ID: 412684
Cookbook: browseurl.jbs
Time: 21:19:56
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

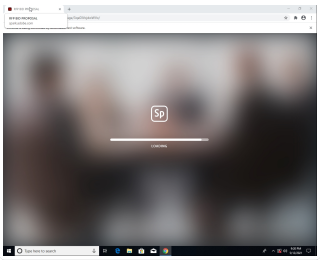
Analysis Report https://spark.adobe.com/page/3qeDIVcj…

Overview

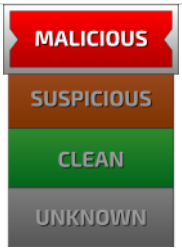
General Information

Sample URL:	http://https://spark.adobe.com/page/3qeDIVcjdwWVx/
Analysis ID:	412684
Infos:	

Most interesting Screenshot:



Detection



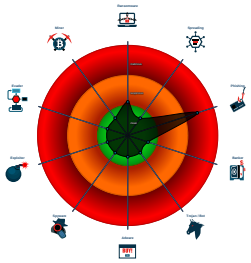
HTMLPhisher

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

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 6064 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://spark.adobe.com/page/3qeDIVcjdwWVx/' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5892 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1568,11667160178596294028,15359971514153105505,131072 --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

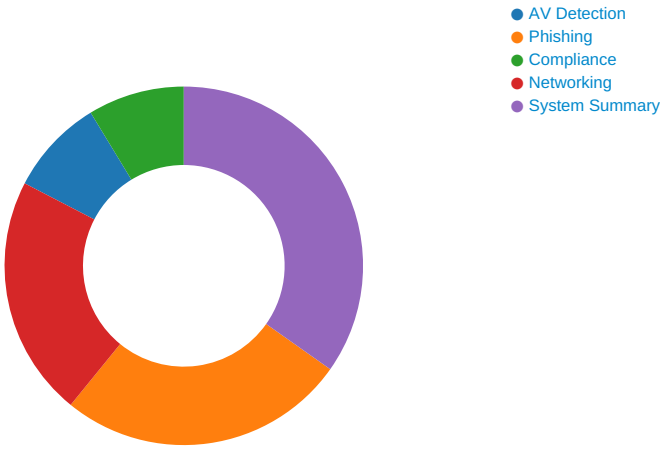
Yara Overview

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:

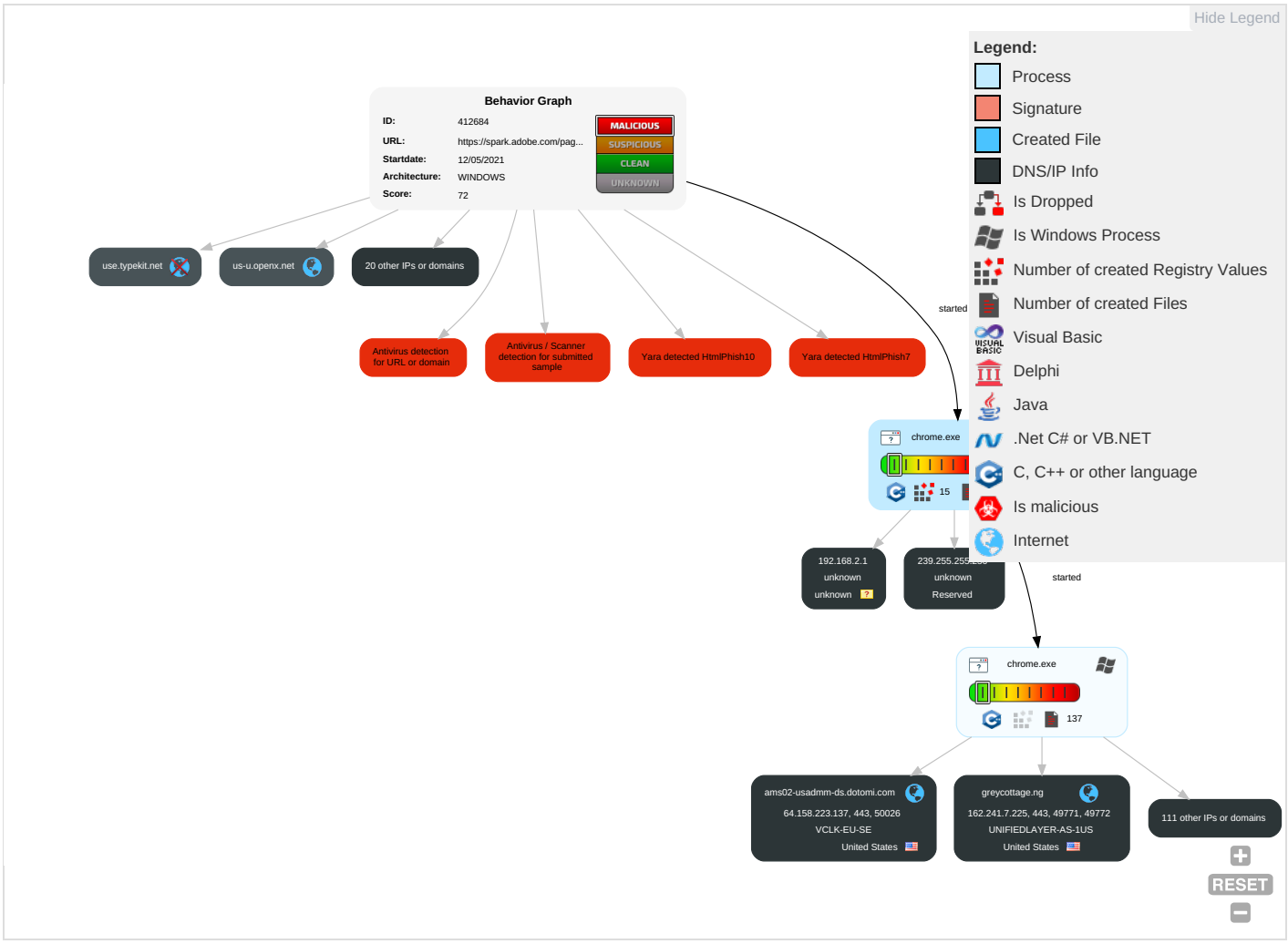
Yara detected HtmlPhish10

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	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

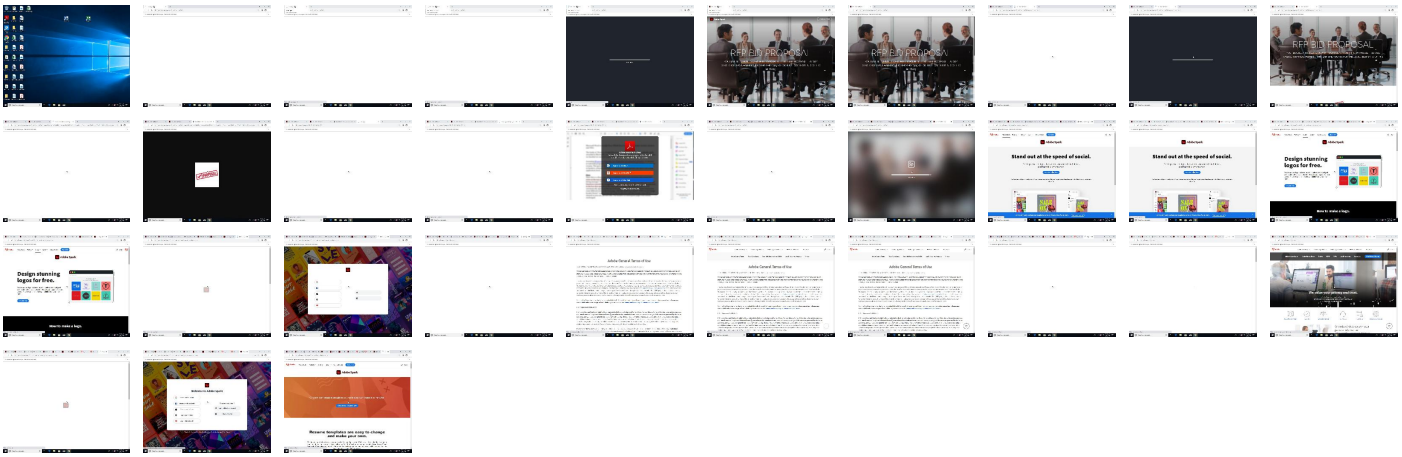
Behavior Graph

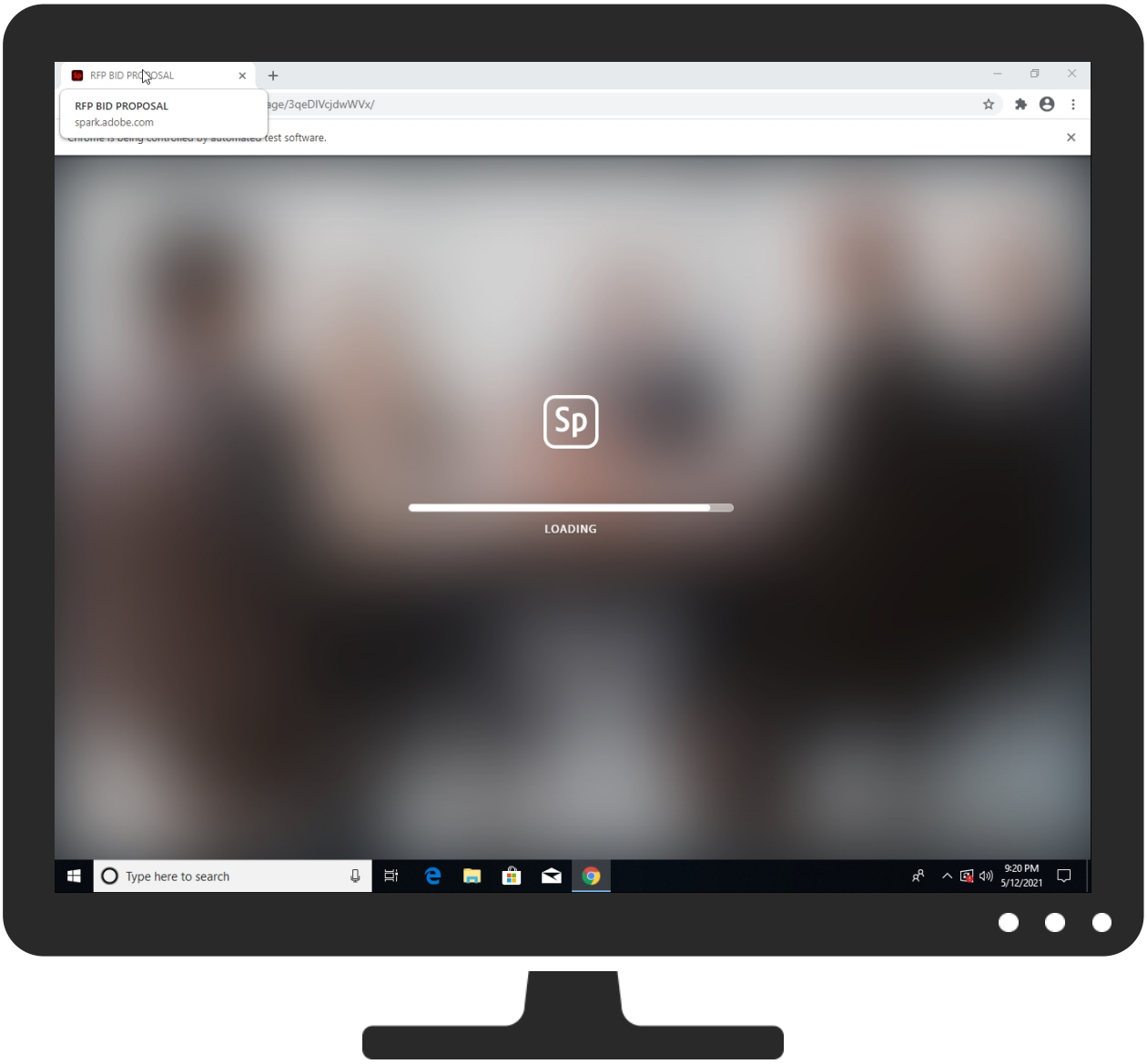


Screenshots

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://spark.adobe.com/page/3qeDIVcjdwWVx/	0%	Avira URL Cloud	safe	
http://https://spark.adobe.com/page/3qeDIVcjdwWVx/	100%	SlashNext	Fake Login Page type: Phishing & Social usering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://https://spark.adobe.com/page/3qeDIVcjdwWVx/?page-mode=static	100%	SlashNext	Fake Login Page type: Phishing & Social usering	
http://https://greycottage.ng/ONLINE%203/PASS%203/	100%	SlashNext	Fake Login Page type: Phishing & Social usering	
http://https://9212252.fls.doubleclick.net)	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://greycottage.ng/favicon.ico	0%	Avira URL Cloud	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://greycottage.ng/ONLINE%203/PASS%203/Share	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://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://sc-static.net/scevent.min.js	0%	URL Reputation	safe	
http://https://sc-static.net/scevent.min.js	0%	URL Reputation	safe	
http://https://sc-static.net/scevent.min.js	0%	URL Reputation	safe	
http://https://greycottage.ng/ONLINE%203/PASS%203//	0%	Avira URL Cloud	safe	
http://https://page.adobespark-assets.com/runtime/1.22/images/favicon.ico	0%	Avira URL Cloud	safe	
http://https://prod.adobeccstatic.com/utilnav/8.2/utilitynav.js	0%	Avira URL Cloud	safe	
http://https://page.adobespark-assets.com/runtime/1.22/runtime-prod.gz.js	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
greycottage.ng	162.241.7.225	true	false		unknown
d1gs6rlbmzcurc.cloudfront.net	13.224.193.115	true	false		high
pug-lhr.pubmatic.com	185.64.190.80	true	false		high
global.px.quantserve.com	91.228.74.134	true	false		high
segments.company-target.com	13.225.74.27	true	false		unknown
tag.device9.com	52.17.98.114	true	false		unknown
tr.snapchat.com	35.186.226.184	true	false		high
platform.twitter.map.fastly.net	199.232.136.157	true	false		unknown
bttrack.com	192.132.33.46	true	false		unknown
s3.amazonaws.com	52.217.103.94	true	false		high
t.co	104.244.42.5	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	142.250.186.130	true	false		high
id.rlcdn.com	35.244.174.68	true	false		high
page.adobespark-assets.com	13.224.193.29	true	false		unknown
sni1gl.wpc.deltacdn.net	152.199.21.175	true	false		unknown
star-mini.c10r.facebook.com	185.60.216.35	true	false		high
match.prod.bidr.io	52.19.106.86	true	false		unknown
pix-us.revjet.com	147.135.65.170	true	false		high
us-u.openx.net	34.98.64.218	true	false		high
s.twitter.com	104.244.42.3	true	false		high
services.prod.ims.adobejanus.com	52.213.176.171	true	false		unknown
sc-static.net	13.225.74.57	true	false		unknown
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
bam.nr-data.net	162.247.242.18	true	false		unknown
googleads.g.doubleclick.net	216.58.212.130	true	false		high
ams01.sync.search.spotxchange.com	185.94.180.126	true	false		high
a.tribalfusion.com	104.18.13.5	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com	52.29.225.117	true	false		high
ml314.com	52.49.20.76	true	false		unknown
googlehosted.l.googleusercontent.com	216.58.212.129	true	false		high
cdn.cookielaw.org	104.16.149.64	true	false		high
dart.l.doubleclick.net	142.250.185.102	true	false		high
pixel-origin.mathtag.com	185.29.133.52	true	false		high
s.tribalfusion.com	104.18.12.5	true	false		high
g2.gumgum.com	52.208.210.171	true	false		high
a97adde81b00f2ca4.awsglobalaccelerator.com	76.223.111.131	true	false		unknown
dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com	34.246.133.154	true	false		high
spark.adobeprojectm.com	13.225.74.123	true	false		unknown
scontent.xx.fbcdn.net	185.60.216.19	true	false		high
idsync.rlcdn.com	35.244.174.68	true	false		high
adobe.com.ssl.d1.sc.omtrdc.net	15.237.136.106	true	false		unknown
demdex.net.ssl.sc.omtrdc.net	15.237.136.106	true	false		unknown
adobe.tt.omtrdc.net	54.75.9.158	true	false		unknown
prod.adobeccstatic.com	13.224.193.20	true	false		unknown
mwsyncpixel.eu-west-1.elasticbeanstalk.com	34.240.86.127	true	false		high
dd20fzx9mj46f.cloudfront.net	13.224.187.69	true	false		high
pixel.tapad.com	35.227.248.159	true	false		high
pagead46.l.doubleclick.net	172.217.23.98	true	false		high
adobelogin-origin.prod.ims.adobejanus.com	63.32.113.5	true	false		unknown
pop-esv5.mix.linkedin.com	108.174.11.37	true	false		high
ethos51-prod-va6-k8s-pub2-0-dd4b5c1747f92a5e.elb.us-east-1.amazonaws.com	3.223.105.97	true	false		high
s.thebrighttag.com	34.248.208.147	true	false		high
ams02-usadmm-ds.dotomi.com	64.158.223.137	true	false		high
api.company-target.com	13.225.74.55	true	false		unknown
www.google.ch	142.250.186.99	true	false		high
ib.anycast.adnxs.com	185.33.220.145	true	false		high
geolocation.onetrust.com	104.20.185.68	true	false		high
scripts.demandbase.com	13.224.193.108	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
api.iperceptions.com	unknown	unknown	false		high
pixel.everesttech.net	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
match.adsrvr.org	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
ds-aksb-a.akamaihd.net	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
www.facebook.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bumper.adobeprojectm.com	unknown	unknown	false		unknown
js-agent.newrelic.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
adservice.google.ch	unknown	unknown	false		high
pixel.quantserve.com	unknown	unknown	false		high
adobe-sync.dotomi.com	unknown	unknown	false		high
sd.iperceptions.com	unknown	unknown	false		high
lasteventf-tm.everesttech.net	unknown	unknown	false		high
www.everestjs.net	unknown	unknown	false		high

