F4D7B146CA0C9BC07D3158170830C8ABB8DF949F4E0F8BB0D332F882C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....._keyhttps://cdn.cookielaw.org/scripttemplates/6.9.0/otBannerSdk.js .https://adobe.com/..V.. /.....Uj.....W(.fp:....e.....O.....Vq.t....%..A..Eo.....qT.6.....A..Eo.....V.. /.`...56534A0BF117B4E0C31441098E2E8A344FE7D3AFCB8C002F38C7B7D578DBEB0EW(.fp:....e.....O.....Vq.t....%..A..Eo.....a..L.....0\r..m.....V....._keyhttps://cdn.cookielaw.org/scripttemplates/6.9.0/otBannerSdk.js .https://adobe.com/j.... /.....$.....W(.fp:....e.....O.....Vq.t....%..A..Eo.....G.C.....A..Eo.....0\r..m.....V....._keyhttps://cdn.cookielaw.org/scripttemplates/6.9.0/otBannerSdk.js .https://adobe.com/..... /.....n.....W(.fp:....e.....O.....Vq.t....%..A..Eo.....{.w=.....A..Eo.....0\r..m.....V....._keyhttps://cdn.cookielaw.org/scripttemplates/6.9.0/otBannerSdk.js .https://adobe.com/.k... /.....W(.fp:....e.....O.....Vq.t....%..A..Eo.....=.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2bec0e299b9329e1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.532397569882116
Encrypted:	false
SSDEEP:	3:m+lSQzl6OA8RzYP2FycyGYWCULLuFvDzL1L2HFLGGqlHC4t9fWAqfFyvSmyszl/B:m00EYerCUsJAyw4xk8vVVJhK6t
MD5:	2A70C64C2CAD34C3C1526F8FE0286DB0
SHA1:	FC418D3685AC35DD01FDE3F027718C9D69914151
SHA-256:	7C8FE42935C1587410E730D1D22F9799AE90115001C71CF90AE7B30289BF47E7
SHA-512:	2D78C09DB83DD113DE2955B9CD1DC208A71872144FF5B01A1246310D8596DAF8BBF134D548C13C3AE3BBBAAC323430F5B5F4BAE883C41D8DCDA62414921C329
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V.../...../...._keyhttps://code.jquery.com/jquery-3.2.1.slim.min.js .https://lindsayknoxwilliams.com/..... /.....b=.....,Qk.....~..idCIk....R.).....A..Eo.....`.').....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2d7f286d74a18ae7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	600
Entropy (8bit):	5.818974291664402
Encrypted:	false
SSDEEP:	12:WjE3xjaE1oux2pmYyye3CMx0DPVcoYN/Cod0pP6PGM:WjEtaEuuyRyyeSVDNcoYN/CB6+M
MD5:	F3AF991881D1C6C778D4324C78840760
SHA1:	70BF5FC8A12FD945152A7A11EFA4639E03128915
SHA-256:	56C6291FD386C6AFB6B7D88AA18D946FCE70600A1720486C3EA1269B71F075F6
SHA-512:	795EA5740128EAC8E2383B03893B09283EB9FCF483B2E869E3042A10EA86DA8EDBAC3D750B6AED47BCBDAA4EECB0EAE9ADC39BE5A73DF7B2BE5BBB8CFFDC08E0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....>...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/983956512/?random=1620171386740&cv=9&fst=1620171386740&num=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&eid=2505059651&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa4l3&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fwww.adobe.com%2Flegal%2Fterms.html&tiba=Legal&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://adobe.com/.... /.....z.F.y....Wm.....%...e....!U.A..Eo.....tb.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2f49560d02f8d583_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	56745
Entropy (8bit):	5.652489404309447
Encrypted:	false
SSDEEP:	768:WYeCHBpcolTn9WJr3vGxIKG1dEuMpidd76jF2BXQuSYQ3x/cCDy3JNbZ:38cR43OgDZ76jp/iF
MD5:	5946301F23D02378B8F80FA07651F91A
SHA1:	A26DAE3279EF3ED2ADDA96CCACADFC80991E5D94
SHA-256:	E51143EC283FDA3E632F5255DCB1D21C8407DB204D0D6721EEFFA337920E6E5B
SHA-512:	3B6A058598780BA57F88B4C87B5FE37FD8ED8E4063264B0E5E1A6676AFCB0AA065763A55ACFDB7D96CB643D2D6CF23874FFB16E753AD1F9660F701148D86C46
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Y.....tZ...._keyhttps://client.messaging.adobe.com/latest/AdobeMessagingClient.js .https://adobe.com/.... /.....o.....^i.....AH..W..Qq.....s..A..Eo.....57(.....A..Eo.....'..3...O.....@so.....<.....(S.H..`L.....L`.....(S...`.....L`.....Q.@2w.....exports...Q.@.....module....Q.@N.....define....Qb.'.....amd.. Q.p.F#@....AdobeMessagingClient..K`....D}.....s.....s.....&.\..&.-...%..H...s.....&.(.....&.|.&.^.....&...s.....&.\..&.-...%...\..&.-...%.....(Rc.....I`....Da..... ..f.....`...p...0.....@.-....PP.1.....A...https://client.messaging.adobe.com/latest/AdobeMessagingClient.js...a.....D`....D`@...D`.....`...&...&..!.&.(S...`.....L`I....(S...`.....<L`.....@Rc.....Qb.....e.....Qb...J....t.....Qb.....n...b$.....I`....Da4.....(S...`.....L`.....a..$..a

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\33cb487341b808d0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	723
Entropy (8bit):	5.77593198524869
Encrypted:	false
SSDEEP:	12:I/wE3eH2sxoux2peyye3CMx0DPViHWC2/ohJuXPmxACsrNl1:DEuH2sauyeyyeSVDNJv/juxAC+
MD5:	45B0F2BFDF811770236677DC2F1F9940
SHA1:	3FF8D0C7DCEF6496A1D8E6999C95B1108C387507
SHA-256:	A2923441B23C1C48608CFCF6A23F986BCC6DDE138683AA48BA1236413E420413
SHA-512:	CED15BF5B993CC64984AA9AB9261E37986BAF3BB2755C66E27DB60D7C3EBA2C27AB434C647427EABA93679CE0A36FF7D160CE956D489DF1783A8A293EF16A6A6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O...f.IV...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/1004494713/?random=1620171389469&cv=9&fst=1620171389469&num=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&eid=2505059650&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa4l3&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fwww.adobe.com%2Fexpress%2Fcreate%2Flogo%3Fr%3Dreader_page_learnmore&tiba=Free%20Logo%20Maker%3A%20Create%20Custom%20Logos%20Online%20in%20Minutes%20%7C%20Adobe%20Spark&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://adobe.com/.W... /.....l.....p..D.K...lt.M..7j.7...r..?b..A..Eo.....,.Y.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\35da886f40383299_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	612
Entropy (8bit):	5.412502567995292

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\35da886f40383299_0	
Encrypted:	false
SSDEEP:	12:aHBWAlwMlYVYHtpk74HBWAlw7eVYHtx14HBWAlwFkVYHtr:mBWVwMlYVYH0cBWVw6VYHJcBWVwaVYHd
MD5:	5AC6F7989346322E8A91E1D23CD7A170
SHA1:	9C56F766FF58A70260ACB026E4CE50AD9E32E27D
SHA-256:	94E5837BE7FE01B223A26E8AA29F060E086DCBE7FABF67B9467F8CC90798428D
SHA-512:	63F2A125CC7066FC5BA004B03189B3123EB155AE74C75D046FEEAE424F00B4520106433FB4CDD0A1A7FF2E4AAF44F96725423C7BEE44F59A8F25EC42C6F1B21
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H...KX.T...._keyhttps://www.adobe.com/express/scripts/scripts.js .https://adobe.com/..t.. /.....b.....J.....t.U....x....<.....f...A..Eo.....E.....A..Eo..... ....0\r..m.....H...KX.T...._keyhttps://www.adobe.com/express/scripts/scripts.js .https://adobe.com/.c... /.....t.....J.....t.U....x....<.....f...A..Eo.....A..Eo..... .....0\r..m.....H...KX.T...._keyhttps://www.adobe.com/express/scripts/scripts.js .https://adobe.com/N... /.....B.....J.....t.U....x....<.....f...A..Eo.....$..l.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\36d0235949f31082_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	13448
Entropy (8bit):	5.834258262206406
Encrypted:	false
SSDEEP:	192:4cDGTpG1cF4T0K6BMgPohuhmuCWS8B03yA1QBU7cLcLdmtpx68j30GvocnivSb+f:E3F4R6BFZhmxWDTueF1gGvbingaTVUW
MD5:	13DD840B18C1285291502C94908BC60A
SHA1:	2A3CF3576736D7C2355F5F4420C84E06797B283E
SHA-256:	51F094D0B3CE1489697469CB593AB1D9731DB4380BFD21F362253F7CC312ACC2
SHA-512:	E99E5C1DC0BA7740269551695C0EC60DA63EE7A3C8C3ABE53793DEF0C12BD203720DA320021281703B648AE289BFB387339A177F33E9E0991FFD509D63854E0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....:....t.<...._keyhttps://use.typekit.net/onz5gap.js .https://adobe.com/.q... /.....M.....F!g..k.89.n.....s...8....[R..A..Eo.....A..Eo.....'.9G.... O....`2..%.....$.....(S.d..`.....$L`.....Qc*g.....window....Q.@.`_,....Typekit.....a>.....M...QcD.e.....1655249...Qb.....c.....`.....M`.....Qe./i.....tk-prox ima-nova.(Qh.v....."proxima-nova",sans-serif.....QeJ.![.....tk-adobe-clean..$Qg...H...."adobe-clean",sans-serif..Qbf.It....fi.....`.....Me.....8...8.. 8.."8....QbFm.Z....fc.....`..... L`.....,a.....Qb.....id..`.....Qc.....family....Qdb..d....proxima-nova..Qb.!.-....src..lQy..7_...https://use.typekit.net/af/949f99/00000000000000003b9b3068/27/{format}{? primer,subset_id,fvd,v}...Qd.....descriptors..,a.....Qc.4r.....weight....Qb.....700..q..!...Qc.>.o....display.....Qc..?.....primer...LQq.QrR@...7cdcb44be4a7db8877ffa5 c0007b8dd865b3bbc383831fe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\39328f08ce663fd2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	786
Entropy (8bit):	5.735064257248774
Encrypted:	false
SSDEEP:	12:fYdMevphwAUNpYdMev54hwAnLpYdMev6ahwAuGKGqhwA:f3wpVgp3w54VLp3w6aVudGqV
MD5:	E9F6E248B22E6B059B77F08FBFEC730A
SHA1:	FF87F4E1B1441DEAD9D79654218A52D8B2AE5A25
SHA-256:	B50EDAE9485138B224F2336ACDE5FA5264F7EBB1F16EFD99A391D957B4015AEA
SHA-512:	52BC6E50D9F33D2F17B627FEA48059F1BEA1D17742F71D5E64B3D55825FF1ACC3FF1FE94B9ECAE8930B262214520AB428ED9E8E2507165120D9BA74FE470FDF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f...P~...._keyhttps://connect.facebook.net/signals/config/1772359959706965?v=2.9.39&r=stable .https://adobe.com/!.>.. /.....q.....1....DJ.D>5...K....*..... ..A..Eo.....&.W.....A..Eo.....0\r..m.....f...P~...._keyhttps://connect.facebook.net/signals/config/1772359959706965?v=2.9.39&r=stable .https://adobe.com/Q.... /.....1....DJ.D>5...K....*.....A..Eo.....Bv.<.....A..Eo.....0\r..m.....f...P~...._keyhttps://connect.facebook.net/signals/config/1772359959706965?v=2.9 .39&r=stable .https://adobe.com/(.... /.....1....DJ.D>5...K....*.....A..Eo.....t.....A..Eo..... /.....1....DJ.D>5...K....*.....A..Eo.....\.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3b89f9a0c0025a5e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	739
Entropy (8bit):	5.789932709358084
Encrypted:	false
SSDEEP:	12:TE31f1K5Emoux2peyye3CMx0DPViHnzj2fP1nCUAKmxACkti1s/7:TElf1K5E/uyeyyeSVDNYzKO9xACO/7
MD5:	36B26FB55B256E41C118D5A8318F710C
SHA1:	7F37B1F3F077F1394E15F5A8FB3C598DBDC8DFC4
SHA-256:	F3821615F7C6B80FC16C75E2D206E8EF9FAA85C8B67F9F1CF651157FDD5C0CD4
SHA-512:	75801F22447FC32EB861417568D2EFEB11AEFBB934EF7576AC5226D3EEF093929426FE61936F4F8C225C750BD99DE0B1608E6E9A92136ED8DA714CF498BDB01

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3b89f9a0c0025a5e_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...F#%....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/987390658/?random=1620171376012&cv=9&fst=1620171376012&num=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&eid=2505059650&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa4l3&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fwww.adobe.com%2Fexpress%2F%3Fr%3Dreader_page_logo&tiba=Make%20Social%20Graphics%2C%20Short%20Videos%2C%20and%20Web%20Pages%20To%20Stand%20Out%E2%80%94In%20Minutes%20%7C%20Adobe%20Spark&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://adobe.com/U.:.. /.....q~.....H#6..K.*f./H.x[y....6&y..!..i.A..Eo.....5N.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\41d997c3ac4f8598_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	128048
Entropy (8bit):	5.688945744209749
Encrypted:	false
SSDEEP:	1536:JfqGg9GHyCu1l87aqolJVqhQWlF6rXCbOoulYGXuaX4jofU2HO8Y1ONOzsddd:sTQHy31l8uFYw3zXHfA8gkv
MD5:	B448A435B85B37834910CDC0DEAB39FB
SHA1:	FCCEB850AF94CD45E353CDC971785C2018F62588
SHA-256:	F5FBA9E849ECCDE51D569015D224040AAD7DCF6922AB85FD3727835A24430C5C
SHA-512:	44167D6F1958BB925BAD5D91EBB5195708B23289B1E6298DD0A8DBFD95794E8960F4DCF8823A4BC605FDC7DEF774474BFDBA7D531666B49F8C172E176A564A0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....v.....9A1D0E2E149F8662F7534CE02BE92BE24D1FC88775C4D685880EF607A64420ED.....'.L'....O,.....0.r.....x...L.....$.....d.....(S.)...`.....L`>....(S...`,....TL`&....PRc$.....Qb.....e.....Qb...J....t.....Qb.....n.....Qb....r.....S.d$.....I`....Da....H....(S...`.....L`.....Qc2w.....exports..$..a.....C..Qb.+.....l...H...5...a.....Qb>.....call...6..K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0..'....&.%.*..&.(...&.(...&...&.'..W.....-...(.....,Rc.....`....Da.....!0....e..... P.....@....@.-....|P.....m...https://www.adobe.com/etc.hawks.dexterlibs/dexter/clientlibs/base/head.fp-1c6b8ee3dfac8039d9ead67e8b6d6138.js...a.....D`....D`....D`.....y....`....&...&..Q+&...(S.....5.a.....Qc.....win

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4c932a6077369a0e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	609
Entropy (8bit):	5.4732388418605
Encrypted:	false
SSDEEP:	12:d2axjPSpF2mOpn2axjPE9AF2mthTn2axjPp3UF2mc7:YezSpFROp2ezEqFRn2ezpEFRc7
MD5:	EC4471E4525D98221BE71276899FD259
SHA1:	E60051B548623E9DF7FD1055F5FFE1CA832E8868
SHA-256:	E8D32C3A01D5227A705432B43BA014809872433BE379DC20414AB101C7A7BF17
SHA-512:	7F6097C78E514135E5CA39A1F95A762242FECFDD85886D8E4E09916F1A44BEAE8F972B4BB3B0BB21B282F481897E659096C713F17F527B8BADA863947E05AD02
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G.....!...._keyhttps://www.adobe.com/marketingtech/main.min.js .https://adobe.com/... /.....'e...../...6.2.(Dqo...RT..^...A..Eo.....}5.B.....A..Eo.....0\r..m.....G.....!...._keyhttps://www.adobe.com/marketingtech/main.min.js .https://adobe.com/9.E.. /...../...6.2.(Dqo...RT..^...A..Eo.....Cb.7.....A..Eo.....0\r..m.....G.....!...._keyhttps://www.adobe.com/marketingtech/main.min.js .https://adobe.com/.<... /...../...6.2.(Dqo...RT..^...A..Eo.....;9.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4d98eb32aad7362d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	664
Entropy (8bit):	5.799093457084794
Encrypted:	false
SSDEEP:	12:VE3evpOmoux2peyye3CMx0DPViH2NRmxACITMH7:VEuvpO/uyeyyeSVDN/OxACHb
MD5:	E71CDFDAF35465F17234993767378761
SHA1:	ED429CCE30147308F45F4C8591114AFC416B70A4
SHA-256:	C1DF65F4A42BF3C43A80AD6759639FB913BA58583948DF71E4CA87BBD58D8992
SHA-512:	8E8C67049BB2FD3952C92A05E82CA72D6A96E1EB296A740E206BDD813E0E8A3A8461FA2157AA1B981230BD902525B8A3494FA12B7368131A1ADDDA9E9B380FFD
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4d98eb32aad7362d_0	
Preview:	0\r..m.....r7....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/1004494713/?random=1620171405795&cv=9&fst=1620171405795&num=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&eid=2505059650&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa4l3&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fwww.adobe.com%2Fexpress%2Fdiscover%2Ftemplates%2Fresume&tiba=Free%20Resume%20Templates%20%7C%20Adobe%20Spark&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://adobe.com/..... /.....,.....i.....Pb./.vs...5...]@.LW7{.A..Eo.....".(A.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4e4147266d5a1b82_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1883
Entropy (8bit):	5.647328870229157
Encrypted:	false
SSDEEP:	48:W5bn1Q5bnhpQ5bn0SQ5bnCPQ5bnK7Q5bnlQ5bnXIN:W1nG1nhy1nG1nh1nKM1nW1nX
MD5:	7DF3668161C747AC2152D0B89E715720
SHA1:	6DB8549530C9B9E2950115E52E6794DC1476E175
SHA-256:	488BA89C94B3D45F523DC072F03D5285F7D3958B511B3C886A1EBC6B27325CD3
SHA-512:	CD171F41A43CC7A991CD3BA33505A31C410E9E7BBBEA091A3B43E68C849A679FD8CAF2577401E8B2A7FDD087D0175D3E32AF159702B03AD26BB9B2FDE50D27EF
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f675e54cc6b6/RC6f46e43fa6d44dbeb45cc5801ffded0e-file.min.js .https://adobe.com/..a../.....4k.....f...?..~..h.!....ck.'.M.>..A..Eo.....z! .....A..Eo.....0\r..m....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f675e54cc6b6/RC6f46e43fa6d44dbeb45cc5801ffded0e-file.min.js .https://adobe.com/.<... /.....f...?..~..h.!....ck.'.M.>..A..Eo.....A..Eo.....0\r..m....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f675e54cc6b6/RC6f46e43fa6d44dbeb45cc5801ffded0e-file.min.js .https://adobe.com/..... /.....f...?..~..h.!....ck.'.M.>..A..Eo.....u.....A..Eo.....0\r..m....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f675e54cc6b6/RC6f46e43fa6d44dbeb45cc5801ffded0e-file.min.js .https://adobe.com/..... /.....V.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4f3af61e14a7c13e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.826004134051625
Encrypted:	false
SSDEEP:	12:RXwE3xjCGoux2pmYyye3CMx0DPViH2NRmxACYFxw:CEtCfuyRyyeSVDN/OxACYFxw
MD5:	96AA09F82939F33E96787A88C935754C
SHA1:	90ECFF9F01CEFE056E868583792DA0D10D585510
SHA-256:	78240E08CEC0A6910E0C496D44CD865D44C6FC5B535FAE3798EAD12D1289EDFF
SHA-512:	B510919EC3A30316351FB49E3DA4029E4E8E1C4A4489FBDD631C70B3728189F2BA5EF73754E77B44C5649FEAFF5F060569269984543832 1A2240571BE9F9C83F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/983956512/?random=1620171405792&cv=9&fst=1620171405792&num=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&eid=2505059651&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa4l3&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fwww.adobe.com%2Fexpress%2Fdiscover%2Ftemplates%2Fresume&tiba=Free%20Resume%20Templates%20%7C%20Adobe%20Spark&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://adobe.com/u.... /.....HM....w*...\...W..Q...T<...^...A..Eo.....a.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\528df7fa00e0aa0d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	965
Entropy (8bit):	5.416481620266299
Encrypted:	false
SSDEEP:	12:sz+OgATae+z+OyTaBT+z+OA7WTag+z+OKnn/WTat+z+OHu9TaL:ApBmpbmpHmpWn3mpHuE
MD5:	7F3A47ED5517866DFC9E7E315FA60A18
SHA1:	2DE56E0EC3F71F461073F221F56205CCD93C12CB
SHA-256:	480133EB30F723EAC3062C99D31F6D65146132831490FF7855F6FA6C048911FC
SHA-512:	9B1A2E740EEBDA4B80136A714EC4DA37733178A66C7158D602F7BA979F489C12DF8DBA423AB979E9CD319EB27A93A22F5C719B41E52B725E5DB609B22234288
Malicious:	false
Reputation:	low
Preview:	0\r..m.....=...E....._keyhttps://static.ads-twitter.com/uwt.js .https://adobe.com/ixr.. /.....o.....m.*.....[...%t]U.....r.8..P..q.A..Eo.....e.....A..Eo.....0\r..m.....=...E....._keyhttps://static.ads-twitter.com/uwt.js .https://adobe.com/..... /.....m.*.....[...%t]U.....r.8..P..q.A..Eo.....Z.....A..Eo.....0\r..m.....=...E.....keyhttps://static.ads-twitter.com/uwt.js .https://adobe.com/..... /.....m.*.....[...%t]U.....r.8..P..q.A..Eo.....a$.....A..Eo.....0\r..m.....=...E....._keyhttps://static.ads-twitter.com/uwt.js .https://adobe.com/;.e.. /.....K.....m.*.....[...%t]U.....r.8..P..q.A..Eo.....W.g.....A..Eo.....0\r..m.....=...E....._keyhttps://static.ads-twitter.com/uwt.js .https://adobe.com/..... /.....m.*.....[...%t]U.....r.8..P..q.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5a7d74a0f248aeed_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	217
Entropy (8bit):	5.482698450601427
Encrypted:	false
SSDEEP:	3:m+l0vaDl/08RzYrSLX8AXRHEEISAhvAWFVR4gtS6delHCBgCW3m4i7yRm17lpK5M:mTCTYGLBBkEIvFV+i3WI2A1XK6t
MD5:	1CA8E41E3E3AF87AFCA58D3EE57CC9E2
SHA1:	CD5DC8DC0FEBFBAD8787F8EEEA1CA1CFFC1EF98A
SHA-256:	2D3B7993C9A6C747A5C46FF56FE87F76D9B66D902208811A122DD20B4BB165D7
SHA-512:	DA936A095E357F760A25B169C3871389BD54C68BC23326E462D234652D8C17856B4B98FF2E4FF735F39CAAC673F4D5FC2334D71C53838F74A0053129D05D1F8D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U...q....._keyhttps://www.adobe.com/express/blocks/full-width/full-width.js .https://adobe.com/w.t.. /.....bd.....M.P.....(;B'.....v....9..A..Eo.....%..... ...A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5ae5bfe5b7b87be2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92088
Entropy (8bit):	6.154403282637216
Encrypted:	false
SSDEEP:	1536:vBtB5nFVNMZZibdrxl0jWJ5FPhUX6etqGBPxGX26xt:rGZIxluWJ5FPy6etqGBPxGm6xt
MD5:	63ACBC9725DF31C2D5119ECD08F3B498
SHA1:	B5D22CEE4614730ED8FC46B3FD180E53BC31B634
SHA-256:	0538756B4C0C23DA95E3231943D0226F5D725B0B01315F0EC5228B2BE1B2E3FF
SHA-512:	A14CA8729DD8A973648BA28B47D09B54B9935478250FEEB9BEC3FB67F4483BE04C10F85832C227091970F851EB0390357B8DE05E665C3930C3A0DA569E42C513
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....-.....BD3CDCA02E1BBB53605A01ABE8432A4A312CE9170F564CBA5C3D975FD4CFF072.....'.....O....xf...d..... .....)..... .....,.....(S.m...`.....dL`.....(S.0.`.....L`.....0Rc.....QbF.....r...`....I`....Da.....(S.t.`.....L`.....TRc&.....Qb.1.....t.....Qb.\3.....n.....Qb. .vf....e.....Qb..$e....o.....R..d$.....$.....A.`....Da,...~.....(S....`.....4L`.....4Rc.....S.`$.....a.`....DaP.....Q...Q.@>.....require..... Qf.C5....Cannot find module '..Qb2i.....'.....Qe..O.....MODULE_NOT_FOUND.9.....a.....Qc&.7:....exports....a.....Qb:f.....call..!..(S.P..`\...]..K`....Dn.....&...*..&...*..&.%.*..&.....&.%...%.&.]....., Rc.....I`....Da>.....c..... .....@.-....\P.a.....P...https://s3.amazonaws.com/adobe-luca-prod-ue1-assets/experiments/chrome/chrome.jsa.....D`....D`....D`..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5db8039e291244de_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	243
Entropy (8bit):	5.486537227496049
Encrypted:	false
SSDEEP:	6:m49YET08NaYWbVOqZUJAyMt3lY9Uh7Le9kH43NK6t:Jg8NaY8ZUJAyIY9I7y+8
MD5:	419CE738DFA2117BCE7CEE3BEF048534
SHA1:	CF1F4141C66CC6787F889FEFED1226E0536CE909
SHA-256:	3C42348B1CC6FF4BE44020526163B1BD5A7BD1E1735215B1D435955A96F4E035
SHA-512:	2F7F6F92848AE75BC7DA2BC109BDD11BA19CE7D4C92D004472D6D1293BA70086ADBBD9B783FB3B91B83E73E07F48A940AC19B38D7D4F4129785CF5A10DAB0E A0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....o....kk....._keyhttps://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js .https://lindsayknoxwilliams.com/\R... /.....>...../.....K...z.zm.....N.=... ...k.A..Eo.....].O.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5f6f8ddc9b9453d5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	5.439913193653194
Encrypted:	false
SSDEEP:	6:mfXXYkb8E9xEvAErUJAyhBGVlAt/l2Qs3yP4O5RK6t:CXzv46JAyWelhs3yPHp
MD5:	61EBAF55152B1729A83BA5EC230188FA
SHA1:	F49F92844BF5C12CA1A9B839ECCCF300F5E28278

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5f6f8ddc9b9453d5_0	
SHA-256:	E8E32D16BBD5D69372421BE1A51AC64661C393AB1F3A7B62E3FC586C59E74162
SHA-512:	27D60DBB2C9A47DC8D3988733D694759170316465D363DF3D68704C4807B040FD884BA7AC5444CC877CCE234EDB6C4E33B01FB0B8784021550B8907AEE40CE7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....l....7[|...._keyhttps://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js .https://lindsayknoxwilliams.com/.d... /.....U?.....9.....VL.L...F..w.6..u.0...A ..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5f9866b4455c9fbb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	237
Entropy (8bit):	5.439687566711081
Encrypted:	false
SSDEEP:	6:mn/VY68E9xEEUgLErUJAy4AO//kTh2mkeTxbK6t:wbYgHJAyS//kTgm5xN
MD5:	F075FDE209512E7C9A8C955033C825FE
SHA1:	640AC30070EEB44FDF17C8BA56D5ED791353BBBF
SHA-256:	51EF9EF07A84F87BAC7628119D2D2E8B8B8DD73259BD95335B55C2AA0DA7B7D4
SHA-512:	F4D2B736F1182E5B04B6687142A0C33DF63BE225113F967A02C322BE658FD9953546C8D56D104A5E0AAEF28F9667350CB6FC686C52BC483B928C2DB5FBEA49C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i.....Zo...._keyhttps://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js .https://lindsayknoxwilliams.com/.9... /.....>.....K.k.].o.....Cll..F7.._ ....5.A..Eo.....g.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\64e1e9138b0983c6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	200000
Entropy (8bit):	6.048929947366639
Encrypted:	false
SSDEEP:	1536:PtpLo4WzUq8xsti8PAlQoeETTx+lZRhT5nmfo+v5nmfOMehqwYXIRRN94MiL4KJ0:1No4okeWoQhpewapEl
MD5:	D3AB0EAEE5F2D7EF3D47AC0D805038DF
SHA1:	1290D20F43BA191E56E1D457DD23B5E4C066DBF8
SHA-256:	74A211605ECC52CCDB21D2C9C174296AD299B8E91E4F1AB9E5EEA75B5DC65CED
SHA-512:	AFF1BE8423A9FAD1C1581594672505682BA2848D737705974262CF9301BD6476AC6E536DEC63E7F21BBD039BFE7D708925601C2BC28A65E8141B93BDF0070992
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....f....2BBDC71DF0A8567A6C11D37DBC8E165A212D8926DE98F1EFC0F2432935677075.....'.YS....O/.....eN.....P8..... .....D...\.....(S.0..`.....L`.....(S...Q8.`Vp.....L`<.....Rc.....Z.....Qb...i....o.....Qb...M....s.... ..M...Qb.k.....d.....Qbbj.....k.....Qb.....t.....Qb..m.....c.....Qb.....n.....Qb.ck.....r.....S...Qb.....l.....R....Qb..0....p.....Qb.0.....h.....Qb.e^.....y.....Qb..^.....f.....O...Qb..Q.....C... ..QbV@.q....w.....Qb.....A.....QbF?.....S.....Qb.t.....l.....Qbj._....U.....Qb..7....E.....Qb".m.....V.....Qb.....D.....Qb.....O.....Qb..0....M.....Qb.....q.....Qbj.....R.....Qb.w..... W.....Qb.R.....Y.....Qb&.....Q.....Qb..H....Z.....Qb.....X.....Qbb..w....ee....Qb...p....te....Qb.5.....oe....Qb.6.6....ne....Qb&..a....se....Qb.N.4....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\67b7e7530ed32021_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1614
Entropy (8bit):	5.651301439714393
Encrypted:	false
SSDEEP:	48:O5jXpxro5jWiFo5j+6mo5jxNo5jIio5jzk4A:Ox5CxWiuxR5xxWxI9xF
MD5:	5A7F3578C96E84334B6B51B3A3F7D918
SHA1:	6F5E23251B299B4BC9C1AA06C91BD71DB31918AE
SHA-256:	8199C4D8CED3D3B5D59E21637C09128E2163A6A727944C2A256811C14D3924A6
SHA-512:	89890F2BCF05C186DEEF6133D6B51329F8B27FBD37FB14B486E1065421A884CEF86DE56E53F5F1C241447C48D9733DD834C531B38DF6140C1E7BF1F62BDAD76
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f675e54cc6b6/RC1a83c357d323419db9d2ba211efeeaae-file.min.js .https://adobe.com/..`.. /.....0k.....o[>.n..o.....*.a.On.h..7+/..E..A..Eo.....D.....A..Eo.....0\r..m....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f67 5e54cc6b6/RC1a83c357d323419db9d2ba211efeeaae-file.min.js .https://adobe.com/.A... /.....o[>.n..o.....*.a.On.h..7+/..E..A..Eo.....eS.....A..Eo..... ..0\r..m....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f675e54cc6b6/RC1a83c357d323419db9d2ba211efeeaae-file.min.js .https://adobe.co m/..... /.....T.....o[>.n..o.....*.a.On.h..7+/..E..A..Eo.....B.50.....A..Eo.....0\r..m....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f 675e54cc6b6/RC1a83c357d323419db9d2ba211efeeaae-file.min.js .https://adobe.com/*sA.. /.....o[>.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6a11233d0598b9fe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	213
Entropy (8bit):	5.5986154162108255
Encrypted:	false
SSDEEP:	3:m+lZwR1gOA8RzYP2FycyG8ZFvDzL1L2HFLGG5lHCCcn/lllfT+r3/U3wkyP5mIxB:mh1gEYeMrJAyLlEr3c3vm4InK6t
MD5:	926AC81FEAB2C2EC13FB62DE4E7398A6
SHA1:	F8A8F07FF0641BC4C93158FE7AA2E91C53CF0363
SHA-256:	3E6F458BBEECD9624CDEBDC2B5046E54678B335BC0EE635FE4F214E24435A19D
SHA-512:	36C7440E810AE7417C4056F5700DC4B28DCDD2E5CF11C59CFBA04318EB943335A19E22C2C2E39EF48E303D3B137F5797BE6F2D534F883AB79EA13BA44874794
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q...4.4Z...._keyhttps://code.jquery.com/jquery-3.1.1.min.js .https://lindsayknoxwilliams.com/!.... /.....'9.....6.T_*>*G.#.....\..5...`..A..Eo.....|.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6a9fad8381d66bfe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1010
Entropy (8bit):	5.558530052306321
Encrypted:	false
SSDEEP:	12:BWjq/Z+243DWjqqc8DWjql67DWjqTeTDWjqrnt7:BWeZg3DWLc8DWM67DW3TDW61
MD5:	776699F98A2062E3057B9CA7901AC1E5
SHA1:	B659413F487508C37F59F764CC8F07F10068030B
SHA-256:	B7CC0FBC30E21826723A251B73E4C3163F1E265775688FC2D4D6EB7AE9EAE77D
SHA-512:	A16B8A0B0B0B87F3E08B7955067BD40D4FE36A6810F4D7CA147123C1E6569D285B8578E9F766E95843E1EAA49794E45DEE6CCF3D3E11E4FD9BE0724C49A2FCE9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....F...W8H....._keyhttps://scripts.demandbase.com/qQQxkRp0.min.js .https://adobe.com/._?.. /.....;q.....8@v3.Q....D.....p....L.d.[....l.A..Eo.....G.....A..Eo.....0\r..m.....F...W8H....._keyhttps://scripts.demandbase.com/qQQxkRp0.min.js .https://adobe.com/8.... /.....e.....8@v3.Q....D.....p....L.d.[....l.A..Eo.....8.....A..Eo.....0\r..m.....F...W8H....._keyhttps://scripts.demandbase.com/qQQxkRp0.min.js .https://adobe.com/..... /.....8@v3.Q....D.....p....L.d.[....l.A..Eo.....Rf.....A..Eo.....0\r..m.....F...W8H....._keyhttps://scripts.demandbase.com/qQQxkRp0.min.js .https://adobe.com/..e.. /.....8@v3.Q....D.....p....L.d.[....l.A..Eo.....]D.....A..Eo.....0\r..m.....F...W8H....._keyhttps://scripts.demandbase.com/qQQxkRp0.min.js .https://adobe.com/.#... /.....8@v3.Q....D.....p....L.d.[....l.A..Eo.....J.W.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6b09f94034ecad4c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.569138079520645
Encrypted:	false
SSDEEP:	3:m+lv0tl6v8RzYP2FycyGCSPsRzL1L2HFLGGuNlHCUtZUlkY8Vad/YkRmnt1pK5kt:me0tVYeSS0NJAyMAUFk/YhnJK6t
MD5:	7ED7A8E83F962B5FADE6E1C6C4B23536
SHA1:	23AB24BED58311A80A91B23E3742A960D7079221
SHA-256:	40B2FFF0CFC486E271CE609CB6324C9000C514C344A32CECB752AF1D85D44D50
SHA-512:	A378CC0043BD2B5BF29BDA36D571464B502CEF48176927F31457BAFCCE9035B3A13ACF793C22187C937434D3A141DDFBE8852FC21703F054DFF7592441893280
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M.....2....._keyhttps://code.jquery.com/jquery-3.3.1.js .https://lindsayknoxwilliams.com/.... /.....L9.....X..`..P.c....u.R.D~.-)..~....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\710aae0a4f4502a8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	251
Entropy (8bit):	5.448178463868822
Encrypted:	false
SSDEEP:	6:mgfPYGLXyAG0X5MA+vTqGQzHlw9LEFez4kK6t:NfBGzv2GQLlw9
MD5:	493D71BEE22D75EC35144F50EDC0FE69

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\710aae0a4f4502a8_0	
SHA1:	886447DDB8557F37C20EECA4A6B4BB5ED62865DA
SHA-256:	710FA861D6778EC77A1E97CFA1607D746BD44F234DB5172EC03680E632435B00
SHA-512:	2AE8FF66C5BD40DD040531C3984A16DE0D2793459FC5AB65F4854F5B7D5A03202E95D187F57D9C1409112541F22471912E16195410360994E82306CDBE93025A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....w....64/...._keyhttps://www.adobe.com/services/feds.res_1.js/head/en/acom/corporate-mega-menu/legal-localnav.js .https://adobe.com/.... /.....a.....s. ...U...i.;n.^.....>M^.A..Eo.....'.8.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7451b1541ed8a461_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	249296
Entropy (8bit):	5.8212104489848135
Encrypted:	false
SSDEEP:	6144:94+ooNWUeyU7Z67NlyfXxJS71faaZPmXVHmNiLb:WDXxJ8PAH9n
MD5:	B6EAAE9515DAEE54642128A2C20B2319
SHA1:	E37343943A86FD1F63EC87C2FAEE1A421FA7952D
SHA-256:	63242154712F12C7452EEDD5BDFC95253E2FB8A8DE1F3B46D8DBD95B768934D5
SHA-512:	EC9162856D5167C21709C731BA80CD7C180CD4CAE30A8D23E83FA1518AB77327BEA149F8A8DFAE73FBAC3919AF0EA93C2EE07A497A87814A9B4DE17614853AE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....U....FC89AB3B245556B8C3ABB596D39E2CA3D49EF7D9A215CEC9BE7CEAD5DD47D6DF.....'.R.....ON.....l...H....l..... .....|.....,.....x..... .....(S....`0....@L`.....L`.....Qd.s.H....marvelcommon.(S...`.....LL`"....@Rc.....Qb.U.....t.....QbRX.....e.....Qb.6Jh....n...b$.....I`....Da2...J....(S...`.....L`.....Q.@z).....exports..$..a.....S.C..Qb.P.....l...H.....a.....Qb.'./....call..a...K`.....4KkT..... ... .....\. .....0.K.....}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&...&.'..W.....-...(.....,Rc.....`....Da`...X.....e..... P.....@....@.-....DP.....7...https

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\770596cc8722ce6f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	199
Entropy (8bit):	5.450754944889381
Encrypted:	false
SSDEEP:	3:m+lZwjla8RzYgGK8IhVxhoD4gtGirFK1lHC8l/ll3srG3CQhdDhnzmwPtlpK5kt:mbVYgGKZllirFK68ZsrGFdDxKQK6t
MD5:	0B6A54E26C4B9F0F2F7900257035D2B3
SHA1:	B0A2B057B8252FD18A3F4C7CABEDC89AA03F795A
SHA-256:	6B3537EF7EFC7A0DFA607602EBD46FB31DF45F9B6E5F2809F727085FF4961FB1
SHA-512:	90687369325F9440BB7D8FD41FCB10A483736135713A7090811026461B2DA5FF11B4B0830186FE7530BFAE500BD714EB311C14CA9B52E14839B9DCC395163428
Malicious:	false
Reputation:	low
Preview:	0\r..m.....C.....V....._keyhttps://spark.adobe.com/m-setup-982dbd2b.js .https://adobe.com/?(G.. /.....L.....6v.c..Y...._c...g E..:B..A..Eo.....P.7.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\78076ae97804cb59_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1150
Entropy (8bit):	5.683704996637835
Encrypted:	false
SSDEEP:	24:bXyDYbjC9XyD5Dr9XyDXw9XyD5J9XyDL11:zyDYbWFyDVrFyDgFyD3FyDB1
MD5:	28650FE95568914353AA222B07E59D83
SHA1:	2A961406A64C23F3304DD9EC0C318956217D7BF6
SHA-256:	A172B7C4EE236C786FFF972293A85125EFF872B1A7B93805511DFCD0EB347B81
SHA-512:	7A6F30E417C74FB0C2DF3E8E9420A6A7B280DEF5058C30D41B13F22EF6A0A3D2FC3B3A56BEA7399B78D181A311C05E129B7E6FC55A635C97C482AE5896974AF3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\78076ae97804cb59_0	
Preview:	0\r..m.....b...R.8....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-1004494713&l=dataLayer&cx=c .https://adobe.com/.9?.. /.....q.....=e..~o6!...=..p....Ci..t..A..Eo.....A.....A..Eo.....0\r..m.....b...R.8....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-1004494713&l=dataLayer&cx=c .https://adobe.com/o.... /.....=e..~o6!...=..p....Ci..t..A..Eo...../%.....A..Eo.....0\r..m.....b...R.8....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-1004494713&l=dataLayer&cx=c .https://adobe.com/..... /.....=e..~o6!...=..p....Ci..t..A..Eo.....A..Eo.....0\r..m.....b...R.8....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-1004494713&l=dataLayer&cx=c .https://adobe.com/T?... /.....=e..~o6!...=..p....Ci..t..A..Eo.....!.....A..Eo.....0\r..m.....b...R.8....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-10044

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7812293e5d091f0b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	960
Entropy (8bit):	5.454279620535523
Encrypted:	false
SSDEEP:	12:gxaacOvIKyxzhqcOvIBTTyx9vcOvIxlzNyxXPcOvIXyxiJcOvIu7:60YodBbTo9UBNoX05oiec7
MD5:	CED55712B4F16863EFFB3E683DC4F17C
SHA1:	9D9606D729C5E4A138EEF7D9824DD1D685EC72BE
SHA-256:	4D0F22C464FCFDA488F01952C7A97B99D8907522D55241702891F5F6454B8D77
SHA-512:	99E8E1514F1AE1B9687AC740D8B9D0DEB6168E89AE2C1AD0E018C75083FBE87475D8E923EAE4C9781A4EE3FEE7420DAED47C52D774E03C8A836E3B9006C5BC 4F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<.....L...._keyhttps://sc-static.net/scevent.min.js .https://adobe.com/P.s.. /.....o.....Z.l.[6.=....J..v.w...Z.....A..Eo.....<.....A..Eo.....0\r..m.....<.....L...._keyhttps://sc-static.net/scevent.min.js .https://adobe.com/..... /.....Z.l.[6.=....J..v.w...Z.....A..Eo.....q.>.....A..Eo.....0\r..m.....<.....L...._keyhttps://sc-static.net/scevent.min.js .https://adobe.com/.... /.....Z.l.[6.=....J..v.w...Z.....A..Eo.....A..Eo.....0\r..m.....<.....L...._keyhttps://sc-static.net/scevent.min.js .https://adobe.com/.e.. /.....Z.l.[6.=....J..v.w...Z.....A..Eo.....5.....A..Eo.....0\r..m.....<.....L...._keyhttps://sc-static.net/scevent.min.js .https://adobe.com/.E... /.....Z.l.[6.=....J..v.w...Z.....A..Eo.....+.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7a906a6be84e1af0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	199688
Entropy (8bit):	6.04923689280988
Encrypted:	false
SSDEEP:	1536:8cxo9Nrff3qMqmzdoks5f2gBuhT5nmfo+v5nmfGzmfopBGDD0st3q5K5+WAaq8pr:zgrff0rk2fhsOsAp9afEe
MD5:	14C9629BC388AC5E1599250FDF4C17E9
SHA1:	8732D71534C347ED40AF3BEA7BB3AA0B75203F42
SHA-256:	5F012414A1BC820BDAD7E3A3834A05AEC303E96A16BA7AB50E71223FD43E2BFB
SHA-512:	21CEF0376C96F5FB1D14799D8AFB7C90B323D65C9E9F4C36FB7EE0FDF47849CF16724670AC75C2DEC3395AD279FCB562431F8ECF66C21974D7DE2C70EFD5EC C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....56534A0BF117B4E0C31441098E2E8A344FE7D3AFCB8C002F38C7B7D578DBEB0E.....'.YS....O/...x...W.....P8..... .....D...\.....(S.0..`.....L`.....(S...Q8.`Vp.....L`<.....Rc.....Z.....QbF..r....o.....Qb...[....s.... ..M...Qb:.....d.....QbnkAO....k.....Qb.j.....t.....Qb.b.....c.....Qb..l.....n.....Qb...%....r.....S...Qb..Y.....l.....R....QbR .....p.....Qb..d....h.....Qb...0....y.....Qbj.:.....f.....O...Qbn.~.....C... ..Qb*.~....w.....Qb.^.F....A.....Qb2.Uv....S.....Qb.....I.....Qb*.....U.....Qb2.cZ....E.....Qb~".*....V.....Qb::.3....D.....Qb.....O.....Qb^.....M.....Qb:.....q.....Qb.....R.....Qb..g.... W.....Qb..d.....Y.....Qb.j.....Q.....Qb"^.H....Z.....Qb.....X.....Qb"P.....ee....Qb...^....te....Qb.D.....oe....Qb...c....ne....Qb.G.....se....Qb..\;....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7ad07de8579b1fd1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	740
Entropy (8bit):	5.83775425791422
Encrypted:	false
SSDEEP:	12:cE3eVdoux2pmYyye3CMx0DPViHnzj2fP1nCUAKmxAC0xezF7:cEuVmuyRyyeSVDNYzKO9xAC0yt
MD5:	60D1321449BD32C6B1BF7E3883EA9703
SHA1:	36E2E0F0A4D1499CFC2EBAA9A4C0EC63095CC114
SHA-256:	0EC395073ECB0BAD432C7F3E154876EB2896740F1E4A93EE081D1006C00172F9
SHA-512:	56EDF2114FA0F22515D5FC1B83C9E1806C42A42197B31AB7B874DFD5A7D4E3F4A215EB0AA931BD034EE876A6D095D20BA37CE121869C5CA64D58EE2E3CE8B7 5E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7ad07de8579b1fd1_0	
Preview:	0\r..m.....`...C.?....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/1004494713/?random=1620171376026&cv=9&fst=1620171376026&num=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&eid=2505059651&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa4l3&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fwww.adobe.com%2Fexpress%2F%3Fr%3Dreader_page_logo&tiba=Make%20Social%20Graphics%2C%20Short%20Videos%2C%20and%20Web%20Pages%20To%20Stand%20Out%E2%80%94In%20Minutes%20%7C%20Adobe%20Spark&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://adobe.com/..?.. /.....wS0;.....*...R.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7df26fdd7801d759_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	194
Entropy (8bit):	5.312973795416208
Encrypted:	false
SSDEEP:	3:m+lKwllA8RzYrSLX8E7/wTRdhgtMu+11lHCKlYlJnOpjCjk5mLV/pK5kt:mUlXYGLFETRTf16K6JnOtCjk4LLK6t
MD5:	0262CEBB5550A6602C401B14E7CAC966
SHA1:	F8480ED58BEFEE97085550010B574F9912C90420
SHA-256:	EF6E3194C34F3CECAD1D32826EC36658DCE362EC6D553E2B11EF479DA4871B32
SHA-512:	DC810FCFB36D0F3C1B1FC36C2FD64DF3000E054EFF471F19514EE0E543EF69C5DD295F561D7D39CCDB348A1408EFCC0D35F08A319F1F4B3B90AFCD6D42A24AC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....>...Yr....._keyhttps://www.adobe.com/akam/11/7dc64881 .https://adobe.com/23w.. /.....Yd.....+.....AGp.\..M ...A..Eo.....F.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\82543c65333d2a14_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1345
Entropy (8bit):	5.66344315358689
Encrypted:	false
SSDEEP:	24:w56MbfTi5CMbfxi5yBMbfMi5ySMbfvqi5fSMbfbT:w56Mbri5CMbpi5yBMbki5ySMbHqi5aMr
MD5:	AC9DB09033EC59C1DC9EF664F1974743
SHA1:	56080B94F6C9C79C76157287E87266BF2C023843
SHA-256:	205D4DD53A43F0BE46150AAF38972835E5E480E368AB559D59435312A73EA0EB
SHA-512:	0C1FC4106123F51E954B26FF288D7391E6BB70E45AC36552B720885850FA8FD9582FBD0F4B197EAE44C6AA496F493D1420A91252CD2F1D7A1FD0C589F4EF4E69
Malicious:	false
Reputation:	low
Preview:	0\r..m.....6....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f675e54cc6b6/RC7a33ddeb7b1e4806b478d6bc282efd1f-file.min.js .https://adobe.com/.Rh.. /.....m.....5v..../....E.M.1..;....I.H.d..#.A..Eo.....\.....A..Eo.....0\r..m.....6....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f675e54cc6b6/RC7a33ddeb7b1e4806b478d6bc282efd1f-file.min.js .https://adobe.com/..... /.....5v..../....E.M.1..;....I.H.d..#.A..Eo.....V.....A..Eo.....0\r..m.....6....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f675e54cc6b6/RC7a33ddeb7b1e4806b478d6bc282efd1f-file.min.js .https://adobe.com/6..../.....5v..../....E.M.1..;....I.H.d..#.A..Eo.....G.....A..Eo.....0\r..m.....6....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f675e54cc6b6/RC7a33ddeb7b1e4806b478d6bc282efd1f-file.min.js .https://adobe.com/..U.. /.....1.....5v..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\866fbb1b46da4c51_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	428
Entropy (8bit):	5.469703262153602
Encrypted:	false
SSDEEP:	6:mAYtVYGLJxoxDMV2o/9mYBprnEK6tWAYtVYGLJxoxDMVnNyqHmYBprRK6t:ItraxDemYBpzWKtraxD0rmYBp3
MD5:	B411B258372F56F651F071AC5AEE1D89
SHA1:	75F0555638194B6180EA744E7BE261E1BAE8F93A
SHA-256:	7A3760FCAC6DC27259FA2FA888876E7E910136C0513E7182D5F234E9F443B089
SHA-512:	CBAD0EE7040FCE18F6D4B82664FCFE355637F8D4C951BB2BF42235083996FC9D056E929698F503FC4AECE7BE0A1E7CB8EC115239513A67E4BB16C7CFAE84E91
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....U....._keyhttps://www.adobe.com/marketingtech/main.no-promise.min.js .https://adobe.com/NPr.. /.....G.....o..I.L.....??..>...-.s...p.A..Eo.....<V.....A..Eo.....0\r..m.....R....U....._keyhttps://www.adobe.com/marketingtech/main.no-promise.min.js .https://adobe.com/".'.. /.....U.....o..I.L.....??..>...-.s...p.A..Eo.....H..G.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8c42284ea9fac8ba_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8c42284ea9fac8ba_0	
File Type:	data
Category:	dropped
Size (bytes):	739
Entropy (8bit):	5.823952195980377
Encrypted:	false
SSDEEP:	12:FqjE3xjSfNKl4oux2peyye3CMx0DPViHnzj2fP1nCUAKmxACXtV3qlN:QjEtSfNtuyeyyeSVDNYzKO9xACXralN
MD5:	40F87E4B3BD5AD31746808A70A3ACC44
SHA1:	BD2E99A984BD8D64F71EDC4264703728A6DB688B
SHA-256:	34A1D02F2671C2D11AE1B4D37754A884221AFD5F1BA82E25C9ED9134DBF26BD8
SHA-512:	D0E4C2FC6E99EC0078DE55F3B8BCA26AF3A90DCEFFB08D58D2433E09888037BFB84AD53160F92590A177052F3FEF9E53B2DD11F97310536A7B9E9CEFA139128 0
Malicious:	false
Reputation:	low
Preview:	0\r..m....._....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/983956512/?random=1620171376030&cv=9&fst=1620171376030&num =1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&eid=2505059650&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=fa lse&u_nplug=1&u_nmime=2&gtm=2oa4l3&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fwww.adobe.com%2Fexpress%2F%3Fr%3D reader_page_logo&tiba=Make%20Social%20Graphics%2C%20Short%20Videos%2C%20and%20Web%20Pages%20To%20Stand%20Out%E2%80%94In%20Minutes% 20%7C%20Adobe%20Spark&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://adobe.com/..?.. /.....6..... ..@U.D4P..`.5.qT....^..A..Eo.....aG..... .A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8d858bba8e7cc695_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.419539189828827
Encrypted:	false
SSDEEP:	3:m+l5Kf/yv8RzYrSLX8AXRHEElJY7sD4gtGmK1lHCelVLs5DL75ai5uRg9k5m81lB:mYEYGLBBkEH7swmK6e3s5l+4+K6t
MD5:	96CB3FE17B74E4204B46F1E80088510B
SHA1:	206087C6FBEA491DA4B4A25362EA5922DD47FD36
SHA-256:	CCF7DB485BFBA789997519F432407816BBAF228F57B9CFE8448E1A9ED3BBA754
SHA-512:	7C6E4EA57D35C7CD1CEB674801329C6A00D4CA5D8F22DAF3FF35B8C3FC1F40EB4246DCDEF0537F274A02B26A5010980C4A94732C5FED82145E5208AAFA1726 E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O..../...../....._keyhttps://www.adobe.com/express/blocks/columns/columns.js .https://adobe.com/.:... /.....u.....3...#..+..N..U.W..`.B...C..4t..A..Eo.....0.....A.. Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8dbf3e0616fc3365_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	446
Entropy (8bit):	5.4710093490666525
Encrypted:	false
SSDEEP:	6:mhynYGLBBkKsdwyB16KZyxH8g4ARK6tWhynYGLBBkKsdwyYqHhZyxH8g4ZaK6t:HBqd3DPMxzjrFBqd3YsMxzks
MD5:	D5C68C3AB95A0CBD281143AAFDA2F475
SHA1:	D44CC290A3C6ACF9DCBA04E83CB84E46AA91B765
SHA-256:	15348F64DF6764538282E59B8EA5285F191273DFDE05EB5AC7B0C179AF57EEDD
SHA-512:	828308B69BD03CA19499CF85412689642F0D447F06BC8BCDC26ECCF6B8FDD837FBF0FB41117F1B42B59ECBD9888E86F65BFCAA57AEBB287182B6AB5D425154 6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....[...2.*W...._keyhttps://www.adobe.com/express/blocks/template-list/template-list.js .https://adobe.com/..... /.....u.....Ff.....T .....h..F..(...A..Eo..... .....A..Eo.....0\r..m.....[...2.*W...._keyhttps://www.adobe.com/express/blocks/template-list/template-list.js .https://adobe.com/.... /.....B.....Ff.....T .....h..F ..(...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8ea8fd6251ae6b4d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	304504
Entropy (8bit):	6.267666123190005
Encrypted:	false
SSDEEP:	3072:ZQynSbYZ6Ds4u6cZrNwnDPXYuAtYCP8QjgTUNj3N5jNPEz:Z3SUZCs4HakLXYuiYCFJ9/E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8ea8fd6251ae6b4d_0	
MD5:	5F6F878C22637D75833F7847629438C5
SHA1:	85848A8985157F1685F5FE91B3E5B1A33F905490
SHA-256:	76B3F4F0D63EF5CB526B7D10A2FA051F89B3F8313F6C179C968047B5F406B708
SHA-512:	7E93B2FC18789DA5E302610E482E18A572DB8ABE3DA3577366F9753B323AF613A2D361889A22AEE9284E38BE48622D9D2DB4DA00EC11B47103103A554D8AC27
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....p.....6A67EE335E7E388812FDFD0F391ED75FA380A715D1E03AD4D3E9FEDE9F41F373.....'.YS....OK...x.....T.....P8.....L.....H.....(.....t.....D...\.....h.....@.....T.....(S.0..`.....L`.....(S...Q8.`Vp.....L`<.....Rc.....Z.....Qb.....o.....Qbf..C....s.....M...Qb.....d.....Qb.-^z....k.....Qb..s.....t.....Qb.....c.....Qb*Y1.....n.....Qb66.~....r.....S...Qb*..%....I..R....Qb.<.....p.....Qb>.8.....h.....Qb^]/.....y.....Qb..%I....f.....O...Qb.i.....C.....QbBx.....w.....Qb.^.....A.....QbR.8.....S.....Qb.....I.....Qb.Z.....U.....Qb.NB.....E.....Qb.....V..Qb..Q....D.....Qb:.r.....O.....Qb..cK....M.....Qb..H....q.....Qbn.F.....R.....Qb.6.~....W.....Qb.....Y.....Qb.w\.....Q.....Qb^.B.....Z...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8f03a761ab0a7cc9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	739
Entropy (8bit):	5.804662205534548
Encrypted:	false
SSDEEP:	12:MlgE3G3+4oux2pmYyye3CMx0DPViHnzj2fP1nCUAKmxACamSGcy:MlgEW3EuyRyyeSVDNYzKO9xACamSGJ
MD5:	58A0FB20D758E0B12FF32D7FF2144CEA
SHA1:	4A7441CAF498005C28D3FAFD6180CC9CF886298C
SHA-256:	8E894A7C594A3C25B3C18E0667E31322903D8B4DC59F301CB89D10FCE6608AAE
SHA-512:	9FFC3197AE0D26165DBFA708BCC5FC3C37B034BDD443F81AD2A84E662E6935C1D5EF5ADDB0C3EB64E0D4820BA82F1023EE8BE301DF29FE84E6064CE18F39ACA
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...>d....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/951622910/?random=1620171375999&cv=9&fst=1620171375999&num=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&eid=2505059651&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa4l3&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fwww.adobe.com%2Fexpress%2F%3Fr%3Dreader_page_logo&tiba=Make%20Social%20Graphics%2C%20Short%20Videos%2C%20and%20Web%20Pages%20To%20Stand%20Out%E2%80%94In%20Minutes%20%7C%20Adobe%20Spark&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://adobe.com/..:.. /.....r~.....Sz.6#..o>.....yA.....WV.{.*..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8faec8b628066d9d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	576
Entropy (8bit):	5.805231290960975
Encrypted:	false
SSDEEP:	12:aXo4MW6IDXrcXo4MW65AD3tTDp+swIuFDK:aYLW68XrcYLW65k3tTDBwIeK
MD5:	C33005FB3EB6EDAD426C8528E6FE0953
SHA1:	2BA37D2AAB45953F51891074F3466F36EC21F8F5
SHA-256:	A6E7EB8641EF6BB963155C50A8DA5116A28AE916FFF1043AB224A347363AB310
SHA-512:	6453839C3BA97979AF26B44EF8EB689E02B887B58AD39DA83A6257D087FC65462B41C79758EEF6A215DF1329EA6B76454846BC401715A516E033C1C38173E7E7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z....._keyhttps://page.adobespark-assets.com/runtime/1.22/runtime-prod.gz.js .https://adobe.com/o... /.....}.....-.t.@d":. $.{F|on.j.... J.A..Eo.....E.....A..Eo.....0\r..m.....Z....._keyhttps://page.adobespark-assets.com/runtime/1.22/runtime-prod.gz.js .https://adobe.com/Nx2.. /.....}.....-.t.@d":. $.{F|on.j.... J.A..Eo.....`V/.....A..Eo.....Nx2.. /.8!..7A1551EAE279D3967EC7691F686D0C93827AC7A866D9991161502F899FED97D3}.....-.t.@d":. $.{F|on.j.... J.A..Eo.....UL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\98450737dd098ac8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	403
Entropy (8bit):	5.923991266122815
Encrypted:	false
SSDEEP:	6:mH/VYGLBg5KAJjNezKIWBQ1FBTLQrhoCTieG2H4mzRK6t/uuLikVbulWDGMoTie6:Ajg5KsjNuffFpL0E2HVzrO34loE2H
MD5:	D561147A135F6AE2CEFE456FDEAA6045
SHA1:	773BC8FC87C66D1A0C739BF6F02865D59676C3A6
SHA-256:	0E9384D1F0986782DF806CCB9F1F50459F9C11E4BC04E9F921A786C960E7D337
SHA-512:	77BA223F3EC23D02D5D7DC5D722338688196C833DC9D20BF091D25BCDF558D9862154147B0E75B76DCF54604FC1626DB1D6BD2C7A37EB6784021803ABA485D
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\98450737dd098ac8_0	
Reputation:	low
Preview:	0\r..m.....^....._keyhttps://www.adobe.com/etc.hawks.dexterlibs/hawks/clientlibs/publish.combined.fp-d40a7373dc7cdb5edbfd059d0f2c60db.js .https://adobe.com/..... /.....C..7....9....8....2.d..W.D.....A..Eo..... P.....A..Eo..... /.....77C5B9843C359EBA0D464DABF1BEA1ECFD26DB272BD6C78F4DE54B7D0090 40E0C..7....9....8....2.d..W.D.....A..Eo.....,{4.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9d8177d41f917273_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	450176
Entropy (8bit):	3.579522544702963
Encrypted:	false
SSDEEP:	6144:sAO7vD3xylyQ7LDGnlxYpgry3T3zoWBnH46/KOe90joPkSXG635/XKMHZsxav05N:sSI2T+WMbdFkB
MD5:	9503AAFC68FF6F9D91670890154FBBEC
SHA1:	F819899DA9E4B74550DABD5FFA5263FF115E94E2
SHA-256:	898A4E65E77ABCA62368B47AB9F272CF52C78BCF1C3CD9AE50C8F9E4C1520D0C
SHA-512:	7F3ECAC3F7653BDB7CA2BEDC304FD417B5483CCDDC1832F265F94150058B45ED9C165EB6668F9543509F96DF6C4E2683FD8E3729A926AED73EEE4B305B166F E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...7..1....DF65FCC5F276FD513710634973084C84F142EE89DB1E704B491AB9AF20836B45.....'.....O.....(S.t. .`.....$L`.....L`.....Qdf-'.....localeBundle.(S...`.....LL`"....@Rc.....QbRX.....e.....M...Qb.U.....t...b$.....I`.....5.a.....1...Pb.....10.a2...L....(S...`.....L`.....Q.@z) .....exports..$..a.....S.C..Qb.P.....l...H..A....a.....Qb.'./....call..!...K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&....&.'..W.....-...( .....,Rc.....1.`....Da`...X.....e..... P.....@....@.-....LP.!.....?...https://spark.adobe.com/static/locales/en-US_bundle-bf6634f5.js.a.....D`....D`....D`.....P...`$... &...&....&....&.(S.....Pb.....t.d.a.....l.....d.....&.(S.....Pb.....t.r.a.....l.....d.....&.(S.....Pb.....t.t.a.....d.....0@..I..d