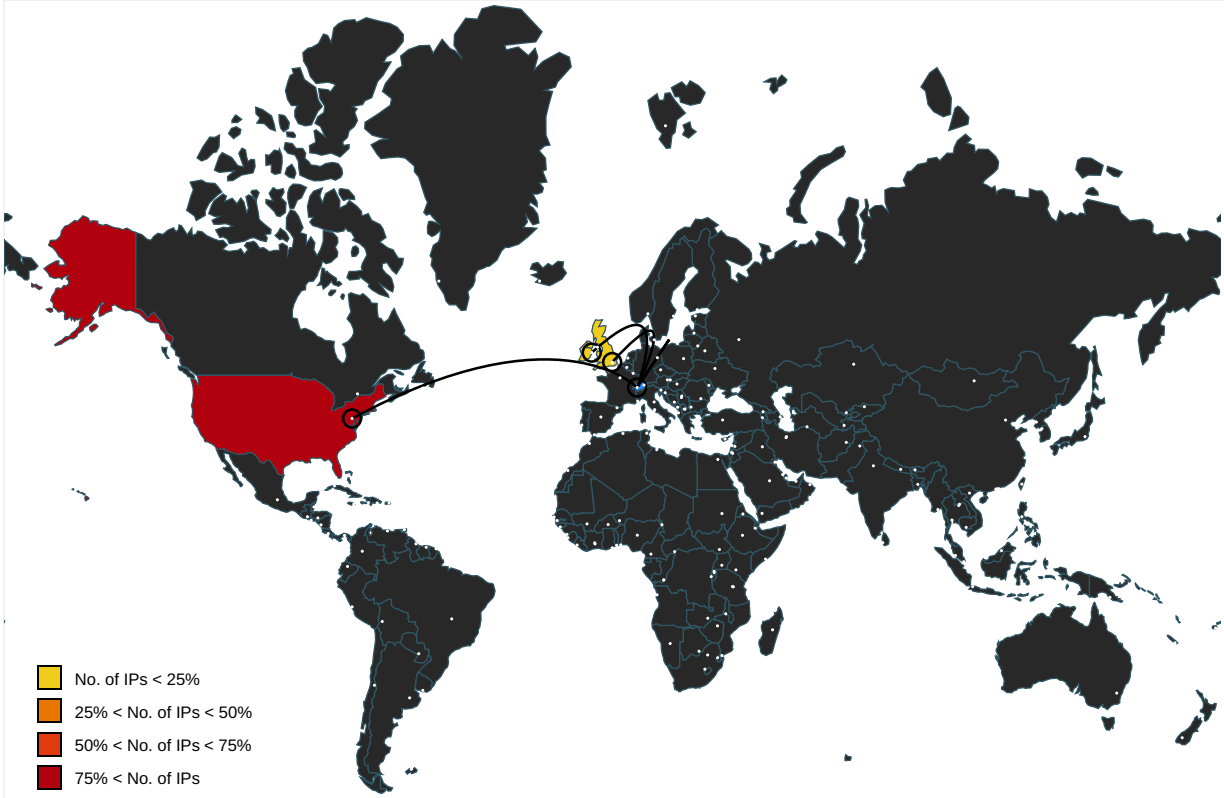
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://universal.iperceptions.com/iFrame.html	Current Session.0.dr	false		high
http://https://centinelapi.cardinalcommerce.com/V2/Cruise/StepUp	eea62f17a0097fed_0.0.dr	false		high
http://https://universal.iperceptions.com/core/Ipuser_v78.0.jsaD	850d10ed47f5161b_0.0.dr	false		high
http://https://code.jquery.com/jquery-3.2.1.slim.min.js	f4bbb5d8755bc352_0.0.dr	false		high
http://https://9212252.fls.doubleclick.net)	Current Session.0.dr	false	• Avira URL Cloud: safe	low
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://json-schema.org/draft/2019-09/vocab/	3f469e2e71221b43_0.0.dr	false		high
http://https://giphy.com/	6f013d296b22569e_0.0.dr	false		high
http://https://9212252.fls.doubleclick.net	Current Session.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/983956512/?random=1620879713948&cv=	c2a6bb76704a0b65_0.0.dr	false		high
http://https://universal.iperceptions.com/	000003.log0.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/987390658/?random=1620879713755&cv=	7b3710c5e15f5c32_0.0.dr	false		high
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://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC48990c37b3504a02838f190f73e1266	7f92142ba76e4116_0.0.dr	false		high
http://https://connect.facebook.net/en_US/fbevents.js	d6595452d2846755_0.0.dr	false		high
http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC6f46e43fa6d44dbeb45cc5801ffded0	e57ec720d2271f49_0.0.dr	false		high
http://https://kit.fontawesome.com/585b051251.js	eb1f518e395f4045_0.0.dr	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js	386d87b204bd71b7_0.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/1004494713/?random=1620879713939&cv	a88a0ba16fc3e3ef_0.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/987390658/?random=1620879701600&cv=	399d65171bfe4109_0.0.dr	false		high
http://https://a.nel.cloudflare.com/report?s=wC8hgUShnecY9AGYErkEMzR07HeMG8NJ9SEoT150xcqYpXGOZ9MtDoKEy9zbUL	Reporting and NEL.2.dr	false		high
http://https://universal.iperceptions.com/wrapper.js	ce2c17b9c6edf534_0.0.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	6f013d296b22569e_0.0.dr	false		high
http://https://servedby.flashtalking.com	Current Session.0.dr	false		high
http://https://dns.google	ca6d3c7d-5d1d-402d-a149-005357 2954c4.tmp.2.dr, f5a7c197-48f2-4d66-bde5-3bb52ed45dde.tmp.2.dr, 1fff30dd-5e94-4459-8cd7-5c6d1262659d.tmp.2.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cdn.cookielaw.org/scripttemplates/6.9.0/otBannerSdk.js	2354abbff3a2b46a_0.0.dr, 61a30 ef70fc39466_0.0.dr	false		high
http://https://greycottage.ng/favicon.ico	Favicons-journal.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://ims-na1-stg1.adobelogin.com	1adee9e8e0f07959_0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://use.typekit.net/	Network Action Predictor-journal.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/951622910/?random=1620879708283&cv=	fc13a0d1a2bae8ac_0.0.dr	false		high
http://https://prod.adobeccstatic.com/utilnav/8.2/utilitynav.css	6f013d296b22569e_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://maxcdn.bootstrapcdn.com/	Network Action Predictor-journal.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/987390658/?random=1620879706908&cv=	3556fd62a32d504e_0.0.dr	false		high
http://https://fb.me/react-async-component-lifecycle-hooks	752e2a75dd6c4851_0.0.dr	false		high
http://https://use.typekit.net/af/edcf1e/00000000000000000000158d9/26/	04e3f25e64ef23bc_0.0.dr	false		high
http://https://centinelapistag.cardinalcommerce.com/V2/Cruise/StepUp	eea62f17a0097fed_0.0.dr	false		high
http://https://blog.adobespark.com/wp-json/wp/v2/	6f013d296b22569e_0.0.dr, ba23d8ecda68de77_1.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://greycottage.ng/ONLINE%203/PASS%203/	Current Session.0.dr, History-journal.0.dr	true	• SlashNext: Fake Login Page type: Phishing & Social usering	unknown
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://greycottage.ng/ONLINE%203/PASS%203/Share	History-journal.0.dr	true	• Avira URL Cloud: safe	unknown
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)	3f469e2e71221b43_0.0.dr	false		high
http://https://d9.flashtalking.com/d9core	9f7e885e8c444e3d_0.0.dr	false		high
http://https://static.adobelogin.com/	Network Action Predictor-journal.0.dr	false		high
http://crl.godaddy.com/repository/gdroot.crl0J	EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D0.2.dr	false		high
http://https://adobespark.zendesk.com/hc/en-us/articles/219243657	3c3e507928304ed9_0.0.dr	false		high
http://https://cdn.cookielaw.org/	Network Action Predictor-journal.0.dr	false		high
http://https://cookiepedia.co.uk/host/.app.onetrust.com?_ga=2.157675898.1572084395.1556120090-1266459230.15	61a30ef70fc39466_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://tr.snapchat.com/p	Current Session.0.dr	false		high
http://https://universal.iperceptions.com/wrapper.jsaD	ce2c17b9c6edf534_0.0.dr	false		high
http://https://use.typekit.net/onz5gap.jsaD	36d0235949f31082_0.0.dr	false		high
http://https://www.cookiepro.com/products/cookie-consent/	61a30ef70fc39466_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://use.typekit.net/nil6fkt.css	1adee9e8e0f07959_0.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/987390658/?random=1620879724159&cv=	cdddce82ff221457_0.0.dr	false		high
http://https://ims-na1.adobelogin.com	1adee9e8e0f07959_0.0.dr	false		high
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/983956512/?random=1620879701650&cv=	10eb3732fd97b16b_0.0.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	3c3e507928304ed9_0.0.dr	false		high
http://https://universal.iperceptions.com/core/Ipuser_v78.0.js	850d10ed47f5161b_0.0.dr	false		high
http://https://npms.io/search?q=ponyfill.	7c2374a7be8500e8_0.0.dr	false		high
http://https://ds-aksb-a.akamaihd.net/aksb.min.js	30ffca376f519f71_0.0.dr	false		high
http://https://sc-static.net/scevent.min.js	7812293e5d091f0b_0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: 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/1004494713/?random=1620879701662&cv	7368ed71bdfa2868_0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/987390658/?random=1620879705806&cv=	7866e75e8abf4ad4_0.0.dr	false		high
http://https://flashtalking.com/XDK	9f7e885e8c444e3d_0.0.dr	false		high
http://https://opsparc.gsfc.nasa.gov/?sdid=MC95SNMJ&mv=social	3c3e507928304ed9_0.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/1004494713/?random=1620879724355&cv	ba0481563fc1e268_0.0.dr	false		high
http://https://servedby.flashtalking.com/	000003.log0.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/1004494713/?random=1620879705769&cv	d94e7e60d38602de_0.0.dr	false		high
http://https://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC5e5d1b9fe0a942c38190dc219952994	d3bfb1b0df4d6ef4_0.0.dr	false		high
http://https://greycottage.ng/ONLINE%203/PASS%203//	History-journal.0.dr	true	• 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
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
http://https://use.typekit.net/rbi5aua.jsaD	04e3f25e64ef23bc_0.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/983956512/?random=1620879724358&cv=	2a0cbdd7970c264d_0.0.dr	false		high
http://https://ka-f.fontawesome.com/	Network Action Predictor-journal.0.dr	false		high
http://https://prod.adobeccstatic.com/utilnav/8.2/utilitynav.js	6f013d296b22569e_0.0.dr, ba23d8ecda68de77_1.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/951622910/?random=1620879724352&cv=	00af15e6f7222ed0_0.0.dr	false		high
http://https://use.typekit.net/af/74fc30/00000000000000000000158d4/26/	04e3f25e64ef23bc_0.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/951622910/?random=1620879701657&cv=	b3e035f953ffa5ce_0.0.dr	false		high
http://https://page.adobespark-assets.com/runtime/1.22/runtime-prod.gz.js	8faec8b628066d9d_0.0.dr, 327de93fb0e7a719_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://use.typekit.net/af/949f99/00000000000000003b9b3068/27/	36d0235949f31082_0.0.dr	false		high
http://https://use.typekit.net/af/6c57c4/00000000000000000000158d6/26/	04e3f25e64ef23bc_0.0.dr	false		high
http://https://www.everestjs.net/static/le/last-event-tag-latest.min.jsa	1aed6b6619289abf_0.0.dr	false		high
http://https://centinelapistag.cardinalcommerce.com/V1/Cruise/Collect	eea62f17a0097fed_0.0.dr	false		high
http://https://cdn.cookielaw.org/scripttemplates/6.9.0/otBannerSdk.jsaD	61a30ef70fc39466_0.0.dr	false		high
http://https://snap.licdn.com/li.lms-analytics/insight.min.jsaD	c1edc6da6ebfc6d9_0.0.dr	false		high
http://https://adobesparkpost.app.link/qtImaging	6f013d296b22569e_0.0.dr	false		high
http://https://cdn.cookielaw.org/scripttemplates/otSDKStub.jsaD	0ba91aa6ae29d08a_0.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.225.74.124	api.demandbase.com	United States		16509	AMAZON-02US	false
13.225.74.123	spark.adobeprojectm.com	United States		16509	AMAZON-02US	false
142.250.185.102	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false
162.241.7.225	greycottage.ng	United States		46606	UNIFIEDLAYER-AS-1US	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
13.224.187.69	dd20fzx9mj46f.cloudfront.net	United States		16509	AMAZON-02US	false
13.225.74.57	sc-static.net	United States		16509	AMAZON-02US	false
185.60.216.35	star-mini.c10r.facebook.com	Ireland		32934	FACEBOOKUS	false
13.225.74.55	api.company-target.com	United States		16509	AMAZON-02US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
152.199.21.175	sni1gl.wpc.deltacdn.net	United States		15133	EDGECASTUS	false
35.244.174.68	id.rlcdn.com	United States		15169	GOOGLEUS	false
35.186.226.184	tr.snapchat.com	United States		15169	GOOGLEUS	false
108.174.11.37	pop-esv5.mix.linkedin.com	United States		14413	LINKEDINUS	false
185.29.133.52	pixel-origin.mathtag.com	United Kingdom		30419	MEDIAMATH-INCUS	false
52.49.20.76	ml314.com	United States		16509	AMAZON-02US	false
142.250.186.130	cm.g.doubleclick.net	United States		15169	GOOGLEUS	false
52.214.120.236	unknown	United States		16509	AMAZON-02US	false
52.19.106.86	match.prod.bidr.io	United States		16509	AMAZON-02US	false
91.228.74.134	global.px.quantserve.com	United Kingdom		27281	QUANTCASTUS	false
52.217.103.94	s3.amazonaws.com	United States		16509	AMAZON-02US	false
104.20.185.68	geolocation.onetrust.com	United States		13335	CLOUDFLARENETUS	false
162.247.242.18	bam.nr-data.net	United States		23467	NEWRELIC-AS-1US	false
199.232.136.157	platform.twitter.map.fastly.net	United States		54113	FASTLYUS	false
52.17.98.114	tag.device9.com	United States		16509	AMAZON-02US	false
13.225.74.27	segments.company-target.com	United States		16509	AMAZON-02US	false
34.246.133.154	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
15.237.136.106	adobe.com.ssl.d1.sc.omtrdc.net	United States		16509	AMAZON-02US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.29.225.117	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
13.224.193.29	page.adobespark-assets.com	United States		16509	AMAZON-02US	false
76.223.111.131	a97adde81b00f2ca4.awsglobalaccelerator.com	United States		16509	AMAZON-02US	false
64.158.223.137	ams02-usadmm-ds.dotomi.com	United States		41041	VCLK-EU-SE	false
13.224.193.20	prod.adobeccstatic.com	United States		16509	AMAZON-02US	false
13.224.193.108	scripts.demandbase.com	United States		16509	AMAZON-02US	false
3.223.105.97	ethos51-prod-va6-k8s-pub2-0-dd4b5c1747f92a5e.elb.us-east-1.amazonaws.com	United States		14618	AMAZON-AESUS	false
216.58.212.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
172.217.23.98	pagead46.l.doubleclick.net	United States		15169	GOOGLEUS	false
216.58.212.130	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
142.250.186.99	www.google.ch	United States		15169	GOOGLEUS	false
54.75.9.158	adobe.tt.omtrdc.net	United States		16509	AMAZON-02US	false
104.244.42.3	s.twitter.com	United States		13414	TWITTERUS	false
104.244.42.5	t.co	United States		13414	TWITTERUS	false
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
104.16.149.64	cdn.cookielaw.org	United States		13335	CLOUDFLARENETUS	false
185.60.216.19	scontent.xx.fbcdn.net	Ireland		32934	FACEBOOKUS	false
147.135.65.170	pix-us.revjet.com	United States		16276	OVHFR	false
52.213.176.171	services.prod.ims.adobejanus.com	United States		16509	AMAZON-02US	false
104.18.13.5	a.tribalfusion.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412684
Start date:	12.05.2021
Start time:	21:19:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://spark.adobe.com/page/3qeDIVcjdwWVx/
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:	9
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal72.phis.win@50/324@87/52
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://spark.adobe.com/page/3qeDIVcjdwWVx/?page-mode=static • Browse: https://spark.adobe.com/page/3qeDIVcjdwWVx/images/353e3ed0-04ef-40a3-b2de-adbe1af942d2.jpg?asset_id=d7a0d027-e0c0-4946-8311-28d93d716082&img_etag=%226ce59f82347e60b2d88a054229a5f51e%22&size=1024 • Browse: https://greycottage.ng/ONLINE%203/PASS%203 • Browse: https://spark.adobe.com/page/3qeDIVcjdwWVx • 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 • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 92.122.145.220, 13.64.90.137, 142.250.185.110, 216.58.212.173, 142.250.185.206, 95.168.222.144, 95.168.222.76, 52.255.188.83, 23.32.238.210, 23.32.238.192, 142.250.184.195, 23.37.33.211, 142.250.74.202, 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, 216.58.212.138, 142.250.185.74, 172.217.16.138, 142.250.185.106, 142.250.185.138, 142.250.185.170, 142.250.185.202, 142.250.185.234, 52.147.198.201, 8.238.85.254, 8.241.79.126, 67.26.139.254, 8.241.82.126, 8.253.145.120, 69.16.175.42, 69.16.175.10, 104.18.22.52, 104.18.23.52, 142.250.181.227, 172.64.101.17, 172.64.100.17, 20.82.209.183, 95.101.22.195, 95.101.22.203, 92.122.213.194, 92.122.213.247, 23.57.81.34, 23.57.80.54, 13.225.74.13, 13.225.74.111, 13.225.74.48, 13.225.74.74, 192.124.249.24, 192.124.249.23, 192.124.249.41, 192.124.249.36, 192.124.249.22, 23.37.44.206, 209.197.3.19, 23.57.82.43, 151.101.2.49, 151.101.66.49, 151.101.130.49, 151.101.194.49, 142.250.185.200, 204.79.197.200, 13.107.21.200, 99.80.199.35, 34.246.227.69, 52.18.11.109, 142.250.186.34, 142.250.185.66, 142.250.74.208, 142.250.186.48, 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, 151.101.2.110, 151.101.66.110, 151.101.130.110, 151.101.194.110, 13.107.42.14, 142.250.184.196, 34.253.145.149, 99.81.11.244, 54.171.42.33, 54.194.191.134, 34.255.166.243, 34.250.153.194, 13.224.193.115, 13.224.193.34, 13.224.193.82, 13.224.193.52, 54.217.68.10, 54.216.49.61, 52.138.200.61, 52.86.79.254, 54.156.10.186, 46.228.164.13, 193.0.160.129, 216.58.212.131, 172.217.16.131, 2.23.155.193, 2.23.155.186, 69.173.144.165, 69.173.144.138, 69.173.144.139, 23.57.81.215, 20.82.210.154, 2.20.84.251, 23.57.80.111, 95.168.222.83, 52.155.217.156, 20.54.26.129 • 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, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.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, api-traffic01.trafficmanager.net, au-bg-shim.trafficmanager.net, dual-a-0001.a-msedge.net, cm.everesttech.net.akadns.net, ris-prod.trafficmanager.net, a-emea.rfihub.com.akadns.net, r1.sn-n02xgoxufvg3-2gbl.gvt1.com, iperceptions01.azureedge.net, ris.api.iris.microsoft.com, a1910.dscq.akamai.net, 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, r1---sn-n02xgoxufvg3-2gbl.gvt1.com, adservice.google.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, e9706.dscg.akamaiedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, www.googletagmanager.com, arc.trafficmanager.net, iperceptions01.ec.azureedge.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, client.messaging.adobe.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, accounts.google.com, fonts.gstatic.com, cc-api-data.adobe.io, stls.adobe.com-cn.edgesuite.net, skypedataprdcoleus16.cloudapp.net, adobeid-na1.services.adobe.com, e7808.dscg.akamaiedge.net, wildcard.licdn.com.edgekey.net, cdn.cp.adobe.io, r8---sn-n02xgoxufvg3-2gbl.gvt1.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net, e6653.dscf.akamaiedge.net, cds.s5x3j6q5.hwcdn.net, commerce.adobe.com, spark.adobe.com, ds-aksb-a.akamaihd.net.edgesuite.net, r8.sn-n02xgoxufvg3-2gbl.gvt1.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, api-iperceptions03.cloudapp.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, r5.sn-n02xgoxufvg3-2gbs.gvt1.com, sparkbumper-production1-va6.cloud.adobe.io, commerce.adobe.com.edgekey.net, www.googleapis.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, a1815.dscr.akamai.net, www.googleadservices.com, pixel.rubiconproject.net.akadns.net, store-images.s-microsoft.com-c.edgekey.net, r5---sn-n02xgoxufvg3-2gbs.gvt1.com, a1449.dscg2.akamai.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, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, kit.fontawesome.com.cdn.cloudflare.net, www-linkedin-com.l-0005.l-msedge.net, sstats.adobe.com, p.typekit.net-v3.edgekey.net, www-googletagmanager.l.google.com, f4.shared.global.fastly.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, sync.search-gtm.spotxchange.com.akadns.net, skypedataprdcoleus17.cloudapp.net, bat-bing-com.a-0001.a-msedge.net, ocsp.godaddy.com, a1988.dscg1.akamai.net, www.adobe.com

- Report size exceeded maximum capacity and may have missing behavior information.

- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtQueryVolumeInformationFile calls found.
- Report size getting too big, too many NtWriteFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.
- VT rate limit hit for: https://spark.adobe.com/page/3qeDIVcjdwWVx/

Simulations

Behavior and APIs

Time	Type	Description
21:21:13	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
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false

C:\Program Files\Google\Chrome\Application\Dictionaries\en-US-9-0.bdic	
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):	7.301698998198966
Encrypted:	false
SSDEEP:	48:panitqjPAzkWn17SIYnita8lnitq1+Zvl3oXS9As5RmEWqu5H99:pWakWkkz1+boavLJpu5
MD5:	2AF13F5C8466F0AFADBA5D350A37C883
SHA1:	D80C9F1127EF3BC8B8F0B9D00D2485C7EDE8C39A
SHA-256:	3DCE64D26D1D0DE49281FA037ABBB2B671BAEA105A78FD82D3B39613C663B2F6
SHA-512:	237C223382EB2F254819389FCE5383A6E3F3043765830A50EC1C1D670A9702C4F25E55C2A2AF6E5743A74791DF0CA331BB3CA7177D3ADB56F95176BA9C7334F0
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..20210511205259Z0d0b0:0...+.....#o..K.....#....+...:....g(.....An .....20210511205259Z....20210513085259Z0...*.H.....q&..%.....H.7...#.oL..:.{&.1..P&...d^\.K.T..qM....'.....&..M.~.%=. i...?....6.....F..9.x2..b.m..u...e..l"3...0<H..m>..5.I..?i.f.....w`^.q..WI.cC..&...O^G:.....~W.....w.B.nW.iI5.....B.su.{..^7.Di....Va...kUj...>.i+.8.T.mi5k.....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, 59863 bytes, 1 file
Category:	dropped
Size (bytes):	59863
Entropy (8bit):	**7.99556910241083**
Encrypted:	**true**
SSDEEP:	1536:Gs6cdy9E/ABKQPOrdweEz480zdPMHXNY/gLHfIZN:GNOqOrdDdJPAX1LHA/
MD5:	15775D95513782F99CDFB17E65DFCEB1
SHA1:	6C11F8BEE799B093F9FF4841E31041B081B23388
SHA-256:	477A9559194EDF48848FCE59E05105168745A46BDC0871EA742A2588CA9FBE00
SHA-512:	AC09CE01122D7A837BD70277BADD58FF71D8C5335F8FC599D5E3ED42C8FEE2108DD043BCE562C82BA12A81B9B08BD24B961C0961BF8FD3A0B8341C87483CDE7
Malicious:	false
Reputation:	low
Preview:	MSCF.....,.....I.....b.....R.i .authroot.stl.qqp.4..CK..8T....c_.d....A.F....m"...AH)-.%.QIR..$t)Kd.-QQ*..~.L.2.L.....sx.}...~....$....yy.A.8;....|.%OV.a0xN....9..C..t.z.,X...,..1Qj,.p.E.y..ac`.<.e.c.aZW..B.jy....^]..+)..!...r.X:.O.. ..Y..j.^.8C.....n7R....p!|_.+..<...A.Wt.=. .sV..`.9O...CD./.s.\#.t#..s..Jeiu..B$.....8..(g..tJ....=,...r.d.].xqX4.....g.lF...Mn.y".W.R....K\..P.n._..7.....@pm.. Q....(#.....=.)...1..kC.`.....AP8.A..<....7S.L....S...^.R.).hqS...DK.6.j....u_.0.(4g.....!,.L`.....h:.a]?.....J9.\..Ww.....%.....4E....q.QA.0.M<.&.^*aD.....,.]*....5.....\../ d.F>.V....._.J....."....wI..'..z...j..Ds....Z...[.....N<.d.?<....b.,...n.....;....YK.X..0..Z.....?...9.3.+9T.%.l...5.YK.E.V...aD.0...Y../e.7...c..g....A..=.....+..u2..X.~....O....\=...&...U.e...?...z....$.)S..T...r.!?M..;....r,QH.B <.(t..8s3..u[.N8gL.%...v....f...W.y...cz-.EQ.....c...o..n.....D*.....2.

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):	7.270810098218166
Encrypted:	false
SSDEEP:	48:snitqJYcaXbM/uVnitqsXA49e5REMeZ6+23wQ:UJYcUXsw49eEMeZ6+Y
MD5:	DA0A688A938BFFF2E870E4D701B2FB6B
SHA1:	89A80D5D89A761E9884949B6066B73A169FBC820
SHA-256:	7D45BCC2DD7AC6596654A78D8FBB72B93064E51B2ADBF6EAD6E15DC09010BA30
SHA-512:	8987B8BA323CE3913C8F9716DE1B872222FB4010AE673DF35E06294C86079D22DE50BBC215343659AD006799E89D756BD4274B00043D784069C808485A294C37
Malicious:	false

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D	
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..20210512015251Z0f0d0<0...+..... .....]..J^.y_..F<.....L.q.a.=...j.....20210512015251Z....20210513135251Z0...*.H.....E...r..$..Wz..g....rj4..d.....s....h....x.e..q...y.x.....q..c..~...N..a2.:.....p(.2..(=J....*..dHH.P..>3e.<.t.o...JSLx.Un\..x.....Xp.%...u"..nex./...(.....i.&...m"...2.6.N.\|H5A..H3#.3...(.G.Q..... 7..6.. [.....eT.K....aw.4..GW.(DR..!...Y.\=-..-.J...b0..^0..Z0..B.....1g...r.0...*.H.....0c1.0...U....US1!0...U....The Go Daddy Group, Inc.110/..U...(Go Daddy Class 2 Certification Authority0...161213070000Z..211213070000Z0..1.0...U....US1.0...U....Arizona1.0...U....Scottsdale1.0...U....GoDaddy.com, Inc.100...U...'Go Daddy Root Validation Authority - G10.."0...*.H.....0.....}...@.H.....j.b.2.c....'eSA...6""2.hf.m.m9....._N."gV..{.J"{..0f.W$.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):	3.7728199299414276
Encrypted:	false
SSDEEP:	24:7OwyPV13MhmyFq1QXyhDyOwyPV13MhmyFq1Qq:awkV1XyFuPwkV1XyFuD
MD5:	FF962F1827119EB8B81DE7FB58732EB9
SHA1:	92D9C73C6C8C34AB93519E5772B63742469EE379
SHA-256:	359B9F88104409F5717BB820803CAB5284A8C3C293B3FF66EC803817B78BF977
SHA-512:	639ACEA705D633B6BECBEDB679DBCDF9B3DE9F1D2B4ABEE0CA596AE02E276EA11C6D77A8495105BFAD62ED01250CE9D94AEC8B4EE2333C53E394A1591A7106BC
Malicious:	false
Reputation:	low
Preview:	p..... .....G..(..... .....F.....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...".d.8.0.c.9.f.1.1.2.7.e.f.3.b.c.8.b.8.f.0.b.9.d.0.0.d.2.4.8.5.c.7.e.d.e.8.c.3.9.a."...p..... .....G..(.....F....._.G....._.G.. .....F.....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...".d.8.0.c.9.f.1.1.2.7.e.f.3.b.c.8.b.8.f.0.b.9.d.0.0.d.2.4.8.5.c.7.e.d.e.8.c.3.9.a."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.140842466552086
Encrypted:	false
SSDEEP:	6:kKJ8pkQSN+SkQlPlEGYRMY9z+4KlDA3RUeSKyzkOt:uphZkPlE99SNxAhUeSKO
MD5:	2461684EF084F735E46B6834173EDB84
SHA1:	B0916B4D59AC51838FA21EC0F57A415A7FB0493C
SHA-256:	EDBFBA4FE607FF018B20E0CCB71216FA791B1A804F7D5A898172CF605066F9B4
SHA-512:	E215B21A22E3DBA2C8E817F96CE6AD94FAB5B679B2DFA44BCF7E467AF5EC671BFD760492FD6D14C18551F72A9028ECC5005D84692F257555E2D98DD29A03D80
Malicious:	false
Reputation:	low
Preview:	p..... .....h.G..(..... .....Y5.....$.....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...".8.0.f.8.8.3.5.9.3.5.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):	3.7908253144003545
Encrypted:	false
SSDEEP:	12:FnrQEFDsFrvgxE0P6GANMp2FpAGpqlr2PtZCCrQEFDsFrvgxE0P6GANMp2FpAGpJ:FnV4xaVSGAm+pbPtZCCV4xaVSGAm+pb1
MD5:	65AB76B747B8224B25080AFE24A489A9
SHA1:	90BB5B924EEB60AF20C1FE8B1598790DB1FB09B4
SHA-256:	F34D03BEBFCA3B94D6D2895F6DC5250AE1ADC3ABC54286DBBCCE99442C41734B
SHA-512:	9443D44E08593397A10D66A302D6AA6C8686F5A46DFF869322510034D43D82CE7AB78FF971EC28B2CF47D46DA033784841EEFCCFEBCA374AE0E585FE6CFBED7
Malicious:	false
Reputation:	low

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EB2C4AB8B68FFA4B7733A9139239A396_D76DB901EE986B889F30D8CC06229E2D	
Preview:	p..... .....=...G..(..... .....['..F.....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...".8.9.a.8.0.d.5.d.8.9.a.7.6.1.e.9.8.8.4.9.4.9.b.6.0.6.6.b.7.3.a.1.6.9.f.b.c.8.2.0."...p..... .....=...G..(.....['..F.....C.G.....C.G.. .....['..F.....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...".8.9.a.8.0.d.5.d.8.9.a.7.6.1.e.9.8.8.4.9.4.9.b.6.0.6.6.b.7.3.a.1.6.9.f.b.c.8.2.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\6195d0e3-f64c-402a-96c3-222a2542f701.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):	372140
Entropy (8bit):	6.049763095905352
Encrypted:	false
SSDEEP:	6144:bVwsB8g4WG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinV:5vKPWGNPUZ+w7wJHyEtAWE
MD5:	FF0DF0D8041CC6090E779B40B71523BF
SHA1:	0F3EEC6769C82E515A7E26C6A680605167275F56
SHA-256:	DEADB26DDCC702EEB771FA45324F28ABEA67B0537CA04331BAB41D1ADE663A97
SHA-512:	AEBB9A3B60D567815C83A9E7BF19D3C2F4FF8765464B83EFC5BBAD3A9F7FD493D455C50610D63F6288490A7A7194E3A0700310D8A0A1A563F00EA1AF76D5866
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":1.620879652247575e+12,"network":1.620847254e+12,"ticks":158190717.0,"uncertainty":4553386.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\85e1183b-7860-4c6a-ae8e-8a062343e16d.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):	363673
Entropy (8bit):	6.028441702840896
Encrypted:	false
SSDEEP:	6144:rVwsB8g4WG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinV:JvKPWGNPUZ+w7wJHyEtAWE
MD5:	D620EF290771BC0F3349837904762B63
SHA1:	6C19AEFF954B46ECA8F31D72C3674F8A5F3F371B
SHA-256:	0E8BFF7E544541BC70176B6EA9B0C36A0967F359D9C61076E0E18320DACFE333
SHA-512:	269FFA80717C03879C1B0DB6B63A822476B00387C896A60832DA8596F3C00165F0BA1184A023E8BEA1EAE1635D0BB5DD5798E851CA37655ACEC86479B956D78A
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":1.620879652247575e+12,"network":1.620847254e+12,"ticks":158190717.0,"uncertainty":4553386.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488079548"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\8a8cf18e-8dc3-486e-a514-ff5e8446a62f.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):	372140
Entropy (8bit):	6.049763181466883
Encrypted:	false
SSDEEP:	6144:SVwsB8g4WG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinV:4vKPWGNPUZ+w7wJHyEtAWE
MD5:	FE667D89086CFC982F6F5294305390D9
SHA1:	DD288A2861052C83F22359C9F37FD02A2C9FC9E0
SHA-256:	1737C2ED153362FF238906A8B18F18CEF29F2DFA962C4CAA76A75E7AA77A913D
SHA-512:	438C07126816D7808145A8BFE0F620D87A278F371C962A6EB0B0682F586619B5C6414B3DD5170FB8C2B56722DDEC08180CD71B76EABFFEC55D5720CCD974A0D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\8a8cf18e-8dc3-486e-a514-ff5e8446a62f.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":1.620879652247575e+12,"network":1.620847254e+12,"ticks":158190717.0,"uncertainty":4553386.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488079548"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\948dd4d1-5a7c-4322-bb39-9c96bda0ce17.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):	363673
Entropy (8bit):	6.028440923054444
Encrypted:	false
SSDEEP:	6144:hVwsB8g4WG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinV:bvKPWGNPUZ+w7wJHyEtAWE
MD5:	1060F020D04E16B26CA60E0B2DF4C8F3
SHA1:	B029DE5231F95A74053B9819E51FB95435D1BD3E
SHA-256:	680DD7F04C1B6F04007852209EA2859EC27968844CDEAD1406340B39258C564A
SHA-512:	087708E8385DE1DEF651CCC842E5BAD4A0711803B0C3D8BD8C634FA50B17DC74138E7545D49A2CDF8FD2F0E60454A887EC4990EC0F3C80BDC2E610224095CAC
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":1.620879652247575e+12,"network":1.620847254e+12,"ticks":158190717.0,"uncertainty":4553386.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488079548"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXEwozZHGftEwozZHGftEwozZHn:+EwozZHGVEwozZHGVEwozZHn
MD5:	4829695F153A750ADF50C6E979E8E8F3
SHA1:	2F697EF207460D03671E4B59670BC73328D60D6E
SHA-256:	1AACF1304FD42C84FF41DDD2F2252E5C0EDE7362352661B7957648F2EA4C2683
SHA-512:	6D16A6EF4BB20B25B1B14757C475E9F8C3A40D6181F718D563A628BA41DA9426E1B586C472D4F8729FD65FCA014151B7D46FBFAAE171BFF9A6D937DB7A7A2C02
Malicious:	false
Reputation:	low
Preview:	sdPC.....y3..M.Y.NbD.sdPC.....y3..M.Y.NbD.sdPC.....y3..M.Y.NbD.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\035f0f2b-3c3d-4383-81fd-72f2e4a8ae15.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):	5.535898578085945
Encrypted:	false
SSDEEP:	384:8MRrt+LlhiX31kXqKf/pUZNCgVLH2HfD3rUKHGAnTupEel4p:2Ll231kXqKf/pUZNCgVLH2HfLrUaGAnn
MD5:	6238C658ADA3CF77D382711400515D62
SHA1:	AE096569174ED6C60E049B3AACB893C0F9EC6F55
SHA-256:	2139CA5BE09EFE31FE15000DDD078F1F2D79B975086A946CE98A0BFEC3205EBF
SHA-512:	91B077AF1A602FE3BCCB9ED13682FC88B13A0DD18F7D32BEEEBB773EEC1B3B8A4F24270FFEC8E8FC33D4CB69178AC28F6D489C69EFB6E1C628027D8AEC4B244
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\035f0f2b-3c3d-4383-81fd-72f2e4a8ae15.tmp	
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":"13265353249009481","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\10016e9a-7023-497e-bc33-2d8b877aac0b.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5763
Entropy (8bit):	5.185947719952308
Encrypted:	false
SSDEEP:	96:n2XbsW/k2t7aAVqSxk0JCKL8yky1fCMbOTQVuwn:n2Xbsp2x9Uq4KrkyBd
MD5:	39737B87E039F7DEEAB4714ADF0150B5
SHA1:	9EFAA119E17A9EBAAE6580CBC5439AB03EE686C4
SHA-256:	D0FBE44547E248CD45AB5C75791E540CEB189000EE580D50AA281214C11A322D
SHA-512:	C3F53F86ABC171D18651BC4ABE6B92DBAD70157778531651DDB9265B9BAFC7B2392E4ADF67FAAAE8EF2F0CEC0381A36599A70A72ED3C125658415431CFF1EAA2
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13265353249338570","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\2a67d60b-fc0b-414a-8845-ca6254fe520f.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):	1207
Entropy (8bit):	5.578704162086783
Encrypted:	false
SSDEEP:	24:Y7cI7wUi6H0Uhcgf/wULG1KUe4aUewb7wUeU3RUeHQ:YPEUi6UUhciwU2KUe4aUeYwUeUhUew
MD5:	2B994A649AEA8C1054CE179A7C4CE6C9
SHA1:	082F90714D7F3AF7CFCCFF215958E89DDA7A04DA
SHA-256:	71A89F8E6174CA3E2A3A30C032D91B58BF0FF97B03B08EA8B1A126F96A00753F
SHA-512:	1AE5D392FD91DC8BD4E2F9B6366BF4B2FE4CE5670870322E297AC389F739EF7AD44DD951A8BE944840DE6DB2411C459458176318EF916DF6C313D7ECB567DE2
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1652415664.696807,"host":"OJAwwDug+gPr+xWjx2kFIFhHDQULu5ljftVMMZ74I4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620879664.696812},{"expiry":1633015352.675531,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601479352.675536},{"expiry":1652415662.084715,"host":"YBf+o277nAvW3A1uFG7ThwT6zuF7asaeDH6RPNOXinc=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620879662.08472},{"expiry":1633015352.520557,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601479352.52056},{"expiry":1633015352.455722,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601479352.455726},{"expiry":1633015295.599948,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3065d386-fc91-4dd4-9dca-bdd611b628cc.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):	4883
Entropy (8bit):	5.605577500491252
Encrypted:	false
SSDEEP:	96:q8sU9UwUPCUneaieURUulUUa/UlMUQUR+URFUcwUJfUMglTU0tUEUcUSU3KUCUnH:q8sU9UwUPCUnVURUWUUa/UuUQUR+ULUC
MD5:	7CF97DE2485B9F3769E81099CF9FF5A8
SHA1:	3106F39867C3C5825E7284B2829B34D4DB7916CA
SHA-256:	4FBA01A92E59654AE9E3EA8DAAE80118272537371D95B725881A89C06014E83A
SHA-512:	F9675605487EC36114E20009A570173105A01754B18798D3807AB86E466D5FFCB0E38030C734DD007B50B1B91083B03C1A8135E98973FC734EE18192F4AF773F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3065d386-fc91-4dd4-9dca-bdd611b628cc.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1652415812.317662,"host":"CJ6kx0n19VtUkGfz4J6tLFRfDatw73CAqzbGpnezKw0=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620879812.317667},{"expiry":1623471813.802793,"host":"Dg14fIaciUHGX6Lc+OnYmaNiAA/ADiwumtIyPrC3d6U=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620879813.802799},{"expiry":1636659677.156215,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620879677.15622},{"expiry":1652415798.545467,"host":"Hi4bEdMq563Qsqn4sVyUls/uVk7U80lxMa3wyWVUqWU=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620879798.54547},{"expiry":1652415813.707595,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620879813.707599},{"expiry":1652415831.47753,"host":"OJAwwDug+gPr+xWjx2kFIFhHDQULu5ljftVMMZ74I4o=","mode":"force-https","sts_include_subdomains":true,"sts_obser

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4bf2ac05-542a-4ceb-b9a8-46160871a541.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):	5728
Entropy (8bit):	5.188562794189941
Encrypted:	false
SSDEEP:	96:n2XbS/k2t7aAVqkxk0JCKL8yky1fCMbOTQVuwn:n2Xbd2x9UU4KrkyBd
MD5:	96A32F2A5FC23EDB59D06A95DC548CD9
SHA1:	5A18541771BD5EA93D2DF8EB2E4BB98D276EA43A
SHA-256:	1FC08FF61301DA4B43618D2E69324103ABF1679040D6EC24398C67A1E1BF5245
SHA-512:	D7502BB08341265FA19DAF8AF51777408DDA97D006731EE4BA7D38D3FA17BC02F658963FAA0789F191BE12DEAF2B622E649A1B60E7427D166955DF6185A55DC
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13265353249338570","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\5a2db8eb-b63b-43fc-8e30-b84a273d9ef4.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):	18940
Entropy (8bit):	5.568717085672168
Encrypted:	false
SSDEEP:	384:8MRrtXLlhiX31kXqKf/pUZNCgVLH2HfD3rUAHGv1EPl4j:vLl231kXqKf/pUZNCgVLH2HfLrUEG90C
MD5:	D114759F5A0CF64400B406D0BAFD154C
SHA1:	5C3D1CE650773FFEB132A062AA017872E370FE22
SHA-256:	762A581CF85DFE2150F5FC2D753256CE16F7BDC00F8BA1980C899F6A8BF7F6B5
SHA-512:	94B77FF24FFD3026846400632D125CFD8456E36CC2583518B38D2C8A369A8B5D78DBF625527DBCA7CD1E545833D1BA632BCB630896B4C7801B2AFF551087871
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":"13265353249009481","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\60cdb687-b45b-407f-90af-e76a8f6bea85.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):	4884
Entropy (8bit):	5.605405769834784
Encrypted:	false
SSDEEP:	96:q8sU9UwUPCUneaieU0Uc4UUa/UlMUQUR+URFUcwUJfUMglTU0tUEUcUSU3KUCUnH:q8sU9UwUPCUnVU0Uc4UUa/UuUQUR+ULP
MD5:	CFBA539FC56AE6F69EF882339BAFBD69
SHA1:	C30A1D6E8CE151C10A8395932A3A391521DD2458
SHA-256:	CB49D32EB6077A0D3EA40883534D70B8832797A2710552B7AC0921AF195092A9
SHA-512:	D1B593C5BC0BE83C75BD16835DCD9F72BD6D0DFFE0B181CA6FD14B0653892CE38C9C448AACF61720357F1AE3A3118644D1EA08AFC1C3066E8F7FDB06680BD28
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\60cdb687-b45b-407f-90af-e76a8f6bea85.tmp	
Preview:	{"expect_ct":[],"sts":[{"expiry":1652415812.317662,"host":"CJ6kx0n19VtUkGfz4J6tLFRfDatw73CAqzbGpnezKw0=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620879812.317667},{"expiry":1623471813.802793,"host":"Dg14fIaciUHGX6Lc+OnYmaNiAA/ADiwumtIyPrC3d6U=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620879813.802799},{"expiry":1636659677.156215,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620879677.15622},{"expiry":1652415798.545467,"host":"Hi4bEdMq563Qsqn4sVyUls/uVk7U80lxMa3wyWVUqWU=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620879798.54547},{"expiry":1652415813.707595,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620879813.707599},{"expiry":1652415824.789931,"host":"OJAwwDug+gPr+xWjx2kFIFhHDQULu5ljftVMMZ74I4o=","mode":"force-https","sts_include_subdomains":true,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7902fe14-1c8f-4931-9586-a1f4e85a9442.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):	1207
Entropy (8bit):	5.578329908627083
Encrypted:	false
SSDEEP:	24:YQ7wU76H0Uhcgf/wULG1KUe4aUewb7wUeU3RUeHQ:YQEU76UUhciwU2KUe4aUeYwUeUhUew
MD5:	C5570634DC054C20DCBAB22531EB76C1
SHA1:	0E8CD745351B1EC2DC4882AEBB5E5EE255A864EA
SHA-256:	36DBD4D4977004F47044250174F00BE2C2CC9A538EF96BB62B49B3138A9F294E
SHA-512:	1150A160A2FB5DFFCEE6A5F0CBE61770386FE6B29D7B5BA37412F9B6DDB0BF3A815BD49130B0CA3050BFFF081E8E2699747E394FB897F44C79FE1C45D9D426E0
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1652415662.310942,"host":"OJAwwDug+gPr+xWjx2kFIFhHDQULu5ljftVMMZ74I4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620879662.310948},{"expiry":1633015352.675531,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601479352.675536},{"expiry":1652415662.084715,"host":"YBf+o277nAvW3A1uFG7ThwT6zuF7asaeDH6RPNOXinc=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620879662.08472},{"expiry":1633015352.520557,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601479352.52056},{"expiry":1633015352.455722,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601479352.455726},{"expiry":1633015295.599948,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7f3d5d9b-8fc7-4ed2-825d-4cca2e3549d8.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):	1709
Entropy (8bit):	5.579016578416879
Encrypted:	false
SSDEEP:	48:YWVwU9EU2v6UUhc2eUMwU2dKUmaUeYwUejsYU3hUew:4UuUtUUa/UxUYKUmaUsUFYUxUD
MD5:	7043E75F2DB14CC37ADECE05B59C081A
SHA1:	C9BEA6558D12B526583BDD74476BCF84C8E1B25E
SHA-256:	F7A9BC5D2BCA5F9DD18F4E62E9865573D76DD4335C6D66A287F7EA19EC81C38F
SHA-512:	1D3A573A2AC50B3BA16C0829725D05E326C448494F8A2B4FECCC851C386A120C2D2B2197AF3F1A8FB49FAB3D3D9BA7567A96CD62C292B199C9AB5706D299E09
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1636659677.156215,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620879677.15622},{"expiry":1652415684.673371,"host":"OJAwwDug+gPr+xWjx2kFIFhHDQULu5ljftVMMZ74I4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620879684.673376},{"expiry":1633015352.675531,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601479352.675536},{"expiry":1652415676.7291,"host":"PmHKo9+NfFu9AjQSxw3MoTtfuXIu9G3fM8KGQt4xie4=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1620879676.729106},{"expiry":1652415684.025216,"host":"YBf+o277nAvW3A1uFG7ThwT6zuF7asaeDH6RPNOXinc=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1620879684.025221},{"expiry":1652415676.574645,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\981d5f2b-0d96-4910-97e2-f63e4deb906e.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):	6526
Entropy (8bit):	5.1961710349170875
Encrypted:	false
SSDEEP:	96:n2Xb/O7k2t7aAVqQxku2JCKL8yky1ykuj7nbOTQVogwn:n2Xbn2x9Uq24KrkyAkuHc
MD5:	993B2D08E75060DB5AB759060D13049F
SHA1:	40B4EE4942C3AC02D957A8CBAB52EF5829937BB3
SHA-256:	3E3F9C3CB98AF044D473B02D2E9FA634967414AA2AFFE70A74F95B4CAD738B1A
SHA-512:	6949A29F6936FD45DD82FFA1AC278FCD988FFEF830F3D24C1652CD7CFBF843CB2C294BDB3EAA81D0AD9947FC8E3AFF5A15C1483ECF27594F9565DCBC5B6F9E5
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\981d5f2b-0d96-4910-97e2-f63e4deb906e.tmp	
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13265353249338570","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9a80962f-4dcc-460d-9854-a9f4a41faf39.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):	6568
Entropy (8bit):	5.200457072723071
Encrypted:	false
SSDEEP:	96:n2Xb/Omk2t7aAVqTxku2JCKL8yky16k5JtrbOTQVogwn:n2Xbk2x9Un24KrkyUk5Xg
MD5:	4E6F120F10AA000E8983C79FB3C37171
SHA1:	C8E6051DD1A6129CAFF023C6984B6E3DFFB56C29
SHA-256:	09A766D9BB2E70D1F8D52CABB7A03F6FDB3BBC0CF5ACBB87F299B20D76A134BD
SHA-512:	EF3CA6AFEAC2328E8DD3F4D0F16C06174FBB410C261A3554EAC5C37C7F36FF6D0C6EA9B5BBBB789E17FB7AE4A73FC1BF25FD15CCFDE7D30FF071EDA1072D3CDD
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13265353249338570","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245952891998324","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245952963463509","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1501624"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	340
Entropy (8bit):	5.096496673135432
Encrypted:	false
SSDEEP:	6:mX7n4q2PN723iKKdK9RXXTZIFUtp87saJZmwP87FsDkwON723iKKdK9RXX5LJ:s7n4vVa5Kk7XT2FUtp87saJ/P87FsD5D
MD5:	69BEA96E688BA70C5AB83067AD50C96D
SHA1:	B119FFBD9C53A6275BF6E18C328E2B901ED8BC14
SHA-256:	301C1B3F95B93EC0667EEFD0444A969A10FC5A357573BD7434FDA54EE4DE2CB3
SHA-512:	056EE6C3EEFA17DDBBCFD4325C376E4895EDA39554285990EEF7B8B0DDC7A92BF4AC9352AD684AE8EF3BAD6F0F43DDAD9B616BD7E4B88785970C11AF78E56 2D9
Malicious:	false
Reputation:	low
Preview:	2021/05/12-21:20:59.029 1b20 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/05/12-21:20:59.030 1b20 Recovering log #3.2021/05/12-21:20:59.031 1b20 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.099985547314556
Encrypted:	false
SSDEEP:	6:mX7yN4q2PN723iKKdKyDZIFUtp87jJZmwP87WDkwON723iKKdKyJLJ:s7yN4vVa5Kk02FUtp87jJ/P87WD5Oa5A
MD5:	4C29590C5BF0C7EE81BF59741B7320AC
SHA1:	41962855120E1C33001FA464275FA70520D4983B
SHA-256:	B24C81B1405F1325F7B623313E8D81FC23033405A8FD7D127CC2CCEF851C713F
SHA-512:	E0ED71E8942AD6C9D219D45E3512521BBB3A4740041F3112492A213C0C4965A5A8EFE0653AB48B2E4C30151E1833DCC368240F83BE471E26D376E2AA09FD16B
Malicious:	false
Reputation:	low
Preview:	2021/05/12-21:20:59.024 1b20 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/05/12-21:20:59.025 1b20 Recovering log #3.2021/05/12-21:20:59.026 1b20 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\00a73600649a63ce_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1145
Entropy (8bit):	5.6732997607888676
Encrypted:	false
SSDEEP:	12:Q/GpDN/VjTm/GpDEq/VjhTm/GpDKN/Vam/GpD6K5Z/VbX7m/GpDweb/V3O:bDN/dFDEq/3FDw/sFD6qZ/l7FDw4/l
MD5:	F5919DFC0BDD8060A5DD7AC7390C6E69
SHA1:	D89035883121A9ACD932DC1844D17A5441A95C55
SHA-256:	502DD5D9793683DA5507DDEEBE2EA395457116E926807DEAFB61C02E3DF4216A
SHA-512:	E60D3CE3FC139903558C0FCB07B19CBB462AEB7B8030E8AEC02E3BB141BB63A67A208373512D3554F07825B29068237DC98625EECF3E43AE86820B17975F202D
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/>o_.. /.....(.....q...|.K...y.....YL...;..>J..A..Eo.....".6V.....A..Eo.....0\r..m.....a...&[....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-951622910&l=dataLayer&cx=c .https://adobe.com/.q... /.....f:.....q...|.K...y.....YL...;..>J..A..Eo.....aM.....A..Eo.....0\r..m.....a...&[....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-951622910&l=dataLayer&cx=c .https://adobe.com/:.... /.....SD.....q...|.K...y.....YL...;..>J..A..Eo.....-.....A..Eo.....0\r..m.....a...&[....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-951622910&l=dataLayer&cx=c .https://adobe.com/..m.. /.....Z.....q...|.K...y.....YL...;..>J..A..Eo.....u|.....A..Eo.....0\r..m.....a...&[.....keyhttps://www.googletagmanager.com/gtag/js?id=AW-951622910

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\00af15e6f7222ed0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.785273265992884
Encrypted:	false
SSDEEP:	12:NE3Gyi/g4oux2peyye3CMx6sDPViH2NRmxAC4GN37N:NEWyi/gBuyeyyeSmDN/OxACzNrN
MD5:	E9585D6B6CC8A91E38782C56AA6A565E
SHA1:	21C35046EA2AD139E2E686D3184307510FB7EBEC
SHA-256:	59668CA5277EE12820B673DBC73B375AD76539AE7EBD8EF433F28F6BD0490F01
SHA-512:	124B4D0A70A76F589378C69ADE1CE388D000C4C906E94CC7890E5887E1FB961907700D60D07D8293D9B41A31789EC3E0737F475DEF51ACB00A0BBB8355284D9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....^....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/951622910/?random=1620879724352&cv=9&fst=1620879724352&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=2oa550&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... /.....R.....y....9.D.5...r.%Q..r.|.G....R..A..Eo.....S.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\01e4a1902bbe068b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	739
Entropy (8bit):	5.799978233811547
Encrypted:	false
SSDEEP:	12:g/oE3xjt9ueoux2pmYyye3CMx6sDPViHnzj2fP1nCUAKmxACNkuPr:bEt/kuyRyyeSmDNYzKO9xACNkur
MD5:	AFC02CFC1740F9C7F03B4212718BBE55
SHA1:	7E741D2993F0250B935FD7F769F119610817B015
SHA-256:	02A8586F69A0C2212BD7528B80B70594C239141AD14C7805F4565DBDD24B79A7
SHA-512:	FDFA777BED147137BD40D74B47BFA53F8F3E6DEE0BA015403DFD87EB578C9ACA8A391B262B96A36BA4917608E59203FE15BEA7378AF4A9ED8BF12E0530288475
Malicious:	false
Reputation:	low
Preview:	0\r..m....._...O....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/983956512/?random=1620879708280&cv=9&fst=1620879708280&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=2oa550&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/.H... /.....7E.....#`.c6V#.._.....%.;F.~.T...A..Eo.....K.....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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\04e3f25e64ef23bc_0	
Size (bytes):	13832
Entropy (8bit):	5.856322474710908
Encrypted:	false
SSDEEP:	192:vRcME7lq/rEYOHAZBsEADQdUo5bNrxmujQqhYvK8c2ZTVUw:dwWhOHunaExzNhYCVaTVUw
MD5:	16BA299658AF4E675428330B99875AFF
SHA1:	2681DA7A67565C472EC448D229262C0A204C2C59
SHA-256:	011A1E4A37DFA866B842506C9C454F97256700F59C5DC5FD8BB373FFF11B1A42
SHA-512:	F94F4895D92948826D30550E3B83A3726AC8A4A49F0823FFC2BDAFDA82021515BDA6115A306725403E56A1346142B969862D72959ED2FE45CEA3623680189D02
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.....M..I.....A..Eo.....'..J....O.....3...j.....H.....(S.d..`.....$L`.....Qc.:d....window....Q.@.....Typekit.....a>.....M...QcD.e.....1655249...Qb.h.....c.....`.....M`.....Qe.....tk-proxima-nova.(Qhni.%...."proxima-nova",sans-serif....(Qh.....tk-proxima-nova-condensed...0Qj.#..#..."proxima-nova-condensed",sans-serif...QbN!.....fi.....`.....,Mi....V...X...Z...\...^...`....*...*..$.....Qb.EPF....fc.....`.....,L`.....,a.....Qb^s.....id..`V.....Qc^~.....family....Qd"..Z....proxima-nova..QbN.....src..lQy^z._...https://use.typekit.net/af/e030d3/00000000000000000000158d3/26/{format}{?primer,subset_id,fvd,v}...Qdz1.....descriptors..,.a.....Qc...[....weight....Qb.....100..q..!...QcRs<@....display.....Qd..f.....subset_id...`.....,.a.....

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):	77324
Entropy (8bit):	6.183804904369285
Encrypted:	false
SSDEEP:	1536:uce+j8tV6mBmgX3/ng0QU+f6PC7M/yYcfM3ogvXLv/Q:uNnF4gX3vfC7MKYPLvY
MD5:	B2DD7CBA4DA022CA713104AF29CC8861
SHA1:	DEE81DFC391752D6D5000435165C815219F27921
SHA-256:	DB28A36940C1471859681634B6724DF7A005E845B0AC18C64ABA2BD9069E3BE6
SHA-512:	6D9735739123AFB3CAD52D327ABEA96218DD68B9C94BDDCB02827726800D20F63010F3ABF8A0A28DDA894FCE735DA48E9BC7D27335CB74141429BD036543669
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N...f.n....._keyhttps://cdn.cookielaw.org/scripttemplates/otSDKStub.js .https://adobe.com/..|.. /.....^...T.Q..'nm..;...m'..E...r.4.^..A..Eo.....;.....A..Eo.....0\r..m.....N...f.n....._keyhttps://cdn.cookielaw.org/scripttemplates/otSDKStub.js .https://adobe.com/.....'..C....O.....a....F.....4.....(S.@..'<.....L`.....L`.....Qd..;V....OneTrustStub.(S....`:.....L`J....@Rc.....QbZ._.....ee....Qb.sAB....te....Qb.....oe..b.....l`....Da2.....(S..`.....L`B....8Rc.....Qb..NE....c...a.....Qb.QL.....ae..`....Da&a..J.....(..Qc.-.....iabType...Qd...,....iabTypeAdded..Qd..V.....crossOrigin...Qc.....isAmp...I..QcB.B.....domainId..QcJ.jp....isReset...Qd.....isPreview.....Qd.....geoFromUrl...(S...E..`B.....L`b....4Rc.....Qbb.....o...`....l`..... Qf.o.B....addBannerSDKScript..a.b...m.....0...1..QbrfX.....IAB...QdJ.^....getRegio

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0bcfd05c4e8b8f53_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1076
Entropy (8bit):	5.693424747640042
Encrypted:	false
SSDEEP:	24:b5M6lHvp5MRxlPHyp5MclXHzp5MXclHs:b5MSPp5MRxtSp5MUXTp5MXgM
MD5:	CB36595DC49A400602C86A2CDFBBF222
SHA1:	9235DEFFFCD4CDEA66735EA1C3642821715887CF
SHA-256:	384E644FF0B1569D83D155050225D57D247E4CA4781B096330C6A2729B3755DC
SHA-512:	0B46B26CD855872F8ACB4E7BE9DF1D46C35A4B43BC84675844B3367335440F6D5D2E111B4A23A2B08BC08D6C01566948F3E1E1A4141CE603DBA73589F2D10BD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....zZ...._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC60ae8fab30be42269b5f052e4064e263-file.min.js .https://adobe.com/H,O.. /.....o|U.../..H.N..|.!:~..A..Eo.....l.....A..Eo.....0\r..m.....zZ...._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC60ae8fab30be42269b5f052e4064e263-file.min.js .https://adobe.com/eE... /.....7.....o|U.../..H.N..|.!:~..A..Eo.....W9.....A..Eo.....0\r..m.....zZ...._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC60ae8fab30be42269b5f052e4064e263-file.min.js .https://adobe.com/+.e.. /.....X.....o|U.../..H.N..|.!:~..A..Eo.....y..f.....A..Eo.....0\r..m.....zZ...._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC60ae8fab30be42269b5f052e4064e263-file.min.js .https://adobe.com/a.... /.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\10eb3732fd97b16b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	722
Entropy (8bit):	5.78210521556892
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\10eb3732fd97b16b_0	
SSDEEP:	12:R1E3xjxdkA1oux2pmYyye3CMx6sDPViHWC2/ohJuXPmxACxe3Q:XEt7YuyRyyeSmDNJv/juxACxQQ
MD5:	14A9EB75719902539C3592C29A898432
SHA1:	087C4D98E0D23B814DB4DE39CE4810876E679167
SHA-256:	83FDBA5B2F2348BCF359C873479ED27201835E6E27F357E881A3528859E862A4
SHA-512:	13C99944A54C80814E929FA9008992E4C8FD7B70471BD2D9E12B38B3F0D8B0F55D01ED052BFC7A556B0A94D94EF21373C5AEE86FA05463D624C9DBB7C929D8E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N.....G...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/983956512/?random=1620879701650&cv=9&fst=1620879701650&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=2oa550&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/5.... /.....+.....a...D.h.l.....x..3.Q*n.Y....A..Eo.....@.0.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\121f6dee74be6bdb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94200
Entropy (8bit):	5.772895189447203
Encrypted:	false
SSDEEP:	1536:RVx+CGdcf2khg1kKjMFzK4jp8kcCFgsQ9uWRxRu8orUrtVXi9G1qvSPi:Rn4dg2kLdY5kDFgsG7RurrU/b1ql
MD5:	5A4BEE37F3563877849020266D4A4F09
SHA1:	24EAECD3DB31B90227839C7C0A639ADDA3B690F5
SHA-256:	3225538F05D847E9D5B4E6135F6F680325A740F6FD8BB4696A0AB012BDC22A9A
SHA-512:	1D6F5AFBB7BC30AF3FC8288AD1B56EDB7B8820BA3128293AE7AC605DF8C62BDE854A13DC1C38E33E1DD64643B1FFEF95AB3F900F7E42A8DA2C770282349C0412
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...(.....A9C4AC75DDE272C6B803BD90C0AF297E96E17CCC5DD886152280C4862B2D8716.....'.JN....O ....n....Z.....!.....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....*.....Q.@B.pv....module....Q.@.....exports...Qc.....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.....QbJp8.....d.....Qb..aD....e.....Qb.....f.....Qb.?.r....h.....S...Qbn.Q!....j.....Qb".....k.....Qb..r.....l.....QbfG.v....n.....Qb...N....o.....QbZ`E.....p.....Qb...a....q.....Qb...Z....r.....Qbf.QB....s.....R....Qb.....v.....Qb.....w.....QbJ.....x.....Qb.....y....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1adee9e8e0f07959_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	450192
Entropy (8bit):	6.161723869763289
Encrypted:	false
SSDEEP:	6144:Vv3Irug4zYyqt0ueRwy0YBHItbAbGJRcI/g0cWehNU:qiLnk4wWItbAbGJNx1eha
MD5:	D10D2A9EA85B5BEA596555596B153BDC
SHA1:	2A450517F5A2269AEC6181C6DB944D5E3EDD478D
SHA-256:	B709A294D2581C89FEB55E571770ABEA92E8ACCC8084A2EFD44C532B8A842C1
SHA-512:	600BD1D270D9AEC26765F7A484BFBDAD1287D852166C01BA8341614F1AEEBD6E031F089F4FE8DD9489C8255D3EDD2625D197E09692F9EB5BF8524841F6C0F83
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....A76D02127A130EB42F8DE51D72F268A0F8227A7DF39FB3EB07E43C5D46FF3D5B.....'..U....O.....:.j.....(...D.....4.....x.....p.....(.....H.....(.....H.....,.....L.....$.....@.....p.....8.....(S...E...`>2.....Lc`...*.....Qc6:.L....window....Q.P.~.h....webpackJsonp..Qb.5.7....push.....`.....L`.....`.....Ma.....`.....`.....L`.....`.....Md.....`.....Lat.....E`....Ea.....E`....Ec.....E`....E`....E`....Ed.....Ea.....Ea.....Eb.....