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9efdd4a8d8632664_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1345
Entropy (8bit):	5.742748734837047
Encrypted:	false
SSDEEP:	24:35FRMW1F5FRTKSF5FRs1TF5FRLEF5FRMht1:35FRMyF5FRmSF5FRsFF5FRLEF5FRWD
MD5:	1A8C0F97A438DA5F9804BBF2A1CAEC35
SHA1:	361E40A46EC7C97E7D39ED79C26E8369550D0403
SHA-256:	E2CA2DD12E4E469665D4D9822F89C949A1328BEADEAE04C486B362CC49929CE8
SHA-512:	8F26D3CA20A149870BF75BC7F59336966B0E6C7EDC239729417A1EE6A4A826856F48A3DC05CBAC44534D7D63A0227F31E3956AD5BF9BC157F8AC2F18424DCA1
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f675e54cc6b6/RCcb1611437f6c42849c41ffe54a71d59f-file.min.js .https://adobe.com /.Oh.. /.....l.....DJmo..d.n.U(..@.PN.|Z.q."...A..Eo.....QN.....A..Eo.....0\r..m....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f6 75e54cc6b6/RCcb1611437f6c42849c41ffe54a71d59f-file.min.js .https://adobe.com/Q.... /.....DJmo..d.n.U(..@.PN.|Z.q."...A..Eo.....h.....A..Eo..... ..0\r..m....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f675e54cc6b6/RCcb1611437f6c42849c41ffe54a71d59f-file.min.js .https://adobe.com/\.... /.....C.....DJmo..d.n.U(..@.PN.|Z.q."...A..Eo.....A..Eo.....0\r..m....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/ f675e54cc6b6/RCcb1611437f6c42849c41ffe54a71d59f-file.min.js .https://adobe.com/].U.. /.....!.....DJ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9f5aed4e4f46c7af_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1060
Entropy (8bit):	5.679542709901257
Encrypted:	false
SSDEEP:	24:S58FQkcrk5WQkfTk5yOQk91k5oiQk61k5rQkZ:SXkAk1kakn
MD5:	FD544CD5E14CD64A4136C6E196347CDF
SHA1:	A5F766BBF0C0080B98170E488378F988C5DA963B
SHA-256:	64B1475296B8DF6FD9C6394CB704816A843873404E476B82A0140244405A56B8
SHA-512:	ECC21D8AFC6FFD29B780366F55F498ADF558D09A64E14DC84DFD5A971FD46C58F8FD47DE0091925BA92652931D460CE6C5D814CB2F336A90282E24BB583AF7 D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9f5aed4e4f46c7af_0	
Preview:	0\r..m.....P....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-987390658 .https://adobe.com/#{r.. /.....o.....<.U#..r.....[...<U....tQ.u...A..Eo.....x.Q.....A..Eo.....0\r..m.....P....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-987390658 .https://adobe.com/N.... /.....<.U#..r.....[...<U....tQ.u...A..Eo.....!q.....A..Eo.....0\r..m.....P....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-987390658 .https://adobe.com/.... /.....<.U#..r.....[...<U....tQ.u...A..Eo.....BTo.....A..Eo.....0\r..m.....P....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-987390658 .https://adobe.com/.Tc.. /.....<.U#..r.....[...<U....tQ.u...A..Eo.....s.....A..Eo.....0\r..m.....P....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-987390658 .https://adobe.com/.>... /.....y.....<.U#..r.....[...<U.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9f7e885e8c444e3d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	18105
Entropy (8bit):	6.063667874868546
Encrypted:	false
SSDEEP:	384:f02hOuzYfj4fa3VepAKAdYeQQj+4viH7k:8BaGcfAe2YlJ4Kw
MD5:	716C83A317C58711675445AECECB5158
SHA1:	C800DBFEFC18681B2F398DFDB67944FF6E871733
SHA-256:	6112B8375574B696FFA9AB7D34AF2F08FD61D201573825E3C9A04CF6BBF028D3
SHA-512:	809FC867E89687EEFA4DE42F0E2DBEC7475F311D76DB225195D5D0144138665AB83A9E1AF01A52B20801727143FAA855DF27B6A896AE976D5C82EA4FE1F5BBFA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....A....y....._keyhttps://d9.flashtalking.com/d9core .https://flashtalking.com/..... /.....z...../0AsR..0"...{.\Z.uy.{.B....I.A..Eo.....A..Eo.....'..*....O....HE.....(S.0..`.....L`.....(S..`.....LL`"....Rc>.....Qenwo"....coreElementId.....Qd._.....container.....Qc.N.{....isApi.....Qb..m.....d9d...Qe..(C....collectSignals....Qc..x.....d9api.....Qc...P....initFt....Qc.....d9legacy...k.....I`....Da....*T...(S....`.....L`V....Y...QcR&>3....windo w....QcR0.Z....screen....Qc6..e....width.....Qc..U.....D9_101....Qc.....height....Qcv.....D9_102....Qe~j.....devicePixelRatio..Qc.....D9_103....QcNP.x....getTime...Qc*..%. ...D9_110... QfBm.....getTimezoneOffset.....Qc.L J....D9_111....QdbQ.....navigator.....QczTm.....platform..Qc.H,'....D9_120.....Qe>.cI....browserLanguage...Qc2..... D9_121....Qd..au....appC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a35f42e17cb0ecfc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	915
Entropy (8bit):	5.433919818088149
Encrypted:	false
SSDEEP:	24:khPLfNp+hNfNh+hNLfNj+hBfNn+hazfNH:ITNpgNhoNjcNnpLNH
MD5:	02D5B22D7FE0486326909E2727A8ABC7
SHA1:	ABD1A507EBF62ECC0D6BFB190AC8D814D931B878
SHA-256:	D6FB7A62E7DE5A881FBCCD15852BBE949A4014FE2B4037FD3A85ACF01BEC6A1B
SHA-512:	AC22BFB00EDA750B29500B97DEE18162E08A71FCE2B390D9A60C255E33402E7999A699A404A45FA3FAF66CD4A4A1AC32681B2C47F617782DF584B1928C72C4B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3.....?....._keyhttps://bat.bing.com/bat.js .https://adobe.com/.ir.. /.....|o.....J.Ns];.<O.F..h'R...=;*..]....A..Eo.....A..Eo.....0\r..m.....3.....?.....keyhttps://bat.bing.com/bat.js .https://adobe.com/<.... /.....J.Ns];.<O.F..h'R...=;*..]....A..Eo.....$..?.....A..Eo.....0\r..m.....3.....?....._keyhttps://bat.bing.com/bat.js .https://adobe.com/O.... /.....J.Ns];.<O.F..h'R...=;*..]....A..Eo.....Y!G.....A..Eo.....0\r..m.....3.....?....._keyhttps://bat.bing.com/bat.js .https://adobe.com/5qf.. /.....J.Ns];.<O.F..h'R...=;*..]....A..Eo.....Y!G.....A..Eo.....0\r..m.....3.....?....._keyhttps://bat.bing.com/bat.js .https://adobe.com/.b... /.....V.....J.Ns];.<O.F..h'R...=;*..]....A..Eo.....).....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a50eb5a5ca8535be_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.86636392655311
Encrypted:	false
SSDEEP:	6:muVYgGKHR9IDqisKl16wRICVpkbaprnqRK6t3l1H3nej4IFcBe+ICVpkbaprlc:zdnEqizxRPgehq1H3ej5mBe+Pge0
MD5:	C68DE984347C5DBD750576D204330F17
SHA1:	9826978BD70CE0EDF2FF03156FB5F7E20F7C6464
SHA-256:	490A13B7F2D23E72B3DBECBF0956FF9D3111C977D097AF74DD379908D9508B47
SHA-512:	FF1442E4A5F3A208036679CAEE7198DA43AA9982D7F884C55C565DF343949CFB7AB75FC3AAEC16758CA2623E17D88CF21332892E077614851681AD6710746A4B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H.... V....._keyhttps://spark.adobe.com/static/m-web-8d2d9d44.js .https://adobe.com/.cI.. /.....)...{.....a.....i[m.s..G.!n.A..Eo.....A..Eo.....cI.. /....54229C962BB643AAC07FCCB37B052171FBC0DAAAEC83AAD74D80093E72E55A54.)...{.....a.....i[m.s..G.!n.A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a6942155eb9698ff_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1476
Entropy (8bit):	5.684564593121433
Encrypted:	false
SSDEEP:	24:KiXe8o47Aiy3e8Kg+e8siLe8SAi+e8sAiht/e8NAiCIJe8zR:KspAjnKDsYSAdsAItPNAL09
MD5:	5856D2AA1A1B3F83A57D270859B7660E
SHA1:	A27EF539489E2B0AF95FB37E166E3A320305E953
SHA-256:	BD99EC63599879580D2CC2E5C9DF5D0318E08DA2CC5EF43C8972D0958685192C
SHA-512:	1FA1C272FB3250320222652E862956D214CC9787C0BF92685EC029BC08287F366F4D63D5F78DE192DBDDDBB189A0694914CB9C8B8B1044595908F958522A4E75
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d....._keyhttps://assets.adobedtm.com/launch-EN919758db9a654a17bac7d184b99c4820.min.js .https://adobe.com/.BK.. /.....g.....YA..H4&.2....K.V.H54.d.1.j.Q..b..A..Eo.....A..Eo.....0\r..m.....d....._keyhttps://assets.adobedtm.com/launch-EN919758db9a654a17bac7d184b99c4820.min.js .https://adobe.com/cYG.. /.....YA..H4&.2....K.V.H54.d.1.j.Q..b..A..Eo.....d.....A..Eo.....C\;.. /.....I.....YA..H4&.2....K.V.H54.d.1.j.Q..b..A..Eo.....J.w.....0\r..m.....d....._keyhttps://assets.adobedtm.com/launch-EN919758db9a654a17bac7d184b99c4820.min.js .https://adobe.com/... /.....B.....YA..H4&.2....K.V.H54.d.1.j.Q..b..A..Eo.....R.....A..Eo.....0\r..m.....d....._keyhttps://assets.adobedtm.com/launch-EN919758db9a654a17bac7d184b99c4820.min.js .https://adobe.com/1.+.. /.....YA..H4&.2....K.V.H54.d.1.j.Q..b..A..Eo.....Z.}V.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a8448f8e0f201664_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1442
Entropy (8bit):	5.505266250569193
Encrypted:	false
SSDEEP:	24:r7PtFQj9Q157Pcpj9X57PcMj9C57PMj9T57Pmj9qr57PIj9W57PN1j9z:rLtFQj9c5Lcpj9X5LcMj9C5LMj9T5Lm4
MD5:	D2DEFA412E4F51CE01ECADBE69C7FFBE
SHA1:	D2598773925BD0731980C64561B89CE26DC18751
SHA-256:	CCED26A69D465A1DFB7B7D741CF6577CE344AC511BC46B3950AFFF793D09C856
SHA-512:	B359847DD3C7D70D1EF84ADF44BD213E8387DA060964CB26AF283088673DC82A64E3449C3B4863C83D4FDA394E2E65DDD0D2EC163145ABF4A2EE9D30407A6C3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J....4....._keyhttps://static.adobelogin.com/imslib/imslib.min.js .https://adobe.com/..... /.....Fe.....Q>-.-:.*'){..Zd..=.[N.,.Un.a....A..Eo.....Pvr.....A..Eo.....0\r..m.....J....4....._keyhttps://static.adobelogin.com/imslib/imslib.min.js .https://adobe.com/'=8.. /.....8}.....Q>-.-:.*'){..Zd..=.[N.,.Un.a....A..Eo.....B.?.....A..Eo.....0\r..m.....J....4....._keyhttps://static.adobelogin.com/imslib/imslib.min.js .https://adobe.com/..G.. /.....v.....Q>-.-:.*'){..Zd..=.[N.,.Un.a....A..Eo.....=.....A..Eo.....0\r..m.....J....4....._keyhttps://static.adobelogin.com/imslib/imslib.min.js .https://adobe.com/.... /.....&.....Q>-.-:.*'){..Zd..=.[N.,.Un.a....A..Eo.....A..Eo.....0\r..m.....J....4....._keyhttps://static.adobelogin.com/imslib/imslib.min.js .https://adobe.com/k.'.. /.....Q>-.-:.*'){..Zd..=.[N.,.Un.a....A..Eo.....C..f..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ab4f59045e28d03f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	699
Entropy (8bit):	5.556084627054714
Encrypted:	false
SSDEEP:	12:3Gz5WYm1Tg9ytGz5WYm9DFT8ItGz5WYmYTLr:c5WLg9yi5WN8li5WGLr
MD5:	314DBB3A60FE720F44E50A574EC84BB4
SHA1:	E6B7CFEBA2D85DB44E9C5A512F87E91143B65173
SHA-256:	3D8D1845C38000C546BA4D5C8DADD26446435EADCF583740989609CBC4B79F36
SHA-512:	A04F955BDEDD19685DAB73853EA4B3D509F45E8178E1889B31AB8C777218993DF49DE3438191A13BDF4D4DE4BDB212C7ADADBF0B03FEAFC2D64C7E5FA0E98F9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e...>.W$...._keyhttps://www.adobe.com/services/feds.res_1.js/head/en/cc-express/spark-gnav.js .https://adobe.com/..t.. /....."h.....#&H1..|....x.' ..5....x\#.%...A..Eo.....;.....A..Eo.....0\r..m.....e...>.W$...._keyhttps://www.adobe.com/services/feds.res_1.js/head/en/cc-express/spark-gnav.js .https://adobe.com/..... /.....#&H1..|....x.' ..5....x\#.%...A..Eo.....J.....A..Eo.....0\r..m.....e...>.W$...._keyhttps://www.adobe.com/services/feds.res_1.js/head/en/cc-express/spark-gnav.js .https://adobe.com/(.... /.....*.....#&H1..|....x.' ..5....x\#.%...A..Eo.....s.X.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ac3dcbd7fa5d1a93_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1130

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ac3dcbd7fa5d1a93_0	
Entropy (8bit):	5.490361317486859
Encrypted:	false
SSDEEP:	24:xgasrz1Drngasrz1S5rngasrz12Engasrz1yxngasrz144:xzsrz5nzsrzcnzsrz9nzsrzYnzsrzP
MD5:	6C93B08C4649164E8D3FC798FF21B294
SHA1:	8D2572613BE3FB36CD6BAA3CBA13AE77718A8C6D
SHA-256:	FD377FBE32F53BD69654C1310B07A75B8FB8A0ADFC4FA0A3753A4902F0AAF77D
SHA-512:	DD5CC97305BF83DB8D931E55FC6C8D07C3880D8E7C8B73B892E43ADBEAD94D74297A13738126A980751848DEF29B4349317A4E376B5ABA201A7D055F0CC530 B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....^...._keyhttps://www.adobe.com/etc.clientlibs/globalnav/clientlibs/base/feds.js .https://adobe.com/n^r.. /.....e.....5g..y..5..O..:L.....?..R.$.....A..Eo.....% .....A..Eo.....0\r..m.....^...._keyhttps://www.adobe.com/etc.clientlibs/globalnav/clientlibs/base/feds.js .https://adobe.com/.6.. /.....\|.....5g..y..5..O..:L..... ?..R.$.....A..Eo.....\#T.....A..Eo.....0\r..m.....^...._keyhttps://www.adobe.com/etc.clientlibs/globalnav/clientlibs/base/feds.js .https://adobe.com/.u... /..... .....5g..y..5..O..:L.....?..R.$.....A..Eo.....Z.~.....A..Eo.....0\r..m.....^...._keyhttps://www.adobe.com/etc.clientlibs/globalnav/clientlibs/base/feds.js .https:// adobe.com/g.'.. /.....5g..y..5..O..:L.....?..R.$.....A..Eo.....A..Eo.....0\r..m.....^...._keyhttps://www.adobe.com/etc.clientlibs/globalnav/clientlibs /base/feds.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\af374cb4784ea935_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	180088
Entropy (8bit):	5.877601800647117
Encrypted:	false
SSDEEP:	1536:9kcOxCLvV+zHb+Jmq/qQUhBoDjlnLt3jKer+54av42FL36nuUkk5CDo46LpYF1iB:9kcOY+7b+AqFUCkehDkk5COLC1Ru
MD5:	6D175B3D91867444B8DE93972759569F
SHA1:	05A9FCA1125D604ADDC97400F66FA11B988D571E
SHA-256:	BEFCE80E168C240BA50D6568AA09A6625805C7BF70E07F88EC042812683C208C
SHA-512:	2A9E20ABFCAD420C7BC5D957B9A2E5D369BE462B54AFA5A371FD2ECD1455BC976D2EC7454250184F95AD5217A7A7070815B8D197F8AA1D7E81CBF7A1B63A95 65
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...x%;.....54229C962BB643AAC07FCCB37B052171FBC0DAAAEC83AAD74D80093E72E55A54.....'.....O9.....h.....p..... .....`.....@.....l.....`".....(S.....`.....y.L`.....(S...5..`$.....L`<....XRc(..... ....QbRX.....e.....Qb.6Jh....n.....Qb.n.....r.....Qbb.p.....o.....S...R..e$.....l`....Da....6P...(S.....Ia.....Qb.U.....t.....@.-....<P.....0...https://spark.adobe.com/s tatic/m-web-8d2d9d44.jsa.....D`....D`$...D`.....`....&...&...=&..1.&...(S....`.....L`.....Q.@z).....exports..$..a.....S.C..Qb.P.....l...H..A....a.....Qb.'./....call..!...K`.. ..D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&...&.'..W.....-...(.....,Rc.....`....Da^...V.....e.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b4793c6ab5fdd872_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	397
Entropy (8bit):	5.931263820481823
Encrypted:	false
SSDEEP:	12:Zg5Ksh4Z1nWub6AEDrrxpr/hSu4+JrfG:ZgToo+6jzrpSP
MD5:	57730CAD30267BA8ED4B5045DE5B395B
SHA1:	2604706987ED7DDBB128497296BF00FE2DFA2521
SHA-256:	7285646AA02572D23CAF77353714C16B0BED62E730A0FA3ED42E11E71B02BE86
SHA-512:	984FFDE559101C0C0CF34686C4054B9D001F00FC0159F438783ADA6EF545DA829A8143B3AF89CA4EACA181F82F6B64FCA1C3FDDD63079EB0B14036D71B7756A E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....{....._keyhttps://www.adobe.com/etc.hawks.dexterlibs/dexter/clientlibs/base/head.fp-1c6b8ee3dfac8039d9ead67e8b6d6138.js .https://adobe.com/.Wr.. /..... .....]....?o..$.o.C,#Io..c.M.{$w.}..A..Eo.....J.6.....A..Eo.....Wr.. /.....9A1D0E2E149F8662F7534CE02BE92BE24D1FC88775C4D685880EF607A64420ED. ....?o..$.o.C,#Io..c.M.{$w.}..A..Eo..... ..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b4ebc6e75ba68880_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	351
Entropy (8bit):	6.010262093425912
Encrypted:	false
SSDEEP:	6:m3EYgGKHRUUHDxLBO6IKFv6K21CLraRK6tEnuTQAXmhGSjMsA1h21CLr:ldiClc6RvM1CLurmnuTQ+IdqE1CL
MD5:	52E7D58511F82C08536BB94771D2ECE3

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b4ebc6e75ba68880_0	
SHA1:	7C6C42C14D701E79894C82949F4DE673D3160CC2
SHA-256:	52810B4CDF6CF5BFF7ECBD916D9B6CD59BD12B3F980811EE549104AF9DA02435
SHA-512:	247CFF3E80F175EAF56AFC3C23F2A5681A3647F6857318C92BCD630B5E7EE8F85CBE0BBF78B16CCD3A2307737D7DCACF01116A19F16F9CFE2D4D98B511A21AE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....._keyhttps://spark.adobe.com/static/locales/en-US_bundle-bf6634f5.js .https://adobe.com/X.G.. /.....y..A.....k..?._y.....\..K(.A..Eo.....:..... ..A..Eo.....X.G.. /.....DF65FCC5F276FD5137106349730 84C84F142EE89DB1E704B491AB9AF20836B45.....y..A.....k..?._y.....\..K(.A..Eo.....iB.4L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bd72fd9df2e083f3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.7881582671469145
Encrypted:	false
SSDEEP:	12:uE31f1KGV5moux2peyye3CMx0DPViH2NRmxAC0shg+1:uElf1KGV5/uyeyyeSVDN/OxACXx1
MD5:	697DB3EF06218430DD1CFF2AFB5E1317
SHA1:	4DAA216127E294F9423701A5021C343D30280038
SHA-256:	2E6DA590B816F24050DE2538498A71D14801FDF8F99BD8554FAB7084E0A7F3AE
SHA-512:	57F399D43DBD2A0B1CF9D31248B4A7D18E0BA135D42401DA1AEC52FB2764D77C93B8775FBFCAE73F6659A7A0811CEA064E7B2D43335535E8A1D82A67939512E2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M:....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/987390658/?random=1620171405675&cv=9&fst=1620171405675&num=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&eid=2505059650&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa4l3&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fwww.adobe.com%2Fexpress%2Fdiscover%2Ftemplates%2Fresume&tiba=Free%20Resume%20Templates%20%7C%20Adobe%20Spark&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://adobe.com/Zf... /.....s. .!%.D`..b...R....'.....pI.A..Eo.....t.m.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c04d129d37789be7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1205
Entropy (8bit):	5.58126618957442
Encrypted:	false
SSDEEP:	12:ikg/BcbXgkg/U+FBgkg/Q1thP7gkg/0ldfgkg/p8Op:5g/AXrg/U+/rg/gjP7rg/Srg/N
MD5:	184B7E39C7828D060B4409A422BEE6C4
SHA1:	7316C883786247AC5C011378E61A8E6CA81D0273
SHA-256:	CA0447043116BE2ACD1FAE0E632BCF9C1C84BC079ED34343B8C1DD298ECDEBCB
SHA-512:	513019B362502294E35C4DA8A3A6FC07B1EE66CE913905C041556D7166A723AE2DA5177CCAF191F3776EFFA30343E887145361A5B1CE93002EA889E241674504
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m....-Q....._keyhttps://www.adobe.com/etc/beagle/public/globalnav/adobe-privacy/latest/privacy.min.js .https://adobe.com/.... /.....4e.....6g..X.h.....=v...f!1.F.....N...A..Eo.....y4_8.....A..Eo.....0\r..m.....m....-Q...._keyhttps://www.adobe.com/etc/beagle/public/globalnav/adobe-privacy/latest/privacy.min.js .https://adobe.com/.n6.. /.....|.....6g..X.h.....=v...f!1.F.....N...A..Eo.....A..Eo.....0\r..m.....m....-Q...._keyhttps://www.adobe.com/etc/beagle/public/globalnav/adobe-privacy/latest/privacy.min.js .https://adobe.com/+_G.. /.....6g..X.h.....=v...f!1.F.....N...A..Eo.....A..Eo.....0\r..m.....m....-Q...._keyhttps://www.adobe.com/etc/beagle/public/globalnav/adobe-privacy/latest/privacy.min.js .https://adobe.com/.j{.. /.....6g..X.h.....=v...f!1.F.....N...A..Eo.....u.....A..Eo.....0\r..m.....m....-Q...._keyhttps://

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c1edc6da6ebfc6d9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7310
Entropy (8bit):	5.969317633281159
Encrypted:	false
SSDEEP:	96:7KUdkZmUjKIJXjxq92XsHhxo6SeB9pUMQWKsra5suqXh9KhBsmMYSQtCPz:7ZkZDKIJXjxqQXQDnpecQqxghBsG3k
MD5:	97025916B6684CD7521ED66E02DF1915
SHA1:	FDA0FBC64F4A88403B431C626E0B6E4186937BB0
SHA-256:	8825B3B05E2C771FE1839AB407228486AAC71C62F850FFEDF635C6E9426B9320
SHA-512:	4ED4B986F7E2BFEC9C903820A34950D01FCB2474E1B89B4F179E90B35BBB3CC862E1C7F6DB1C844FAC3CCA9D92642961B07BDFA7C832BF2ED55617582CD3B899
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c1edc6da6ebfc6d9_0	
Preview:	0\r..m.....N....T....._keyhttps://snap.licdn.com/li.lms-analytics/insight.min.js .https://adobe.com/@.r.. /.....o..... ...{..@...R.%.m....H.m.?&..A..Eo.....A..Eo.. .....'.....O.....i.....(S.0..`.....L`.....(S...`.....L`J.....Rc`.....(.....Qb.....l.....Qb.0....._.....Qbv(.....t.....Qb.[l....s.....Qb...y....r.....Qb.x. (....c.....Qb.ET.....v.....Qb^..k....p.....QbJ!3.....f.....Qb6.&.....w.....Qb.OM.....h.....Qbf.2.....R.....QbRY@.....C.....Qb~t.%....U.....O...Qb>b.....E.....Qb.QP.....x.....Qbn.N.....D. ....Qb. .....L.....Qb...b....T...s.....l`....Da.....!...(S.<.`.....L`....Y...Qc.&V>....getTime...K`....Di.....&.e....&.(...&.X.....,Rc... .....Qb..4....n...`....DaF.....a.....c.....P.....@.-....DP.....6...https://snap.licdn.com/li.lms-analytics/insight.min.js..a.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c4108758c85239bd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	600
Entropy (8bit):	5.817077001690959
Encrypted:	false
SSDEEP:	12:yME31f1KeyUmoux2peyye3CMx0DPVcoYN/CfTfqm:FElf1KeH/uyeyyeSVDNcoYN/CfbZ
MD5:	4B6C8BFCC94AB8896C2B508AA7E3D1DD
SHA1:	0D3A3F1BEEAE4F597A15581134EB485E9A6CB394
SHA-256:	B4ED48FE6F62419A101562D4416E990BCA41288833E62A8BED739FD25ED6D763
SHA-512:	BBB0C8222FF04B7A48F7E8EFBB1579D86FE16378B86A376CA194AA0E3ECE232A3482FD9EAB582F814311D0CD65B764098EC107F88CE4696723F1AD4E20733DF 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/987390658/?random=1620171386745&cv=9&fst=1620171386745&num =1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&eid=2505059650&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=fa lse&u_nplug=1&u_nmime=2&gtm=2oa4l3&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fwww.adobe.com%2Flegal%2Fterms.html&tiba=Leg al&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://adobe.com/..... /.....Y....u....F.M!s.0...+j...V...$.A..Eo.....n.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c49b643286829a7c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1883
Entropy (8bit):	5.722393628945738
Encrypted:	false
SSDEEP:	24:e5kAw5JXFbw5ysMw5Dk2Tw5pLw5Zjw58Fr:e5/w5JRw5yjw5DJTw5Nw5hw52r
MD5:	CDB01F074400B92D3D2128B8E970BFBF
SHA1:	A45CA6F66441E2678CFC77E299143AA73FBEE3E1
SHA-256:	D25E6B596CD5849D88398F7AFEDFBEA6F6B03A2F4880528C80DBE5A5568500D5
SHA-512:	39DFC69DD081D316AD932FAB649591A061288D854C93009F38D3469D705089E8A265AB03A8716673DA40C2781C094B6EE33177BB7FF8C25442E8363C97A29E15
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f675e54cc6b6/RC5e5d1b9fe0a942c38190dc2199529941-file.min.js .https://adobe.com /..`.. /.....-k.....2...P8.9.....*./..}J.,yO.?....A..Eo.....A..Eo.....0\r..m.....N....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/ f675e54cc6b6/RC5e5d1b9fe0a942c38190dc2199529941-file.min.js .https://adobe.com/ <... /.....2...P8.9.....*./..}J.,yO.?....A..Eo.....]....A..Eo.....0\r. .m.....N....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f675e54cc6b6/RC5e5d1b9fe0a942c38190dc2199529941-file.min.js .https://adobe.com/.... /.....2...P8.9.....*./..}J..yO.?....A..Eo.....>.....A..Eo.....0\r..m.....N....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/f675e5 4cc6b6/RC5e5d1b9fe0a942c38190dc2199529941-file.min.js .https://adobe.com/..... /.....D.....2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ca2fc668617d27cb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94200
Entropy (8bit):	5.77056365077779
Encrypted:	false
SSDEEP:	1536:zUskXVw/KM90ikfjLhtUhz/Uj3pkzOosjOgXWox79qO/o/adrudgp9G1qvSPL:oroheJoOkSosjpGw79jw/adqR1qE
MD5:	ACE7C865AAF8435914AD09001CA52FC7
SHA1:	26CA32708C4FE7BB8F092761190349E4E2508775
SHA-256:	DC49C06D001C56C63D58231A3FD7EA966843C6FA4A203D1B9F1235171D6A587C
SHA-512:	21F6182CA44D5AA978F5914E109262A1510F91F0DF808F3C917967CFE6C4EBC1503D245954CABB387E95D6B1318B227C8C49BC67654B3C17E3C60A4381645DC/
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....%....A20E39BA81960CF84FE4CF8C4114910A068DC3C9B72527BAB0025D9BA4A4BB0E.....'.JN....O ....n..#..#.....!..... .....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....*.....Q.@..t.....module....Q.@.e.....exports...Qc..aZ....document. (S.....5.a.....a.....a.....a.....a.....Pc.....exportsa.....I.....@.-....LP.!.....@...https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.jsa..... .D`....D`....D`.....`z...&...&..!.&....&.(S....!..`.C.....q.L`.....Rc@.....M.....Qb.E.....d.....Qb&.....e.....Qb.w.x....f.....Qbr.W.....h.....S...Qb..)....j.....Qb6.....k.....Qb... ....l.....Qb..o.....n.....Qb^fG.....o.....Qb.....p.....Qb...B....q.....QbFM.....r.....QbZ.....s.....R....Qb..3.....v.....Qb..$.....w.....Qb. ~M....x.....Qb.....y....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cd03638b5373976d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	612
Entropy (8bit):	5.441840144541519
Encrypted:	false
SSDEEP:	12:wBWAIEtdN/QN+BWAIEcN1+BWAIEwkRNm7:wBWVEtdtc+BWVEcf+BWVEwkRk
MD5:	08235CCE85CE8F0F3D1458A2646B8B91
SHA1:	454D1360998871C447F664A59B2B056E35BCC1D1
SHA-256:	28CDC87DB4E45B163A0DFB807582A773033AE146E7624DC8A88BD7DC408D6E28
SHA-512:	9BA0208B822376811A7E3D115994D497AE9C5704C28AC0FFEF854B76530D3C2DA4F29EC1EDCD22F650DF98C014060DE3323670B4C673ABBA17EE22A32D4F883
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H.....>u...._keyhttps://www.adobe.com/express/scripts/martech.js .https://adobe.com/..x.. /.....d.....m.~TI.G.I..Y....c...W....C..F..A..Eo.....A..Eo..... .....0\r..m.....H.....>u...._keyhttps://www.adobe.com/express/scripts/martech.js .https://adobe.com/.M5.. /.....k|.....m.~TI.G.I..Y....c...W....C..F..A..Eo.....n.s..... ...A..Eo.....0\r..m.....H.....>u...._keyhttps://www.adobe.com/express/scripts/martech.js .https://adobe.com/..... /.....m.~TI.G.I..Y....c...W....C..F..A..Eo... ...|.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d1e9bca73e9ccebd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	400
Entropy (8bit):	5.486144519622724
Encrypted:	false
SSDEEP:	6:moEYFEDL5VTRdxzSTlD4ZumVr9koyP4OIK6tWoEYFEDL5VTRdxHNu1h/l74ZumVv:+lmZD4FzyP48lo/h4FzyPcl
MD5:	702685143EEC59775B0ADD0D7285CE90
SHA1:	B1BE7D7C137049189517551DB9581A8714424180
SHA-256:	309F0C1A475348D98646695D03F6B0E5B3B77AEA004318703733FB337BE74488
SHA-512:	EB2E682BB5E477B9E5FEE350DA543F316ABCFDF1B63875B307F082A52DA700BC31511A5C8F3C68DCE04FD2F41A2EEACD46DB456B1467282A43DD9BA64A0F83 2B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....D....@.[...._keyhttps://js-agent.newrelic.com/nr-1177.min.js .https://adobe.com/. ... /.....Z....p.....Lg,.i...Y.X_ny..A..Eo.....6.....A..Eo.....0\ r..m.....D....@.[...._keyhttps://js-agent.newrelic.com/nr-1177.min.js .https://adobe.com/.E... /.....Z....p.....Lg,.i...Y.X_ny..A..Eo.....[(.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d3b37b1b026dc6fb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	343
Entropy (8bit):	5.950506854415318
Encrypted:	false
SSDEEP:	6:mMIYgGKHRa+ztsv6FRcVBhn7K6tQO6FKXA8AcVZwUW2hGhyWr3RcVBhnv:WdM+ztsCReBv6OuKj3ZwUVghj7ReBp
MD5:	733F24AA62245F27D5D986137A32191E
SHA1:	EB344A9705CA6EF30B4C71046FC5D6F1B799D9DA
SHA-256:	C33DF7C7494ADE840BE54891E70F76C9511970AC030D9CFC2903D80585E9CC7E
SHA-512:	61FE09006992B681B1BB6CD2BA2068D67046F2C5E94D0E043B473FC96C38F2B07E60F7FE40107C656FDE813CD70039F9E453344FA1B1A1E46C3E365616E8CF86
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O....<T....._keyhttps://spark.adobe.com/static/marvelcommon-51100480.js .https://adobe.com/..H.. /.....W..)....q\..?.d...!!.^.^...A..Eo.....nz.....A..Eo... .....H.. /.(...FC89AB3B245556B8C3ABB596D39E2CA3D49EF7D9A215CEC9BE7CEAD5DD47D6DF...W..)....q\..?.d...!!.^.^...A..Eo.....@...L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d6595452d2846755_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1010
Entropy (8bit):	5.503683189753928
Encrypted:	false
SSDEEP:	24:4He5L7huHe5jL7MuHe5hb7KuHe5RA47ouHe5HI7/:WKLlkKHAkKhbukKtskKor
MD5:	AB14184068F76ACB84EE9065AEA8370A
SHA1:	AB925FED65C89657E332733C970039C9DCDE96D6
SHA-256:	1BDF56612AEC7A29C0E2F676D2B7CC50D3036F8005D09ED21B164EC1F021C967

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d6595452d2846755_0	
SHA-512:	0156100B7D6AF5257A0F1432AE536862083D63C0F5CB89AEF28A5F025B82892A96DBEB92F599F9DBD705E33E7487F01844EC26444A7DF083956697B167A9A4A4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....F.....T<...._keyhttps://connect.facebook.net/en_US/fbevents.js .https://adobe.com/;d=.. /.....9p.....W.l.....|&.B..)....k:y.qf..J.A..Eo.....O..X.....A..Eo..... .....0\r..m.....F.....T<...._keyhttps://connect.facebook.net/en_US/fbevents.js .https://adobe.com/..... /.....W.l.....|&.B..)....k:y.qf..J.A..Eo.....O.....A..Eo..... .....0\r..m.....F.....T<...._keyhttps://connect.facebook.net/en_US/fbevents.js .https://adobe.com/!.... /.....5.....W.l.....|&.B..)....k:y.qf..J.A..Eo.....y.....A..Eo..... .....0\r..m.....F.....T<...._keyhttps://connect.facebook.net/en_US/fbevents.js .https://adobe.com/.e.. /.....W.l.....|&.B..)....k:y.qf..J.A..Eo.....A..Eo..... ...0\r..m.....F.....T<...._keyhttps://connect.facebook.net/en_US/fbevents.js .https://adobe.com/..... /.....5.....W.l.....|&.B..)....k:y.qf..J.A..Eo.....O.mq.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d9cf9443d75c501a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	613
Entropy (8bit):	5.799651887495283
Encrypted:	false
SSDEEP:	12:mFgE3G9UbcUv4oux2peyye3CMx0DPV2myYJyCt4zk/9r1:mFgEW2blvBuyeyyeSVDN2myY4CWi5
MD5:	2C7C2474290C9D8F430F8D6E9ABC5629
SHA1:	E2332E96AF32DD65BC853E19FFE93B841BBAB5B2
SHA-256:	7B7FBA9E31F5B7DF24C85FDE09E3FAEA8CDD3547F2DC73DBDE0EE7FADC77E8CC
SHA-512:	F73E7E19C3596A9C46267B4340650FEE04C6106D42F26FC947BAA012F21C5CA9CA2606043563B0974E1F8013E786C774E5CDF433DE407120C58E87E356332440
Malicious:	false
Reputation:	low
Preview:	0\r..m.....NK...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/951622910/?random=1620171405914&cv=9&fst=1620171405914&nu m=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&eid=2505059650&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=f alse&u_nplug=1&u_nmime=2&gtm=2oa4l3&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fwww.adobe.com%2Fprivacy.html&tiba=Adobe%20 Privacy%20Center&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://adobe.com/.:... /.....o.-....Y..p.Bn./..@.^>6!c..A..Eo.....t.e.....A..Eo..... .....

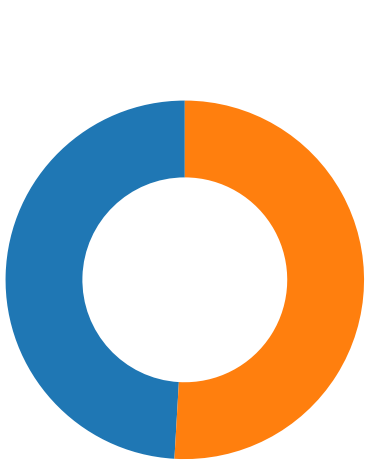
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\da69805e79f76b31_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	600
Entropy (8bit):	5.8109485760895385
Encrypted:	false
SSDEEP:	12:u+E3GHyIzoux2pmYyye3CMx0DPVcoYN/CQRWPNn1:lEWSI0uyRyyeSVDNcoYN/C71
MD5:	5FE8E47A68838BC5207537D08D4AC3B7
SHA1:	A6B491BC086A38522DD77A74E11A609164DE7661
SHA-256:	C80AC37D2E82B3D23C7D6D2DAC2BD664A19E8D7A9809FBF9F12BCE800167F3FA
SHA-512:	665368935411FF3158AC01818A7F65FA80E1F9E06E288A8B856A3409B9E832BFDAA89526C5F178583B7B6EB2646AFD99A8FA574E7FEB5461677B117CDDA9837A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....2....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/951622910/?random=1620171386728&cv=9&fst=1620171386728&nu m=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&eid=2505059651&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=f alse&u_nplug=1&u_nmime=2&gtm=2oa4l3&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fwww.adobe.com%2Flegal%2Fterms.html&tiba=Le gal&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://adobe.com/`.... /.....%..:...Ti}~.I]C.so...r....A..Eo.....5B.U.....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
May 4, 2021 16:35:16.840792894 CEST	443	49702	131.253.33.200	192.168.2.5
May 4, 2021 16:35:16.843508959 CEST	443	49701	131.253.33.200	192.168.2.5
May 4, 2021 16:35:16.843694925 CEST	49701	443	192.168.2.5	131.253.33.200
May 4, 2021 16:35:16.844048023 CEST	443	49701	131.253.33.200	192.168.2.5
May 4, 2021 16:35:16.845683098 CEST	443	49702	131.253.33.200	192.168.2.5
May 4, 2021 16:35:16.845716000 CEST	443	49702	131.253.33.200	192.168.2.5
May 4, 2021 16:35:16.845731020 CEST	443	49702	131.253.33.200	192.168.2.5
May 4, 2021 16:35:16.845834970 CEST	49702	443	192.168.2.5	131.253.33.200
May 4, 2021 16:35:16.845881939 CEST	49702	443	192.168.2.5	131.253.33.200
May 4, 2021 16:35:16.856508017 CEST	443	49702	131.253.33.200	192.168.2.5
May 4, 2021 16:35:16.856544971 CEST	443	49702	131.253.33.200	192.168.2.5
May 4, 2021 16:35:16.856735945 CEST	49702	443	192.168.2.5	131.253.33.200
May 4, 2021 16:35:20.875797987 CEST	49699	443	192.168.2.5	131.253.33.200
May 4, 2021 16:35:20.875940084 CEST	49699	443	192.168.2.5	131.253.33.200
May 4, 2021 16:35:20.876002073 CEST	49699	443	192.168.2.5	131.253.33.200
May 4, 2021 16:35:20.876034021 CEST	49699	443	192.168.2.5	131.253.33.200
May 4, 2021 16:35:20.876105070 CEST	49699	443	192.168.2.5	131.253.33.200
May 4, 2021 16:35:20.876128912 CEST	49699	443	192.168.2.5	131.253.33.200
May 4, 2021 16:35:20.876157999 CEST	49699	443	192.168.2.5	131.253.33.200
May 4, 2021 16:35:20.876213074 CEST	49699	443	192.168.2.5	131.253.33.200
May 4, 2021 16:35:20.876235008 CEST	49699	443	192.168.2.5	131.253.33.200
May 4, 2021 16:35:20.923197031 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.923243999 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.923266888 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.923283100 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.923296928 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.923311949 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.923710108 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.923753023 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.923784018 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.923825026 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.923865080 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.923901081 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.923917055 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.923930883 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.923949003 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.923985004 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924016953 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924058914 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924092054 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924107075 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924120903 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924134970 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924145937 CEST	443	49699	131.253.33.200	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 16:35:20.924163103 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924179077 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924192905 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924233913 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924266100 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924279928 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924293995 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924309015 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924335957 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924350977 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924379110 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924392939 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924422026 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924459934 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924475908 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924493074 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924509048 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924524069 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924537897 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924551964 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924566984 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924582005 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924597025 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924607992 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924616098 CEST	49699	443	192.168.2.5	131.253.33.200
May 4, 2021 16:35:20.924617052 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924635887 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924650908 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924665928 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924680948 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924695015 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924704075 CEST	49699	443	192.168.2.5	131.253.33.200
May 4, 2021 16:35:20.924709082 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924724102 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.924736977 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.991478920 CEST	443	49699	131.253.33.200	192.168.2.5
May 4, 2021 16:35:20.991575003 CEST	49699	443	192.168.2.5	131.253.33.200
May 4, 2021 16:35:34.108756065 CEST	49716	443	192.168.2.5	205.139.111.113
May 4, 2021 16:35:34.116597891 CEST	49719	443	192.168.2.5	205.139.111.113
May 4, 2021 16:35:34.235006094 CEST	443	49716	205.139.111.113	192.168.2.5
May 4, 2021 16:35:34.235090017 CEST	49716	443	192.168.2.5	205.139.111.113
May 4, 2021 16:35:34.243333101 CEST	443	49719	205.139.111.113	192.168.2.5
May 4, 2021 16:35:34.243443012 CEST	49719	443	192.168.2.5	205.139.111.113
May 4, 2021 16:35:34.251163006 CEST	49716	443	192.168.2.5	205.139.111.113
May 4, 2021 16:35:34.251921892 CEST	49719	443	192.168.2.5	205.139.111.113
May 4, 2021 16:35:34.376051903 CEST	443	49716	205.139.111.113	192.168.2.5
May 4, 2021 16:35:34.376557112 CEST	443	49719	205.139.111.113	192.168.2.5
May 4, 2021 16:35:34.377511024 CEST	443	49716	205.139.111.113	192.168.2.5
May 4, 2021 16:35:34.377590895 CEST	443	49716	205.139.111.113	192.168.2.5
May 4, 2021 16:35:34.377649069 CEST	443	49716	205.139.111.113	192.168.2.5
May 4, 2021 16:35:34.377676964 CEST	49716	443	192.168.2.5	205.139.111.113
May 4, 2021 16:35:34.380470037 CEST	443	49719	205.139.111.113	192.168.2.5
May 4, 2021 16:35:34.380494118 CEST	443	49719	205.139.111.113	192.168.2.5
May 4, 2021 16:35:34.380507946 CEST	443	49719	205.139.111.113	192.168.2.5
May 4, 2021 16:35:34.380618095 CEST	49719	443	192.168.2.5	205.139.111.113
May 4, 2021 16:35:34.489777088 CEST	49716	443	192.168.2.5	205.139.111.113