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):	5.433461901974198
Encrypted:	false
SSDEEP:	96:Fz3GsPo/oicNCDGRbJTwJycAzQBk7hkhnnmuyWw22Nge:t3cW1B9wJyJQ67ChmlJ23e
MD5:	3F4713F83AFE87AAD3C86499A645C0EF
SHA1:	81AC871753BBECA86FE2029B4EDEFAC78258B31A
SHA-256:	1A433ED4412D8C7C06B0235CCDFB72FBB93A4D8005351EF370E4BBD258526A83
SHA-512:	80967488CAE28B941AC68C13234CE7207051A337907280B51FC6F08FD572E20DAAEBE68A4C81E9DF0EBD8612D1D112540E1D0BF58A01A9720F56E25C6CD8C46

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1aed6b6619289abf_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X..../....._keyhttps://www.everestjs.net/static/le/last-event-tag-latest.min.js .https://adobe.com/..=.. /.....T.....d....hbo)&.-.d..B..U..l....c.9}.A..Eo.....G.p.... .....A..Eo.....=.. /.0.....'.h.....O.....M[.....(.....(S...`d....<L`.....(S.x.`.....L`.....PRc$.....Qb.....d.....Qb..T.....s.....M...R....Qb.N.H....l.. .d$.....$.....QbNT+K....r...`....Da....X....(S...`.....4L`.....4Rc.....Qb.y.....t...`$....`....Da:.....Q.@.9c.....require..... Qf'._.....Cannot find module '..Qb2.....' .....Qe".&.....MODULE_NOT_FOUND.9.....a.....Qc.....exports....a.....Qb.qW.....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`P...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):	2276
Entropy (8bit):	5.7007819001507825
Encrypted:	false
SSDEEP:	24:eHS3IHE7IHOpIH7xSQNIH6IHMIHg3YIHKPNIHWIHgyDJg:eSIk7IupIbRIaIsIGYIqPNI2IAyDJg
MD5:	563C446C9B6B5B096E81E71F2196277A
SHA1:	7E11044F47B30311289DCFC925B075D84068DB11
SHA-256:	FC14AD8FC615FC94E7E6A663CFFCCDD59E5DD650F626E76987355AA5EC9CC925
SHA-512:	58B4A48C12FFB128533F3A3C549FCB8E3D367EE00881873DF9A388571CFF35DBFC7480389068A362002A4011037838BD598C97E082784D6661386F86CDF2E23C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....._keyhttps://cdn.cookielaw.org/scripttemplates/6.9.0/otBannerSdk.js .https://adobe.com/4.... /.....b.....W(.fp:....e.....O.....Vq.t....%..A..Eo.....@Zw ....A..Eo.....0\r..m.....V....._keyhttps://cdn.cookielaw.org/scripttemplates/6.9.0/otBannerSdk.js .https://adobe.com/f^... /.....8.....W(.fp:....e.....O.....Vq .t....%..A..Eo.....K(.....A..Eo.....0\r..m.....V....._keyhttps://cdn.cookielaw.org/scripttemplates/6.9.0/otBannerSdk.js .https://adobe.com/,fG.. /..... ....W(.fp:....e.....O.....Vq.t....%..A..Eo.....A..Eo.....0\r..m.....V....._keyhttps://cdn.cookielaw.org/scripttemplates/6.9.0/otBannerSdk.js .https://adobe. com/,fG.. /....FE1D2E8509C4DC984BB5B4666F07911FC3439A41D5A8CE77C4E7C970C9B8E655W(.fp:....e.....O.....Vq.t....%..A..Eo....._.L.....A..Eo.....0 \r..m.....V....._keyhttps://cdn.cookielaw.org/scripttemplates/6.9.0/otBa

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2928343e5bb5fca5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	600
Entropy (8bit):	5.785963631554422
Encrypted:	false
SSDEEP:	12:vaE3xjYXhsoux2peyye3CMx6sDPVcoYN/C8XxRzv1:iEtYXhVuyeyyeSmDNcoYN/Cczt
MD5:	6AC7A2DA5AA02C4CFD6C066A7F8DC55D
SHA1:	771677CAF5C5A194F391E06E1ED037332088C16B
SHA-256:	14F12C6C9F3BAB756C33A5184741DD3DD10AB87C7586E643FA380D8843928724
SHA-512:	36D9585C90EE654D3B400EFBCA8887A93180B7FDECCBC898F0D798B154EA89129598CC241A683D46CA14A32700A85312DDD9D199C8E84FB9818127ECD9A616 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....l.....keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/983956512/?random=1620879705811&cv=9&fst=1620879705811&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=2oa550&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/.'... /.....;.....T.1..ax....l~../.R.^...<..Gb....A..Eo.....q..3.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2a0cbdd7970c264d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.822171658020848
Encrypted:	false
SSDEEP:	12:8E3xjy+II/+B4oux2peyye3CMx6sDPViH2NRmxACb9utQmg:8Ety+II/+BBuyeyyeSmDN/OxAC+Pg
MD5:	28C890A20C1895EFCB0E4BCB63C5B3A6
SHA1:	ADD0D7111C21DC85BB1DFCA55676ADF5CD92EE25
SHA-256:	BC603916838A67CA70917D00C4121F1BDFCD09743A02C7CF468D5E7559188AE4
SHA-512:	7FA6B205E5B0A6907E408E6F4579D1E1944EDFFAE182BE9C0B63104B8D0AC5E8A3B72248B81FF3716B62DB292E157CE52D6A64DF7C2C697E10A0E0EAC9CB7E DE
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2a0cbdd7970c264d_0	
Preview:	0\r..m.....0....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/983956512/?random=1620879724358&cv=9&fst=1620879724358&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=2oa550&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.....Ot^./S...pg....'.....S.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2ac26e1537710ace_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92088
Entropy (8bit):	6.157540403810358
Encrypted:	false
SSDEEP:	1536:5CS0bUhZBjghodOZi0zWxl0JWenSmUfcDfQOBPq8MBI:SYLFOCxlUWenSXcDfQOBPq7BI
MD5:	39446BC1DF6FF0F9C11050345795D811
SHA1:	0770C83EE35B6B79E4AA883C6723B70EBF6ABB39
SHA-256:	D5D18E6D7D1FFAB6450D6ACAA0EC1C9CDDA401110C441AF0DDD46B950EF83F99
SHA-512:	1B21DD22BDEFAEF8BD208EE0E4B00CCFDC06D4AB9E0B79722FF18225F71E6A3A807FC1D37651FC59195E3E78FCEC313EA48171450469F036C881E444C604B28
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....8705829C11F004CAE9C459A5566A105D88AFAD9F62C1EEAA62C1A89FA53A4F11.....'.....O....xf.....).....,.....(S.m...`.....dL`.....(S.0.`.....L`.....0Rc.....Qb..N.....r...`....I`....Da.....(S.t.`.....L`.....TRc&.....Qb.}.....t.....Qb.I".....n.....Qb.R.....e.....Qb2.X/....o.....R..d$.....$.....A.`....Da,...~.....(S....`.....4L`.....4Rc.....S.`$.....a.`....DaP.....Q...Q.@&O.<....require.... Qf>2<j....Cannot find module '..Qbv.Z-....'.....Qe.Ty....MODULE_NOT_FOUND.9.....a.....Qc..i.....exports....a.....Qbz.}x....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\2f49560d02f8d583_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	57329
Entropy (8bit):	5.654575553796878
Encrypted:	false
SSDEEP:	768:mnbqyDWz+DrKXG+R1P5EFpAvCxuqhex++y5md/RNF0/4fMmQ6AWX6XDDNXdJSUTx:mu5QYRE3DxMxtyK7F0/bTPJki
MD5:	EB9319454A2BCA0A21F06C6156AC4FA5
SHA1:	19D805FAE23683581A757B526C8CCA5F557D69D8
SHA-256:	CFB2582810AA4818833F12B95040160B4A1345C587FB9C2238D146177DBCCD0B
SHA-512:	05E85ABBC524A6717CCBF6A3CBDB7A180AEDDE5DA21CD7F4EE5A181A78044765384176E24010EB01C0D3089E84C55D069E8B7B53464E26FD47EE0D4E339CD75
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Y.....tZ...._keyhttps://client.messaging.adobe.com/latest/AdobeMessagingClient.js .https://adobe.com/..... /.....4.....^i.....AH..W..Qq.....s..A..Eo.....j.....A..Eo.....'..8....O....8.....;.....(S.H..`L.....L`.....(S...`.....L`.....Q.@..D....exports...Q.@j?lz....module....Q.@6V0.....define....Qb.@.....amd.. Q.p..:O....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`B...D`.....`....&...&..!.&.(S...`.....L`I....(S...`.....<L`.....@Rc.....QbBM|.....e.....Qb..2.....t.....Qbv..'....n...b$.....I`....Da4.....(S...`.....L`.....a..$..a

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\301af8026e76f451_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1883
Entropy (8bit):	5.684887632977885
Encrypted:	false
SSDEEP:	48:D5MzLqaV5MzLSnV5MzLJtPV5MzLrk0V5MzLUc1V5MzLLVoIV5MzLwdN7:DOPqIOPSVOPrNOPrk6OPUGOPpXOPwdN
MD5:	748E97D014E7E74B414EB8A43FA4EBB9
SHA1:	CC6599B5520A41AC61A4DFD21F8D6AA3C6B7BACC
SHA-256:	52D11B07372C53D6CCBB0B91E9863A7167916A709E5CB2E098FC17CF1B098102
SHA-512:	887457BF38BEC9230DD78E10EDC93C5ABD7F061DAAAB4C645E0E5C1DEA0EC72F9BF69BCCC9FA4AA3C4296E3FC6DC74CDF83C61B3F16C8E5558E30E8C4B565A53
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\301af8026e76f451_0	
Preview:	0\r..m.....&.j....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC1a83c357d323419db9d2ba211efeeaae-file.min.js .https://adobe.com/,z... /.....k..i...G.>gh.j..&.hv.}..PU...A..Eo.....M.....A..Eo.....0\r..m.....&.j....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC1a83c357d323419db9d2ba211efeeaae-file.min.js .https://adobe.com/%.E.. /.....x.....k..i...G.>gh.j..&.hv.}..PU...A..Eo.....t.....A..Eo.....0\r..m.....&.j....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC1a83c357d323419db9d2ba211efeeaae-file.min.js .https://adobe.com/.6... /.....7%.....k..i...G.>gh.j..&.hv.}..PU...A..Eo.....j.....A..Eo.....0\r..m.....&.j....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC1a83c357d323419db9d2ba211efeeaae-file.min.js .https://adobe.com/.l... /.....5.....k

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\30ffca376f519f71_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	198
Entropy (8bit):	5.333197277101813
Encrypted:	false
SSDEEP:	3:m+ly1WllLA8RzYWQtce1x/PWFvD4gt1ObHtlHCFlllNa0R9wYPST3LM7b9kZmY3Z:mnW/VYWsdP/PdbyfEpYqPoZh+DK6t
MD5:	EBD309283AD556E3F9EB8174E4D78B1B
SHA1:	CCED5F2B1381D2179E0C63E8E62C8E1589CCE326
SHA-256:	CA94E29ED48E1E9CE58D7B9D177CC5B1CDD69AC42879B52C43A92B5CF7763839
SHA-512:	A23BAAEDC29EB64506665B4A71B5AD1BE3EA65C995506A409F493A10A386DE813D8D770B557E41ED056D0B2559F52322268F6CA630397556912DAD4386CD503
Malicious:	false
Reputation:	low
Preview:	0\r..m.....B....._keyhttps://ds-aksb-a.akamaihd.net/aksb.min.js .https://adobe.com/..... /.....mt.....=...he..t..MUB.A.#x.>(v.n.);.~.A..Eo.....E..t.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\327de93fb0e7a719_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	355856
Entropy (8bit):	5.770656399973949
Encrypted:	false
SSDEEP:	3072:zSp8TLJMT4NKVEqU7QnUWTvevqB7GvANWLC5sduHNTqgpPROySrAk7fMEyLPq:Op8PJ/WEqU7QUWT3aqpZOyg0C
MD5:	A53D909E6D906DB576203B78730675E2
SHA1:	65B7DDC050DCFB1EE96E5F5023275E28AE164674
SHA-256:	3250E66721E984C5352937B04242773990D757606F95026F140B21D76CA0C36B
SHA-512:	87CAC9ADBF9EE5F8B08E3F85B3AA572F4883C0D647C1F52A8B7A4432630A10E066BE990BB8EA28AA07EE1E046CA39ABB3B3762A79FF77BA9D503A41B6E4E8F01
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....L....44ABFBF7918EA02CDAA8F85A4455B7DBFEA9519C2D15F5CC6553B655406F29E4.....'..;....Om....k..843H.....X'.....d.....`.....d.....l.....T.....p.....(S.....`.....M.L`.....(S.``.`z.... L`.....@Rc.....M....O...Qb.h.....c...b$.....I`....Da....~....(S...`.....L`.....Qc6\|g.....exports..$..a.....a.....Qb^s.....id..C..Qc..9.....loaded..H.....Qb^.v_....call.....K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&...&.'..W.....-...(.....,Rc.....`....Da....<.....!.....e..... P

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3556fd62a32d504e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	739
Entropy (8bit):	5.814811119663643
Encrypted:	false
SSDEEP:	12:7E31f1KjlYoux2peyye3CMx6sDPViHnzj2fP1nCUAKmxAC8VRiqZR:7Elf1KjlhuyeyyeSmDNYzKO9xAC87iqD
MD5:	A1B35D28B3118882881F997D47A29461
SHA1:	A4BA3385E5B4CADCC29DE925A19ADFBE83D3DB3B
SHA-256:	7E477F92FF1B803ADF7BA7AA4AC8BD651C59A540789AEC07F5AD33141ECAA0BF
SHA-512:	22BC19C4408B66AE8E6EDC9460466B24113FC9C8A178F12AC88A12C77B0293E39A6AB81B3028E0618840610184AD5DF6023B08ED6ED6763CE601D56EAD1E428
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`.....`.....`....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/987390658/?random=1620879706908&cv=9&fst=1620879706908&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=2oa550&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/.e... /.....D.....V....qU}.+Y.e..kqV.9..e.]^.=..[.A..Eo.....b.....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):	5.468095387693402
Encrypted:	false
SSDEEP:	12:aHBWAIwFVYHtv4HBWAIwopVYHtf4HBWAIwCx4VYHtAlN:mBWVwFVYHFcBWVwqVYHpcBWVwnVYHq
MD5:	2897B6BAD7A6B5F6A235392A8D99036B
SHA1:	826B060AC050B7813C60D97EC1A4570AB251AE67
SHA-256:	97D042684E14173E6A8322AA01DB308EA4E4C1EC07CF474FE8B0A9F6025DFE0B
SHA-512:	EA28C3C09FEA6BCA9C1880B2567C7AE3A3479A51D03A02BF8E68606C342384C3FFAF2B88DA24CD146D5FA5CEDB1616CE0E95A7BED0051F357836C908B610C9E5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H...KX.T...._keyhttps://www.adobe.com/express/scripts/scripts.js .https://adobe.com/..... /.....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/.... /.....J.....t.U....x....<.....f...A..Eo.....l.Z.....A..Eo..... .....0\r..m.....H...KX.T...._keyhttps://www.adobe.com/express/scripts/scripts.js .https://adobe.com/..... /.....r.....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):	5.83438304143347
Encrypted:	false
SSDEEP:	192:1RcXYqnSczUhLUGoYOHsNB033A1QBU7cLcLdmtuP30Gvocn8vK8x2ZTVUW:gJzUpUG9OHyMuefGvb8CYaTVUW
MD5:	FF5EF20DA8DCFCCF272C89A4D2B43071
SHA1:	7592B0C24AAD32F05A2756EB877A40F4ECDE89E2
SHA-256:	1D8FAF724702FF69883938EC8E38D0A229DDD58A0E421D7C6D8E78C249F63C5B
SHA-512:	C92EF791532A2669AA7A9A7CC0F8CB9A24C7F2023714C78A8E7B7635FB6B7F8DDB5B3EB7B5A2ACBD05A976937272784A37413FBA1F9F3BC0DED6ECAA973EAA71
Malicious:	false
Reputation:	low
Preview:	0\r..m.....:....t.<...._keyhttps://use.typekit.net/onz5gap.js .https://adobe.com/?.... /.....bo.....F!g..k.89.n.....s...8....[R..A..Eo.....H.....A..Eo.....'.9G... .O....`2....73.....$.....(S.d..`.....$L`.....Qc.:d....window....Q.@.....Typekit.....a>.....M...QcD.e.....1655249...Qb.h.....c.....`.....M`.....Qe.....tk-proxima-nova.(Qhni.%...."proxima-nova",sans-serif.....Qe.g.....tk-adobe-clean..$QgR.+....."adobe-clean",sans-serif..QbN!.....fi.....`.....Me.....8...8.. 8.."8....Qb.EPF....fc.... .`.....L`.....,a.....Qb^s.....id..`.....Qc^~.....family....Qd"..Z....proxima-nova..QbN.....src..lQyJ..X_...https://use.typekit.net/af/949f99/00000000000000003b9b3068/27/{format}{?primer,subset_id,fvd,v}...Qdz1.....descriptors..,a.....Qc...[....weight....Qb.....700..q..!...QcRs<@....display.....Qc...c....primer...LQq.HQ.@...7cdcb44be4a7db8877ffa5c0007b8dd865b3bbc383831fe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\386d87b204bd71b7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.454392677514644
Encrypted:	false
SSDEEP:	6:m0FXY68E9xEEUgLEreY73lY3tYJzfZnK6t:pYg+3+tYJf
MD5:	E66573674212BC6A501474445A324C9C
SHA1:	9DA3C52F5C2CAB65F9D28074FB614F4C8F4C7B88
SHA-256:	E0E4CC53DB5BE437048F9ABD0BFF0CD09DAD575E306CCB6FDCE68C078173AC30
SHA-512:	CE7A943D872781C1FEA908A58B7C5AAC6ECF63BEFA9AB713242E9DB8204CDF8B0726EBC1055F085F67DA5C85DF1CB358F61BE785A3049F35F24809C96DCFEC33
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`.....w...._keyhttps://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js .https://greycottage.ng/.... /.....O.....l7..Q-..E....Lv..$.{.e..n....A..Eo..... [4.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\391462c089298afe_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	428
Entropy (8bit):	5.377247189244846
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\391462c089298afe_0	
SSDEEP:	6:mInY07A0NApRKPR/AyvYGXlrYkXnvwYabK6tWlnY07A0NApRKPR/3vYhrYkXnvw5:tMKPKS9MkXwNvMKP0MkXm
MD5:	285A822D631F6955EB10218403DB77FE
SHA1:	0427019BC74272DBC9E8A31335BDCF536B9445B8
SHA-256:	49879525A956CB4D731A84A0EE0AAD8FBA23187AE18B795D3C25754D780AACD1
SHA-512:	B7A5C96B4005B45C73D4E7EBD8082D3BB1EB41F50397C71CD5105D48E623AE105280BD43846220808E865BB06BBDA36B1ACF6F681AE5F6CEB1AA4ED2AA084E76
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...4.J....._keyhttps://commerce.adobe.com/checkout/js/fontfaceobserver.js .https://adobe.com/..... /.....R..<K.....b'/.dM?.L.wzk..A..Eo.....QQ .....A..Eo.....0\r..m.....R...4.J....._keyhttps://commerce.adobe.com/checkout/js/fontfaceobserver.js .https://adobe.com/..... /.....R..<K.....b'/.dM?. L.wzk..A..Eo.....A..Eo.....