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 16:35:19.977015018 CEST	61733	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:20.028891087 CEST	53	61733	8.8.8.8	192.168.2.5
May 4, 2021 16:35:20.993664980 CEST	65447	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:21.045358896 CEST	53	65447	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 16:35:22.200864077 CEST	52441	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:22.252382040 CEST	53	52441	8.8.8.8	192.168.2.5
May 4, 2021 16:35:23.047750950 CEST	62176	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:23.099735975 CEST	53	62176	8.8.8.8	192.168.2.5
May 4, 2021 16:35:24.011568069 CEST	59596	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:24.072716951 CEST	53	59596	8.8.8.8	192.168.2.5
May 4, 2021 16:35:25.234777927 CEST	65296	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:25.286474943 CEST	53	65296	8.8.8.8	192.168.2.5
May 4, 2021 16:35:26.168378115 CEST	63183	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:26.218761921 CEST	53	63183	8.8.8.8	192.168.2.5
May 4, 2021 16:35:26.449625015 CEST	60151	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:26.511274099 CEST	53	60151	8.8.8.8	192.168.2.5
May 4, 2021 16:35:27.012758970 CEST	56969	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:27.064456940 CEST	53	56969	8.8.8.8	192.168.2.5
May 4, 2021 16:35:33.517210960 CEST	54757	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:33.570132971 CEST	53	54757	8.8.8.8	192.168.2.5
May 4, 2021 16:35:34.032929897 CEST	49992	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:34.034018993 CEST	60075	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:34.043368101 CEST	55016	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:34.081048965 CEST	64345	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:34.091239929 CEST	53	49992	8.8.8.8	192.168.2.5
May 4, 2021 16:35:34.094461918 CEST	53	55016	8.8.8.8	192.168.2.5
May 4, 2021 16:35:34.098807096 CEST	53	60075	8.8.8.8	192.168.2.5
May 4, 2021 16:35:34.147476912 CEST	53	64345	8.8.8.8	192.168.2.5
May 4, 2021 16:35:34.660418987 CEST	54791	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:34.738514900 CEST	53	54791	8.8.8.8	192.168.2.5
May 4, 2021 16:35:35.007150888 CEST	50463	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:35.067145109 CEST	53	50463	8.8.8.8	192.168.2.5
May 4, 2021 16:35:35.078718901 CEST	50394	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:35.127418041 CEST	53	50394	8.8.8.8	192.168.2.5
May 4, 2021 16:35:35.579317093 CEST	58530	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:35.636398077 CEST	53	58530	8.8.8.8	192.168.2.5
May 4, 2021 16:35:37.138756990 CEST	54450	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:37.197983027 CEST	53	54450	8.8.8.8	192.168.2.5
May 4, 2021 16:35:39.042181015 CEST	59261	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:39.103637934 CEST	53	59261	8.8.8.8	192.168.2.5
May 4, 2021 16:35:39.544537067 CEST	57151	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:39.593442917 CEST	53	57151	8.8.8.8	192.168.2.5
May 4, 2021 16:35:39.979644060 CEST	59413	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:40.061850071 CEST	53	59413	8.8.8.8	192.168.2.5
May 4, 2021 16:35:40.645349979 CEST	60516	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:40.706604958 CEST	53	60516	8.8.8.8	192.168.2.5
May 4, 2021 16:35:40.925235987 CEST	51649	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:40.987078905 CEST	53	51649	8.8.8.8	192.168.2.5
May 4, 2021 16:35:41.972501040 CEST	65086	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:42.024051905 CEST	53	65086	8.8.8.8	192.168.2.5
May 4, 2021 16:35:42.542412043 CEST	52929	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:42.600725889 CEST	53	52929	8.8.8.8	192.168.2.5
May 4, 2021 16:35:46.581769943 CEST	61004	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:46.649342060 CEST	53	61004	8.8.8.8	192.168.2.5
May 4, 2021 16:35:47.423048019 CEST	56895	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:47.481231928 CEST	53	56895	8.8.8.8	192.168.2.5
May 4, 2021 16:35:49.800525904 CEST	62372	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:49.857685089 CEST	53	62372	8.8.8.8	192.168.2.5
May 4, 2021 16:35:50.200392008 CEST	61515	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:50.269063950 CEST	53	61515	8.8.8.8	192.168.2.5
May 4, 2021 16:35:52.824846983 CEST	56675	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:52.882914066 CEST	53	56675	8.8.8.8	192.168.2.5
May 4, 2021 16:35:56.237423897 CEST	57172	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:56.307451963 CEST	53	57172	8.8.8.8	192.168.2.5
May 4, 2021 16:35:56.821916103 CEST	55267	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:56.885488987 CEST	53	55267	8.8.8.8	192.168.2.5
May 4, 2021 16:35:57.949173927 CEST	50969	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:57.950303078 CEST	64362	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 16:35:57.951344013 CEST	54766	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:57.952341080 CEST	61446	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:57.953488111 CEST	57515	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:57.999918938 CEST	53	64362	8.8.8.8	192.168.2.5
May 4, 2021 16:35:58.011312008 CEST	53	50969	8.8.8.8	192.168.2.5
May 4, 2021 16:35:58.011342049 CEST	53	61446	8.8.8.8	192.168.2.5
May 4, 2021 16:35:58.014784098 CEST	53	54766	8.8.8.8	192.168.2.5
May 4, 2021 16:35:58.014803886 CEST	53	57515	8.8.8.8	192.168.2.5
May 4, 2021 16:35:59.092804909 CEST	58199	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:59.163340092 CEST	53	58199	8.8.8.8	192.168.2.5
May 4, 2021 16:35:59.181607962 CEST	65221	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:59.238867998 CEST	53	65221	8.8.8.8	192.168.2.5
May 4, 2021 16:35:59.289593935 CEST	61573	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:59.295790911 CEST	56562	53	192.168.2.5	8.8.8.8
May 4, 2021 16:35:59.357285976 CEST	53	61573	8.8.8.8	192.168.2.5
May 4, 2021 16:35:59.358895063 CEST	53	56562	8.8.8.8	192.168.2.5
May 4, 2021 16:36:02.399399996 CEST	53591	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:02.460293055 CEST	53	53591	8.8.8.8	192.168.2.5
May 4, 2021 16:36:09.072215080 CEST	59688	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:09.152755976 CEST	53	59688	8.8.8.8	192.168.2.5
May 4, 2021 16:36:09.581547022 CEST	56032	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:09.585766077 CEST	61150	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:09.592408895 CEST	63458	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:09.640296936 CEST	53	56032	8.8.8.8	192.168.2.5
May 4, 2021 16:36:09.648161888 CEST	53	61150	8.8.8.8	192.168.2.5
May 4, 2021 16:36:09.684140921 CEST	53	63458	8.8.8.8	192.168.2.5
May 4, 2021 16:36:10.379460096 CEST	50422	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:10.450848103 CEST	53	50422	8.8.8.8	192.168.2.5
May 4, 2021 16:36:10.509460926 CEST	53247	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:10.569983006 CEST	53	53247	8.8.8.8	192.168.2.5
May 4, 2021 16:36:10.671173096 CEST	58544	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:10.686285973 CEST	53814	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:10.743021011 CEST	53	58544	8.8.8.8	192.168.2.5
May 4, 2021 16:36:10.750243902 CEST	53	53814	8.8.8.8	192.168.2.5
May 4, 2021 16:36:10.780833960 CEST	51305	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:10.839915037 CEST	53	51305	8.8.8.8	192.168.2.5
May 4, 2021 16:36:10.941067934 CEST	53670	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:11.004300117 CEST	53	53670	8.8.8.8	192.168.2.5
May 4, 2021 16:36:11.236730099 CEST	55160	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:11.262213945 CEST	61414	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:11.289531946 CEST	53	55160	8.8.8.8	192.168.2.5
May 4, 2021 16:36:11.330197096 CEST	53	61414	8.8.8.8	192.168.2.5
May 4, 2021 16:36:12.101944923 CEST	63847	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:12.159795046 CEST	53	63847	8.8.8.8	192.168.2.5
May 4, 2021 16:36:12.359375954 CEST	61523	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:12.394469023 CEST	50551	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:12.415762901 CEST	62847	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:12.417165995 CEST	57712	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:12.417439938 CEST	61064	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:12.417674065 CEST	61891	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:12.437231064 CEST	61585	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:12.438015938 CEST	53	61523	8.8.8.8	192.168.2.5
May 4, 2021 16:36:12.458005905 CEST	53	50551	8.8.8.8	192.168.2.5
May 4, 2021 16:36:12.463016033 CEST	65163	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:12.466420889 CEST	53	61064	8.8.8.8	192.168.2.5
May 4, 2021 16:36:12.466459036 CEST	53	61891	8.8.8.8	192.168.2.5
May 4, 2021 16:36:12.471347094 CEST	58969	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:12.472249985 CEST	53977	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:12.475930929 CEST	53	62847	8.8.8.8	192.168.2.5
May 4, 2021 16:36:12.509572029 CEST	57147	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:12.515057087 CEST	53	57712	8.8.8.8	192.168.2.5
May 4, 2021 16:36:12.517256975 CEST	53	61585	8.8.8.8	192.168.2.5
May 4, 2021 16:36:12.536024094 CEST	53	53977	8.8.8.8	192.168.2.5
May 4, 2021 16:36:12.536050081 CEST	53	65163	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 16:36:12.560095072 CEST	53	58969	8.8.8.8	192.168.2.5
May 4, 2021 16:36:12.576776981 CEST	53	57147	8.8.8.8	192.168.2.5
May 4, 2021 16:36:13.243103027 CEST	52381	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:13.247792959 CEST	49231	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:13.247970104 CEST	53217	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:13.256773949 CEST	52554	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:13.259849072 CEST	49603	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:13.260762930 CEST	64476	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:13.297168016 CEST	53	49231	8.8.8.8	192.168.2.5
May 4, 2021 16:36:13.300024986 CEST	53	53217	8.8.8.8	192.168.2.5
May 4, 2021 16:36:13.305301905 CEST	53	52381	8.8.8.8	192.168.2.5
May 4, 2021 16:36:13.305623055 CEST	53	52554	8.8.8.8	192.168.2.5
May 4, 2021 16:36:13.319303989 CEST	53	49603	8.8.8.8	192.168.2.5
May 4, 2021 16:36:13.319907904 CEST	53	64476	8.8.8.8	192.168.2.5
May 4, 2021 16:36:13.392424107 CEST	49975	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:13.451991081 CEST	53	49975	8.8.8.8	192.168.2.5
May 4, 2021 16:36:13.533850908 CEST	57701	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:13.537612915 CEST	60334	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:13.538229942 CEST	64958	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:13.539073944 CEST	58504	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:13.594815016 CEST	53	57701	8.8.8.8	192.168.2.5
May 4, 2021 16:36:13.596571922 CEST	53	60334	8.8.8.8	192.168.2.5
May 4, 2021 16:36:13.598303080 CEST	53	58504	8.8.8.8	192.168.2.5
May 4, 2021 16:36:13.601154089 CEST	53	64958	8.8.8.8	192.168.2.5
May 4, 2021 16:36:14.614466906 CEST	58041	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:14.674010992 CEST	53	58041	8.8.8.8	192.168.2.5
May 4, 2021 16:36:14.697282076 CEST	57764	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:14.728560925 CEST	57973	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:14.769978046 CEST	53	57764	8.8.8.8	192.168.2.5
May 4, 2021 16:36:14.793672085 CEST	53	57973	8.8.8.8	192.168.2.5
May 4, 2021 16:36:15.083512068 CEST	57974	443	192.168.2.5	142.250.185.102
May 4, 2021 16:36:15.139008999 CEST	443	57974	142.250.185.102	192.168.2.5
May 4, 2021 16:36:15.139039993 CEST	443	57974	142.250.185.102	192.168.2.5
May 4, 2021 16:36:15.139056921 CEST	443	57974	142.250.185.102	192.168.2.5
May 4, 2021 16:36:15.139866114 CEST	57974	443	192.168.2.5	142.250.185.102
May 4, 2021 16:36:15.141444921 CEST	57974	443	192.168.2.5	142.250.185.102
May 4, 2021 16:36:15.141978979 CEST	57974	443	192.168.2.5	142.250.185.102
May 4, 2021 16:36:15.204286098 CEST	443	57974	142.250.185.102	192.168.2.5
May 4, 2021 16:36:15.210251093 CEST	57974	443	192.168.2.5	142.250.185.102
May 4, 2021 16:36:15.216312885 CEST	443	57974	142.250.185.102	192.168.2.5
May 4, 2021 16:36:15.216368914 CEST	443	57974	142.250.185.102	192.168.2.5
May 4, 2021 16:36:15.222986937 CEST	57974	443	192.168.2.5	142.250.185.102
May 4, 2021 16:36:15.810332060 CEST	63286	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:15.867326021 CEST	53	63286	8.8.8.8	192.168.2.5
May 4, 2021 16:36:16.239702940 CEST	52589	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:16.308409929 CEST	53	52589	8.8.8.8	192.168.2.5
May 4, 2021 16:36:16.394752026 CEST	54875	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:16.420583963 CEST	49862	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:16.456599951 CEST	53	54875	8.8.8.8	192.168.2.5
May 4, 2021 16:36:16.486377954 CEST	53	49862	8.8.8.8	192.168.2.5
May 4, 2021 16:36:16.879678965 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:16.935347080 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:16.935374975 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:16.935405970 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:16.936584949 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:16.938488007 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:16.939220905 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:16.939487934 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:16.994224072 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:16.994630098 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:16.994735003 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:17.009931087 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:17.009951115 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:17.009993076 CEST	443	49863	142.250.185.130	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 16:36:17.010005951 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:17.010180950 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:17.010221958 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:17.013473988 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:17.013596058 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:17.013654947 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:17.157808065 CEST	50119	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:17.165545940 CEST	60159	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:17.214167118 CEST	53	60159	8.8.8.8	192.168.2.5
May 4, 2021 16:36:17.216871977 CEST	53	50119	8.8.8.8	192.168.2.5
May 4, 2021 16:36:17.357510090 CEST	49464	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:17.425421000 CEST	53	49464	8.8.8.8	192.168.2.5
May 4, 2021 16:36:17.925564051 CEST	64650	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:17.992420912 CEST	53	64650	8.8.8.8	192.168.2.5
May 4, 2021 16:36:18.347618103 CEST	52633	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:18.420730114 CEST	53	52633	8.8.8.8	192.168.2.5
May 4, 2021 16:36:21.489171982 CEST	56124	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:21.540673018 CEST	53	56124	8.8.8.8	192.168.2.5
May 4, 2021 16:36:21.909977913 CEST	55552	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:21.961424112 CEST	53	55552	8.8.8.8	192.168.2.5
May 4, 2021 16:36:24.748500109 CEST	60813	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:24.823822021 CEST	53	60813	8.8.8.8	192.168.2.5
May 4, 2021 16:36:25.046418905 CEST	50930	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:25.114356041 CEST	53	50930	8.8.8.8	192.168.2.5
May 4, 2021 16:36:25.369937897 CEST	51582	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:25.435973883 CEST	53	51582	8.8.8.8	192.168.2.5
May 4, 2021 16:36:26.022053003 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:26.085585117 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:26.085603952 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:26.086218119 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:26.087003946 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:26.114729881 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:26.161505938 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:26.176932096 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:26.176951885 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:26.177323103 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:26.180655003 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:26.234354973 CEST	56831	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:26.251674891 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:26.255098104 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:26.299551010 CEST	53	56831	8.8.8.8	192.168.2.5
May 4, 2021 16:36:26.314383030 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:26.314403057 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:26.316286087 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:26.376715899 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:26.454016924 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:26.520283937 CEST	56981	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:26.574295044 CEST	53	56981	8.8.8.8	192.168.2.5
May 4, 2021 16:36:26.867782116 CEST	57974	443	192.168.2.5	142.250.185.102
May 4, 2021 16:36:26.907604933 CEST	56984	443	192.168.2.5	35.186.226.184
May 4, 2021 16:36:26.931550026 CEST	443	57974	142.250.185.102	192.168.2.5
May 4, 2021 16:36:26.932137012 CEST	443	57974	142.250.185.102	192.168.2.5
May 4, 2021 16:36:26.951652050 CEST	443	56984	35.186.226.184	192.168.2.5
May 4, 2021 16:36:26.951687098 CEST	443	56984	35.186.226.184	192.168.2.5
May 4, 2021 16:36:26.957864046 CEST	57974	443	192.168.2.5	142.250.185.102
May 4, 2021 16:36:26.962657928 CEST	56984	443	192.168.2.5	35.186.226.184
May 4, 2021 16:36:26.966345072 CEST	56984	443	192.168.2.5	35.186.226.184
May 4, 2021 16:36:26.985923052 CEST	57974	443	192.168.2.5	142.250.185.102
May 4, 2021 16:36:27.014113903 CEST	443	56984	35.186.226.184	192.168.2.5
May 4, 2021 16:36:27.014565945 CEST	56984	443	192.168.2.5	35.186.226.184
May 4, 2021 16:36:27.028434992 CEST	443	56984	35.186.226.184	192.168.2.5
May 4, 2021 16:36:27.055988073 CEST	443	57974	142.250.185.102	192.168.2.5
May 4, 2021 16:36:27.056333065 CEST	443	57974	142.250.185.102	192.168.2.5
May 4, 2021 16:36:27.059257984 CEST	57974	443	192.168.2.5	142.250.185.102

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 16:36:27.062700033 CEST	56984	443	192.168.2.5	35.186.226.184
May 4, 2021 16:36:27.102962971 CEST	56984	443	192.168.2.5	35.186.226.184
May 4, 2021 16:36:27.126849890 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:27.131386042 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:27.135739088 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:27.139143944 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:27.168612003 CEST	443	56984	35.186.226.184	192.168.2.5
May 4, 2021 16:36:27.180167913 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:27.187935114 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:27.193901062 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:27.194031954 CEST	56984	443	192.168.2.5	35.186.226.184
May 4, 2021 16:36:27.194312096 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:27.194395065 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:27.194614887 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:27.194781065 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:27.194948912 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:27.200738907 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:27.201466084 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:27.201570034 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:27.201684952 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:27.227809906 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:27.580781937 CEST	63599	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:27.631227016 CEST	53	63599	8.8.8.8	192.168.2.5
May 4, 2021 16:36:28.194986105 CEST	61009	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:28.245738029 CEST	53	61009	8.8.8.8	192.168.2.5
May 4, 2021 16:36:28.295989990 CEST	57676	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:28.357857943 CEST	53	57676	8.8.8.8	192.168.2.5
May 4, 2021 16:36:28.399872065 CEST	50687	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:28.472760916 CEST	53	50687	8.8.8.8	192.168.2.5
May 4, 2021 16:36:28.518877029 CEST	53246	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:28.577956915 CEST	53	53246	8.8.8.8	192.168.2.5
May 4, 2021 16:36:28.641983986 CEST	60242	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:28.708729982 CEST	53	60242	8.8.8.8	192.168.2.5
May 4, 2021 16:36:28.766860008 CEST	49674	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:28.815610886 CEST	53	49674	8.8.8.8	192.168.2.5
May 4, 2021 16:36:28.890281916 CEST	50811	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:28.962428093 CEST	53	50811	8.8.8.8	192.168.2.5
May 4, 2021 16:36:29.008043051 CEST	64331	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:29.064735889 CEST	53	64331	8.8.8.8	192.168.2.5
May 4, 2021 16:36:29.155864954 CEST	56789	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:29.189018011 CEST	57974	443	192.168.2.5	142.250.185.102
May 4, 2021 16:36:29.216964006 CEST	53	56789	8.8.8.8	192.168.2.5
May 4, 2021 16:36:29.248394012 CEST	443	57974	142.250.185.102	192.168.2.5
May 4, 2021 16:36:29.248514891 CEST	443	57974	142.250.185.102	192.168.2.5
May 4, 2021 16:36:29.248739004 CEST	57974	443	192.168.2.5	142.250.185.102
May 4, 2021 16:36:29.251477957 CEST	57974	443	192.168.2.5	142.250.185.102
May 4, 2021 16:36:29.256881952 CEST	63680	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:29.309895992 CEST	53	63680	8.8.8.8	192.168.2.5
May 4, 2021 16:36:29.321130037 CEST	56984	443	192.168.2.5	35.186.226.184
May 4, 2021 16:36:29.325895071 CEST	443	57974	142.250.185.102	192.168.2.5
May 4, 2021 16:36:29.325927973 CEST	443	57974	142.250.185.102	192.168.2.5
May 4, 2021 16:36:29.326442957 CEST	57974	443	192.168.2.5	142.250.185.102
May 4, 2021 16:36:29.375443935 CEST	443	56984	35.186.226.184	192.168.2.5
May 4, 2021 16:36:29.402254105 CEST	56984	443	192.168.2.5	35.186.226.184
May 4, 2021 16:36:29.467030048 CEST	59706	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:29.555002928 CEST	53	59706	8.8.8.8	192.168.2.5
May 4, 2021 16:36:29.585756063 CEST	55029	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:29.645601034 CEST	56984	443	192.168.2.5	35.186.226.184
May 4, 2021 16:36:29.648282051 CEST	53	55029	8.8.8.8	192.168.2.5
May 4, 2021 16:36:29.691565037 CEST	51986	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:29.709005117 CEST	443	56984	35.186.226.184	192.168.2.5
May 4, 2021 16:36:29.735301971 CEST	56984	443	192.168.2.5	35.186.226.184
May 4, 2021 16:36:29.762073994 CEST	53	51986	8.8.8.8	192.168.2.5
May 4, 2021 16:36:29.777965069 CEST	49863	443	192.168.2.5	142.250.185.130

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 16:36:29.797312021 CEST	64913	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:29.842633963 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:29.842997074 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:29.843410015 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:29.845844030 CEST	53	64913	8.8.8.8	192.168.2.5
May 4, 2021 16:36:29.859793901 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:29.865367889 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:29.885998964 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:29.914140940 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:29.923870087 CEST	58438	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:29.927658081 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:29.927687883 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:29.928097963 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:29.928682089 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:29.928931952 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:29.929089069 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:29.958607912 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:29.958765984 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:29.959054947 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:29.977612019 CEST	53	58438	8.8.8.8	192.168.2.5
May 4, 2021 16:36:29.987910986 CEST	49414	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:30.026565075 CEST	61135	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:30.048892021 CEST	53	49414	8.8.8.8	192.168.2.5
May 4, 2021 16:36:30.075228930 CEST	53	61135	8.8.8.8	192.168.2.5
May 4, 2021 16:36:30.301780939 CEST	61137	443	192.168.2.5	142.250.186.98
May 4, 2021 16:36:30.354720116 CEST	49373	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:30.358911037 CEST	443	61137	142.250.186.98	192.168.2.5
May 4, 2021 16:36:30.358963013 CEST	443	61137	142.250.186.98	192.168.2.5
May 4, 2021 16:36:30.358979940 CEST	443	61137	142.250.186.98	192.168.2.5
May 4, 2021 16:36:30.359246969 CEST	61137	443	192.168.2.5	142.250.186.98
May 4, 2021 16:36:30.360435009 CEST	61137	443	192.168.2.5	142.250.186.98
May 4, 2021 16:36:30.360759020 CEST	61137	443	192.168.2.5	142.250.186.98
May 4, 2021 16:36:30.408977032 CEST	52434	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:30.413202047 CEST	53	49373	8.8.8.8	192.168.2.5
May 4, 2021 16:36:30.423666954 CEST	443	61137	142.250.186.98	192.168.2.5
May 4, 2021 16:36:30.424555063 CEST	61137	443	192.168.2.5	142.250.186.98
May 4, 2021 16:36:30.434142113 CEST	443	61137	142.250.186.98	192.168.2.5
May 4, 2021 16:36:30.434170008 CEST	443	61137	142.250.186.98	192.168.2.5
May 4, 2021 16:36:30.434524059 CEST	61137	443	192.168.2.5	142.250.186.98
May 4, 2021 16:36:30.490358114 CEST	53	52434	8.8.8.8	192.168.2.5
May 4, 2021 16:36:30.606345892 CEST	56456	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:30.665821075 CEST	53	56456	8.8.8.8	192.168.2.5
May 4, 2021 16:36:31.032773972 CEST	53715	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:31.084315062 CEST	53	53715	8.8.8.8	192.168.2.5
May 4, 2021 16:36:31.458852053 CEST	60677	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:31.526870966 CEST	53	60677	8.8.8.8	192.168.2.5
May 4, 2021 16:36:32.368776083 CEST	59658	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:32.391911030 CEST	56873	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:32.394264936 CEST	51402	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:32.426292896 CEST	53	59658	8.8.8.8	192.168.2.5
May 4, 2021 16:36:32.443655014 CEST	61487	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:32.445710897 CEST	53	51402	8.8.8.8	192.168.2.5
May 4, 2021 16:36:32.451194048 CEST	53	56873	8.8.8.8	192.168.2.5
May 4, 2021 16:36:32.473104000 CEST	59026	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:32.500669003 CEST	53	61487	8.8.8.8	192.168.2.5
May 4, 2021 16:36:32.521677017 CEST	53	59026	8.8.8.8	192.168.2.5
May 4, 2021 16:36:33.137681961 CEST	58616	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:33.141846895 CEST	49232	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:33.190589905 CEST	53	49232	8.8.8.8	192.168.2.5
May 4, 2021 16:36:33.198729992 CEST	53	58616	8.8.8.8	192.168.2.5
May 4, 2021 16:36:34.087447882 CEST	55390	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:34.135998011 CEST	53	55390	8.8.8.8	192.168.2.5
May 4, 2021 16:36:34.158139944 CEST	61057	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:34.217178106 CEST	53	61057	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 16:36:34.461515903 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:34.524844885 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:34.524938107 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:34.525336981 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:34.526082993 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:34.552495956 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:34.601941109 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:34.617269993 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:34.617646933 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:34.617943048 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:34.619149923 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:34.653049946 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:34.693180084 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:34.716403961 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:34.716443062 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:34.716866970 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:34.717519045 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:34.790951014 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:40.262448072 CEST	62975	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:40.322649002 CEST	53	62975	8.8.8.8	192.168.2.5
May 4, 2021 16:36:40.456829071 CEST	62623	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:40.513672113 CEST	53	62623	8.8.8.8	192.168.2.5
May 4, 2021 16:36:40.518981934 CEST	57974	443	192.168.2.5	142.250.185.102
May 4, 2021 16:36:40.579807997 CEST	443	57974	142.250.185.102	192.168.2.5
May 4, 2021 16:36:40.584944010 CEST	57974	443	192.168.2.5	142.250.185.102
May 4, 2021 16:36:40.654913902 CEST	443	57974	142.250.185.102	192.168.2.5
May 4, 2021 16:36:40.654994011 CEST	443	57974	142.250.185.102	192.168.2.5
May 4, 2021 16:36:40.655442953 CEST	57974	443	192.168.2.5	142.250.185.102
May 4, 2021 16:36:41.188930035 CEST	60626	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:41.261626005 CEST	53	60626	8.8.8.8	192.168.2.5
May 4, 2021 16:36:41.454989910 CEST	64199	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:41.512324095 CEST	53	64199	8.8.8.8	192.168.2.5
May 4, 2021 16:36:43.191802979 CEST	56984	443	192.168.2.5	35.186.226.184
May 4, 2021 16:36:43.246889114 CEST	443	56984	35.186.226.184	192.168.2.5
May 4, 2021 16:36:43.274123907 CEST	56984	443	192.168.2.5	35.186.226.184
May 4, 2021 16:36:43.653716087 CEST	56984	443	192.168.2.5	35.186.226.184
May 4, 2021 16:36:43.716177940 CEST	443	56984	35.186.226.184	192.168.2.5
May 4, 2021 16:36:43.746109962 CEST	56984	443	192.168.2.5	35.186.226.184
May 4, 2021 16:36:45.362504005 CEST	61137	443	192.168.2.5	142.250.186.98
May 4, 2021 16:36:45.436417103 CEST	443	61137	142.250.186.98	192.168.2.5
May 4, 2021 16:36:45.671892881 CEST	56984	443	192.168.2.5	35.186.226.184
May 4, 2021 16:36:45.726286888 CEST	443	56984	35.186.226.184	192.168.2.5
May 4, 2021 16:36:45.752585888 CEST	56984	443	192.168.2.5	35.186.226.184
May 4, 2021 16:36:45.817961931 CEST	56984	443	192.168.2.5	35.186.226.184
May 4, 2021 16:36:45.880295992 CEST	443	56984	35.186.226.184	192.168.2.5
May 4, 2021 16:36:45.912996054 CEST	56984	443	192.168.2.5	35.186.226.184
May 4, 2021 16:36:45.932756901 CEST	57974	443	192.168.2.5	142.250.185.102
May 4, 2021 16:36:45.994931936 CEST	443	57974	142.250.185.102	192.168.2.5
May 4, 2021 16:36:45.994998932 CEST	443	57974	142.250.185.102	192.168.2.5
May 4, 2021 16:36:46.000348091 CEST	57974	443	192.168.2.5	142.250.185.102
May 4, 2021 16:36:46.071722031 CEST	57974	443	192.168.2.5	142.250.185.102
May 4, 2021 16:36:46.081471920 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:46.138461113 CEST	443	57974	142.250.185.102	192.168.2.5
May 4, 2021 16:36:46.140170097 CEST	443	57974	142.250.185.102	192.168.2.5
May 4, 2021 16:36:46.140902042 CEST	57974	443	192.168.2.5	142.250.185.102
May 4, 2021 16:36:46.145246029 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:46.145428896 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:46.146895885 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:46.180497885 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:46.183819056 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:46.189009905 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:46.213423967 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:46.232455015 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:46.244883060 CEST	443	49863	142.250.185.130	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 16:36:46.244951010 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:46.245312929 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:46.251698971 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:46.252155066 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:46.252871990 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:46.277692080 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:46.278070927 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:46.279023886 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:46.297799110 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:46.303073883 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:46.341804981 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:46.351895094 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:46.361990929 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:46.362176895 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:46.362653971 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:46.371947050 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:46.372227907 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:46.372411013 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:46.392348051 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:46.392376900 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:46.392797947 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:46.408468962 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:46.408615112 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:36:46.408981085 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:36:50.016988039 CEST	64289	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:50.069876909 CEST	53	64289	8.8.8.8	192.168.2.5
May 4, 2021 16:36:54.645032883 CEST	63509	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:54.707834959 CEST	53	63509	8.8.8.8	192.168.2.5
May 4, 2021 16:36:54.938929081 CEST	62707	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:55.000077963 CEST	53	62707	8.8.8.8	192.168.2.5
May 4, 2021 16:36:57.823297977 CEST	60328	53	192.168.2.5	8.8.8.8
May 4, 2021 16:36:57.898382902 CEST	53	60328	8.8.8.8	192.168.2.5
May 4, 2021 16:37:00.935936928 CEST	57974	443	192.168.2.5	142.250.185.102
May 4, 2021 16:37:01.012604952 CEST	443	57974	142.250.185.102	192.168.2.5
May 4, 2021 16:37:01.082963943 CEST	49863	443	192.168.2.5	142.250.185.130
May 4, 2021 16:37:01.157632113 CEST	443	49863	142.250.185.130	192.168.2.5
May 4, 2021 16:37:22.539664030 CEST	51927	53	192.168.2.5	8.8.8.8
May 4, 2021 16:37:22.588323116 CEST	53	51927	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 16:35:34.032929897 CEST	192.168.2.5	8.8.8.8	0x1a76	Standard query (0)	protect-us .mimecast.com	A (IP address)	IN (0x0001)
May 4, 2021 16:35:39.042181015 CEST	192.168.2.5	8.8.8.8	0xe9a6	Standard query (0)	lnkd.in	A (IP address)	IN (0x0001)
May 4, 2021 16:35:39.544537067 CEST	192.168.2.5	8.8.8.8	0x7ca9	Standard query (0)	www.linked in.com	A (IP address)	IN (0x0001)
May 4, 2021 16:35:40.645349979 CEST	192.168.2.5	8.8.8.8	0x3978	Standard query (0)	page.adobe spark-assets.com	A (IP address)	IN (0x0001)
May 4, 2021 16:35:40.925235987 CEST	192.168.2.5	8.8.8.8	0x3ecc	Standard query (0)	use.typekit.net	A (IP address)	IN (0x0001)
May 4, 2021 16:35:41.972501040 CEST	192.168.2.5	8.8.8.8	0x8616	Standard query (0)	s3.amazona ws.com	A (IP address)	IN (0x0001)
May 4, 2021 16:35:42.542412043 CEST	192.168.2.5	8.8.8.8	0xe5da	Standard query (0)	p.typekit.net	A (IP address)	IN (0x0001)
May 4, 2021 16:35:47.423048019 CEST	192.168.2.5	8.8.8.8	0x82ba	Standard query (0)	page.adobe spark-assets.com	A (IP address)	IN (0x0001)
May 4, 2021 16:35:49.800525904 CEST	192.168.2.5	8.8.8.8	0x6871	Standard query (0)	clients2.g oogleuserc ontent.com	A (IP address)	IN (0x0001)
May 4, 2021 16:35:56.237423897 CEST	192.168.2.5	8.8.8.8	0xaa5c	Standard query (0)	lindsaykno xwilliams.com	A (IP address)	IN (0x0001)
May 4, 2021 16:35:57.950303078 CEST	192.168.2.5	8.8.8.8	0xefaf	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
May 4, 2021 16:35:57.951344013 CEST	192.168.2.5	8.8.8.8	0xebb8	Standard query (0)	maxcdn.boo tstrapcdn.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 16:35:57.953488111 CEST	192.168.2.5	8.8.8.8	0xe2a8	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
May 4, 2021 16:35:59.181607962 CEST	192.168.2.5	8.8.8.8	0xe7a4	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
May 4, 2021 16:35:59.289593935 CEST	192.168.2.5	8.8.8.8	0x58bf	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
May 4, 2021 16:35:59.295790911 CEST	192.168.2.5	8.8.8.8	0x953f	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:02.399399996 CEST	192.168.2.5	8.8.8.8	0x48a5	Standard query (0)	lindsayknoxwilliams.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:09.581547022 CEST	192.168.2.5	8.8.8.8	0x2d26	Standard query (0)	assets.adobedtm.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:09.585766077 CEST	192.168.2.5	8.8.8.8	0xfd5f	Standard query (0)	cdn.cookielaw.org	A (IP address)	IN (0x0001)
May 4, 2021 16:36:09.592408895 CEST	192.168.2.5	8.8.8.8	0xc203	Standard query (0)	static.adobelogin.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.671173096 CEST	192.168.2.5	8.8.8.8	0x49a8	Standard query (0)	adobe.tt.omtrdc.net	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.686285973 CEST	192.168.2.5	8.8.8.8	0xfed0	Standard query (0)	geolocation.onetrust.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.780833960 CEST	192.168.2.5	8.8.8.8	0x2e09	Standard query (0)	dpm.demdex.net	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.941067934 CEST	192.168.2.5	8.8.8.8	0x3bcb	Standard query (0)	ims-na1.adobelogin.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:11.262213945 CEST	192.168.2.5	8.8.8.8	0x74c1	Standard query (0)	adobedc.demdex.net	A (IP address)	IN (0x0001)
May 4, 2021 16:36:12.101944923 CEST	192.168.2.5	8.8.8.8	0x2623	Standard query (0)	api.demandbase.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:12.394469023 CEST	192.168.2.5	8.8.8.8	0xe067	Standard query (0)	www.everestjs.net	A (IP address)	IN (0x0001)
May 4, 2021 16:36:12.415762901 CEST	192.168.2.5	8.8.8.8	0x9419	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:12.417165995 CEST	192.168.2.5	8.8.8.8	0xf6a7	Standard query (0)	scripts.demandbase.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:12.437231064 CEST	192.168.2.5	8.8.8.8	0x493d	Standard query (0)	pixel.everesttech.net	A (IP address)	IN (0x0001)
May 4, 2021 16:36:12.463016033 CEST	192.168.2.5	8.8.8.8	0x15eb	Standard query (0)	servedby.flashtalking.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:12.471347094 CEST	192.168.2.5	8.8.8.8	0x8bab	Standard query (0)	sc-static.net	A (IP address)	IN (0x0001)
May 4, 2021 16:36:12.472249985 CEST	192.168.2.5	8.8.8.8	0x6ca4	Standard query (0)	static.ads-twitter.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:12.509572029 CEST	192.168.2.5	8.8.8.8	0x151f	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.243103027 CEST	192.168.2.5	8.8.8.8	0x2515	Standard query (0)	lasteventf-tm.everesttech.net	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.247792959 CEST	192.168.2.5	8.8.8.8	0xd254	Standard query (0)	analytics.twitter.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.247970104 CEST	192.168.2.5	8.8.8.8	0xc16	Standard query (0)	t.co	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.256773949 CEST	192.168.2.5	8.8.8.8	0xb76e	Standard query (0)	tr.snapchat.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.260762930 CEST	192.168.2.5	8.8.8.8	0xd7a8	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.533850908 CEST	192.168.2.5	8.8.8.8	0xa68d	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.537612915 CEST	192.168.2.5	8.8.8.8	0x9c31	Standard query (0)	id.rlcdn.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.538229942 CEST	192.168.2.5	8.8.8.8	0x9a99	Standard query (0)	api.company-target.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.539073944 CEST	192.168.2.5	8.8.8.8	0xe818	Standard query (0)	match.prod.bidr.io	A (IP address)	IN (0x0001)
May 4, 2021 16:36:14.614466906 CEST	192.168.2.5	8.8.8.8	0x470e	Standard query (0)	d9.flashtalking.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:14.728560925 CEST	192.168.2.5	8.8.8.8	0xe4d6	Standard query (0)	9212252.fls.doubleclick.net	A (IP address)	IN (0x0001)
May 4, 2021 16:36:16.239702940 CEST	192.168.2.5	8.8.8.8	0x8c60	Standard query (0)	adservice.google.de	A (IP address)	IN (0x0001)
May 4, 2021 16:36:16.394752026 CEST	192.168.2.5	8.8.8.8	0xf50b	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
May 4, 2021 16:36:16.420583963 CEST	192.168.2.5	8.8.8.8	0xcdd4	Standard query (0)	segments.company-target.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 16:36:17.165545940 CEST	192.168.2.5	8.8.8.8	0xa4a5	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)
May 4, 2021 16:36:17.357510090 CEST	192.168.2.5	8.8.8.8	0x3748	Standard query (0)	prod.adobe ccstatic.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:18.347618103 CEST	192.168.2.5	8.8.8.8	0x27bf	Standard query (0)	bumper.ado beprojectm.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:21.489171982 CEST	192.168.2.5	8.8.8.8	0x7b58	Standard query (0)	js-agent.n ewrelic.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:21.909977913 CEST	192.168.2.5	8.8.8.8	0x91e5	Standard query (0)	bam.nr-data.net	A (IP address)	IN (0x0001)
May 4, 2021 16:36:24.748500109 CEST	192.168.2.5	8.8.8.8	0x8c2c	Standard query (0)	cm.everest tech.net	A (IP address)	IN (0x0001)
May 4, 2021 16:36:25.369937897 CEST	192.168.2.5	8.8.8.8	0x80ac	Standard query (0)	adobe.demd ex.net	A (IP address)	IN (0x0001)
May 4, 2021 16:36:27.580781937 CEST	192.168.2.5	8.8.8.8	0xc136	Standard query (0)	aa.agkn.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:28.194986105 CEST	192.168.2.5	8.8.8.8	0xa0a	Standard query (0)	sync.matht ag.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:28.295989990 CEST	192.168.2.5	8.8.8.8	0x30ce	Standard query (0)	idsync.rlcdn.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:28.399872065 CEST	192.168.2.5	8.8.8.8	0x8d44	Standard query (0)	d.turn.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:28.518877029 CEST	192.168.2.5	8.8.8.8	0x3a5e	Standard query (0)	pixel.tapad.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:28.641983986 CEST	192.168.2.5	8.8.8.8	0x85af	Standard query (0)	cm.g.doubl eclick.net	A (IP address)	IN (0x0001)
May 4, 2021 16:36:28.766860008 CEST	192.168.2.5	8.8.8.8	0xf063	Standard query (0)	rtd.tubemo gul.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:28.890281916 CEST	192.168.2.5	8.8.8.8	0x2521	Standard query (0)	p.rfihub.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.008043051 CEST	192.168.2.5	8.8.8.8	0xa250	Standard query (0)	rtd-tm.eve resttech.net	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.155864954 CEST	192.168.2.5	8.8.8.8	0x69b	Standard query (0)	pixel.quan tserve.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.467030048 CEST	192.168.2.5	8.8.8.8	0xa8af	Standard query (0)	adobe-sync .dotomi.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.585756063 CEST	192.168.2.5	8.8.8.8	0xb272	Standard query (0)	a.tribalfusion.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.691565037 CEST	192.168.2.5	8.8.8.8	0xac47	Standard query (0)	ml314.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.797312021 CEST	192.168.2.5	8.8.8.8	0xcc9b	Standard query (0)	bttrack.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.923870087 CEST	192.168.2.5	8.8.8.8	0xb11b	Standard query (0)	pix-us.revjet.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.987910986 CEST	192.168.2.5	8.8.8.8	0xa0f3	Standard query (0)	s.tribalfusion.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:30.026565075 CEST	192.168.2.5	8.8.8.8	0xcabd	Standard query (0)	sync-tm.ev eresttech.net	A (IP address)	IN (0x0001)
May 4, 2021 16:36:30.408977032 CEST	192.168.2.5	8.8.8.8	0x54af	Standard query (0)	pixel.rubi conproject.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:30.606345892 CEST	192.168.2.5	8.8.8.8	0x4e09	Standard query (0)	dsum-sec.c asalemedia.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:31.032773972 CEST	192.168.2.5	8.8.8.8	0x66bc	Standard query (0)	ib.adnxs.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:32.368776083 CEST	192.168.2.5	8.8.8.8	0x4284	Standard query (0)	match.prod .bidr.io	A (IP address)	IN (0x0001)
May 4, 2021 16:36:32.391911030 CEST	192.168.2.5	8.8.8.8	0xaff7	Standard query (0)	id.rlcdn.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:32.443655014 CEST	192.168.2.5	8.8.8.8	0xfe5b	Standard query (0)	image2.pub matic.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:33.137681961 CEST	192.168.2.5	8.8.8.8	0x43f9	Standard query (0)	segments.c ompany-tar get.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:33.141846895 CEST	192.168.2.5	8.8.8.8	0xf0f2	Standard query (0)	us-u.openx.net	A (IP address)	IN (0x0001)
May 4, 2021 16:36:34.087447882 CEST	192.168.2.5	8.8.8.8	0x91ea	Standard query (0)	sync.searc h.spotxcha nge.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:40.262448072 CEST	192.168.2.5	8.8.8.8	0x2ee8	Standard query (0)	g2.gumgum.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:40.456829071 CEST	192.168.2.5	8.8.8.8	0x4548	Standard query (0)	s.thebrigh ttag.com	A (IP address)	IN (0x0001)
May 4, 2021 16:36:41.454989910 CEST	192.168.2.5	8.8.8.8	0xc18e	Standard query (0)	partner.me diawallahs cript.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 16:36:54.938929081 CEST	192.168.2.5	8.8.8.8	0x6ee	Standard query (0)	use.typekit.net	A (IP address)	IN (0x0001)
May 4, 2021 16:37:22.539664030 CEST	192.168.2.5	8.8.8.8	0x9b7c	Standard query (0)	bam.nr-data.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 16:35:34.091239929 CEST	8.8.8.8	192.168.2.5	0x1a76	No error (0)	protect-us.mimecast.com		205.139.111.113	A (IP address)	IN (0x0001)
May 4, 2021 16:35:34.091239929 CEST	8.8.8.8	192.168.2.5	0x1a76	No error (0)	protect-us.mimecast.com		205.139.111.117	A (IP address)	IN (0x0001)
May 4, 2021 16:35:34.091239929 CEST	8.8.8.8	192.168.2.5	0x1a76	No error (0)	protect-us.mimecast.com		207.211.31.64	A (IP address)	IN (0x0001)
May 4, 2021 16:35:34.091239929 CEST	8.8.8.8	192.168.2.5	0x1a76	No error (0)	protect-us.mimecast.com		207.211.31.113	A (IP address)	IN (0x0001)
May 4, 2021 16:35:34.091239929 CEST	8.8.8.8	192.168.2.5	0x1a76	No error (0)	protect-us.mimecast.com		207.211.31.106	A (IP address)	IN (0x0001)
May 4, 2021 16:35:34.091239929 CEST	8.8.8.8	192.168.2.5	0x1a76	No error (0)	protect-us.mimecast.com		205.139.111.12	A (IP address)	IN (0x0001)
May 4, 2021 16:35:39.103637934 CEST	8.8.8.8	192.168.2.5	0xe9a6	No error (0)	lnkd.in		108.174.10.10	A (IP address)	IN (0x0001)
May 4, 2021 16:35:39.593442917 CEST	8.8.8.8	192.168.2.5	0x7ca9	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:35:40.061850071 CEST	8.8.8.8	192.168.2.5	0xa7ae	No error (0)	spark.adobeprojectm.com		143.204.98.51	A (IP address)	IN (0x0001)
May 4, 2021 16:35:40.061850071 CEST	8.8.8.8	192.168.2.5	0xa7ae	No error (0)	spark.adobeprojectm.com		143.204.98.95	A (IP address)	IN (0x0001)
May 4, 2021 16:35:40.061850071 CEST	8.8.8.8	192.168.2.5	0xa7ae	No error (0)	spark.adobeprojectm.com		143.204.98.41	A (IP address)	IN (0x0001)
May 4, 2021 16:35:40.061850071 CEST	8.8.8.8	192.168.2.5	0xa7ae	No error (0)	spark.adobeprojectm.com		143.204.98.8	A (IP address)	IN (0x0001)
May 4, 2021 16:35:40.706604958 CEST	8.8.8.8	192.168.2.5	0x3978	No error (0)	page.adobespark-assets.com		13.224.193.29	A (IP address)	IN (0x0001)
May 4, 2021 16:35:40.706604958 CEST	8.8.8.8	192.168.2.5	0x3978	No error (0)	page.adobespark-assets.com		13.224.193.122	A (IP address)	IN (0x0001)
May 4, 2021 16:35:40.706604958 CEST	8.8.8.8	192.168.2.5	0x3978	No error (0)	page.adobespark-assets.com		13.224.193.81	A (IP address)	IN (0x0001)
May 4, 2021 16:35:40.706604958 CEST	8.8.8.8	192.168.2.5	0x3978	No error (0)	page.adobespark-assets.com		13.224.193.108	A (IP address)	IN (0x0001)
May 4, 2021 16:35:40.987078905 CEST	8.8.8.8	192.168.2.5	0x3ecc	No error (0)	use.typekit.net	use-stls.adobe.com.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:35:42.024051905 CEST	8.8.8.8	192.168.2.5	0x8616	No error (0)	s3.amazonaws.com		52.216.79.14	A (IP address)	IN (0x0001)
May 4, 2021 16:35:42.600725889 CEST	8.8.8.8	192.168.2.5	0xe5da	No error (0)	p.typekit.net	p.typekit.net-v3.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:35:47.481231928 CEST	8.8.8.8	192.168.2.5	0x82ba	No error (0)	page.adobespark-assets.com		13.224.193.29	A (IP address)	IN (0x0001)
May 4, 2021 16:35:47.481231928 CEST	8.8.8.8	192.168.2.5	0x82ba	No error (0)	page.adobespark-assets.com		13.224.193.122	A (IP address)	IN (0x0001)
May 4, 2021 16:35:47.481231928 CEST	8.8.8.8	192.168.2.5	0x82ba	No error (0)	page.adobespark-assets.com		13.224.193.81	A (IP address)	IN (0x0001)
May 4, 2021 16:35:47.481231928 CEST	8.8.8.8	192.168.2.5	0x82ba	No error (0)	page.adobespark-assets.com		13.224.193.108	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 16:35:49.857685089 CEST	8.8.8.8	192.168.2.5	0x6871	No error (0)	clients2.google usercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:35:49.857685089 CEST	8.8.8.8	192.168.2.5	0x6871	No error (0)	googlehosted.l.googleusercontent.com		216.58.212.129	A (IP address)	IN (0x0001)
May 4, 2021 16:35:50.269063950 CEST	8.8.8.8	192.168.2.5	0x58a8	No error (0)	spark.adobeprojectm.com		143.204.98.95	A (IP address)	IN (0x0001)
May 4, 2021 16:35:50.269063950 CEST	8.8.8.8	192.168.2.5	0x58a8	No error (0)	spark.adobeprojectm.com		143.204.98.8	A (IP address)	IN (0x0001)
May 4, 2021 16:35:50.269063950 CEST	8.8.8.8	192.168.2.5	0x58a8	No error (0)	spark.adobeprojectm.com		143.204.98.41	A (IP address)	IN (0x0001)
May 4, 2021 16:35:50.269063950 CEST	8.8.8.8	192.168.2.5	0x58a8	No error (0)	spark.adobeprojectm.com		143.204.98.51	A (IP address)	IN (0x0001)
May 4, 2021 16:35:56.307451963 CEST	8.8.8.8	192.168.2.5	0xaa5c	No error (0)	lindsayknoxwilliams.com		69.49.234.124	A (IP address)	IN (0x0001)
May 4, 2021 16:35:57.999918938 CEST	8.8.8.8	192.168.2.5	0xefaf	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:35:58.014784098 CEST	8.8.8.8	192.168.2.5	0xebb8	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
May 4, 2021 16:35:58.014784098 CEST	8.8.8.8	192.168.2.5	0xebb8	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
May 4, 2021 16:35:58.014803886 CEST	8.8.8.8	192.168.2.5	0xe2a8	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:35:59.238867998 CEST	8.8.8.8	192.168.2.5	0xe7a4	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
May 4, 2021 16:35:59.238867998 CEST	8.8.8.8	192.168.2.5	0xe7a4	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
May 4, 2021 16:35:59.357285976 CEST	8.8.8.8	192.168.2.5	0x58bf	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:35:59.358895063 CEST	8.8.8.8	192.168.2.5	0x953f	No error (0)	stackpath.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
May 4, 2021 16:35:59.358895063 CEST	8.8.8.8	192.168.2.5	0x953f	No error (0)	stackpath.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
May 4, 2021 16:36:02.460293055 CEST	8.8.8.8	192.168.2.5	0x48a5	No error (0)	lindsayknoxwilliams.com		69.49.234.124	A (IP address)	IN (0x0001)
May 4, 2021 16:36:09.640296936 CEST	8.8.8.8	192.168.2.5	0x2d26	No error (0)	assets.adobedtm.com	cn-assets.adobedtm.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:09.648161888 CEST	8.8.8.8	192.168.2.5	0xfd5f	No error (0)	cdn.cookielaw.org		104.16.148.64	A (IP address)	IN (0x0001)
May 4, 2021 16:36:09.648161888 CEST	8.8.8.8	192.168.2.5	0xfd5f	No error (0)	cdn.cookielaw.org		104.16.149.64	A (IP address)	IN (0x0001)
May 4, 2021 16:36:09.684140921 CEST	8.8.8.8	192.168.2.5	0xc203	No error (0)	static.adobelogin.com	adobelogin-static.prod.ims.adobejanus.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:09.684140921 CEST	8.8.8.8	192.168.2.5	0xc203	No error (0)	adobelogin-static.prod.ims.adobejanus.com	dd20fzx9mj46f.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:09.684140921 CEST	8.8.8.8	192.168.2.5	0xc203	No error (0)	dd20fzx9mj46f.cloudfront.net		13.224.187.69	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.569983006 CEST	8.8.8.8	192.168.2.5	0x6865	No error (0)	services.prod.ims.adobejanus.com		63.32.113.5	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.569983006 CEST	8.8.8.8	192.168.2.5	0x6865	No error (0)	services.prod.ims.adobejanus.com		54.73.76.208	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 16:36:10.569983006 CEST	8.8.8.8	192.168.2.5	0x6865	No error (0)	services.prod.ims.adobejanus.com		54.76.80.163	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.569983006 CEST	8.8.8.8	192.168.2.5	0x6865	No error (0)	services.prod.ims.adobejanus.com		52.213.176.171	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.569983006 CEST	8.8.8.8	192.168.2.5	0x6865	No error (0)	services.prod.ims.adobejanus.com		34.249.255.145	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.569983006 CEST	8.8.8.8	192.168.2.5	0x6865	No error (0)	services.prod.ims.adobejanus.com		99.81.92.132	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.743021011 CEST	8.8.8.8	192.168.2.5	0x49a8	No error (0)	adobe.tt.omtrdc.net		54.75.9.158	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.743021011 CEST	8.8.8.8	192.168.2.5	0x49a8	No error (0)	adobe.tt.omtrdc.net		34.252.156.174	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.743021011 CEST	8.8.8.8	192.168.2.5	0x49a8	No error (0)	adobe.tt.omtrdc.net		52.212.193.208	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.743021011 CEST	8.8.8.8	192.168.2.5	0x49a8	No error (0)	adobe.tt.omtrdc.net		34.252.166.160	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.743021011 CEST	8.8.8.8	192.168.2.5	0x49a8	No error (0)	adobe.tt.omtrdc.net		52.18.150.20	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.743021011 CEST	8.8.8.8	192.168.2.5	0x49a8	No error (0)	adobe.tt.omtrdc.net		52.51.251.137	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.743021011 CEST	8.8.8.8	192.168.2.5	0x49a8	No error (0)	adobe.tt.omtrdc.net		52.212.164.82	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.743021011 CEST	8.8.8.8	192.168.2.5	0x49a8	No error (0)	adobe.tt.omtrdc.net		52.213.168.74	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.750243902 CEST	8.8.8.8	192.168.2.5	0xfed0	No error (0)	geolocation.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.750243902 CEST	8.8.8.8	192.168.2.5	0xfed0	No error (0)	geolocation.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.839915037 CEST	8.8.8.8	192.168.2.5	0x2e09	No error (0)	dpm.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:10.839915037 CEST	8.8.8.8	192.168.2.5	0x2e09	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:10.839915037 CEST	8.8.8.8	192.168.2.5	0x2e09	No error (0)	edge-irl1.demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:10.839915037 CEST	8.8.8.8	192.168.2.5	0x2e09	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		18.200.233.208	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.839915037 CEST	8.8.8.8	192.168.2.5	0x2e09	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		63.33.120.132	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.839915037 CEST	8.8.8.8	192.168.2.5	0x2e09	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.171.219.200	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.839915037 CEST	8.8.8.8	192.168.2.5	0x2e09	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.76.54.153	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.839915037 CEST	8.8.8.8	192.168.2.5	0x2e09	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.170.210.188	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.839915037 CEST	8.8.8.8	192.168.2.5	0x2e09	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.30.200.197	A (IP address)	IN (0x0001)
May 4, 2021 16:36:10.839915037 CEST	8.8.8.8	192.168.2.5	0x2e09	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.50.19.208	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 16:36:10.839915037 CEST	8.8.8.8	192.168.2.5	0x2e09	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.243.47.58	A (IP address)	IN (0x0001)
May 4, 2021 16:36:11.004300117 CEST	8.8.8.8	192.168.2.5	0x3bcb	No error (0)	ims-na1.adobelogin.com	adobelogin.prod.ims.adobejanus.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:11.004300117 CEST	8.8.8.8	192.168.2.5	0x3bcb	No error (0)	adobelogin.prod.ims.adobejanus.com	adobelogin-origin.prod.ims.adobejanus.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:11.004300117 CEST	8.8.8.8	192.168.2.5	0x3bcb	No error (0)	adobelogin-origin.prod.ims.adobejanus.com		54.73.76.208	A (IP address)	IN (0x0001)
May 4, 2021 16:36:11.004300117 CEST	8.8.8.8	192.168.2.5	0x3bcb	No error (0)	adobelogin-origin.prod.ims.adobejanus.com		52.213.176.171	A (IP address)	IN (0x0001)
May 4, 2021 16:36:11.004300117 CEST	8.8.8.8	192.168.2.5	0x3bcb	No error (0)	adobelogin-origin.prod.ims.adobejanus.com		34.249.255.145	A (IP address)	IN (0x0001)
May 4, 2021 16:36:11.004300117 CEST	8.8.8.8	192.168.2.5	0x3bcb	No error (0)	adobelogin-origin.prod.ims.adobejanus.com		99.81.92.132	A (IP address)	IN (0x0001)
May 4, 2021 16:36:11.004300117 CEST	8.8.8.8	192.168.2.5	0x3bcb	No error (0)	adobelogin-origin.prod.ims.adobejanus.com		54.76.80.163	A (IP address)	IN (0x0001)
May 4, 2021 16:36:11.004300117 CEST	8.8.8.8	192.168.2.5	0x3bcb	No error (0)	adobelogin-origin.prod.ims.adobejanus.com		63.32.113.5	A (IP address)	IN (0x0001)
May 4, 2021 16:36:11.289531946 CEST	8.8.8.8	192.168.2.5	0x4b0d	No error (0)	adobe.com.ssl.d1.sc.omtrdc.net		35.181.18.61	A (IP address)	IN (0x0001)
May 4, 2021 16:36:11.289531946 CEST	8.8.8.8	192.168.2.5	0x4b0d	No error (0)	adobe.com.ssl.d1.sc.omtrdc.net		15.237.76.117	A (IP address)	IN (0x0001)
May 4, 2021 16:36:11.289531946 CEST	8.8.8.8	192.168.2.5	0x4b0d	No error (0)	adobe.com.ssl.d1.sc.omtrdc.net		15.237.136.106	A (IP address)	IN (0x0001)
May 4, 2021 16:36:11.330197096 CEST	8.8.8.8	192.168.2.5	0x74c1	No error (0)	adobedc.demdex.net	demdex.net.ssl.sc.omtrdc.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:11.330197096 CEST	8.8.8.8	192.168.2.5	0x74c1	No error (0)	demdex.net.ssl.sc.omtrdc.net		35.181.18.61	A (IP address)	IN (0x0001)
May 4, 2021 16:36:11.330197096 CEST	8.8.8.8	192.168.2.5	0x74c1	No error (0)	demdex.net.ssl.sc.omtrdc.net		15.237.136.106	A (IP address)	IN (0x0001)
May 4, 2021 16:36:11.330197096 CEST	8.8.8.8	192.168.2.5	0x74c1	No error (0)	demdex.net.ssl.sc.omtrdc.net		15.237.76.117	A (IP address)	IN (0x0001)
May 4, 2021 16:36:12.159795046 CEST	8.8.8.8	192.168.2.5	0x2623	No error (0)	api.demandbase.com		13.225.74.124	A (IP address)	IN (0x0001)
May 4, 2021 16:36:12.159795046 CEST	8.8.8.8	192.168.2.5	0x2623	No error (0)	api.demandbase.com		13.225.74.37	A (IP address)	IN (0x0001)
May 4, 2021 16:36:12.159795046 CEST	8.8.8.8	192.168.2.5	0x2623	No error (0)	api.demandbase.com		13.225.74.58	A (IP address)	IN (0x0001)
May 4, 2021 16:36:12.159795046 CEST	8.8.8.8	192.168.2.5	0x2623	No error (0)	api.demandbase.com		13.225.74.112	A (IP address)	IN (0x0001)
May 4, 2021 16:36:12.458005905 CEST	8.8.8.8	192.168.2.5	0xe067	No error (0)	www.everestjs.net	www.everestjs.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:12.475930929 CEST	8.8.8.8	192.168.2.5	0x9419	No error (0)	snap.licdn.com	wildcard.licdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:12.515057087 CEST	8.8.8.8	192.168.2.5	0xf6a7	No error (0)	scripts.demandbase.com		13.224.193.78	A (IP address)	IN (0x0001)
May 4, 2021 16:36:12.515057087 CEST	8.8.8.8	192.168.2.5	0xf6a7	No error (0)	scripts.demandbase.com		13.224.193.53	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 16:36:12.515057087 CEST	8.8.8.8	192.168.2.5	0xf6a7	No error (0)	scripts.de mandbase.com		13.224.193.116	A (IP address)	IN (0x0001)
May 4, 2021 16:36:12.515057087 CEST	8.8.8.8	192.168.2.5	0xf6a7	No error (0)	scripts.de mandbase.com		13.224.193.108	A (IP address)	IN (0x0001)
May 4, 2021 16:36:12.517256975 CEST	8.8.8.8	192.168.2.5	0x493d	No error (0)	pixel.ever esttech.net	tp00.everesttech.net.akad ns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:12.536024094 CEST	8.8.8.8	192.168.2.5	0x6ca4	No error (0)	static.ads- twitter.com	platform.twitter.map.fastly .net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:12.536024094 CEST	8.8.8.8	192.168.2.5	0x6ca4	No error (0)	platform.t witter.map .fastly.net		199.232.136.157	A (IP address)	IN (0x0001)
May 4, 2021 16:36:12.536050081 CEST	8.8.8.8	192.168.2.5	0x15eb	No error (0)	servedby.f lashtalking.com	cds.f7f2q8c3.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:12.560095072 CEST	8.8.8.8	192.168.2.5	0x8bab	No error (0)	sc-static.net		13.225.74.126	A (IP address)	IN (0x0001)
May 4, 2021 16:36:12.560095072 CEST	8.8.8.8	192.168.2.5	0x8bab	No error (0)	sc-static.net		13.225.74.57	A (IP address)	IN (0x0001)
May 4, 2021 16:36:12.560095072 CEST	8.8.8.8	192.168.2.5	0x8bab	No error (0)	sc-static.net		13.225.74.54	A (IP address)	IN (0x0001)
May 4, 2021 16:36:12.560095072 CEST	8.8.8.8	192.168.2.5	0x8bab	No error (0)	sc-static.net		13.225.74.36	A (IP address)	IN (0x0001)
May 4, 2021 16:36:12.576776981 CEST	8.8.8.8	192.168.2.5	0x151f	No error (0)	connect.fa cebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:12.576776981 CEST	8.8.8.8	192.168.2.5	0x151f	No error (0)	scontent.x x.fbcdn.net		31.13.92.14	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.297168016 CEST	8.8.8.8	192.168.2.5	0xd254	No error (0)	analytics. twitter.com	ads.twitter.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:13.297168016 CEST	8.8.8.8	192.168.2.5	0xd254	No error (0)	ads.twitter.com	s.twitter.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:13.297168016 CEST	8.8.8.8	192.168.2.5	0xd254	No error (0)	s.twitter.com		104.244.42.195	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.297168016 CEST	8.8.8.8	192.168.2.5	0xd254	No error (0)	s.twitter.com		104.244.42.3	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.297168016 CEST	8.8.8.8	192.168.2.5	0xd254	No error (0)	s.twitter.com		104.244.42.67	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.297168016 CEST	8.8.8.8	192.168.2.5	0xd254	No error (0)	s.twitter.com		104.244.42.131	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.300024986 CEST	8.8.8.8	192.168.2.5	0xc16	No error (0)	t.co		104.244.42.133	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.300024986 CEST	8.8.8.8	192.168.2.5	0xc16	No error (0)	t.co		104.244.42.197	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.300024986 CEST	8.8.8.8	192.168.2.5	0xc16	No error (0)	t.co		104.244.42.69	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.300024986 CEST	8.8.8.8	192.168.2.5	0xc16	No error (0)	t.co		104.244.42.5	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.305301905 CEST	8.8.8.8	192.168.2.5	0x2515	No error (0)	lasteventf- tm.everes ttech.net	lasteventf.tubemogul.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:13.305301905 CEST	8.8.8.8	192.168.2.5	0x2515	No error (0)	lasteventf .tubemogul.com	h2.shared.global.fastly.ne t		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:13.305623055 CEST	8.8.8.8	192.168.2.5	0xb76e	No error (0)	tr.snapchat.com		35.186.226.184	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.319907904 CEST	8.8.8.8	192.168.2.5	0xd7a8	No error (0)	px.ads.lin kedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 16:36:13.319907904 CEST	8.8.8.8	192.168.2.5	0xd7a8	No error (0)	mix.linkedin.com	glb-na.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:13.319907904 CEST	8.8.8.8	192.168.2.5	0xd7a8	No error (0)	glb-na.mix.linkedin.com	pop-eda6.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:13.319907904 CEST	8.8.8.8	192.168.2.5	0xd7a8	No error (0)	pop-eda6.mix.linkedin.com		108.174.11.69	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.594815016 CEST	8.8.8.8	192.168.2.5	0xa68d	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:13.594815016 CEST	8.8.8.8	192.168.2.5	0xa68d	No error (0)	star-mini.c10r.facebook.com		31.13.92.36	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.596571922 CEST	8.8.8.8	192.168.2.5	0x9c31	No error (0)	id.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.598303080 CEST	8.8.8.8	192.168.2.5	0xe818	No error (0)	match.prod.bidr.io		52.19.106.86	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.598303080 CEST	8.8.8.8	192.168.2.5	0xe818	No error (0)	match.prod.bidr.io		52.209.246.140	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.598303080 CEST	8.8.8.8	192.168.2.5	0xe818	No error (0)	match.prod.bidr.io		52.210.44.111	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.598303080 CEST	8.8.8.8	192.168.2.5	0xe818	No error (0)	match.prod.bidr.io		52.48.151.83	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.598303080 CEST	8.8.8.8	192.168.2.5	0xe818	No error (0)	match.prod.bidr.io		52.49.40.147	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.598303080 CEST	8.8.8.8	192.168.2.5	0xe818	No error (0)	match.prod.bidr.io		52.215.139.246	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.601154089 CEST	8.8.8.8	192.168.2.5	0x9a99	No error (0)	api.company-target.com		143.204.98.86	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.601154089 CEST	8.8.8.8	192.168.2.5	0x9a99	No error (0)	api.company-target.com		143.204.98.59	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.601154089 CEST	8.8.8.8	192.168.2.5	0x9a99	No error (0)	api.company-target.com		143.204.98.79	A (IP address)	IN (0x0001)
May 4, 2021 16:36:13.601154089 CEST	8.8.8.8	192.168.2.5	0x9a99	No error (0)	api.company-target.com		143.204.98.72	A (IP address)	IN (0x0001)