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):	1170
Entropy (8bit):	5.692811704598931
Encrypted:	false
SSDEEP:	24:f3wkVdp3w4Vjp3wHjV57p3wHVvp3wyV0lT:f3LVdp3nVjp3kVZp3MVvp3VVg
MD5:	5EDEB3163521E38AF24DBD27767BBE4A
SHA1:	C40A8E97DF082F7D3BF82AA923FF20E682669F98
SHA-256:	5D65954E39DC8C7F2AFE89D33D39E04CCA5559D570600356BF74478F74A252F6
SHA-512:	853245F2FE544F29248F358224E23D380E8E33ACFBA20426E4719F7C848D36638F0F7298D2B424EECDB93677436C70C0B5A33033461867820B5D400D2A465189
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/.)\.. /.....1....DJ.D>5...K....*..... ..A..Eo.....}:.....A..Eo.....0\r..m.....f...P~....._keyhttps://connect.facebook.net/signals/config/1772359959706965?v=2.9.39&r=stable .https://adobe.com/n.... /.....:.....1....DJ.D>5...K....*.....A..Eo.....0.....A..Eo.....0\r..m.....f...P~....._keyhttps://connect.facebook.net/signals/config/1772359959706965?v=2. 9.39&r=stable .https://adobe.com/(.... /.....D.....1....DJ.D>5...K....*.....A..Eo.....F.....A..Eo.....0\r..m.....f...P~....._keyhttps://connect.facebook.net/signals/ config/1772359959706965?v=2.9.39&r=stable .https://adobe.com/.ro.. /.....Z.....1....DJ.D>5...K....*.....A..Eo.....A..Eo.....0\r..m.....f...P~....._k eyhttps://connect.facebook.net/signals

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\399d65171bfe4109_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	722
Entropy (8bit):	5.782833060512241
Encrypted:	false
SSDEEP:	12:5E31f1KHYPbOoux2peyye3CMx6sDPViHWC2/ohJuXPmxACTYo0dUv7:5Elf1Kq7uyeyyeSmDNJv/juxAC0okUD
MD5:	401B67F86E3477B5B7AE2D675694A198
SHA1:	CEED81C150599E453B4D5817A3AA52480B0AEFB8
SHA-256:	7D94599F1FF89D8D1AC5AF4FFCF8F1A3C6B7100D7B0B5B84D67EFD8C81DCDFA2
SHA-512:	C7172F77069328363DED1D8255E67CF207FDDBB6CB3AB071904E4CC8EEF1F161E08414FED9D76E7060F3CA8FD71E940AF42B3B7B6DBADF0836A45CD554F827B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N...\y=....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/987390658/?random=1620879701600&cv=9&fst=1620879701600&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=2oa550&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%20 Spark&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://adobe.com/..... /.....,.....}_P.d.....M.*kS..Z.8..1q/..A..Eo.....].....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3c3e507928304ed9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	450184
Entropy (8bit):	3.5800806654835036
Encrypted:	false
SSDEEP:	6144:goO7vD3xylyQ7LDGnlxYpgry3T3zoWBnH46/KOe90joPkSXG635/XKMHZsxav05X:gKI2T+WMbdFk7
MD5:	97E03E3EDB963BF3FE93782DB407F9BB
SHA1:	F0169DEB4F17E22D579AFBDACF849F3D5413EC03
SHA-256:	8A31CC21A7FA947B2FF97CF1529EDB2CA3137E9933951634F69D3B2C6EA0B261

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3c3e507928304ed9_0	
SHA-512:	C33D92E2627E027D2F7B0DDA2360E631D7B1B1DC0155549ED5F202A0CC54C528E2E68A5560B4B8BA28D4D68A9C3DBD3F9004EA626D81F54D50C6BE7391EBA3 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....EE2D21DE3F87B41F3D6F099D64D6ACDAFF37F5793003A5CCEA22E546293FAD63.....'.....O.....I.;q.....(S.t.. `.....$L`.....L`.....Qd:.."....localeBundle.(S...`.....LL`"....@Rc.....Qb.....e.....M...Qb.....t...b$.....I`.....5.a.....1...Pb.....10.a2...L....(S...`.....L`.....Q.@r... ....exports..$..a.....S.C..Qb.....I...H..A....a.....Qb..a.....call..!...K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&.(...&...&.'..W.....-...(... .....,Rc.....1.`....Da`...X.....e..... P.....@....@.-....LP.!.....?...https://spark.adobe.com/static/locales/en-US_bundle-6a358124.js.a.....D`....D`"...D`.....P...`$...&.. .&....&....&.(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\3d5529574664a4c8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1225
Entropy (8bit):	5.712013902736833
Encrypted:	false
SSDEEP:	24:34w3MYXKKpfjY54w3MYX5pfa54w3MYXcpfm54w3MYXa1pfL54w3MYXHlpfk:3l3M865l3M8e5l3M8T5l3M8aT5l3M88
MD5:	73CBB8FFBF87085E8788299A199B973F
SHA1:	8962063304CE22CE41FAEB3F6DE209017AC1B41C
SHA-256:	2CE0E54AE469EB0E7C46A84A292BFFDD618AF9742FA8F63BD51C3C189A8CE0B6
SHA-512:	AD7756AABA78FC562D257808362F83B6100AE23EF665A9736B25F06EA1771D4398F6C955293FA3273C9AF38469BBCDD4169CB0F5E720C6A3A19C37B3025EC1C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....q...>n....._keyhttps://sd.iperceptions.com/ius-359cd6b861125d638f6cea04ffb14739/29293_637562934893077826 .https://adobe.com/.J... /.....=.....8.!.. .z....=..\.....k{..{.).A..Eo.....Ra.....A..Eo.....0\r..m.....q...>n....._keyhttps://sd.iperceptions.com/ius-359cd6b861125d638f6cea04ffb14739/29293_6375629348 93077826 .https://adobe.com/..... /.....D.....8.!...z....=..\.....k{..{.).A..Eo.....Ld.I.....A..Eo.....0\r..m.....q...>n....._keyhttps://sd.iperceptions.com/ius-359cd6b86 1125d638f6cea04ffb14739/29293_637562934893077826 .https://adobe.com/.... /.....D.....8.!...z....=..\.....k{..{.).A..Eo.....6.....A..Eo.....0\r..m.....q...>n. ....._keyhttps://sd.iperceptions.com/ius-359cd6b861125d638f6cea04ffb14739/29293_637562934893077826 .https://adobe.com/..s.. /.....[.....8.!...z....=..\.....k{.. {.).A..Eo.....(;.....A..Eo.....0\r..m.....q...>n..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3f469e2e71221b43_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	180088
Entropy (8bit):	5.875128545230414
Encrypted:	false
SSDEEP:	1536:2eyT+X67DTWI7xqbUhYThsimLJz0er+OGNmO4ncLxrrb0kkBf8Md46U8PPB66R/E:2/T1DTd7gUHFOaukkkBf+3YBN6
MD5:	B4D53ACDE1D28C0A808FAEAA64CCE11B
SHA1:	FA37BC513E4BD6FF2DB36E3C63AB79884D6F34CE
SHA-256:	B780B3BA4F642104CF26B238F369DA90859089FEE59F20A6141632A7E8C789D2
SHA-512:	EAC7BE78E4924823F7C8F11E999F3502296917A1AB4C4CF3AEAF97B39836C0BEB03357E4E09538AE39AE3E7E4BED87E0C19DD7611A48D511336A281627B756C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....85926E018E7CF0ED8059DF9E7F7F7C9CD97B8ED39AE414911CCAC6C1C74B7F82.....'.....O9.....Y.....h.....p..... .....`.....@.....I.....`"....(S....`.....y.L`.....(S...5..`$.....L`<....XRc(.....Qb... .....e.....Qb.<.@....n.....Qb..I.....r.....Qb.....o.....S...R..e$.....I`....Da....6P...(S.....Ia.....Qb.....t.....@.-....<P.....0...https://spark.adobe.com/static/m-web- 5eef92de.jsa.....D`....D`&...D`.....`....&...&...=&..1.&...(S....`.....L`.....Q.@r.....exports..$..a.....S.C..Qb.....I...H..A....a.....Qb..a.....call..!...K`....D}8.....& .%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&.(...&...&.'..W.....-...(.....,Rc.....`....Da^...V.....e.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\410e8948813eab56_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	132
Entropy (8bit):	5.434276556282505
Encrypted:	false
SSDEEP:	3:g1zPdUnQyXUK3WskmjfbkE0QVTN8glJfeol0sBc59k44mkFtt:gxOQqUK3WhmjTkXQYoJf10gB4rw
MD5:	F6D22099124296956D9443DE8B853A0F
SHA1:	9E1EE25E38CAF77709E3FFCA7FDA96BAAD1500C9
SHA-256:	2C011DBDEB4AAE4A7373B0DBF33A37C17CDF31220A0C10E3FFE15CB86F44866F
SHA-512:	94DED4187F923CF538EEC4970817D9B71EFB186EA873E802B71793A65B507F761DE79DCEB88CC156561F74ACC58E82394BDA209F70083F7ADF0CB1819A67D39
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\410e8948813eab56_0	
Preview:	fd... /.....DD0081AE1C5A321EB6ECE1D944300A57FBEC8D32DC95152A3E549C181D8060BE.....R...\r.9....j!.....{8;\.A..Eo.....D..-L.....

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):	1015
Entropy (8bit):	5.4802106439398255
Encrypted:	false
SSDEEP:	24:YezXFRIe2ezIFRM12eziFRTw72ezPFRe2ez5FRk:rlgc+2
MD5:	33BE05B1817096013E53B7AAD4EECB21
SHA1:	D94E4D522897AB42D8E5AFE1E24F7717AD58DD2C
SHA-256:	3FC545BBDC917629F897933EF20FD48A20571DB7CC24D34A41B149F6249CEF44
SHA-512:	26C7372D3FD10DE356B03BFEE061B58F3771357CFECEE4CA8F88170A305BB79C973D70E00A0817A8415FD27F150BEB452E6173F2F9DDD0DFE21AE9128D315FF B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G.....!...._keyhttps://www.adobe.com/marketingtech/main.min.js .https://adobe.com/..... /...../...6.2.(Dqo...RT..^...A..Eo.....#.E{.....A..Eo..... .....0\r..m.....G.....!...._keyhttps://www.adobe.com/marketingtech/main.min.js .https://adobe.com/?.>.. /...../...6.2.(Dqo...RT..^...A..Eo.....A. .Eo.....0\r..m.....G.....!...._keyhttps://www.adobe.com/marketingtech/main.min.js .https://adobe.com/v.m.. /.....Y...../...6.2.(Dqo...RT..^...A..Eo.....%.A .....A..Eo.....0\r..m.....G.....!...._keyhttps://www.adobe.com/marketingtech/main.min.js .https://adobe.com/5?... /.....`...../...6.2.(Dqo...RT..^...A..E o.....i.....A..Eo.....0\r..m.....G.....!...._keyhttps://www.adobe.com/marketingtech/main.min.js .https://adobe.com/..... /.....{|...../...6.2.(Dqo...RT..^...A.. Eo.....A..Eo...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4fb7ad7f096851e3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	357
Entropy (8bit):	5.912088175875216
Encrypted:	false
SSDEEP:	6:myVYSHT8NWQAlKPUQy9Y7ZSYUnWqlZMEnK6t9K9THKRgU4vtZF:R7z8NWQCUUQwnWqqEpGVKR1m
MD5:	23C4230D02226E2C51C7DECC01B91257
SHA1:	662AF2B4DC0E06B3D8CC41966DEB39F49C5C0695
SHA-256:	E78CF7874ED6410FF8B7BEFDFA5429318AFEA3E5627732867B0D3CA24824C527
SHA-512:	557DFE0603615FDC777C24CE8582C9A9C9B7BF8026BAA42A38087515AC4A33498C2810277B1142119EAEFEC8F65779A30F4051A8BD359C8E204C6FA2AF56AEE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....'".....keyhttps://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js .https://greycottage.ng/.... /.....H...H_.j..R.o...e.....c!....A..Eo.....r]Ja.....A ..Eo..... /.Po..A9C4AC75DDE272C6B803BD90C0AF297E96E17CCC5DD886152280C4862B2D8716...H...H_.j..R.o...e.....c!....A..Eo.....O.iRL.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\50ebd0bb3900b07d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	128048
Entropy (8bit):	5.68833690784994
Encrypted:	false
SSDEEP:	1536:ZINZGIDZHZgqfnnjIldAzSatytC7LquADMytG1PWHO6OzjEIIa:ZgXFHZVfnsTiLsDMytiPXjFt
MD5:	C094B7B59E12BD5BDCE548BDFADEDE5E
SHA1:	312EE253A1B69B77799DB2CB840AC0C184098570
SHA-256:	F299C142D4CCF948B76E9F43B7D1777F06898E42BDB4510CAACBE4463FFE1A70
SHA-512:	78C815EB24A6531A671855E1D949A9E30D85602DE8A5F0F573924193C8DBEEAA0F6F1B6F556D970302338805906ACDDE8E1EED36F67BA0E1E3022076B5BF9A2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...kE.....7B7F2E27D9F2A0474F830339A2F9A91AE13807C17F5654EB1E83E2AEF143FCB4.....'..'....O,.....m.....x...L.....$..... .....d.....(S.)...`.....L`>....(S...`,....TL`&....PRc$.....QbBM|.....e.....Qb..2.....t.....Qbv..'....n.. ...Qb.M9K....r.....S.d$.....l`....Da....H....(S...`.....L`.....Qc..D....exports..$..a.....C..Qb.+6.....l...H...5...a.....Qbr..~....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-00a38324dab316803fdc74cba4ad7ab9.js...a.....D`....D`....D`.....y....`....&...&..Q+&...(S.....5.a.....Qc6:.L....win

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\528df7fa00e0aa0d_0	
Size (bytes):	856
Entropy (8bit):	5.413724247029239
Encrypted:	false
SSDEEP:	12:sz+OpoTam+z+OOTaIX7KTaNgz+OZwDTaY+z+Omo+TaS:AppCmpKX7H8pZCmpk
MD5:	E4D55707421240BEF8DDDED72EECF586
SHA1:	1577E55F2097A219AE110901469380A11236D2CD
SHA-256:	A26D93101C9E0DDFCBF27B22E2CCB90F870038C1AA1E194764AF5909C78AA002
SHA-512:	85C6970896816AFCBE34F2F22611BF88BB8F35DFF1EFD2F8A1E98CC782144105ED13585A07C989DB07F679C266BE5CD37F932EC6C3DA4B958CE60BD85C68FA E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....=...E....._keyhttps://static.ads-twitter.com/uwt.js .https://adobe.com/BgW.. /.....m.*.....[...%t]U.....r.8..P..q.A..Eo.....6T.....A..Eo.....0\r..m... ...=...E....._keyhttps://static.ads-twitter.com/uwt.js .https://adobe.com/.p... /.....8.....m.*.....[...%t]U.....r.8..P..q.A..Eo.....A..Eo.....B~... /.....a<.... .m.*.....[...%t]U.....r.8..P..q.A..Eo.....0\r..m.....=...E....._keyhttps://static.ads-twitter.com/uwt.js .https://adobe.com/E7g.. /.....X.....m.*.....[...%t]U.....r.8..P..q. A..Eo.....A..Eo.....0\r..m.....=...E....._keyhttps://static.ads-twitter.com/uwt.js .https://adobe.com/U.... /.....P.....m.*.....[...%t]U.....r.8..P..q.A..Eo... ...u.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\556dfd1078234902_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	336
Entropy (8bit):	5.891785891713527
Encrypted:	false
SSDEEP:	6:mnYgGKHR9IR5hwyTFLNsrt/zrUK6tOkPVMQcFVMLNsrt/zrW:idnORFLmR/zKJ4FVMLmR/zC
MD5:	95B8CF24F9FA26C6429434FBE4A25353
SHA1:	A4A4FB95E10253D78D21F0851B16430DB41C7B6B
SHA-256:	491BA458A9ECADCFECE6FE33A6FC04D1A538B709350450C41E4A8071D41093F0
SHA-512:	E208D9914A3440495F60948156A90C746BEB83BF03455D0B274E0FC6BB56A47906CDD8EB600AF556CADB07F39FD912187BE37A41B3BE6BACFFD7337EA8299BD 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H...~N....._keyhttps://spark.adobe.com/static/m-web-5eef92de.js .https://adobe.com/..n.. /.....P..$.6.x ..l6&..).g....1..cP.A..Eo.....~.....A..Eo..... .....n.. /....85926E018E7CF0ED8059DF9E7F7F7C9CD97B8ED39AE414911CCAC6C1C74B7F82..P..$.6.x ..l6&..).g....1..cP.A..Eo.....;..QL.....

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):	5.5347120749231
Encrypted:	false
SSDEEP:	3:m+l0vaDl/08RzYrSLX8AXRHEEISAhvAWFVR4gtMsFgtlHCLUXgCW3m4i7yRmBoXB:mTCTYGLBBkEIvFVAsFTLUhWI2ABiK6t
MD5:	8575DA5F57131DC73E00AA55CA68704B
SHA1:	94237B70EF6B22404C97C43AB83827F43C9AC7C6
SHA-256:	F4C2EB07BED0CF92F5419E7C1A54F5A092190BFBA277B2B4871EE23C448AFD40
SHA-512:	F4372B620B69EEA994A214342DB92D777A64E5FEDF82316D4479A46F1BF7E10AC305CE9F016BB534B5A88651E37837B7767F5B36CADFAC890793403D992B0EDE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U...q....._keyhttps://www.adobe.com/express/blocks/full-width/full-width.js .https://adobe.com/..... /.....M.P.....(;B'.....v....9..A..Eo.....@. ....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\61a30ef70fc39466_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	304504
Entropy (8bit):	6.266594112009344
Encrypted:	false
SSDEEP:	3072:gsnGOG5m/Q4WWRa8wNSoyfrHMG8oFgdNGTJvDL2pEK:1G95mTWoTwAoyTHMzINeR
MD5:	EFA503B2803DDDBAEF5D4F5623AAE057
SHA1:	C9777BE722D720B39BEACEF07CA84BC60DFB27CC
SHA-256:	8DA0D8192A4CA368AD516E19741AEBC7E0008F14FD5B35249D237AA648180A60
SHA-512:	1BD42D4EB6C5CB3E413B6328985D5113F563678B13B2781C5D8E72DC9D76C18A8B5043115B9C922442AAD7514058D2C09A325D429A7973C16B81D22202BE868(

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\61a30ef70fc39466_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...4I.M....60D846F922CD9C4F8696C2B255A5961ABBE41E691F4ED49CAA856305993B3B50.....'.YS....OK...x....Q.....P8..... .....L.....H.....(.....t.....D...\.....h.....@.....T..... (S.0..`.....L`.....(S...Q8.`Vp.....L`<.....Rc.....Z.....Qb.a.....o.....Qb.+.....s.....M...Qb.~.....d.....Qb..$.....k.....Qb.....t.....Qb.....c.....Qb.....n.....Qb...y....r.....S...Qb./ .....l.....R....Qb^.@&....p.....Qb.....h.....Qb2.....y.....QbVe.....f.....O...Qb.G.M....C.....Qb.....w.....Qb.....A.....Qb.d.....S.....QbN;.G....I.....Qb.'.....U.....Qb...-....E.....Qb b.....V.....Qb"..".....D.....Qb.o.....O.....Qb.v.....M.....Qb...-....q.....Qb..].....R.....Qb..k.....W.....Qb...%....Y.....Qb.H.N....Q.....Qb...-....Z...

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):	892
Entropy (8bit):	5.556128887544446
Encrypted:	false
SSDEEP:	12:BWjqjGlom5xGIoaWjqvLePDWjq5P9dDWjqrQteG:BWaAGaWOLePDWyFdDWVeG
MD5:	A500CB0EBAAB10A986889BE3CA15BCF7
SHA1:	1B6730BB6537737CF76503935AC9899571E28922
SHA-256:	DBB01A2EB682D3D279D4D33A7B6383670C8804F36D4658BA8F9CB2F597319430
SHA-512:	A22831F640EA71752DF0F71710E4824124F5E434D7611BDC63A16AA4AD64B7385017D924EA68758703F8953E36778AB191EECBFC26BCA4C56FABAD565D554AA2
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..... .....A.. /.....?).....8@v3.Q....D.....p....L.d.[....l.A..Eo.....0\r..m.....F...W8H...._keyhttps://scripts.demandbase.com/qQQxkRp0.min.js .https://adobe.com/..... /.....X9.....8@v3.Q....D.....p....L.d.[....l.A..Eo.....P.....A..Eo.....0\r..m.....F...W8H...._keyhttps://scripts.demandbase.com/qQQxkRp0.min.js .https://ad obe.com/..f.. /.....X.....8@v3.Q....D.....p....L.d.[....l.A..Eo.....iM.....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.....p.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6b77bbc38c24f02e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	440
Entropy (8bit):	5.481088088715941
Encrypted:	false
SSDEEP:	6:m6xY07A0NApRKhII6f+YLOiTzp+YvP4UchK6tW6xY07A0NApRKhII64YRt/bzp+U:jMKmGoTzQGPo7hMKmt1bzQGPj
MD5:	2EA24CE19393E21DED4DCD3DF3DA8CB7
SHA1:	D1E81864A93419D80DB1FF7A69B097C6DC92603C
SHA-256:	8679B8E4BCFA4894565ADDC0128D067D1C76FD06C4E5D2CE0DEE75F3E11B6A1F
SHA-512:	5BAF231E142C7A74D23C76B3F7B61E476DC749AAD328D6CA17770FB2ADAE2F18546A204387B678A008BD98D5A790D244DDFDF257966972F8ED477453274455A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X....+....._keyhttps://commerce.adobe.com/checkout/_nuxt/commons.app.f6f17c7.js .https://adobe.com/..... /.....9P.7E..Y..f.4T-....I.....CO+L..A..Eo... .....%.....A..Eo.....0\r..m.....X....+....._keyhttps://commerce.adobe.com/checkout/_nuxt/commons.app.f6f17c7.js .https://adobe.com/<1... /..... 9P.7E..Y..f.4T-....I.....CO+L..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6f013d296b22569e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	28827
Entropy (8bit):	5.83655174050762
Encrypted:	false
SSDEEP:	384:nDOJDET/vNLnXKm95G8SsJvCKuCxjtbsWqhMlHittgietZst4bX7LsBZC3WK:cik2JvCytzqhOirgietK4T7p3WK
MD5:	05809A187801173879C73727D5964920
SHA1:	9860C9438458C8C0048A8A41CAC4DDE5D9D8B8A7
SHA-256:	808AD8A6D8460C22023F5B8C692782F6668E8723CD48E7770BA2E33D0B0FC0D2
SHA-512:	09520E24B3C8534D4741DB82F941271DA243A8B2957C0139CB2320627A38C5D41B04BE68AB5FF821AB943E321191F2D8AE1D2815FAC631D59E6511256D96D94D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....C...S.{...._keyhttps://spark.adobe.com/m-setup-58e9a4b9.js .https://adobe.com/.n.. /.....O.....y.....H.....(u.q.'..+..!B....p.4.A..Eo.....-.is.....A..Eo..... .....'..S....O.....o..!>.....4.....(S....`.....L`>.....L`.....Qd..'....globalObject..A...Qcn.....window....QbN..z....self....%...a.....Qd:.#.....build Version. Qf.O.s....4f1bb381cf87318d60f7..Qdz..(....environment...Qb..&.....prod..Qcb.....snapi....<Qm^Ea.-...cc-spark-services-snapi-prod[SUFFIX].adobe.io.....Qd*..b... .postsnapi....(Qh.M.....projectm-postsnapi.adobe.io...Qd..0*....postsnapi2... Qf.....postsnapi.adobe.io....QcR3.....fluxo....0Qj"=..#...fluxo-us-east-1.prod.adobesna pi.com...Qb.....ss...0Qj....#...cc-api-storage-creativesdk.adobe.io...Qc:.....links.....Qe..^.....links.adobe.io....Qd.J.....sparkEduHost.(Qh.X.:....https://spark-cs.adobe.io. ....Qc.K.W....collab... Qf...b....invitations.adobe.io. Q

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):	5.424838660881077
Encrypted:	false
SSDEEP:	6:mgfPYGLXyAG0X5MA+vTqGQzHlr1GbFez4DHK6t:NfBGzv2GQLl8J
MD5:	FEBD5A0E7528DC77F718B255622CE542
SHA1:	D6C6B5F7703E2F75A0CBAD529AD919D987D616E8
SHA-256:	7DD0616C8890FD59C008A88EF06B98F023B4BCE11AFBC5B6D02EA349E6E6F8FE
SHA-512:	C5839069081230E48C5E2AB6FB2B8BC0E85628C58C66E8E0AEE4AB9D399DE03C3B3EFD2C7B4F7BC06AA6726A075AD22AEB0DC112E384E8BDA8AB5604542BE9F2
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/[[... /.....h1.....a.....s....U...i.;n.^.....>M^.A..Eo.....0.Y.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7368ed71bdfa2868_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	723
Entropy (8bit):	5.760060377615049
Encrypted:	false
SSDEEP:	12:42E3ea2oux2peyye3CMx6sDPViHWC2/ohJuXPmxACvP3bB:42EuaPuyeyyeSmDNJv/juxACX31
MD5:	186A30A83EDEF92D85C156BBADAD7A39
SHA1:	118010513038F8AC98E0F5D91B2719ADB03FF735
SHA-256:	FCF99AF4BAA0F9C8BAA3F3B52FFB34CF7AF7C1FDC57566B55C0B93766A85D300
SHA-512:	3828F4776F41034B31359621B7DC1A9AA66A36ED46F35A160647ACB37A56970D3FD29CAC511D70F7F8D4948AFBE46D3CD6DFC74D6A64583DEDCAAC9566A1BF3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O...4c....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/1004494713/?random=1620879701662&cv=9&fst=1620879701662&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=2oa550&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/sL... /.....5.....3p.|U..3o..(2.v.....j... `.A..Eo.....O.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\752e2a75dd6c4851_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	662520
Entropy (8bit):	5.854840249379631
Encrypted:	false
SSDEEP:	12288:zC7fVKD3OovmTc/7JqozOprjSifuEcc22xZkKjvwtjrPOOlYSGzYq9HDFBqH1xb2:zobvRV870V
MD5:	50ACA7361CE23AA320A1B318C462E6C4
SHA1:	03086EA1C77E4556F62666E4C70A8A1712B8DE6E
SHA-256:	F4112894CB92E452278972DACA9D6B3BF6F6B1CA240A32654C6B8EA1A94CCB2D
SHA-512:	29BAB49E260DFC109B120EDD7EEC3E4AEE7D42E6F11293598659A68E1B1E3B23B652A5AD2339D2F96E4666CBA7C66DB9FFDFEFBC4E6CF2A7804A9DAB62CB3327
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...F.7.....B45FD79F31738CF8C30460611BFAD38F4CEA6DA8E1DB84A3774F00894080B86A.....'.0.....O.... ....._.....(.....\G.....I...D.....%.....8.....|.....X.....d.....`.....H.....L.....D.....`.....I.....I.....x.....(S.....``9.....I.L`.....Q.P.~.h....webpackJsonp.....`.....Ma.....b.....C`...