May 4, 2021 16:36:14.674010992 CEST	8.8.8.8	192.168.2.5	0x470e	No error (0)	d9.flashtalking.com	ft.device9.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:14.674010992 CEST	8.8.8.8	192.168.2.5	0x470e	No error (0)	ft.device9.com	tag.device9.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:14.674010992 CEST	8.8.8.8	192.168.2.5	0x470e	No error (0)	tag.device9.com		34.251.104.84	A (IP address)	IN (0x0001)
May 4, 2021 16:36:14.674010992 CEST	8.8.8.8	192.168.2.5	0x470e	No error (0)	tag.device9.com		52.211.172.236	A (IP address)	IN (0x0001)
May 4, 2021 16:36:14.674010992 CEST	8.8.8.8	192.168.2.5	0x470e	No error (0)	tag.device9.com		54.154.210.254	A (IP address)	IN (0x0001)
May 4, 2021 16:36:14.674010992 CEST	8.8.8.8	192.168.2.5	0x470e	No error (0)	tag.device9.com		52.19.17.157	A (IP address)	IN (0x0001)
May 4, 2021 16:36:14.674010992 CEST	8.8.8.8	192.168.2.5	0x470e	No error (0)	tag.device9.com		54.171.117.141	A (IP address)	IN (0x0001)
May 4, 2021 16:36:14.674010992 CEST	8.8.8.8	192.168.2.5	0x470e	No error (0)	tag.device9.com		52.19.132.126	A (IP address)	IN (0x0001)
May 4, 2021 16:36:14.674010992 CEST	8.8.8.8	192.168.2.5	0x470e	No error (0)	tag.device9.com		34.247.239.226	A (IP address)	IN (0x0001)
May 4, 2021 16:36:14.674010992 CEST	8.8.8.8	192.168.2.5	0x470e	No error (0)	tag.device9.com		52.48.136.43	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 16:36:14.793672085 CEST	8.8.8.8	192.168.2.5	0xe4d6	No error (0)	9212252.fls.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:14.793672085 CEST	8.8.8.8	192.168.2.5	0xe4d6	No error (0)	dart.l.doubleclick.net		142.250.185.102	A (IP address)	IN (0x0001)
May 4, 2021 16:36:16.308409929 CEST	8.8.8.8	192.168.2.5	0x8c60	No error (0)	adservice.google.de	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:16.308409929 CEST	8.8.8.8	192.168.2.5	0x8c60	No error (0)	pagead46.l.doubleclick.net		142.250.186.162	A (IP address)	IN (0x0001)
May 4, 2021 16:36:16.456599951 CEST	8.8.8.8	192.168.2.5	0xf50b	No error (0)	googleads.g.doubleclick.net		142.250.185.130	A (IP address)	IN (0x0001)
May 4, 2021 16:36:16.486377954 CEST	8.8.8.8	192.168.2.5	0xcdd4	No error (0)	segments.company-target.com		13.225.74.27	A (IP address)	IN (0x0001)
May 4, 2021 16:36:16.486377954 CEST	8.8.8.8	192.168.2.5	0xcdd4	No error (0)	segments.company-target.com		13.225.74.92	A (IP address)	IN (0x0001)
May 4, 2021 16:36:16.486377954 CEST	8.8.8.8	192.168.2.5	0xcdd4	No error (0)	segments.company-target.com		13.225.74.112	A (IP address)	IN (0x0001)
May 4, 2021 16:36:16.486377954 CEST	8.8.8.8	192.168.2.5	0xcdd4	No error (0)	segments.company-target.com		13.225.74.75	A (IP address)	IN (0x0001)
May 4, 2021 16:36:17.214167118 CEST	8.8.8.8	192.168.2.5	0xa4a5	No error (0)	www.google.de		142.250.184.195	A (IP address)	IN (0x0001)
May 4, 2021 16:36:17.425421000 CEST	8.8.8.8	192.168.2.5	0x3748	No error (0)	prod.adobeccstatic.com		13.224.193.51	A (IP address)	IN (0x0001)
May 4, 2021 16:36:17.425421000 CEST	8.8.8.8	192.168.2.5	0x3748	No error (0)	prod.adobeccstatic.com		13.224.193.53	A (IP address)	IN (0x0001)
May 4, 2021 16:36:17.425421000 CEST	8.8.8.8	192.168.2.5	0x3748	No error (0)	prod.adobeccstatic.com		13.224.193.78	A (IP address)	IN (0x0001)
May 4, 2021 16:36:17.425421000 CEST	8.8.8.8	192.168.2.5	0x3748	No error (0)	prod.adobeccstatic.com		13.224.193.20	A (IP address)	IN (0x0001)
May 4, 2021 16:36:18.420730114 CEST	8.8.8.8	192.168.2.5	0x27bf	No error (0)	bumper.adobeprojectm.com	sparkbumper-production1-va6.cloud.adobe.io		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:18.420730114 CEST	8.8.8.8	192.168.2.5	0x27bf	No error (0)	ethos.ethos51-prod-va6.ethos.adobe.net	ethos51-prod-va6-k8s-pub2-0-dd4b5c1747f92a5e.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:18.420730114 CEST	8.8.8.8	192.168.2.5	0x27bf	No error (0)	ethos51-prod-va6-k8s-pub2-0-dd4b5c1747f92a5e.elb.us-east-1.amazonaws.com		3.223.65.39	A (IP address)	IN (0x0001)
May 4, 2021 16:36:18.420730114 CEST	8.8.8.8	192.168.2.5	0x27bf	No error (0)	ethos51-prod-va6-k8s-pub2-0-dd4b5c1747f92a5e.elb.us-east-1.amazonaws.com		3.223.105.97	A (IP address)	IN (0x0001)
May 4, 2021 16:36:18.420730114 CEST	8.8.8.8	192.168.2.5	0x27bf	No error (0)	ethos51-prod-va6-k8s-pub2-0-dd4b5c1747f92a5e.elb.us-east-1.amazonaws.com		3.221.4.225	A (IP address)	IN (0x0001)
May 4, 2021 16:36:21.540673018 CEST	8.8.8.8	192.168.2.5	0x7b58	No error (0)	js-agent.newrelic.com	f4.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:21.961424112 CEST	8.8.8.8	192.168.2.5	0x91e5	No error (0)	bam.nr-data.net		162.247.242.19	A (IP address)	IN (0x0001)
May 4, 2021 16:36:21.961424112 CEST	8.8.8.8	192.168.2.5	0x91e5	No error (0)	bam.nr-data.net		162.247.242.18	A (IP address)	IN (0x0001)
May 4, 2021 16:36:21.961424112 CEST	8.8.8.8	192.168.2.5	0x91e5	No error (0)	bam.nr-data.net		162.247.242.20	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 16:36:21.961424112 CEST	8.8.8.8	192.168.2.5	0x91e5	No error (0)	bam.nr-data.net		162.247.242.21	A (IP address)	IN (0x0001)
May 4, 2021 16:36:24.823822021 CEST	8.8.8.8	192.168.2.5	0x8c2c	No error (0)	cm.everest tech.net	cm.everesttech.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:25.435973883 CEST	8.8.8.8	192.168.2.5	0x80ac	No error (0)	adobe.demd ex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:25.435973883 CEST	8.8.8.8	192.168.2.5	0x80ac	No error (0)	gslb-2.dem dex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:25.435973883 CEST	8.8.8.8	192.168.2.5	0x80ac	No error (0)	edge-irl1. demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:25.435973883 CEST	8.8.8.8	192.168.2.5	0x80ac	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		18.200.157.96	A (IP address)	IN (0x0001)
May 4, 2021 16:36:25.435973883 CEST	8.8.8.8	192.168.2.5	0x80ac	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		3.250.252.43	A (IP address)	IN (0x0001)
May 4, 2021 16:36:25.435973883 CEST	8.8.8.8	192.168.2.5	0x80ac	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.252.115.248	A (IP address)	IN (0x0001)
May 4, 2021 16:36:25.435973883 CEST	8.8.8.8	192.168.2.5	0x80ac	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.17.54.18	A (IP address)	IN (0x0001)
May 4, 2021 16:36:25.435973883 CEST	8.8.8.8	192.168.2.5	0x80ac	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.250.160.147	A (IP address)	IN (0x0001)
May 4, 2021 16:36:25.435973883 CEST	8.8.8.8	192.168.2.5	0x80ac	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.214.120.236	A (IP address)	IN (0x0001)
May 4, 2021 16:36:25.435973883 CEST	8.8.8.8	192.168.2.5	0x80ac	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.30.135.179	A (IP address)	IN (0x0001)
May 4, 2021 16:36:25.435973883 CEST	8.8.8.8	192.168.2.5	0x80ac	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		63.33.31.50	A (IP address)	IN (0x0001)
May 4, 2021 16:36:27.631227016 CEST	8.8.8.8	192.168.2.5	0xc136	No error (0)	aa.agkn.com	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:27.631227016 CEST	8.8.8.8	192.168.2.5	0xc136	No error (0)	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com		52.58.248.2	A (IP address)	IN (0x0001)
May 4, 2021 16:36:27.631227016 CEST	8.8.8.8	192.168.2.5	0xc136	No error (0)	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com		3.127.52.31	A (IP address)	IN (0x0001)
May 4, 2021 16:36:27.631227016 CEST	8.8.8.8	192.168.2.5	0xc136	No error (0)	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com		3.120.52.200	A (IP address)	IN (0x0001)
May 4, 2021 16:36:27.631227016 CEST	8.8.8.8	192.168.2.5	0xc136	No error (0)	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com		52.29.225.117	A (IP address)	IN (0x0001)
May 4, 2021 16:36:28.245738029 CEST	8.8.8.8	192.168.2.5	0xa0a	No error (0)	sync.mathtag.com	pixel-origin.mathtag.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:28.245738029 CEST	8.8.8.8	192.168.2.5	0xa0a	No error (0)	pixel-origin.mathtag.com		185.29.133.199	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 16:36:28.245738029 CEST	8.8.8.8	192.168.2.5	0xa0a	No error (0)	pixel-origin.mathtag.com		185.29.135.227	A (IP address)	IN (0x0001)
May 4, 2021 16:36:28.245738029 CEST	8.8.8.8	192.168.2.5	0xa0a	No error (0)	pixel-origin.mathtag.com		185.29.132.144	A (IP address)	IN (0x0001)
May 4, 2021 16:36:28.245738029 CEST	8.8.8.8	192.168.2.5	0xa0a	No error (0)	pixel-origin.mathtag.com		185.29.133.58	A (IP address)	IN (0x0001)
May 4, 2021 16:36:28.357857943 CEST	8.8.8.8	192.168.2.5	0x30ce	No error (0)	idsync.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
May 4, 2021 16:36:28.472760916 CEST	8.8.8.8	192.168.2.5	0x8d44	No error (0)	d.turn.com	d.turn.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:28.577956915 CEST	8.8.8.8	192.168.2.5	0x3a5e	No error (0)	pixel.tapad.com		35.227.248.159	A (IP address)	IN (0x0001)
May 4, 2021 16:36:28.708729982 CEST	8.8.8.8	192.168.2.5	0x85af	No error (0)	cm.g.doubleclick.net		142.250.186.98	A (IP address)	IN (0x0001)
May 4, 2021 16:36:28.815610886 CEST	8.8.8.8	192.168.2.5	0xf063	No error (0)	rtd.tubemogul.com	h2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:28.962428093 CEST	8.8.8.8	192.168.2.5	0x2521	No error (0)	p.rfihub.com	a.rfihub.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:28.962428093 CEST	8.8.8.8	192.168.2.5	0x2521	No error (0)	a.rfihub.com	a.rfihub.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:29.064735889 CEST	8.8.8.8	192.168.2.5	0xa250	No error (0)	rtd-tm.everesttech.net	rtd.tubemogul.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:29.064735889 CEST	8.8.8.8	192.168.2.5	0xa250	No error (0)	rtd.tubemogul.com	h2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:29.216964006 CEST	8.8.8.8	192.168.2.5	0x69b	No error (0)	pixel.quantserve.com	px2.px.quantserve.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:29.216964006 CEST	8.8.8.8	192.168.2.5	0x69b	No error (0)	px2.px.quantserve.com		91.228.74.189	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.216964006 CEST	8.8.8.8	192.168.2.5	0x69b	No error (0)	px2.px.quantserve.com		91.228.74.226	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.216964006 CEST	8.8.8.8	192.168.2.5	0x69b	No error (0)	px2.px.quantserve.com		91.228.74.134	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.216964006 CEST	8.8.8.8	192.168.2.5	0x69b	No error (0)	px2.px.quantserve.com		91.228.74.133	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.216964006 CEST	8.8.8.8	192.168.2.5	0x69b	No error (0)	px2.px.quantserve.com		91.228.74.198	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.555002928 CEST	8.8.8.8	192.168.2.5	0xa8af	No error (0)	adobe-sync.dotomi.com	afp.dotomi.weighted.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:29.555002928 CEST	8.8.8.8	192.168.2.5	0xa8af	No error (0)	iad06-usadmm-ds.dotomi.com		205.180.85.201	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.648282051 CEST	8.8.8.8	192.168.2.5	0xb272	No error (0)	a.tribalfusion.com		104.18.12.5	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.648282051 CEST	8.8.8.8	192.168.2.5	0xb272	No error (0)	a.tribalfusion.com		104.18.13.5	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.762073994 CEST	8.8.8.8	192.168.2.5	0xac47	No error (0)	ml314.com		52.31.168.5	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.762073994 CEST	8.8.8.8	192.168.2.5	0xac47	No error (0)	ml314.com		52.211.195.119	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.762073994 CEST	8.8.8.8	192.168.2.5	0xac47	No error (0)	ml314.com		52.49.20.76	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.762073994 CEST	8.8.8.8	192.168.2.5	0xac47	No error (0)	ml314.com		34.247.104.176	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 16:36:29.845844030 CEST	8.8.8.8	192.168.2.5	0xcc9b	No error (0)	bttrack.com		192.132.33.46	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.977612019 CEST	8.8.8.8	192.168.2.5	0xb11b	No error (0)	pix-us.revjet.com		51.81.46.161	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.977612019 CEST	8.8.8.8	192.168.2.5	0xb11b	No error (0)	pix-us.revjet.com		147.135.105.5	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.977612019 CEST	8.8.8.8	192.168.2.5	0xb11b	No error (0)	pix-us.revjet.com		51.81.245.131	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.977612019 CEST	8.8.8.8	192.168.2.5	0xb11b	No error (0)	pix-us.revjet.com		51.81.46.107	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.977612019 CEST	8.8.8.8	192.168.2.5	0xb11b	No error (0)	pix-us.revjet.com		51.81.109.166	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.977612019 CEST	8.8.8.8	192.168.2.5	0xb11b	No error (0)	pix-us.revjet.com		72.251.235.230	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.977612019 CEST	8.8.8.8	192.168.2.5	0xb11b	No error (0)	pix-us.revjet.com		51.81.109.164	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.977612019 CEST	8.8.8.8	192.168.2.5	0xb11b	No error (0)	pix-us.revjet.com		51.81.67.84	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.977612019 CEST	8.8.8.8	192.168.2.5	0xb11b	No error (0)	pix-us.revjet.com		72.251.232.132	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.977612019 CEST	8.8.8.8	192.168.2.5	0xb11b	No error (0)	pix-us.revjet.com		74.217.31.249	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.977612019 CEST	8.8.8.8	192.168.2.5	0xb11b	No error (0)	pix-us.revjet.com		74.201.172.216	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.977612019 CEST	8.8.8.8	192.168.2.5	0xb11b	No error (0)	pix-us.revjet.com		23.92.178.246	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.977612019 CEST	8.8.8.8	192.168.2.5	0xb11b	No error (0)	pix-us.revjet.com		147.135.65.170	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.977612019 CEST	8.8.8.8	192.168.2.5	0xb11b	No error (0)	pix-us.revjet.com		74.217.31.247	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.977612019 CEST	8.8.8.8	192.168.2.5	0xb11b	No error (0)	pix-us.revjet.com		107.6.93.89	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.977612019 CEST	8.8.8.8	192.168.2.5	0xb11b	No error (0)	pix-us.revjet.com		147.135.105.7	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.977612019 CEST	8.8.8.8	192.168.2.5	0xb11b	No error (0)	pix-us.revjet.com		107.6.88.54	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.977612019 CEST	8.8.8.8	192.168.2.5	0xb11b	No error (0)	pix-us.revjet.com		147.135.65.58	A (IP address)	IN (0x0001)
May 4, 2021 16:36:29.977612019 CEST	8.8.8.8	192.168.2.5	0xb11b	No error (0)	pix-us.revjet.com		51.81.46.116	A (IP address)	IN (0x0001)
May 4, 2021 16:36:30.048892021 CEST	8.8.8.8	192.168.2.5	0xa0f3	No error (0)	s.tribalfusion.com		104.18.12.5	A (IP address)	IN (0x0001)
May 4, 2021 16:36:30.048892021 CEST	8.8.8.8	192.168.2.5	0xa0f3	No error (0)	s.tribalfusion.com		104.18.13.5	A (IP address)	IN (0x0001)
May 4, 2021 16:36:30.075228930 CEST	8.8.8.8	192.168.2.5	0xcabd	No error (0)	sync-tm.everesttech.net	sync.tubemogul.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:30.075228930 CEST	8.8.8.8	192.168.2.5	0xcabd	No error (0)	sync.tubemogul.com	syncf.tubemogul.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:30.075228930 CEST	8.8.8.8	192.168.2.5	0xcabd	No error (0)	syncf.tubemogul.com	h2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:30.490358114 CEST	8.8.8.8	192.168.2.5	0x54af	No error (0)	pixel.rubiconproject.com	pixel.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 16:36:30.665821075 CEST	8.8.8.8	192.168.2.5	0x4e09	No error (0)	dsum-sec.casalemedia.com	dsum-sec.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:31.084315062 CEST	8.8.8.8	192.168.2.5	0x66bc	No error (0)	ib.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:31.084315062 CEST	8.8.8.8	192.168.2.5	0x66bc	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:31.084315062 CEST	8.8.8.8	192.168.2.5	0x66bc	No error (0)	ib.anycast.adnxs.com		37.252.173.38	A (IP address)	IN (0x0001)
May 4, 2021 16:36:31.084315062 CEST	8.8.8.8	192.168.2.5	0x66bc	No error (0)	ib.anycast.adnxs.com		37.252.173.62	A (IP address)	IN (0x0001)
May 4, 2021 16:36:31.084315062 CEST	8.8.8.8	192.168.2.5	0x66bc	No error (0)	ib.anycast.adnxs.com		37.252.172.36	A (IP address)	IN (0x0001)
May 4, 2021 16:36:31.084315062 CEST	8.8.8.8	192.168.2.5	0x66bc	No error (0)	ib.anycast.adnxs.com		37.252.172.45	A (IP address)	IN (0x0001)
May 4, 2021 16:36:31.084315062 CEST	8.8.8.8	192.168.2.5	0x66bc	No error (0)	ib.anycast.adnxs.com		37.252.172.249	A (IP address)	IN (0x0001)
May 4, 2021 16:36:31.084315062 CEST	8.8.8.8	192.168.2.5	0x66bc	No error (0)	ib.anycast.adnxs.com		37.252.172.37	A (IP address)	IN (0x0001)
May 4, 2021 16:36:31.084315062 CEST	8.8.8.8	192.168.2.5	0x66bc	No error (0)	ib.anycast.adnxs.com		37.252.173.22	A (IP address)	IN (0x0001)
May 4, 2021 16:36:31.084315062 CEST	8.8.8.8	192.168.2.5	0x66bc	No error (0)	ib.anycast.adnxs.com		37.252.173.27	A (IP address)	IN (0x0001)
May 4, 2021 16:36:32.426292896 CEST	8.8.8.8	192.168.2.5	0x4284	No error (0)	match.prod.bidr.io		52.19.106.86	A (IP address)	IN (0x0001)
May 4, 2021 16:36:32.426292896 CEST	8.8.8.8	192.168.2.5	0x4284	No error (0)	match.prod.bidr.io		52.209.246.140	A (IP address)	IN (0x0001)
May 4, 2021 16:36:32.426292896 CEST	8.8.8.8	192.168.2.5	0x4284	No error (0)	match.prod.bidr.io		52.210.44.111	A (IP address)	IN (0x0001)
May 4, 2021 16:36:32.426292896 CEST	8.8.8.8	192.168.2.5	0x4284	No error (0)	match.prod.bidr.io		52.48.151.83	A (IP address)	IN (0x0001)
May 4, 2021 16:36:32.426292896 CEST	8.8.8.8	192.168.2.5	0x4284	No error (0)	match.prod.bidr.io		52.49.40.147	A (IP address)	IN (0x0001)
May 4, 2021 16:36:32.426292896 CEST	8.8.8.8	192.168.2.5	0x4284	No error (0)	match.prod.bidr.io		52.215.139.246	A (IP address)	IN (0x0001)
May 4, 2021 16:36:32.451194048 CEST	8.8.8.8	192.168.2.5	0xaff7	No error (0)	id.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
May 4, 2021 16:36:32.500669003 CEST	8.8.8.8	192.168.2.5	0xfe5b	No error (0)	image2.pubmatic.com	pug-lhrc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:32.500669003 CEST	8.8.8.8	192.168.2.5	0xfe5b	No error (0)	pug-lhrc.pubmatic.com	pug-lhr.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:32.500669003 CEST	8.8.8.8	192.168.2.5	0xfe5b	No error (0)	pug-lhr.pubmatic.com		185.64.190.80	A (IP address)	IN (0x0001)
May 4, 2021 16:36:33.190589905 CEST	8.8.8.8	192.168.2.5	0xf0f2	No error (0)	us-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
May 4, 2021 16:36:33.190589905 CEST	8.8.8.8	192.168.2.5	0xf0f2	No error (0)	us-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
May 4, 2021 16:36:33.198729992 CEST	8.8.8.8	192.168.2.5	0x43f9	No error (0)	segments.company-target.com		13.225.74.27	A (IP address)	IN (0x0001)
May 4, 2021 16:36:33.198729992 CEST	8.8.8.8	192.168.2.5	0x43f9	No error (0)	segments.company-target.com		13.225.74.92	A (IP address)	IN (0x0001)
May 4, 2021 16:36:33.198729992 CEST	8.8.8.8	192.168.2.5	0x43f9	No error (0)	segments.company-target.com		13.225.74.112	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 16:36:33.198729992 CEST	8.8.8.8	192.168.2.5	0x43f9	No error (0)	segments.company-target.com		13.225.74.75	A (IP address)	IN (0x0001)
May 4, 2021 16:36:34.135998011 CEST	8.8.8.8	192.168.2.5	0x91ea	No error (0)	sync.search.spotxchange.com	sync.search-gtm.spotxchange.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:34.135998011 CEST	8.8.8.8	192.168.2.5	0x91ea	No error (0)	ams01.sync.search.spotxchange.com		185.94.180.125	A (IP address)	IN (0x0001)
May 4, 2021 16:36:34.135998011 CEST	8.8.8.8	192.168.2.5	0x91ea	No error (0)	ams01.sync.search.spotxchange.com		185.94.180.126	A (IP address)	IN (0x0001)
May 4, 2021 16:36:40.322649002 CEST	8.8.8.8	192.168.2.5	0x2ee8	No error (0)	g2.gumgum.com		54.247.114.64	A (IP address)	IN (0x0001)
May 4, 2021 16:36:40.322649002 CEST	8.8.8.8	192.168.2.5	0x2ee8	No error (0)	g2.gumgum.com		34.254.122.11	A (IP address)	IN (0x0001)
May 4, 2021 16:36:40.322649002 CEST	8.8.8.8	192.168.2.5	0x2ee8	No error (0)	g2.gumgum.com		52.208.41.69	A (IP address)	IN (0x0001)
May 4, 2021 16:36:40.322649002 CEST	8.8.8.8	192.168.2.5	0x2ee8	No error (0)	g2.gumgum.com		52.50.187.150	A (IP address)	IN (0x0001)
May 4, 2021 16:36:40.322649002 CEST	8.8.8.8	192.168.2.5	0x2ee8	No error (0)	g2.gumgum.com		54.77.47.243	A (IP address)	IN (0x0001)
May 4, 2021 16:36:40.322649002 CEST	8.8.8.8	192.168.2.5	0x2ee8	No error (0)	g2.gumgum.com		52.212.126.234	A (IP address)	IN (0x0001)
May 4, 2021 16:36:40.322649002 CEST	8.8.8.8	192.168.2.5	0x2ee8	No error (0)	g2.gumgum.com		52.208.210.171	A (IP address)	IN (0x0001)
May 4, 2021 16:36:40.322649002 CEST	8.8.8.8	192.168.2.5	0x2ee8	No error (0)	g2.gumgum.com		54.194.104.251	A (IP address)	IN (0x0001)
May 4, 2021 16:36:40.513672113 CEST	8.8.8.8	192.168.2.5	0x4548	No error (0)	s.thebrighttag.com		34.248.208.147	A (IP address)	IN (0x0001)
May 4, 2021 16:36:40.513672113 CEST	8.8.8.8	192.168.2.5	0x4548	No error (0)	s.thebrighttag.com		46.137.100.137	A (IP address)	IN (0x0001)
May 4, 2021 16:36:40.513672113 CEST	8.8.8.8	192.168.2.5	0x4548	No error (0)	s.thebrighttag.com		108.128.243.153	A (IP address)	IN (0x0001)
May 4, 2021 16:36:40.513672113 CEST	8.8.8.8	192.168.2.5	0x4548	No error (0)	s.thebrighttag.com		54.195.251.142	A (IP address)	IN (0x0001)
May 4, 2021 16:36:41.261626005 CEST	8.8.8.8	192.168.2.5	0x98ed	No error (0)	spark.adobeprojectm.com		143.204.98.41	A (IP address)	IN (0x0001)
May 4, 2021 16:36:41.261626005 CEST	8.8.8.8	192.168.2.5	0x98ed	No error (0)	spark.adobeprojectm.com		143.204.98.95	A (IP address)	IN (0x0001)
May 4, 2021 16:36:41.261626005 CEST	8.8.8.8	192.168.2.5	0x98ed	No error (0)	spark.adobeprojectm.com		143.204.98.51	A (IP address)	IN (0x0001)
May 4, 2021 16:36:41.261626005 CEST	8.8.8.8	192.168.2.5	0x98ed	No error (0)	spark.adobeprojectm.com		143.204.98.8	A (IP address)	IN (0x0001)
May 4, 2021 16:36:41.512324095 CEST	8.8.8.8	192.168.2.5	0xc18e	No error (0)	partner.mediawallahscript.com	mwsyncpixel.eu-west-1.elasticbeanstalk.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:36:41.512324095 CEST	8.8.8.8	192.168.2.5	0xc18e	No error (0)	mwsyncpixel.eu-west-1.elasticbeanstalk.com		34.240.86.127	A (IP address)	IN (0x0001)
May 4, 2021 16:36:41.512324095 CEST	8.8.8.8	192.168.2.5	0xc18e	No error (0)	mwsyncpixel.eu-west-1.elasticbeanstalk.com		52.51.73.37	A (IP address)	IN (0x0001)
May 4, 2021 16:36:55.000077963 CEST	8.8.8.8	192.168.2.5	0x6ee	No error (0)	use.typekit.net	use-stls.adobe.com.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 16:37:22.588323116 CEST	8.8.8.8	192.168.2.5	0x9b7c	No error (0)	bam.nr-data.net		162.247.242.18	A (IP address)	IN (0x0001)
May 4, 2021 16:37:22.588323116 CEST	8.8.8.8	192.168.2.5	0x9b7c	No error (0)	bam.nr-data.net		162.247.242.20	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 16:37:22.588323116 CEST	8.8.8.8	192.168.2.5	0x9b7c	No error (0)	bam.nr-data.net		162.247.242.21	A (IP address)	IN (0x0001)
May 4, 2021 16:37:22.588323116 CEST	8.8.8.8	192.168.2.5	0x9b7c	No error (0)	bam.nr-data.net		162.247.242.19	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 16:35:34.377649069 CEST	205.139.111.113	443	192.168.2.5	49716	CN=*.mimecast.com, O=Mimecast Services Limited, L=London, C=GB CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Feb 19 01:00:00 CET 2021	Wed Mar 23 00:59:59 CET 2022	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
May 4, 2021 16:35:34.380507946 CEST	205.139.111.113	443	192.168.2.5	49719	CN=*.mimecast.com, O=Mimecast Services Limited, L=London, C=GB CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Feb 19 01:00:00 CET 2021	Wed Mar 23 00:59:59 CET 2022	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
May 4, 2021 16:35:39.372364998 CEST	108.174.10.10	443	192.168.2.5	49732	CN=lnkd.in, O=LinkedIn Corporation, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Jan 07 01:00:00 CET 2021	Wed Jul 07 01:59:59 CEST 2021	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
May 4, 2021 16:35:42.294028044 CEST	52.216.79.14	443	192.168.2.5	49746	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	Mon Aug 09 14:00:00 CEST 2021	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=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
May 4, 2021 16:35:43.537018061 CEST	52.216.79.14	443	192.168.2.5	49749	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		
May 4, 2021 16:35:47.653068066 CEST	13.224.193.29	443	192.168.2.5	49761	CN=spark.adobe.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 SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jun 05 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Fri Jun 10 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
May 4, 2021 16:35:50.361377001 CEST	143.204.98.95	443	192.168.2.5	49776	CN=spark.adobe.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 SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jun 05 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Fri Jun 10 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					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		
May 4, 2021 16:35:50.366698980 CEST	143.204.98.95	443	192.168.2.5	49775	CN=spark.adobe.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 SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Jun 05 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Fri Jun 10 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					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		
May 4, 2021 16:35:56.630297899 CEST	69.49.234.124	443	192.168.2.5	49793	CN=lindsayknoxwilliams.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, 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	Sun May 02 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Aug 01 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 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=COMODO RSA Certification Authority, 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		
May 4, 2021 16:35:56.639621019 CEST	69.49.234.124	443	192.168.2.5	49794	CN=lindsayknoxwilliams.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, 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	Sun May 02 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Aug 01 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, 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		
May 4, 2021 16:35:59.634427071 CEST	69.49.234.124	443	192.168.2.5	49809	CN=lindsayknoxwilliams.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, 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	Sun May 02 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Aug 01 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, 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		
May 4, 2021 16:35:59.636195898 CEST	69.49.234.124	443	192.168.2.5	49811	CN=lindsayknoxwilliams.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, 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	Sun May 02 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Aug 01 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, 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
May 4, 2021 16:35:59.637583971 CEST	69.49.234.124	443	192.168.2.5	49813	CN=lindsayknoxwilliams.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, 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	Sun May 02 02:00:00 CEST 2021	Sun Aug 01 01:59:59 CEST 2021	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, 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		
May 4, 2021 16:35:59.639266968 CEST	69.49.234.124	443	192.168.2.5	49808	CN=lindsayknoxwilliams.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, 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	Sun May 02 02:00:00 CEST 2021	Sun Aug 01 01:59:59 CEST 2021	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, 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		
May 4, 2021 16:35:59.639594078 CEST	69.49.234.124	443	192.168.2.5	49810	CN=lindsayknoxwilliams.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, 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	Sun May 02 02:00:00 CEST 2021	Sun Aug 01 01:59:59 CEST 2021	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, 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
May 4, 2021 16:35:59.641058922 CEST	69.49.234.124	443	192.168.2.5	49812	CN=lindsayknoxwilliams.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, 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	Sun May 02 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Aug 01 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, 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		
May 4, 2021 16:36:02.814022064 CEST	69.49.234.124	443	192.168.2.5	49827	CN=lindsayknoxwilliams.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, 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	Sun May 02 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Aug 01 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, 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		
May 4, 2021 16:36:02.814416885 CEST	69.49.234.124	443	192.168.2.5	49826	CN=lindsayknoxwilliams.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, 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	Sun May 02 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Sun Aug 01 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, 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
May 4, 2021 16:36:10.701297998 CEST	63.32.113.5	443	192.168.2.5	49857	CN=ims-na1.adobelogin.com, O=Adobe Inc., L=San Jose, ST=ca, 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	Wed Feb 24 01:00:00 CET 2021 Wed Sep 23 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Tue Mar 01 00:59:59 CET 2022 Mon Sep 23 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
					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		
May 4, 2021 16:36:10.872520924 CEST	54.75.9.158	443	192.168.2.5	49859	CN=*.tt.omtrdc.net, O=Adobe Inc., L=SAN JOSE, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 02 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Wed Nov 10 00:59:59 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 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		
May 4, 2021 16:36:10.971390963 CEST	18.200.233.208	443	192.168.2.5	49861	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Dec 02 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Mon Jan 03 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 4, 2021 16:36:11.378870964 CEST	54.75.9.158	443	192.168.2.5	49865	CN=*.tt.omtrdc.net, O=Adobe Inc., L=SAN JOSE, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 02 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Wed Nov 10 00:59:59 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 SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 16:36:12.656651974 CEST	199.232.136.157	443	192.168.2.5	49878	CN=ads-twitter.com, OU=Twitter Security, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Aug 14 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Thu Aug 19 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
May 4, 2021 16:36:13.400688887 CEST	104.244.42.195	443	192.168.2.5	49889	CN=*.twitter.com, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Feb 05 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Feb 05 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
May 4, 2021 16:36:13.402298927 CEST	104.244.42.133	443	192.168.2.5	49890	CN=t.co, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Feb 05 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Feb 05 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
May 4, 2021 16:36:13.423166990 CEST	104.244.42.195	443	192.168.2.5	49892	CN=*.twitter.com, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Feb 05 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Feb 05 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
May 4, 2021 16:36:13.424171925 CEST	104.244.42.133	443	192.168.2.5	49893	CN=t.co, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Feb 05 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Feb 05 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 16:36:13.697693110 CEST	108.174.11.69	443	192.168.2.5	49895	CN=px.ads.linkedin.com, O=LinkedIn Corporation, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Apr 15 02:00:00 CEST 2021 Wed Sep 23 02:00:00 CEST 2020	Sat Oct 16 01:59:59 CEST 2021 Mon Sep 23 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
May 4, 2021 16:36:13.788980007 CEST	52.19.106.86	443	192.168.2.5	49899	CN=*.match.prod.bidr.io CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Feb 26 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Mar 28 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 4, 2021 16:36:14.804388046 CEST	34.251.104.84	443	192.168.2.5	49909	CN=tag.device9.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 Aug 06 12:30:28 CEST 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	Fri Sep 17 13:41:56 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		
					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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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		
May 4, 2021 16:36:15.944792986 CEST	52.19.106.86	443	192.168.2.5	49920	CN=*.match.prod.bidr.io CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Feb 26 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Mar 28 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 4, 2021 16:36:16.713304043 CEST	63.32.113.5	443	192.168.2.5	49936	CN=ims-na1.adobelogin.com, O=Adobe Inc., L=San Jose, ST=ca, 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	Wed Feb 24 01:00:00 CET 2021 Wed Sep 23 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Tue Mar 01 00:59:59 CET 2022 Mon Sep 23 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
					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		
May 4, 2021 16:36:16.784668922 CEST	54.75.9.158	443	192.168.2.5	49940	CN=*.tt.omtrdc.net, O=Adobe Inc., L=SAN JOSE, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 02 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Wed Nov 10 00:59:59 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 SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 16:36:16.792901039 CEST	18.200.233.208	443	192.168.2.5	49941	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Dec 02 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Mon Jan 03 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 4, 2021 16:36:21.977057934 CEST	18.200.233.208	443	192.168.2.5	49981	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Dec 02 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Mon Jan 03 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 4, 2021 16:36:22.280740976 CEST	162.247.242.19	443	192.168.2.5	49983	CN=*.nr-data.net, O="New Relic, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Feb 05 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Tue Feb 08 13:00:00 CET 2022 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
May 4, 2021 16:36:23.888289928 CEST	54.75.9.158	443	192.168.2.5	49994	CN=*.tt.omtrdc.net, O=Adobe Inc., L=SAN JOSE, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 02 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Wed Nov 10 00:59:59 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 SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 16:36:24.387825012 CEST	63.32.113.5	443	192.168.2.5	49998	CN=ims-na1.adobelogin.com, O=Adobe Inc., L=San Jose, ST=ca, 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	Wed Feb 24 01:00:00 CET 2021 Wed Sep 23 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Tue Mar 01 00:59:59 CET 2022 Mon Sep 23 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
					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		
May 4, 2021 16:36:24.418760061 CEST	54.75.9.158	443	192.168.2.5	49999	CN=*.tt.omtrdc.net, O=Adobe Inc., L=SAN JOSE, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 02 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Wed Nov 10 00:59:59 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 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		
May 4, 2021 16:36:24.493757963 CEST	18.200.233.208	443	192.168.2.5	50001	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Dec 02 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Mon Jan 03 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 4, 2021 16:36:24.852461100 CEST	54.75.9.158	443	192.168.2.5	50003	CN=*.tt.omtrdc.net, O=Adobe Inc., L=SAN JOSE, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 02 01:00:00 CET 2020 Fri Mar 08 13:00:00 CET 2013	Wed Nov 10 00:59:59 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 SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 16:36:25.593044996 CEST	18.200.157.96	443	192.168.2.5	50013	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Dec 02 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Mon Jan 03 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 4, 2021 16:36:26.609464884 CEST	199.232.136.157	443	192.168.2.5	50027	CN=ads-twitter.com, OU=Twitter Security, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Aug 14 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Thu Aug 19 14:00:00 CEST 2021 Sun Oct 22 14:00:00 CEST 2028	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
May 4, 2021 16:36:26.756308079 CEST	104.244.42.195	443	192.168.2.5	50037	CN=*.twitter.com, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Feb 05 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Feb 05 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
May 4, 2021 16:36:26.757332087 CEST	104.244.42.133	443	192.168.2.5	50038	CN=t.co, O="Twitter, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Feb 05 01:00:00 CET 2021 Thu Sep 24 02:00:00 CEST 2020	Sat Feb 05 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
May 4, 2021 16:36:26.882538080 CEST	108.174.11.69	443	192.168.2.5	50032	CN=px.ads.linkedin.com, O=LinkedIn Corporation, L=Sunnyvale, ST=California, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Apr 15 02:00:00 CEST 2021 Wed Sep 23 02:00:00 CEST 2020	Sat Oct 16 01:59:59 CEST 2021 Mon Sep 23 01:59:59 CEST 2030	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Sep 23 02:00:00 CEST 2020	Mon Sep 23 01:59:59 CEST 2030		
May 4, 2021 16:36:27.038403034 CEST	52.19.106.86	443	192.168.2.5	50044	CN=*.match.prod.bidr.io CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Feb 26 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Mar 28 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 4, 2021 16:36:27.609792948 CEST	34.251.104.84	443	192.168.2.5	50054	CN=tag.device9.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 Aug 06 12:30:28 CEST 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	Fri Sep 17 13:41:56 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		
					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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 16:36:27.726969004 CEST	52.58.248.2	443	192.168.2.5	50056	CN=*.agkn.com CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Jul 25 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006 Mon Nov 06 13:23:33 CET 2017	Sun Sep 18 14:00:00 CEST 2022 Mon Nov 10 01:00:00 CET 2031 Sat Nov 06 13:23:33 CET 2027	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
					CN=RapidSSL RSA CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:23:33 CET 2017	Sat Nov 06 13:23:33 CET 2027		
May 4, 2021 16:36:28.407721043 CEST	185.29.133.199	443	192.168.2.5	50062	CN=*.mathtag.com, O="MediaMath, Inc.", L=New York, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Apr 15 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Fri Apr 22 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		
May 4, 2021 16:36:29.315038919 CEST	91.228.74.189	443	192.168.2.5	50084	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		
May 4, 2021 16:36:29.499070883 CEST	18.200.233.208	443	192.168.2.5	50089	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Dec 02 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Mon Jan 03 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 16:36:29.535609007 CEST	18.200.233.208	443	192.168.2.5	50091	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Dec 02 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Mon Jan 03 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 4, 2021 16:36:29.576586962 CEST	18.200.233.208	443	192.168.2.5	50092	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Dec 02 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Mon Jan 03 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		
May 4, 2021 16:36:29.606112957 CEST	18.200.233.208	443	192.168.2.5	50093	CN=*.demdex.net, OU=Digital Marketing, O=Adobe Systems Incorporated, L=San Jose, ST=California, C=US CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Dec 02 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri Nov 10 01:00:00 CET 2006	Mon Jan 03 00:59:59 CET 2022 Tue Sep 24 01:59:59 CEST 2030 Mon Nov 10 01:00:00 CET 2031	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Sep 24 02:00:00 CEST 2020	Tue Sep 24 01:59:59 CEST 2030		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 16:36:29.807106972 CEST	205.180.85.201	443	192.168.2.5	50094	CN=*.dotomi.com, O=Conversant LLC, OU=Corp, L=Westlake Village, ST=CA, C=US CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Jun 19 18:36:07 CEST 2019	Tue Aug 31 09:59:59 CEST 2021	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
May 4, 2021 16:36:29.892836094 CEST	52.31.168.5	443	192.168.2.5	50099	CN=*.ml314.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Sun Jan 17 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Tue Feb 15 00:59:59 CET 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 4, 2021 16:36:30.115216017 CEST	192.132.33.46	443	192.168.2.5	50100	CN=*.bttrack.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	Mon Mar 29 02:00:00 CEST 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Wed Mar 30 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 16:36:31.239145994 CEST	37.252.173.38	443	192.168.2.5	50112	CN=*.adnxs.com, O=Xandr Inc., L=New York, ST=New York, C=US CN=GeoTrust ECC CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=GeoTrust ECC CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 05 01:00:00 CET 2021 Mon Nov 06 13:24:09 CET 2017	Sun Feb 20 00:59:59 CET 2022 Sat Nov 06 13:24:09 CET 2027	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GeoTrust ECC CA 2018, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 06 13:24:09 CET 2017	Sat Nov 06 13:24:09 CET 2027		
May 4, 2021 16:36:32.552680016 CEST	52.19.106.86	443	192.168.2.5	50123	CN=*.match.prod.bidr.io CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Fri Feb 26 01:00:00 CET 2021 Thu Oct 22 02:00:00 CEST 2015 Mon May 25 14:00:00 CEST 2015 Wed Sep 02 02:00:00 CEST 2009	Mon Mar 28 01:59:59 CEST 2022 Sun Oct 19 02:00:00 CEST 2025 Thu Dec 31 02:00:00 CET 2037 Wed Jun 28 19:39:16 CEST 2034	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 4, 2021 16:36:32.552953959 CEST	35.244.174.68	443	192.168.2.5	50125	CN=*.rlcdn.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Feb 25 01:00:00 CET 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Tue Mar 29 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		