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):	5.657623703308856
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\78076ae97804cb59_0	
SSDEEP:	24:bXyDcti9XyD2DR9XyDSU9XyDvj9XyDy1:zyDDFyD2FFyDRFyD7FyDw
MD5:	968EEC37E88F5B8EA34F34AA8BDC3F99
SHA1:	C7C2DF56C348D59964AC1D9FCDEBCCE9172E882E
SHA-256:	DEB4633C6FFC9AF8C617989ABD1C16AACDC69897000E8716094E3D7239704EB2
SHA-512:	F8F61143C8B720C076F836CE203866679AE8B88512B4004599F897D99801570F5AB6FC2F0C16E7C1E39C92BE8BCEB95BE4C6F9F4D7A27870E9603DE5518B2D77
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b...R.8....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-1004494713&l=dataLayer&cx=c .https://adobe.com/.n_.. /.....(.....=e..~o6!...=..p....Ci..t..A..Eo.....3.....A..Eo.....0\r..m.....b...R.8....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-1004494713&l=dataLayer&cx=c .https://adobe.com/.j... /.....=:.....=e..~o6!...=..p....Ci..t..A..Eo..... .y.....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/..m.. /.....Z.....=e..~o6!...=..p....Ci..t..A..Eo.....l..D.....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):	5.4609806732249915
Encrypted:	false
SSDEEP:	12:gxxXlocOvIzyxtcOvI3LyxxdcOvIiryxXfllocOvIGyxwncOvIh:65l3poqVox6woPfoo7n
MD5:	1A291FB2EA260545BE7846A9B8A6A2FA
SHA1:	FFCFC46407025E245BF5584D9D8CD21F431CB1E1
SHA-256:	3281C4C97344E52397D49C2D943B1D8701C97491E95FB95807C6D9234120B217
SHA-512:	BC96DEA2F86DCF16C5B68A77EAEAD11D1132FCFABE39E0EBEE46128D51D9F783530A9F51DD722C1E5916B0DAD145B1F1CE58A49A577A6A8CD63AE6D75E03E 3CD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<.....L...._keyhttps://sc-static.net/scevent.min.js .https://adobe.com/gfW.. /.....Z.I.[6.=....J..v.w...Z.....A..Eo.....u.....A..Eo.....0\r..m..... <.....L...._keyhttps://sc-static.net/scevent.min.js .https://adobe.com/].... /.....9.....Z.I.[6.=....J..v.w...Z.....A..Eo.....8..(.....A..Eo.....0\r..m.....<.....L... ._keyhttps://sc-static.net/scevent.min.js .https://adobe.com/..... /.....=.....Z.I.[6.=....J..v.w...Z.....A..Eo.....Y.....A..Eo.....0\r..m.....<.....L...._keyhttps://sc-static.net/scevent.min.js .https://adobe.com/".g.. /.....Y.....Z.I.[6.=....J..v.w...Z.....A..Eo.....0.....A..Eo.....0\r..m.....<.....L...._keyhttps://sc-static.net/scevent.min.js .https://adobe.com/S.... /.....=.....Z.I.[6.=....J..v.w...Z.....A..Eo.....D.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7866e75e8abf4ad4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	600
Entropy (8bit):	5.813375991719647
Encrypted:	false
SSDEEP:	12:gE31f1KYVsKhVzOoux2peyye3CMx6sDPVcoYN/CGQ5r:gElf1KY6KhRuyeyyeSmDNcoYN/C55r
MD5:	87E07EB5C9BA47DCB7A36897B00DF60B
SHA1:	BE519139D34BE13165B4E20727BB3F3591E83434
SHA-256:	F382AE9F74E624508ED532FB4367171B59477EAC90DE4A6BCEBB43C6584BCC5C
SHA-512:	9682CCA36011C9008FE48E307224B8F406F75C67088D71F1A1DF0F71AEA5C81942861DE604F328F41655CBD2CDE3BBA48EBCF671A97D8D762C7F09079B69D86
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U2...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/987390658/?random=1620879705806&cv=9&fst=1620879705806&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=2oa550&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/D.... /.....;.....l=.....5..C.....l..>1.V.\);.A..Eo.....g.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7b3710c5e15f5c32_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	613
Entropy (8bit):	5.830554368355018
Encrypted:	false
SSDEEP:	12:mLE31f1K3OF5moux2peyye3CMx6sDPV2myYJyCO1cv9RN:mLElf1Ke3/uyeyyeSmDN2myY4COaN
MD5:	FB0495A215C9C8176D966E6DCCB8450C
SHA1:	B426C9C2CD53948A139950E82F9AA69229A78513
SHA-256:	C54513CA1A840B7125747AD1F0EEB4A7D6807C7FF1920E870BB63AEF4205DCCF

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7b3710c5e15f5c32_0	
SHA-512:	D92BCFF17DDF22DFFA70EF36A6C3804DFB9EED37AD42A37C6463D9D207236F010FC68FA5BF8DCA699FF951C92848AAD5177D3FBD6C9F65EA9D0AFD52F74AD0D
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/987390658/?random=1620879713755&cv=9&fst=1620879713755&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=2oa550&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/<Lp.. /.....Z.....x..s.J'...s.S.K.U.i.1..m...U..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7c2374a7be8500e8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	249304
Entropy (8bit):	5.821003282005214
Encrypted:	false
SSDEEP:	6144:KoRKFdJZUjuoicjrg7xXtxSjJzabLPmX2fXU6V:TwXrtPRMc
MD5:	DD6D0FB756B71974DEEC1423A34E9484
SHA1:	38DD87F4546CDAF296588026E179B2487B34ADE1
SHA-256:	C999779198F8D9AD22A63CDAA7A94F61405C3749350BB0822EF86AD682DA7653
SHA-512:	8EFB2257A95D5A22AA4253BC53C31332CD9E84CD8704CCBAD646624773D4AD7E3104C3A8D80278098D201A24E537D15C2DB5B2675B13A428802E27BA28F1798
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...=..D....2141E28C0719D13C92D31A87BD028FE7AABF71D7537BC982E927E08C86E60690.....'.R.....ON.....u.....l...H...!..... ..|.....x..... .....(S....`0....@L`.....L`.....Qd6.V.....marvelcommon.(S...`.....LL`'....@Rc.....Qb.....t.....Qb.....e.....Qb.<.@....n...b$.....l`....Da2...J....(S...`.....L`.....Q.@r.....exports..$..a.....S.C..Qb.....l...H.....a.....Qb..a.....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\7f92142ba76e4116_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1345
Entropy (8bit):	5.677182660696318
Encrypted:	false
SSDEEP:	24:W5MbHhyEJpZNg5MbHduEJp3g5MbHow/4EJpig5MbHqIEJpeg5MbHvEJpD:W5Mrg5MRRg5MHyg5M+Gg5Mc
MD5:	C65921E0F4D92088A97951E57A01203F
SHA1:	FDDC074B83DCC80180F7ACE81580F2FF2F2AFAC0
SHA-256:	213B53AA4B3911D874AF1309A3D44305DBCA0D0C39CCDCA1E7A444C490F08988
SHA-512:	8D4A4BE7EAA07F18A9062345DAB536B42AB26612A6241790A7F6FFD0C11F2FC2FB6BF783A3C4C2386EDD0553756F6BE6CD709FF96424181643BBF861FFEBBCCA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....>....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC48990c37b3504a02838f190f73e12664-file.min.js .https://adobe.com/.\... /.....).O~.s...p..Q._VTg17...>..D.....A..Eo.....w.....A..Eo.....0\r..m.....>....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC48990c37b3504a02838f190f73e12664-file.min.js .https://adobe.com/s/O.. /.....).O~.s...p..Q._VTg17...>..D.....A..Eo.....`g.C.....A..Eo.....0\r..m.....>....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC48990c37b3504a02838f190f73e12664-file.min.js .https://adobe.com/.L... /.....r7.....).O~.s...p..Q._VTg17...>..D.....A..Eo....._.....A..Eo.....0\r..m.....>....._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RC48990c37b3504a02838f190f73e12664-file.min.js .https://adobe.com/Z e.. /.....IX.....).O~

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\801b3abff355220a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	538
Entropy (8bit):	5.649261191292278
Encrypted:	false
SSDEEP:	12:4ASPRMLdXZshoqfPCKASPRMLdXMVffPLr:K5ML5ZAoo685ML5Ef
MD5:	72BBCCF207B4F414B34E0D002EA2797B
SHA1:	FA6594B07D6CFDE56856A7157EEF595AA4367A26
SHA-256:	274E54AA57E3D2628451768B38C4C7E5D2A2C9EAE7C24FEF7ED72FDF75EE3FF5
SHA-512:	FB458BCD7959C462D57F943CEEAF90A23D46204621D312EB06D2B6DE14802CA1FD7C0B5460F392F82CB8A28266D5C8FB4DDE4C2F65D91A68EFFBF09CE0015EC8
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\801b3abff355220a_0	
Preview:	0\r..m.....L.3y...._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RCbbd93c1920fd422b84787f67ddbfbe55-file.min.js .https://adobe.com/.l... /.....0.....>!(....9.C.....'.....(W.+.....A..Eo.....x.....A..Eo.....0\r..m.....L.3y...._keyhttps://assets.adobedtm.com/d4d114c60e50/f3fbfbe0e7ca/e1d9f552a353/RCbbd93c1920fd422b84787f67ddbfbe55-file.min.js .https://adobe.com/.OF.. /.....KR.....>!(....9.C.....'.....(W.+.....A..Eo.....3b4.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\812225700901227a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	613
Entropy (8bit):	5.82191053183356
Encrypted:	false
SSDEEP:	12:mBE3GaLKBxoux2peyye3CMx6sDPV2myYJyCVLLw1:mBEWaLKBauyeyyeSmDN2myY4C9Lw1
MD5:	E888D2B40E82F8E892BECE722F379F55
SHA1:	EA7EE7FE5B2283FC1B84232AED8E43850DE85D77
SHA-256:	CE58ACF374873F466DC3580AE4B40C1D437D23417B857CB8DC22EAC650E9E3E6
SHA-512:	1B59D66D44F1AA1D8BD1F8BFD51BF6015E3915B04E35200CDED46E03C55B9DA6CF17CF18C21527CB330EB7DDE1ED4C22D61469C5992DCF4ED96B907B4B12800
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L.=...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/951622910/?random=1620879713943&cv=9&fst=1620879713943&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=2oa550&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/Z.r.. /.....4[.....^.V.....y...../..`....A..Eo.....]...A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\850d10ed47f5161b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	5217
Entropy (8bit):	5.353058125031847
Encrypted:	false
SSDEEP:	96:dznK63dJqhL/pu1o8z7o6enJgWteXxwk4L1PKJKphp6AvkikZi/ogpnB:RK63dZ1c6yJgWAXxwk4L1ByAmZQpB
MD5:	D9288AE3CC31A85713D7695180FB333B
SHA1:	6D7741831E476392570486F10EAB60171F8D7942
SHA-256:	28F2A5B275E5E53AD76B7A2C7C21011B863ADED7503B4BB8646903910F67B4B7
SHA-512:	3DEF0FE7A0961888684228317C370ECE802F853640027473594CC40E4474803D62B2203C15F602C3B111FDAB876A322DA862972E2389CDEFE8D5D3A4CBAF0CA7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q...1E.)...._keyhttps://universal.iperceptions.com/core/Ipuser_v78.0.js .https://adobe.com/..... /.....;.....-.>..+...aOv.....?.}...A..Eo.....u.....A..Eo.....'..+....O.....[.....(S.I...`F.....L`t.....L`.....Qdf.{.....iPerceptions.q.....Qb.....trim.(S.....5.a.....a.....a.....Pd.....String.trimaI...q...IE.@.-....HP.....9...https://universal.iperceptions.com/core/Ipuser_v78.0.js...a.....D`....D`....D`.....`<...&...&..Q.&.(S.....a.....5.a.....a.....Qc..A.....ipuser..Pc.....launch.a.....e.....@.....Qc.....launch..E....d.....@.....D&.(S.....a....*.....a.....a.....a..... Qfz..w....hideExistingProjectsa.....E.d.....&.(S.....a....#.....a.....a.....a.....QeFSD.....displayInvite...a.....E.d.....

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):	5.443031419441313
Encrypted:	false
SSDEEP:	6:mAYtVYGLJxoxDMVuTlmYBprtXh5RK6tWAYtVYGLJxoxDMVHWWiS/l3mYBprbNK6t:ItraxDP5mYBpBXvrKtraxDyV9mYBp/n
MD5:	EF670148998D98A621D830F4A27F3959
SHA1:	AAD95B9041345E5A1C514C0659DB78765D4543BE
SHA-256:	DE65491347525E2642E7F2EA8AE8BE62623BC5B82CDB209B94FA4D2D46895849
SHA-512:	5A4C6711187B60F4C9C91EFF15E94525441A4D8D3DFE24FA74BDB0E38C8BAAEF271FE01859CB073E64F2179171A15545A07814AFB8FBE0C8760BE616321A5615
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....U....._keyhttps://www.adobe.com/marketingtech/main.no-promise.min.js .https://adobe.com/... /.....,.....o..I.L.....??..>...-.s...p.A..Eo.....r.....A..Eo.....0\r..m.....R....U....._keyhttps://www.adobe.com/marketingtech/main.no-promise.min.js .https://adobe.com/e.5.. /.....K.....o..I.L.....??..>...-.s...p.A..Eo.....x.....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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8d858bba8e7cc695_0	
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.451552874673204
Encrypted:	false
SSDEEP:	3:m+l5Kf/yv8RzYrSLX8AXRHEEIJY7sD4gtzJlhFKv/tlHCbQllVLs5DL75ai5uRgT:mYEYGLBBkEH7slhwybQ/ds5l+4BxK6t
MD5:	C79269401CBDD1DEBAE8CCB209577E00
SHA1:	69CB3593460260F269F5762D8E1EBA0E1009D788
SHA-256:	A1D602DC2C58D7D25B4C1FA0334CB64BBCED367CDE3808F096FFD40D23F98196
SHA-512:	1C32E063476D66290AC4862369D850B942362B4C442D912FF35437F16542EDA68648AE370BF63CA994B4C9886EE54CA5D18DFF1DE2F7C3EEF4EF745832226632
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O..../....._keyhttps://www.adobe.com/express/blocks/columns/columns.js .https://adobe.com/.X... /.....3...#..+..N..U.W..`.B...C..4t..A..Eo.....-.....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):	5.419353953545765
Encrypted:	false
SSDEEP:	6:mhynYGLBBkKsdwyUxyAyillDZyxH8g4ZZqhK6tWhynYGLBBkKsdwy9TK62ZyxH8b:HBqd3UxflDMxzEZKFBqd3E3Mxz4
MD5:	DB9F045E4B3D1B652F7C0AD0888F5045
SHA1:	73DC72594A3B94B67A7695C868854BB7296135A3
SHA-256:	BDF89408E60660947C7E4AD569FC739E1DE8B458897199048A986F47F081ED94
SHA-512:	9E997002BA53698CB625B89E8FEA74D9EC2F465BBAE79C3F8ECC6E819DF424B692768883D69443B9B15FCAE890CFF219C31A8DCFAD36796B60E467CEB6E8B96
Malicious:	false
Reputation:	low
Preview:	0\r..m.....[...2.*W...._keyhttps://www.adobe.com/express/blocks/template-list/template-list.js .https://adobe.com/.... /.....h.....Ff.....T .....h..F..(...A..Eo.....'.|w. .....A..Eo.....0\r..m.....[...2.*W...._keyhttps://www.adobe.com/express/blocks/template-list/template-list.js .https://adobe.com/..... /.....v.....Ff.....T .....h..F ..(...A..Eo.....=.T.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8f7fc9cd2003df54_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.455277746288617
Encrypted:	false
SSDEEP:	3:m+loEIlv8RzYP2FycyG8ZFvDdA3KRWLAQ+vltlHCdpU3iw2z5TyZm/Qt5llXpK5M:mwYeM1Y7+vYTuiw2z52Y/0/ZK6t
MD5:	D3ABB90123CB3BFAB510D393D3AF34E4
SHA1:	FD4855B3908733818B179AF112A99FE461D5F67B
SHA-256:	EB484C30F64EB60DF28AAEC98E4070B99D70AD1673105EE3688DC6980EDA51A2
SHA-512:	A0DDC00D9A4BABA4AFC33C02E46D6E905A3A1C821FCC1E449C325F43D1293B2F43C865C62EC8487ED40655ED6715D032B19B963D057F52BD7A2320D222E4B7A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H...._.o...._keyhttps://code.jquery.com/jquery-3.1.1.min.js .https://greycottage.ng/.... /.....b.....S....bl...R....T..SR.....~5n.A..Eo.....u.....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):	354
Entropy (8bit):	5.861815676250707
Encrypted:	false
SSDEEP:	6:m55YoDLoxe0HOKbI6e9YJ3ur8+DrxlZK6tqhR6L6UiQEEQ18+Drz:aXo4MW66+aDNlTjLbEEID
MD5:	D90A4E69231DA5E8AB61316B05037464
SHA1:	2F2878D91D90AF61E2B3B15EC671BD3E4346E506
SHA-256:	EB1D60E3FDDB9E2B680ADEBDE848DDA288A626E98ED85B942054E725483C4DF4
SHA-512:	811CF08FEAD1C0DCB2BA3A1308A0EBA86C01ED6F2852A3A46B8B4FE8DC83D34AF82113D2D807F22071C3AEED9ECF18C54E9CFE648876E4DDB10B8CCE54B903C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8faec8b628066d9d_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z....._keyhttps://page.adobespark-assets.com/runtime/1.22/runtime-prod.gz.js .https://adobe.com/.*|.. /.....[q.....}.....-.t.@d":. $.{F|on.j.... J.A..Eo.....'.8. .....A..Eo.....*|.. /.hm..44ABFBF7918EA02CDAA8F85A4455B7DBFEA9519C2D15F5CC6553B655406F29E4}.....-.t.@d":. $.{F\|on.j.... J.A..Eo.....$^L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8fd38fec58c34f40_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	351
Entropy (8bit):	5.922733040545623
Encrypted:	false
SSDEEP:	6:mbEYgGKHRUUHDxLBOuB84HYgf6Mm4NDK6t03tkwTyWoUmNQdnSWAYgf6Mm43:VdiClcu2paAQ63qwTKFQdvaAo
MD5:	6613F16730C9CDA4161432329D7B3836
SHA1:	431013B48F1F68173F91A8FE62A30C7BAF3AC327
SHA-256:	F878C97B3AF4CD60385F634AAAD74296077EF80026E1CF13991226B873C05101
SHA-512:	83A4E8604AE9C5CDA9FE4D3D8F73AB62FD425665BA1AD626B479361F5AC0A76FF9748CA827A7E2A334F6B3A657094727CD3AC23286AE846FE82DE588173ADD 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W...IH....._keyhttps://spark.adobe.com/static/locales/en-US_bundle-6a358124.js .https://adobe.com/=Yo.. /.....U/.9.Q.'[>.....:....w.gM(...A..Eo.....*..... ...A..Eo.....=Yo.. /.....EE2D21DE3F87B41F3D6F099D64D6ACDAFF37F5793003A5CCEA22E546293FAD63U/.9.Q.'[>.....:....w.gM(...A..Eo.....^+L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9dc60bec78382d3e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	600
Entropy (8bit):	5.7863517930057835
Encrypted:	false
SSDEEP:	12:l3E3GmKToux2pmYyye3CMx6sDPVcoYN/CcFPWf:l3EWmKUuyRyyeSmDNcoYN/Caw
MD5:	66DA6797ACFC933EFE1BBAB48A78530E
SHA1:	72DD096E88D0E5717257AFA01B6275531F9E0FC9
SHA-256:	E0CCF16546C469BA89D4D692D1F5117B0BF0870C86054E26399845FA89451A38
SHA-512:	08D4CFCA9CB30CE20848F727F88838E818544AF85CC349AAF7BAE31A02A9DA818B191469DE25E627E727E9D790920B1ADD092342F588FD2D962BE5D123627F0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T3...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/951622910/?random=1620879705799&cv=9&fst=1620879705799&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=2oa550&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/..... /.....;.....Q.i..~+..A..D.COYNd...F..h.w*.A..Eo.....=0.....A..Eo.....

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):	5.666310078836323
Encrypted:	false
SSDEEP:	24:S5/Xl8QkUk5hOQkLk5bmmQk7Ek5IaQkxk5cQkF:SpXlzkL+kRmQEkGckw
MD5:	CA10017651F07A4F18DE5845B3E759F7
SHA1:	445A571CD9D2B4241F14560B1A49B838D9B9B0D5
SHA-256:	8E10E822FDE1132586178E69A64187919CD1116A239BFABD71F43E89984CAB66
SHA-512:	B3F2A5B8D5AF472182E69A19F0A121E22C22F9327E09AA533810C01154E642F5F735136D58606C1D3147C3D299C22D42248B71BFA1E075368591EFEDA6958EB8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-987390658 .https://adobe.com/.hW.. /.....<.U#..r.....[...<U....tQ.u...A..Eo.....p.... .....A..Eo.....0\r..m.....P....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-987390658 .https://adobe.com/..k.. /.....60.....<.U#..r.....[...<U....tQ.u...A ..Eo.....A..Eo.....0\r..m.....P....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-987390658 .https://adobe.com/..... /.....f9.....<.U#..r.....[... <U....tQ.u...A..Eo.....A..Eo.....0\r..m.....P....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-987390658 .https://adobe.com/.Zg.. /.....`Y. .....<.U#..r.....[...<U....tQ.u...A..Eo.....>.....A..Eo.....0\r..m.....P....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-987390658 .https://adobe .com/.!... /.....<.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9f7e885e8c444e3d_0	
File Type:	data
Category:	dropped
Size (bytes):	18105
Entropy (8bit):	6.064508349716162
Encrypted:	false
SSDEEP:	384:wx1sAe2/vuPZIu1l4zPgjwfB/b1vjx69wgQjWH4vip7c:wx1rhvmhS47g0/1x69rfH4KS
MD5:	D8A3178CB207134AF2099803E38A3CFB
SHA1:	32735470F242706D975532941ADE518D89D845A0
SHA-256:	61F31AC3C4849FED2564831D24EDE1ABE96C9B19165CDA636274236E1E250271
SHA-512:	AA6C68141DBD3527C16843C5D53EA25C954D488450B8360BB00199D392872065AB1A615A30F2BC3AEFD2AF1BD8B72BCE3CD68B4FF33CF316B72E5DDB848E13D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....A....y....._keyhttps://d9.flashtalking.com/d9core .https://flashtalking.com/XDK.. /.....W...../0AsR..0"...{.\Z.uy.{.B....l.A..Eo...../.w.....A..Eo.....'..*....O....HE....CW.....(S.0..`.....L`.....(S..`.....LL`".....Rc>.....Qe2.....coreElementId.....Qd:.7 ....container.....Qc:.....isApi.....Qb.....d9d...Qe..".....collectSignals....Qc..0....d9api.....Qc.O.i....initFt....Qc..z.....d9legacy...k.....I`....Da....(T...(S....`.....L`V....Y...Qc.....window....Qc:.TF....screen....Qc..j.....width.....Qc.....D9_101....QcV.....height....Qc.1,.....D9_102....QeRU.....devicePixelRatio..Qc..LI....D9_103....QcV.....getTime...Qc..Z6....D9_110...QfFp.....getTimezoneOffset.....Qc..}.....D9_111....Qd..r.....navigator.....Qcj.....platform..Qc.&8....D9_120.....Qe..fB....browserLanguage...Qc.%.....D9_121....Qdz..>....apC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a00678896dde764a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2748
Entropy (8bit):	5.8662459688616275
Encrypted:	false
SSDEEP:	48:dy2Id8kuzRvKTdJBcjEHugwL5R88slybddNx4K:k2u8zvKTdJBbO3s8+yHf
MD5:	B23C8AD9CF87DB7581443757CDE558EC
SHA1:	EBF361214DED2FD5AE0A12FD70D4EA6ADB4147F1
SHA-256:	4BAF6F2EA123E28298C1855F87E1E40630AFFE1DAAC6D1968EEEF9CEA9CA88E0
SHA-512:	2DDC16CB842BAAD38CDD040B8DA939C0323112A0BA51E07C942B8AD08DFEB8DA1169FC6BBCA244924AF789C45CB9EDACBB4EC9E82A2D866042E9902D6E64B591
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T...R.d3...._keyhttps://commerce.adobe.com/checkout/_nuxt/runtime.f6f17c7.js .https://adobe.com/+.... /....._.H2..w(.L._...!..<..5}|;.k/'.x..A..Eo.....f.....A..Eo.....+.... /.....'.....O...`....H9.....(S.`..`v....Lc...*.....(S...`....lL`2....dRc.....QbBM|.....e.....Qb..2.....t.....Qbv..'....n.....Qbj.....o.....R....Qb.+6....l....Qbf7.@....c...f$.....l`....Da.....,Rc.....c.....Ib..... ..`.....]`.....(S.M..`P....(L`.....M.....Qev.N!....hasOwnProperty....Qbr..~....call..Qb.5.7....push..Qc.....shift.....K`....D...x.....*..&...*..&...*..&..&.|.&.(...i...e%.*..&....&.(...&.(...&.(...&...&.Z.....)..&.%.*....(...&...&.%.*..&..*..&.Y.....&..0.. %.L"&..i.%..Qw.....#.&...B....#.4&....&.(...&.(..$&.(..&&.Z....(....&.%.*.*&.0..,%..&..B.....&.]...(..0..(..2&.X..4&.\.6.....&.(...&.(..8&...&.%...|:&.Z....;..&.\.=....,Rc

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):	5.415821899698805
Encrypted:	false
SSDEEP:	24:khblfNn+h4xSfN++hyfNY+hcfN0r+hl9fNMT:ohNn8N+ZNYbN4aJNQ
MD5:	1898BE08D75119281AA3EDD8750B3986
SHA1:	72E67C5F7DDD6CA2BFBBDD1F2DD75C2A2D646814
SHA-256:	5381DF0AED3DDAFB9CDFE1E3A55FF2C23EE762365C0FF421D4CD643658EEC2C5
SHA-512:	CE09CB05D4BF5839FAF07D3F47E7F5C76F75A91BD75F336EF70532218CE42DECAAC6C13A016495F5C43F7F387FE2261C8B34196722FC58F8560428BF5C1CC45
Malicious:	false
Reputation:	low
Preview:	0\r..m.....3.....?....._keyhttps://bat.bing.com/bat.js .https://adobe.com/.U.. /.....J.Ns];.<O.F..h'R...=;*..]....A..Eo.....;..-.....A..Eo.....0\r..m.....3.....?.....__keyhttps://bat.bing.com/bat.js .https://adobe.com/#.k.. /.....0.....J.Ns];.<O.F..h'R...=;*..]....A..Eo.....N.9.....A..Eo.....0\r..m.....3.....?....._keyhttps://bat.bing.com/bat.js .https://adobe.com/..... /.....9.....J.Ns];.<O.F..h'R...=;*..]....A..Eo.....q.....A..Eo.....0\r..m.....3.....?....._keyhttps://bat.bing.com/bat.js .https://adobe.com/.og.. /.....X.....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.....y.....A..Eo.....

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):	1624

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a6942155eb9698ff_0	
Entropy (8bit):	5.65663998614529
Encrypted:	false
SSDEEP:	24:Kipe8PpAih7tRe8lAiNbe82XAi9ue8LAi/re8VAi3G3e8YAixe8bp:KePpAmBBlA62XAa6LAEVA2GYAObp
MD5:	D453FA23474F815BDCE3A33567066244
SHA1:	16A77B6B7028EA4F2AC541CED464F32A38D96F82
SHA-256:	4BEB019DE50D078D2EEC316AE4E12B99136E519EADF5EDCEC1F635740AEFE2D0
SHA-512:	0675E1EBA0BF17E19C46D1DC4C22EBF6466D67FD061875582C496E2948A9A1BEA66B02B83B337434150920924CC22182517F8EAA070E24EBE670BB508C803982
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d....._keyhttps://assets.adobedtm.com/launch-EN919758db9a654a17bac7d184b99c4820.min.js .https://adobe.com/.]}.. /.....YA..H4&.2....K.V.H54 .d.1.j.Q..b..A..Eo.....l[.....A..Eo.....0\r..m.....d....._keyhttps://assets.adobedtm.com/launch-EN919758db9a654a17bac7d184b99c4820.min.js .https://adobe.com/.{@.. /.....YA..H4&.2....K.V.H54.d.1.j.Q..b..A..Eo.....A..Eo.....0\r..m.....d....._keyhttps://assets.adobedtm.com/launch-EN919758 db9a654a17bac7d184b99c4820.min.js .https://adobe.com/..n.. /.....0.....YA..H4&.2....K.V.H54.d.1.j.Q..b..A..Eo.....v.....A..Eo.....0\r..m.....d....._keyht tps://assets.adobedtm.com/launch-EN919758db9a654a17bac7d184b99c4820.min.js .https://adobe.com/..... /.....|/.....YA..H4&.2....K.V.H54.d.1.j.Q..b..A..Eo.....i.!. .....A..Eo.....0\r..m.....d....._keyhttps://assets.adobedtm.com/launch-EN919758d

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):	5.471147271639644
Encrypted:	false
SSDEEP:	24:r7Pxij9k57PdQzj9d/N57Prj9657P2mj9r57Ptj9T57PArj91157POj9r:rLxij9k5LWj9d/N5Lrj965L2mj9r5Ltd
MD5:	F75CFD9A7A388834575C7D90FDFEA6CA
SHA1:	D8A94BC380637EE528CD9DFC9EEF4F545444EC8E
SHA-256:	396B4177F18458402204043ECF12956282C90C35A18F9B84E413DEBC285E8FE7
SHA-512:	74BC6455AF14199C1AFFF062B030E99C40FE73862CCEC4B58BBAA157A0BE0E24782E2E4796BDB641EAEF870627C0FC8231176C1143FC887E69B9FCBD25DB90 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....J....4....._keyhttps://static.adobelogin.com/imslib/imslib.min.js .https://adobe.com/..{.. /.....Q>-.-:.*'){..Zd..=.[N.,.Un.a....A..Eo.....v.....A..Eo..... .....0\r..m.....J....4....._keyhttps://static.adobelogin.com/imslib/imslib.min.js .https://adobe.com/.h>.. /.....o.....Q>-.-:.*'){..Zd..=.[N.,.Un.a....A..Eo.....p.....A..Eo..... .....0\r..m.....J....4....._keyhttps://static.adobelogin.com/imslib/imslib.min.js .https://adobe.com/.nn.. /.....j.....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/.R5.. /.....MM.....Q>-.-:.*'){..Zd..=.[N.,.Un.a....A..Eo.....g....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a88a0ba16fc3e3ef_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	614
Entropy (8bit):	5.812879791223187
Encrypted:	false
SSDEEP:	12:xjE3eeSoux2pmYyye3CMx6sDPV2myYJyCwIw:xjEuebuyRyyeSmDN2myY4Cwd
MD5:	2DA93C2AA6F2A2B8D55BA5C42D6A1B82
SHA1:	D3788B19F48235758DAA24B3CAA18AD20B9366F7
SHA-256:	CA348C1711F5CD5D8A1BE8A92E56B29EE063E44750CD2313FC2D9EDB12D34181
SHA-512:	EAF152D8207A7A4557DD26E219EA7C84970A53FEDF5F1B2D8F40F806B07F4854D2A5F8DD2F691C43C691C6EC643F40E08F85E581D6751DCAC47260023972F6B
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/1004494713/?random=1620879713939&cv=9&fst=1620879713939&n um=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=2oa550&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fwww.adobe.com%2Fprivacy.html&tiba=Adobe%2 0Privacy%20Center&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://adobe.com/..r.. /.....-[.....[.k<RS&.0.2.. ....;w.z..D.^....A..Eo.....h.*.....A ..Eo.....

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):	5.514748308403449
Encrypted:	false
SSDEEP:	12:3Gz5WYmyT6ptGz5WYmoxtRCTUitGz5WYmK/TTW:c5Ws6i5WutRazi5WA3W
MD5:	B063C9145DF89A3B087A06EB66330482

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ab4f59045e28d03f_0	
SHA1:	DF46927DE30B0EEB8C4CD4D76A6F27D69418A33C
SHA-256:	0823EB7F47FB721EE1717FB9FEED2717A041E387E2118B95459187AF0E1E9CCE
SHA-512:	00D8240009CA0829D1BD8100D4BB4D17CC7DC57B9BFC7530564CB11B69838F9A6360D607208661916603D632339D74259D85C966C600DA40234D36BFD2C8EC8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e...>.W$...._keyhttps://www.adobe.com/services/feds.res_1.js/head/en/cc-express/spark-gnav.js .https://adobe.com/..... /.....U.....#&H1..\|....x.' ..5....x\# .%...A..Eo.....F x.....A..Eo.....0\r..m.....e...>.W$...._keyhttps://www.adobe.com/services/feds.res_1.js/head/en/cc-express/spark-gnav.js .https://adobe.com/a.H.. /.....#&H1..|....x.' ..5....x\#.%...A..Eo.....w.9~.....A..Eo.....0\r..m.....e...>.W$...._keyhttps://www.adobe.com/services/feds.res_1.js/head/en/cc-ex press/spark-gnav.js .https://adobe.com/.Y... /.....&.....#&H1..|....x.' ..5....x\#.%...A..Eo.....a.|.....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):	904
Entropy (8bit):	5.438906706708074
Encrypted:	false
SSDEEP:	24:xgasrz1pUOngasrz1ufngasrz10ungasrz1Wb:xzsrzgOnzsrzmnzsrzhnzsrzu
MD5:	48DFAFCC525A98A36400D7E580F80385
SHA1:	D192FFFD391537CA6B1E47A9DAC030138A8F4C65
SHA-256:	94364602A166D8EB025F74B5B75EA9A494BCD1B8EE18AADC6697906BAD9522BE
SHA-512:	B50964BC8B82B20A68D7F65AA5E7650F01E392BF24D13D0E1140AF88977F32C9184CEC5F5C808427A5D3537316324ECE687CAF96E83084D966E88ACE558587DA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....^....._keyhttps://www.adobe.com/etc.clientlibs/globalnav/clientlibs/base/feds.js .https://adobe.com/..?.. /.....5g..y..5..O..:L.....?..R.$.....A..Eo..... .....A..Eo.....0\r..m.....^....._keyhttps://www.adobe.com/etc.clientlibs/globalnav/clientlibs/base/feds.js .https://adobe.com/3h... /.....,.....5g..y..5..O..:L..... .?..R.$.....A..Eo.....h.c.....A..Eo.....0\r..m.....^....._keyhttps://www.adobe.com/etc.clientlibs/globalnav/clientlibs/base/feds.js .https://adobe.com/r.5.. /..... .....IL.....5g..y..5..O..:L.....?..R.$.....A..Eo.....~.....A..Eo.....0\r..m.....^....._keyhttps://www.adobe.com/etc.clientlibs/globalnav/clientlibs/base/feds.js .https: //adobe.com/.@... /.....\|.....5g..y..5..O..:L.....?..R.$.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b3e035f953ffa5ce_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	722
Entropy (8bit):	5.7627138572002305
Encrypted:	false
SSDEEP:	12:x+E3GPOTmoux2peyye3CMx6sDPViHWC2/ohJuXPmxAC23EuGx1:x+EWWjuyeyyeSmDNJv/juxAC2o
MD5:	C8F8C23FA2595BD67D3AB66F9A2B08C7
SHA1:	AF1AC1CFB9E447013763830F97DAE02BA9445E42
SHA-256:	1849F00AC49155E218C0AC81711F3E05508FA689400BD5AB8DEC2CAD82088430
SHA-512:	421DD2CC5F15889C77606F86348EA1BB54302AD99E4316687A7511CD48D3EE1F3E5B987455DB0128442B43CA641343D1B9B32A7A95009B13B4D414D852BA4997
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N....~....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/951622910/?random=1620879701657&cv=9&fst=1620879701657&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=2oa550&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%20S park&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://adobe.com/..... /.....5.....Uk3...|.....h7a.He.....a7..A..Eo.....s.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ba0481563fc1e268_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	664
Entropy (8bit):	5.810413381789107
Encrypted:	false
SSDEEP:	12:gE3eyP/Vfmoux2pmYyye3CMx6sDPViH2NRmxACx+2EZ:gEuyP/d/uyRyyeSmDN/OxACxZg
MD5:	BD8249AA6BA2D900E512DFD0D0F32083
SHA1:	48D94D05C2490B8142AF2F8B01B96D80079C4D07
SHA-256:	AAF52C67CB5687C3C841EE679A8DAE393996D35CADAB3E64FE8452648CA5B9D4
SHA-512:	DD8041FAD7EB7A215640E7A3B33932A348EEAA1E58B0C8527793F9C064009ED0BF79ADE38198B205686D186E22130E990085281115183E2D153DFD0988A6A843
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ba0481563fc1e268_0	
Preview:	0\r..m.....C."...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/1004494713/?random=1620879724355&cv=9&fst=1620879724355&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=2oa550&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/..... /.....Y.....M.].B.DCz..hk..#.p..?...).../N..A..Eo.....[g.r.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\baf621cf86f40a8e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	403
Entropy (8bit):	5.89352928761236
Encrypted:	false
SSDEEP:	6:mkGEYGLBg5KAJjNezKU5HUHFWV4CCuMSKLFhYK6tMNWkrA1ouMSKLC:8Ag5KsjNu3ZUHYRtOM6Va
MD5:	DBE949AAF00926B280D15410AD34AE40
SHA1:	4DBF72332910001204866447C7183448E554396F
SHA-256:	8206E031977093B8489D6899FE15F47424F6CC6B30E05607AEBDFBD7F7B79C5A
SHA-512:	487F7B1CBEAB8F330F8AF00917EDBF3F88094967259C1E9E649DCF065CFB3CFCE7EC4E029A711BC9733921EE86A5E86329C23F1CC140F7452AB5078FA983414
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://www.adobe.com/etc.hawks.dexterlibs/hawks/clientlibs/publish.combined.fp-4e17ca9de7c6a880fa904bdb1191f422.js .https://adobe.com/.g... /.....x.....dgg8..97.C...WD+dOHC..'..A..Eo.....[.....A..Eo.....g... /.P...B45FD79F31738CF8C30460611BFAD38F4CEA6DA8E1DB84A3774F0089408 0B86A.....dgg8..97.C...WD+dOHC..'..A..Eo.....x.jL.....

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):	5.562690811869143
Encrypted:	false
SSDEEP:	12:ikg/hggkg/i43rnTgkg/9gtQ1gkg/VMNgkg/bhdQ:5g/mrg/B7Trg/9qcrg/GNrg/g
MD5:	F9049937D8C7BCA5B41FAF6E24709956
SHA1:	6C02013CC93537A1A478E8E2CD894197B970965E
SHA-256:	5E8CDD17D1CFFF01E425E13B4111DC2C55319818D9AD70950D8C46E6D71A24A1
SHA-512:	5A59F5A2F49594129ED4FE3A06D87A9F6A76500C772CFC7EA24EB90BB3AA710FC4286D49094CF46A192DFDA493740FD9FF37D2D204B9FAEAC9B1E3943094FAE
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/=.... /.....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/..>.. /.....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/~.n.. /.....6g..X.h.....=v...f!1.F.....N...A..Eo.....Z.....A..Eo.....0\r..m.....m....-Q....._keyhttps://www.adobe.com/etc/beagle/public/globalnav/adobe-privacy/latest/privacy.min.js .https://adobe.com/.I... /.....Qd.....6g..X.h.....=v...f!1.F.....N...A..Eo.....j).....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):	7394
Entropy (8bit):	5.987091746058416
Encrypted:	false
SSDEEP:	192:7ss4jDKBIJXjPOb2G01pnhqxT7EoLlqF3bu:7sxjWy1ib2G+phI7EGqFa
MD5:	BD555E0834A4A4B968776D531826F5F1
SHA1:	2607BE2C5CF69EDAC7EA63D91B8FADCA8E142884
SHA-256:	AACE4704DAE6E704CFBFDAB331B7E204BC52331CC4528A3D73242B239D964698
SHA-512:	21B3D454B8CA201D5B18518E993FC406185FD1067F54AD48797104E1C9C99C5855BB041B56477D7F35FBD97B255F902838CD33AC1455EEF79A01E90A33D6C29E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N....T....._keyhttps://snap.licdn.com/li.lms-analytics/insight.min.js .https://adobe.com/.YA.. /.....5..... ...{..@...R.%.m....H.m.?&..A..Eo..... .....A..Eo.....YA.. /.....)..... ...{..@...R.%.m....H.m.?&..A..Eo.....Xw.....'.....O.....2.....(S.0..`.....L`.....(S....`.....L`J.....Rc`.....(...Qb.*r.....l.....Qb...m...._.....Qbj.uw....t.....Qb...}....s.....Qbr./9....r.....Qb^B.O....c.....Qb.....v.....Qb&r.....p.....Qb.SR.....f.....Qb.....w.....Qb.6.....h.....Qb.....R.....Qb.h6....C.....Qb...)....U.....O...Qb...|....E.....Qb.....x.....Qb^..5....D.....Qb..'....L.....QbVe~.....T...s.....I`....Da.....!...(S.<.`.....L`....Y...Qc.....getTime...K`....Di.....&.e....&.(...&.X.....,Rc.....Qb.....n...`....DaF.....a.....c.....P.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c2a6bb76704a0b65_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	613
Entropy (8bit):	5.8616367814447745
Encrypted:	false
SSDEEP:	12:mcE3xjaqIB9Ooux2peyye3CMx6sDPV2myYJyCdsGJdE7:mcEtaqIBluyeyyeSmDN2myY4Cdst7
MD5:	F99C2F4156DAAADCF836797F963BA208
SHA1:	9767226ABF1FBA1F636A408BFC8E4346FEBC8269
SHA-256:	334E39D671E45CC3A316872DEFE65EB7592A5A07F0EDC5B2BA610B2E308A4562
SHA-512:	2D30C16AAEC3AA028827299C39DB46DF8D5303150C95FEF5AE12F5B85D346871354B82B2D62D716CF6EC7BE8C356762211F85129B157EC9263E7F3054B7FD268
Malicious:	false
Reputation:	low
Preview:	0\r..m.....B....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/983956512/?random=1620879713948&cv=9&fst=1620879713948&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=2oa550&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/Y(s.. /.....O[.....H.D.G!F..:z... 7.....M}X...A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c7e0d0bc770e0d8b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	344
Entropy (8bit):	5.837531612429745
Encrypted:	false
SSDEEP:	6:mcallVY07A0NApRKhHTQ6YpIyKnHrEK6tUYJlClx1uiMRv6SRwnHr3l:HuzMKW6ERMSOYWsQvj8
MD5:	A2156D2BE6C27526E4E7785C688D25A5
SHA1:	056BC33FBD1DD57A638A9A7E2E3819D7072714D8
SHA-256:	92C0850A0A56AF8D93CA4571C0ED0A164011DB2E27D1A0B7E59B052DC0DCC5C9
SHA-512:	0D6CCA27C2F9BB1078E4640D65A229843A8E99B072825834BDBEFFF454437CA8C3E35AC38DDBE5BA310382E272D97526136158616C364219D98362A6226B58D0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....._keyhttps://commerce.adobe.com/checkout/_nuxt/app.f6f17c7.js .https://adobe.com/.... /.....A..W:..X...@.F..K..b.*)[.....A..Eo.....?3.....A..Eo.....A76D02127A130EB42F8DE51D72F268A0F8227A7DF39FB3EB07E43C5D46FF3D5B.A..W:..X...@.F..K..b.*)[.....A..Eo.....L.....

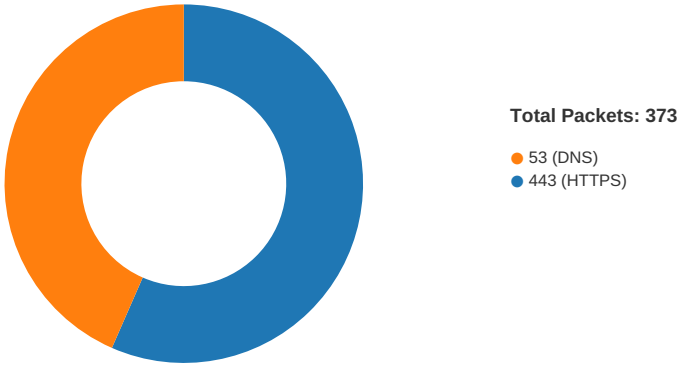
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cb1260c04c646798_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	234
Entropy (8bit):	5.542746610626526
Encrypted:	false
SSDEEP:	6:msXYET08NaYWbVOqZeY7fLlYKkyTawKPX7AWzbK6t:pg8NaY8ZDfLDY7zzN
MD5:	14FD9B1AEE2DDD7CCC422299FD3B9B39
SHA1:	C4BCE98A527119A066919AE2D62EE5E38D214568
SHA-256:	7FA240439641229A5B0CB0703D2483D49AD45A171BF01559C780EFB2E250D882
SHA-512:	844EA40777CF386C8078ECD8EB494688391A15A6B3ED01A990EC789A4213FEE8D0ED163E1732E340F9E9C0FCD2AB77976E9D163B95555434A65FD0A0072CAD8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f....._keyhttps://cdnjs.cloudflare.com/ajax/libs/popper.js/1.12.9/umd/popper.min.js .https://greycottage.ng/.... /.....F.....J..B.BPuJY...KB....gK..>V.....A..Eo....."|.6.....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 12, 2021 21:20:52.445347071 CEST	49713	443	192.168.2.6	13.225.74.123
May 12, 2021 21:20:52.486869097 CEST	443	49713	13.225.74.123	192.168.2.6
May 12, 2021 21:20:52.486982107 CEST	49713	443	192.168.2.6	13.225.74.123
May 12, 2021 21:20:52.488173008 CEST	49713	443	192.168.2.6	13.225.74.123
May 12, 2021 21:20:52.513917923 CEST	443	49713	13.225.74.123	192.168.2.6
May 12, 2021 21:20:52.514091015 CEST	49713	443	192.168.2.6	13.225.74.123
May 12, 2021 21:20:52.530558109 CEST	443	49713	13.225.74.123	192.168.2.6
May 12, 2021 21:20:52.536628008 CEST	443	49713	13.225.74.123	192.168.2.6
May 12, 2021 21:20:52.536676884 CEST	443	49713	13.225.74.123	192.168.2.6
May 12, 2021 21:20:52.536813021 CEST	49713	443	192.168.2.6	13.225.74.123
May 12, 2021 21:20:52.543195009 CEST	443	49713	13.225.74.123	192.168.2.6
May 12, 2021 21:20:52.543236971 CEST	443	49713	13.225.74.123	192.168.2.6
May 12, 2021 21:20:52.543346882 CEST	49713	443	192.168.2.6	13.225.74.123
May 12, 2021 21:20:52.992868900 CEST	49713	443	192.168.2.6	13.225.74.123
May 12, 2021 21:20:52.994143009 CEST	49713	443	192.168.2.6	13.225.74.123
May 12, 2021 21:20:52.994467974 CEST	49713	443	192.168.2.6	13.225.74.123
May 12, 2021 21:20:53.034122944 CEST	443	49713	13.225.74.123	192.168.2.6
May 12, 2021 21:20:53.035284996 CEST	443	49713	13.225.74.123	192.168.2.6
May 12, 2021 21:20:53.035665035 CEST	443	49713	13.225.74.123	192.168.2.6
May 12, 2021 21:20:53.036406994 CEST	443	49713	13.225.74.123	192.168.2.6
May 12, 2021 21:20:53.042538881 CEST	49713	443	192.168.2.6	13.225.74.123
May 12, 2021 21:20:53.089241028 CEST	443	49713	13.225.74.123	192.168.2.6
May 12, 2021 21:20:53.430124998 CEST	443	49713	13.225.74.123	192.168.2.6
May 12, 2021 21:20:53.430166960 CEST	443	49713	13.225.74.123	192.168.2.6
May 12, 2021 21:20:53.430186987 CEST	443	49713	13.225.74.123	192.168.2.6
May 12, 2021 21:20:53.430210114 CEST	443	49713	13.225.74.123	192.168.2.6
May 12, 2021 21:20:53.430232048 CEST	443	49713	13.225.74.123	192.168.2.6
May 12, 2021 21:20:53.430255890 CEST	443	49713	13.225.74.123	192.168.2.6
May 12, 2021 21:20:53.430368900 CEST	49713	443	192.168.2.6	13.225.74.123
May 12, 2021 21:20:53.430403948 CEST	49713	443	192.168.2.6	13.225.74.123
May 12, 2021 21:20:53.431209087 CEST	443	49713	13.225.74.123	192.168.2.6
May 12, 2021 21:20:53.522566080 CEST	49713	443	192.168.2.6	13.225.74.123
May 12, 2021 21:20:53.603332996 CEST	49720	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.603694916 CEST	49721	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.604285002 CEST	49722	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.604720116 CEST	49723	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.604994059 CEST	49724	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.644614935 CEST	443	49720	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.644711971 CEST	49720	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.645036936 CEST	443	49721	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.645103931 CEST	49720	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.645148039 CEST	49721	443	192.168.2.6	13.224.193.29

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:20:53.645466089 CEST	49721	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.645550013 CEST	443	49722	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.645788908 CEST	443	49723	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.645857096 CEST	49723	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.645889997 CEST	49722	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.645998955 CEST	49722	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.646203995 CEST	49723	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.646356106 CEST	443	49724	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.646445990 CEST	49724	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.646953106 CEST	49724	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.656048059 CEST	443	49720	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.656130075 CEST	49720	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.657207966 CEST	443	49721	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.657298088 CEST	49721	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.659040928 CEST	443	49724	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.659126043 CEST	49724	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.662375927 CEST	443	49723	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.662493944 CEST	49723	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.667052984 CEST	443	49722	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.667145967 CEST	49722	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.686362982 CEST	443	49720	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.686500072 CEST	443	49721	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.687083960 CEST	443	49721	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.687108994 CEST	443	49721	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.687151909 CEST	443	49722	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.687160015 CEST	49721	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.687227011 CEST	443	49723	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.687273979 CEST	443	49720	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.687299013 CEST	443	49720	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.687449932 CEST	49720	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.688038111 CEST	443	49724	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.689280033 CEST	443	49721	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.689306021 CEST	443	49721	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.689374924 CEST	49721	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.691262960 CEST	443	49722	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.691340923 CEST	443	49722	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.691425085 CEST	49722	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.691987991 CEST	443	49723	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.692015886 CEST	443	49723	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.692084074 CEST	49723	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.692455053 CEST	443	49720	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.692475080 CEST	443	49720	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.692564964 CEST	49720	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.694153070 CEST	443	49724	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.694189072 CEST	443	49724	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.694271088 CEST	49724	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.695491076 CEST	443	49722	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.695848942 CEST	443	49723	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.702294111 CEST	443	49724	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.702321053 CEST	443	49724	13.224.193.29	192.168.2.6
May 12, 2021 21:20:53.702399015 CEST	49724	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.712491989 CEST	49721	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.714092970 CEST	49720	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.715432882 CEST	49724	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.715909958 CEST	49720	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.716027021 CEST	49724	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.716433048 CEST	49721	443	192.168.2.6	13.224.193.29
May 12, 2021 21:20:53.716495991 CEST	49722	443	192.168.2.6	13.224.193.29