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		
May 4, 2021 16:36:32.615570068 CEST	185.64.190.80	443	192.168.2.5	50127	CN=*.pubmatic.com, O="PubMatic, Inc.", L=Redwood City, ST=California, C=US CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Dec 07 01:00:00 CET 2020 Thu Sep 24 02:00:00 CEST 2020 Fri May 12 20:46:00 CEST 2000	Wed Dec 15 00:59:59 CET 2021 Mon May 12 01:59:59 CEST 2025 Tue May 13 01:59:00 CEST 2025	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert Baltimore TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Thu Sep 24 02:00:00 CEST 2020	Mon May 12 01:59:59 CEST 2025		
					CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri May 12 20:46:00 CEST 2000	Tue May 13 01:59:00 CEST 2025		

Code Manipulations

Statistics

Behavior

chrome.exe
chrome.exe

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 2576 Parent PID: 3880

General

Start time:	16:35:27
Start date:	04/05/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://protect-us.mimecast.com/s/HvV0Cn58k7CA73Ec9v4Fg?domain=lnkd.in'
Imagebase:	0x7ff677c70000
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: 5208 Parent PID: 2576

General

Start time:	16:35:29
Start date:	04/05/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1564,2383217152926214841,18074540432404816 56,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1772 /prefetch:8
Imagebase:	0x7ff677c70000
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

Disassembly