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:20:42.011099100 CEST	53	55074	8.8.8.8	192.168.2.6
May 12, 2021 21:20:42.613434076 CEST	54513	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:20:42.664920092 CEST	53	54513	8.8.8.8	192.168.2.6
May 12, 2021 21:20:44.099006891 CEST	62044	53	192.168.2.6	8.8.8.8
May 12, 2021 21:20:44.151662111 CEST	53	62044	8.8.8.8	192.168.2.6
May 12, 2021 21:20:45.322998047 CEST	63791	53	192.168.2.6	8.8.8.8
May 12, 2021 21:20:45.374624968 CEST	53	63791	8.8.8.8	192.168.2.6
May 12, 2021 21:20:46.665273905 CEST	64267	53	192.168.2.6	8.8.8.8
May 12, 2021 21:20:46.716804981 CEST	53	64267	8.8.8.8	192.168.2.6
May 12, 2021 21:20:47.789921045 CEST	49448	53	192.168.2.6	8.8.8.8
May 12, 2021 21:20:47.839503050 CEST	53	49448	8.8.8.8	192.168.2.6
May 12, 2021 21:20:50.213520050 CEST	60342	53	192.168.2.6	8.8.8.8
May 12, 2021 21:20:50.262177944 CEST	53	60342	8.8.8.8	192.168.2.6
May 12, 2021 21:20:52.034101963 CEST	56023	53	192.168.2.6	8.8.8.8
May 12, 2021 21:20:52.035248041 CEST	58384	53	192.168.2.6	8.8.8.8
May 12, 2021 21:20:52.035871029 CEST	60261	53	192.168.2.6	8.8.8.8
May 12, 2021 21:20:52.042828083 CEST	56061	53	192.168.2.6	8.8.8.8
May 12, 2021 21:20:52.084486008 CEST	53	60261	8.8.8.8	192.168.2.6
May 12, 2021 21:20:52.096326113 CEST	53	56023	8.8.8.8	192.168.2.6
May 12, 2021 21:20:52.097846985 CEST	53	58384	8.8.8.8	192.168.2.6
May 12, 2021 21:20:52.115750074 CEST	53	56061	8.8.8.8	192.168.2.6
May 12, 2021 21:20:53.081893921 CEST	53781	53	192.168.2.6	8.8.8.8
May 12, 2021 21:20:53.147403955 CEST	53	53781	8.8.8.8	192.168.2.6
May 12, 2021 21:20:53.258873940 CEST	54064	53	192.168.2.6	8.8.8.8
May 12, 2021 21:20:53.328038931 CEST	53	54064	8.8.8.8	192.168.2.6
May 12, 2021 21:20:53.332154036 CEST	52811	53	192.168.2.6	8.8.8.8
May 12, 2021 21:20:53.380929947 CEST	53	52811	8.8.8.8	192.168.2.6
May 12, 2021 21:20:53.539518118 CEST	55299	53	192.168.2.6	8.8.8.8
May 12, 2021 21:20:53.600004911 CEST	53	55299	8.8.8.8	192.168.2.6
May 12, 2021 21:20:53.815376997 CEST	63745	53	192.168.2.6	8.8.8.8
May 12, 2021 21:20:53.875915051 CEST	53	63745	8.8.8.8	192.168.2.6
May 12, 2021 21:20:53.990200043 CEST	50055	53	192.168.2.6	8.8.8.8
May 12, 2021 21:20:54.064040899 CEST	53	50055	8.8.8.8	192.168.2.6
May 12, 2021 21:20:54.627326012 CEST	61374	53	192.168.2.6	8.8.8.8
May 12, 2021 21:20:54.680233002 CEST	53	61374	8.8.8.8	192.168.2.6
May 12, 2021 21:20:54.786550045 CEST	50339	53	192.168.2.6	8.8.8.8
May 12, 2021 21:20:54.838016987 CEST	53	50339	8.8.8.8	192.168.2.6
May 12, 2021 21:20:55.036526918 CEST	63307	53	192.168.2.6	8.8.8.8
May 12, 2021 21:20:55.090486050 CEST	53	63307	8.8.8.8	192.168.2.6
May 12, 2021 21:20:57.525540113 CEST	63718	53	192.168.2.6	8.8.8.8
May 12, 2021 21:20:57.608205080 CEST	53	63718	8.8.8.8	192.168.2.6
May 12, 2021 21:20:57.725526094 CEST	62116	53	192.168.2.6	8.8.8.8
May 12, 2021 21:20:57.789710045 CEST	53	62116	8.8.8.8	192.168.2.6
May 12, 2021 21:20:58.183748007 CEST	63816	53	192.168.2.6	8.8.8.8
May 12, 2021 21:20:58.234232903 CEST	53	63816	8.8.8.8	192.168.2.6
May 12, 2021 21:20:58.492057085 CEST	55014	53	192.168.2.6	8.8.8.8
May 12, 2021 21:20:58.564223051 CEST	53	55014	8.8.8.8	192.168.2.6
May 12, 2021 21:21:01.504690886 CEST	51818	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:01.569797039 CEST	53	51818	8.8.8.8	192.168.2.6
May 12, 2021 21:21:07.078243017 CEST	60778	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:07.127002954 CEST	53	60778	8.8.8.8	192.168.2.6
May 12, 2021 21:21:12.384147882 CEST	53799	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:12.435957909 CEST	53	53799	8.8.8.8	192.168.2.6
May 12, 2021 21:21:13.257110119 CEST	54683	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:13.305795908 CEST	53	54683	8.8.8.8	192.168.2.6
May 12, 2021 21:21:13.439686060 CEST	59329	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:13.488878965 CEST	53	59329	8.8.8.8	192.168.2.6
May 12, 2021 21:21:13.981036901 CEST	64021	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:14.034221888 CEST	53	64021	8.8.8.8	192.168.2.6
May 12, 2021 21:21:15.908380032 CEST	56129	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:15.910207033 CEST	58177	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:15.913331032 CEST	50700	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:15.915039062 CEST	54069	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:15.916712046 CEST	61178	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:15.963061094 CEST	53	58177	8.8.8.8	192.168.2.6
May 12, 2021 21:21:15.969769001 CEST	53	56129	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:21:15.972841978 CEST	53	54069	8.8.8.8	192.168.2.6
May 12, 2021 21:21:15.973402023 CEST	53	50700	8.8.8.8	192.168.2.6
May 12, 2021 21:21:15.986399889 CEST	53	61178	8.8.8.8	192.168.2.6
May 12, 2021 21:21:17.034338951 CEST	57017	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:17.091557026 CEST	53	57017	8.8.8.8	192.168.2.6
May 12, 2021 21:21:17.374811888 CEST	56327	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:17.421921015 CEST	50243	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:17.434900999 CEST	53	56327	8.8.8.8	192.168.2.6
May 12, 2021 21:21:17.485511065 CEST	53	50243	8.8.8.8	192.168.2.6
May 12, 2021 21:21:17.675700903 CEST	62055	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:17.724441051 CEST	53	62055	8.8.8.8	192.168.2.6
May 12, 2021 21:21:18.722870111 CEST	61249	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:18.771661043 CEST	53	61249	8.8.8.8	192.168.2.6
May 12, 2021 21:21:19.203511953 CEST	65252	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:19.252346992 CEST	53	65252	8.8.8.8	192.168.2.6
May 12, 2021 21:21:19.326303005 CEST	64367	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:19.383588076 CEST	53	64367	8.8.8.8	192.168.2.6
May 12, 2021 21:21:20.030922890 CEST	55066	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:20.079730988 CEST	53	55066	8.8.8.8	192.168.2.6
May 12, 2021 21:21:21.212078094 CEST	60211	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:21.264300108 CEST	53	60211	8.8.8.8	192.168.2.6
May 12, 2021 21:21:24.436939001 CEST	56570	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:24.494152069 CEST	53	56570	8.8.8.8	192.168.2.6
May 12, 2021 21:21:27.646476030 CEST	58454	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:27.695135117 CEST	53	58454	8.8.8.8	192.168.2.6
May 12, 2021 21:21:27.786263943 CEST	55180	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:27.847755909 CEST	53	55180	8.8.8.8	192.168.2.6
May 12, 2021 21:21:29.755239964 CEST	58721	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:29.812824965 CEST	53	58721	8.8.8.8	192.168.2.6
May 12, 2021 21:21:30.066914082 CEST	57691	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:30.128437042 CEST	53	57691	8.8.8.8	192.168.2.6
May 12, 2021 21:21:30.714517117 CEST	52943	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:30.741446018 CEST	59489	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:30.795042038 CEST	53	52943	8.8.8.8	192.168.2.6
May 12, 2021 21:21:30.799909115 CEST	64022	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:30.802408934 CEST	53	59489	8.8.8.8	192.168.2.6
May 12, 2021 21:21:30.819286108 CEST	60023	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:30.858906984 CEST	53	64022	8.8.8.8	192.168.2.6
May 12, 2021 21:21:30.879559994 CEST	53	60023	8.8.8.8	192.168.2.6
May 12, 2021 21:21:31.019823074 CEST	57193	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:31.033823967 CEST	50248	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:31.079431057 CEST	53	57193	8.8.8.8	192.168.2.6
May 12, 2021 21:21:31.094820976 CEST	53	50248	8.8.8.8	192.168.2.6
May 12, 2021 21:21:31.254123926 CEST	64413	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:31.313230991 CEST	53	64413	8.8.8.8	192.168.2.6
May 12, 2021 21:21:31.427840948 CEST	60429	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:31.491921902 CEST	53	60429	8.8.8.8	192.168.2.6
May 12, 2021 21:21:31.554650068 CEST	60345	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:31.616642952 CEST	53	60345	8.8.8.8	192.168.2.6
May 12, 2021 21:21:32.520409107 CEST	53830	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:32.584969044 CEST	53	53830	8.8.8.8	192.168.2.6
May 12, 2021 21:21:32.586463928 CEST	57226	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:32.640019894 CEST	57880	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:32.654850960 CEST	53	57226	8.8.8.8	192.168.2.6
May 12, 2021 21:21:32.705813885 CEST	53	57880	8.8.8.8	192.168.2.6
May 12, 2021 21:21:33.589492083 CEST	60850	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:33.652601957 CEST	53	60850	8.8.8.8	192.168.2.6
May 12, 2021 21:21:33.779249907 CEST	53187	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:33.860136032 CEST	53	53187	8.8.8.8	192.168.2.6
May 12, 2021 21:21:33.981010914 CEST	55830	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:34.043633938 CEST	53	55830	8.8.8.8	192.168.2.6
May 12, 2021 21:21:34.079061985 CEST	55145	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:34.110538960 CEST	64091	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:34.147519112 CEST	53	55145	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:21:34.159473896 CEST	53	64091	8.8.8.8	192.168.2.6
May 12, 2021 21:21:34.208079100 CEST	55728	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:34.268110037 CEST	53	55728	8.8.8.8	192.168.2.6
May 12, 2021 21:21:34.269778967 CEST	55694	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:34.282058954 CEST	53926	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:34.331413031 CEST	53	55694	8.8.8.8	192.168.2.6
May 12, 2021 21:21:34.341939926 CEST	53	53926	8.8.8.8	192.168.2.6
May 12, 2021 21:21:34.696458101 CEST	65531	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:34.733449936 CEST	65437	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:34.756037951 CEST	53	65531	8.8.8.8	192.168.2.6
May 12, 2021 21:21:34.801822901 CEST	53	65437	8.8.8.8	192.168.2.6
May 12, 2021 21:21:35.049593925 CEST	65439	443	192.168.2.6	142.250.185.102
May 12, 2021 21:21:35.105300903 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:21:35.105369091 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:21:35.105514050 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:21:35.105648994 CEST	65439	443	192.168.2.6	142.250.185.102
May 12, 2021 21:21:35.107098103 CEST	65439	443	192.168.2.6	142.250.185.102
May 12, 2021 21:21:35.107424021 CEST	65439	443	192.168.2.6	142.250.185.102
May 12, 2021 21:21:35.169495106 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:21:35.173562050 CEST	65439	443	192.168.2.6	142.250.185.102
May 12, 2021 21:21:35.183480978 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:21:35.183506966 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:21:35.183844090 CEST	65439	443	192.168.2.6	142.250.185.102
May 12, 2021 21:21:35.460413933 CEST	54590	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:35.490502119 CEST	51318	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:35.493350983 CEST	60888	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:35.494102955 CEST	58474	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:35.517591000 CEST	53	54590	8.8.8.8	192.168.2.6
May 12, 2021 21:21:35.522293091 CEST	64575	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:35.524754047 CEST	59092	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:35.540509939 CEST	53	51318	8.8.8.8	192.168.2.6
May 12, 2021 21:21:35.543649912 CEST	53	60888	8.8.8.8	192.168.2.6
May 12, 2021 21:21:35.572267056 CEST	53	58474	8.8.8.8	192.168.2.6
May 12, 2021 21:21:35.575242043 CEST	53	59092	8.8.8.8	192.168.2.6
May 12, 2021 21:21:35.582792997 CEST	53	64575	8.8.8.8	192.168.2.6
May 12, 2021 21:21:35.595820904 CEST	57483	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:35.651597977 CEST	53830	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:35.653215885 CEST	49809	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:35.654547930 CEST	53	57483	8.8.8.8	192.168.2.6
May 12, 2021 21:21:35.656128883 CEST	52814	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:35.713948011 CEST	53	53830	8.8.8.8	192.168.2.6
May 12, 2021 21:21:35.714782953 CEST	53	49809	8.8.8.8	192.168.2.6
May 12, 2021 21:21:35.715301991 CEST	53	52814	8.8.8.8	192.168.2.6
May 12, 2021 21:21:35.861202955 CEST	51069	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:35.864729881 CEST	65439	443	192.168.2.6	142.250.185.102
May 12, 2021 21:21:35.926114082 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:21:35.926265001 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:21:35.926292896 CEST	53	51069	8.8.8.8	192.168.2.6
May 12, 2021 21:21:35.932604074 CEST	65439	443	192.168.2.6	142.250.185.102
May 12, 2021 21:21:35.960530996 CEST	65439	443	192.168.2.6	142.250.185.102
May 12, 2021 21:21:36.028019905 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:21:36.028136015 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:21:36.028337955 CEST	65439	443	192.168.2.6	142.250.185.102
May 12, 2021 21:21:36.201260090 CEST	56526	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:36.209296942 CEST	50512	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:36.227003098 CEST	51679	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:36.250025988 CEST	53	56526	8.8.8.8	192.168.2.6
May 12, 2021 21:21:36.258224010 CEST	53	50512	8.8.8.8	192.168.2.6
May 12, 2021 21:21:36.278764963 CEST	53	51679	8.8.8.8	192.168.2.6
May 12, 2021 21:21:36.299803019 CEST	56071	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:36.357319117 CEST	53	56071	8.8.8.8	192.168.2.6
May 12, 2021 21:21:36.770916939 CEST	58950	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:36.772147894 CEST	57035	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:36.830018997 CEST	53	58950	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:21:36.835088015 CEST	53	57035	8.8.8.8	192.168.2.6
May 12, 2021 21:21:37.273519039 CEST	54122	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:37.336332083 CEST	53	54122	8.8.8.8	192.168.2.6
May 12, 2021 21:21:37.801129103 CEST	56759	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:37.853029966 CEST	53	56759	8.8.8.8	192.168.2.6
May 12, 2021 21:21:38.109608889 CEST	59220	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:38.180305958 CEST	53	59220	8.8.8.8	192.168.2.6
May 12, 2021 21:21:40.420047045 CEST	62211	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:40.468736887 CEST	53	62211	8.8.8.8	192.168.2.6
May 12, 2021 21:21:40.798075914 CEST	62033	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:40.846952915 CEST	53	62033	8.8.8.8	192.168.2.6
May 12, 2021 21:21:40.998821020 CEST	61244	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:41.065072060 CEST	53	61244	8.8.8.8	192.168.2.6
May 12, 2021 21:21:41.501130104 CEST	53696	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:41.539350986 CEST	50733	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:41.568351984 CEST	53	53696	8.8.8.8	192.168.2.6
May 12, 2021 21:21:41.588181973 CEST	53	50733	8.8.8.8	192.168.2.6
May 12, 2021 21:21:42.082798004 CEST	55770	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:42.132499933 CEST	53	55770	8.8.8.8	192.168.2.6
May 12, 2021 21:21:42.316118002 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:42.363800049 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:42.363822937 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:42.363842964 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:42.364288092 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:42.366313934 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:42.367311954 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:42.398540974 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:42.402626991 CEST	54525	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:42.421130896 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:42.421694994 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:42.439517021 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:42.454022884 CEST	53	54525	8.8.8.8	192.168.2.6
May 12, 2021 21:21:42.454770088 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:42.454788923 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:42.455002069 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:42.455332041 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:42.471285105 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:42.471565008 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:42.471679926 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:42.497689009 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:43.539113045 CEST	61760	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:43.613306046 CEST	53	61760	8.8.8.8	192.168.2.6
May 12, 2021 21:21:43.947962046 CEST	63822	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:44.042687893 CEST	53	63822	8.8.8.8	192.168.2.6
May 12, 2021 21:21:44.801426888 CEST	50957	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:44.859424114 CEST	59666	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:44.864471912 CEST	53	50957	8.8.8.8	192.168.2.6
May 12, 2021 21:21:44.884291887 CEST	52223	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:44.893419981 CEST	60136	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:44.911204100 CEST	53	59666	8.8.8.8	192.168.2.6
May 12, 2021 21:21:44.946295977 CEST	53	52223	8.8.8.8	192.168.2.6
May 12, 2021 21:21:44.950849056 CEST	53	60136	8.8.8.8	192.168.2.6
May 12, 2021 21:21:45.184781075 CEST	55649	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:45.245014906 CEST	53	55649	8.8.8.8	192.168.2.6
May 12, 2021 21:21:45.247562885 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:45.303659916 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:45.303708076 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:45.303744078 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:45.303968906 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:45.306756020 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:45.307480097 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:45.330986977 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:45.369508982 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:45.371210098 CEST	55650	443	192.168.2.6	142.250.186.99

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:21:45.384571075 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:45.384598017 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:45.385503054 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:45.387461901 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:45.387594938 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:45.387753963 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:45.388137102 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:45.438608885 CEST	65439	443	192.168.2.6	142.250.185.102
May 12, 2021 21:21:45.453790903 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:45.500633955 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:21:45.500669956 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:21:45.501219988 CEST	65439	443	192.168.2.6	142.250.185.102
May 12, 2021 21:21:45.565363884 CEST	65439	443	192.168.2.6	142.250.185.102
May 12, 2021 21:21:45.639442921 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:21:45.641046047 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:21:45.641134977 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:21:45.641655922 CEST	65439	443	192.168.2.6	142.250.185.102
May 12, 2021 21:21:45.655107021 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:45.720917940 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:45.741780996 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:45.741805077 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:45.742172003 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:45.782216072 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:45.848170042 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:45.870244026 CEST	55652	443	192.168.2.6	35.186.226.184
May 12, 2021 21:21:45.876600027 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:45.913039923 CEST	443	55652	35.186.226.184	192.168.2.6
May 12, 2021 21:21:45.913065910 CEST	443	55652	35.186.226.184	192.168.2.6
May 12, 2021 21:21:45.915436029 CEST	55652	443	192.168.2.6	35.186.226.184
May 12, 2021 21:21:45.915898085 CEST	55652	443	192.168.2.6	35.186.226.184
May 12, 2021 21:21:45.923602104 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:45.942802906 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:45.966476917 CEST	443	55652	35.186.226.184	192.168.2.6
May 12, 2021 21:21:45.967057943 CEST	55652	443	192.168.2.6	35.186.226.184
May 12, 2021 21:21:45.967479944 CEST	55652	443	192.168.2.6	35.186.226.184
May 12, 2021 21:21:45.980801105 CEST	443	55652	35.186.226.184	192.168.2.6
May 12, 2021 21:21:45.988188982 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:46.008598089 CEST	55652	443	192.168.2.6	35.186.226.184
May 12, 2021 21:21:46.011126041 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:46.011212111 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:46.013995886 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:46.014370918 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:46.026978970 CEST	443	55652	35.186.226.184	192.168.2.6
May 12, 2021 21:21:46.041773081 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:46.053749084 CEST	55652	443	192.168.2.6	35.186.226.184
May 12, 2021 21:21:46.108349085 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:46.113226891 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:46.176719904 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:46.176866055 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:46.177175999 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:46.237020016 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:46.292037964 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:46.292229891 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:46.300745010 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:46.303098917 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:46.306806087 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:46.307998896 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:46.331430912 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:46.350200891 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:46.360722065 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:46.369652033 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:46.370275021 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:46.370497942 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:46.379636049 CEST	55650	443	192.168.2.6	142.250.186.99

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:21:46.393398046 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:46.394824028 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:46.394849062 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:46.395620108 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:46.400407076 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:46.400538921 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:46.404649973 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:46.406279087 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:46.417804956 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:46.425355911 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:46.425725937 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:46.426002979 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:46.430160999 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:46.439229965 CEST	51524	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:46.444978952 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:46.445112944 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:46.445662022 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:46.466451883 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:46.469495058 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:46.469646931 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:46.470038891 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:46.482911110 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:46.484580040 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:46.484849930 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:46.500052929 CEST	53	51524	8.8.8.8	192.168.2.6
May 12, 2021 21:21:46.526153088 CEST	59141	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:46.539649963 CEST	49682	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:46.555052042 CEST	49709	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:46.596760988 CEST	53	49682	8.8.8.8	192.168.2.6
May 12, 2021 21:21:46.606626034 CEST	53	49709	8.8.8.8	192.168.2.6
May 12, 2021 21:21:46.617319107 CEST	53	59141	8.8.8.8	192.168.2.6
May 12, 2021 21:21:46.935827971 CEST	55652	443	192.168.2.6	35.186.226.184
May 12, 2021 21:21:46.991564035 CEST	443	55652	35.186.226.184	192.168.2.6
May 12, 2021 21:21:47.017611980 CEST	55652	443	192.168.2.6	35.186.226.184
May 12, 2021 21:21:47.019771099 CEST	59384	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:47.079744101 CEST	53	59384	8.8.8.8	192.168.2.6
May 12, 2021 21:21:47.816217899 CEST	55652	443	192.168.2.6	35.186.226.184
May 12, 2021 21:21:47.868645906 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:47.875652075 CEST	443	55652	35.186.226.184	192.168.2.6
May 12, 2021 21:21:47.909837961 CEST	55652	443	192.168.2.6	35.186.226.184
May 12, 2021 21:21:47.925225973 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:47.926073074 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:47.926275969 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:48.179645061 CEST	50284	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:48.229043007 CEST	53	50284	8.8.8.8	192.168.2.6
May 12, 2021 21:21:48.279221058 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:48.344120979 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:48.344149113 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:48.344531059 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:48.631136894 CEST	53089	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:48.680860043 CEST	53	53089	8.8.8.8	192.168.2.6
May 12, 2021 21:21:48.729473114 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:48.733664989 CEST	50563	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:48.741000891 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:48.743807077 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:48.782032013 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:48.785264969 CEST	53	50563	8.8.8.8	192.168.2.6
May 12, 2021 21:21:48.786820889 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:48.787045956 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:48.787290096 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:48.800451994 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:48.800745010 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:48.801013947 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:48.806363106 CEST	55650	443	192.168.2.6	142.250.186.99

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:21:48.829267979 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:48.829404116 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:48.829632044 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:48.839030027 CEST	50265	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:48.865186930 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:48.871045113 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:48.871069908 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:48.871362925 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:48.902784109 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:48.927777052 CEST	53	50265	8.8.8.8	192.168.2.6
May 12, 2021 21:21:48.929588079 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:48.929610014 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:48.930612087 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:48.940691948 CEST	55442	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:48.943923950 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:48.966115952 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:48.992058992 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:49.000449896 CEST	53	55442	8.8.8.8	192.168.2.6
May 12, 2021 21:21:49.009032011 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:49.009061098 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:49.009413004 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:49.056749105 CEST	49561	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:49.123723030 CEST	53	49561	8.8.8.8	192.168.2.6
May 12, 2021 21:21:49.220597029 CEST	54097	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:49.277978897 CEST	53	54097	8.8.8.8	192.168.2.6
May 12, 2021 21:21:49.319024086 CEST	59502	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:49.394958019 CEST	53	59502	8.8.8.8	192.168.2.6
May 12, 2021 21:21:49.421844959 CEST	57959	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:49.430138111 CEST	54971	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:49.482047081 CEST	53	57959	8.8.8.8	192.168.2.6
May 12, 2021 21:21:49.487586975 CEST	53	54971	8.8.8.8	192.168.2.6
May 12, 2021 21:21:49.542217970 CEST	50969	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:49.601685047 CEST	53	50969	8.8.8.8	192.168.2.6
May 12, 2021 21:21:49.647980928 CEST	52183	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:49.696608067 CEST	53	52183	8.8.8.8	192.168.2.6
May 12, 2021 21:21:49.910229921 CEST	63354	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:49.978682041 CEST	53	63354	8.8.8.8	192.168.2.6
May 12, 2021 21:21:50.980043888 CEST	61603	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:51.051597118 CEST	53	61603	8.8.8.8	192.168.2.6
May 12, 2021 21:21:52.770406961 CEST	58318	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:52.853352070 CEST	53	58318	8.8.8.8	192.168.2.6
May 12, 2021 21:21:53.545368910 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:53.611483097 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:53.630554914 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:53.630752087 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:53.631041050 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:53.643543959 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:53.643682957 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:53.684411049 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:53.699300051 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:53.699431896 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:53.700212955 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:53.703092098 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:53.735718012 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:53.769504070 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:53.809978008 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:53.815892935 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:53.842958927 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:53.875876904 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:53.879978895 CEST	65439	443	192.168.2.6	142.250.185.102
May 12, 2021 21:21:53.941263914 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:21:53.941289902 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:21:53.941839933 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:53.942466021 CEST	65439	443	192.168.2.6	142.250.185.102

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:21:53.947714090 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:53.960194111 CEST	65439	443	192.168.2.6	142.250.185.102
May 12, 2021 21:21:53.962143898 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:53.962265968 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:53.962621927 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:53.984498024 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:53.987828970 CEST	55652	443	192.168.2.6	35.186.226.184
May 12, 2021 21:21:54.011018991 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:54.011272907 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:54.015398026 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:54.025672913 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:21:54.025775909 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:21:54.027059078 CEST	65439	443	192.168.2.6	142.250.185.102
May 12, 2021 21:21:54.043359041 CEST	443	55652	35.186.226.184	192.168.2.6
May 12, 2021 21:21:54.050712109 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:54.069091082 CEST	55652	443	192.168.2.6	35.186.226.184
May 12, 2021 21:21:54.193629980 CEST	55652	443	192.168.2.6	35.186.226.184
May 12, 2021 21:21:54.226114988 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:54.238857985 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:54.253370047 CEST	443	55652	35.186.226.184	192.168.2.6
May 12, 2021 21:21:54.286252022 CEST	55652	443	192.168.2.6	35.186.226.184
May 12, 2021 21:21:54.291910887 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:54.301372051 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:54.301954985 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:54.307761908 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:54.314030886 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:54.314126015 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:54.314577103 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:54.394881010 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:54.396569014 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:54.400778055 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:54.410012007 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:54.437454939 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:54.450808048 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:54.450932026 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:54.451215029 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:54.452174902 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:54.452477932 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:54.453017950 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:54.462258101 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:54.468579054 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:54.483834982 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:54.485856056 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:54.486015081 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:21:54.486213923 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:21:54.489330053 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:54.489483118 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:54.489677906 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:54.495285034 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:54.517211914 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:54.524463892 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:54.524707079 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:54.525515079 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:54.551800013 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:54.558366060 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:54.558610916 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:54.558723927 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:54.559051037 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:21:54.559596062 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:21:54.634258032 CEST	60826	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:54.693624020 CEST	53	60826	8.8.8.8	192.168.2.6
May 12, 2021 21:21:54.882203102 CEST	57763	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:54.943655014 CEST	53	57763	8.8.8.8	192.168.2.6
May 12, 2021 21:21:58.431173086 CEST	50111	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:21:58.520167112 CEST	53	50111	8.8.8.8	192.168.2.6
May 12, 2021 21:21:58.632989883 CEST	57206	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:58.695900917 CEST	53	57206	8.8.8.8	192.168.2.6
May 12, 2021 21:21:59.618535042 CEST	57132	53	192.168.2.6	8.8.8.8
May 12, 2021 21:21:59.670203924 CEST	53	57132	8.8.8.8	192.168.2.6
May 12, 2021 21:22:00.505672932 CEST	55483	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:00.564548016 CEST	61626	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:00.567595959 CEST	53	55483	8.8.8.8	192.168.2.6
May 12, 2021 21:22:00.631513119 CEST	53	61626	8.8.8.8	192.168.2.6
May 12, 2021 21:22:01.516689062 CEST	59675	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:01.575823069 CEST	53	59675	8.8.8.8	192.168.2.6
May 12, 2021 21:22:03.727763891 CEST	59678	443	192.168.2.6	142.250.186.130
May 12, 2021 21:22:03.783577919 CEST	443	59678	142.250.186.130	192.168.2.6
May 12, 2021 21:22:03.783615112 CEST	443	59678	142.250.186.130	192.168.2.6
May 12, 2021 21:22:03.783638954 CEST	443	59678	142.250.186.130	192.168.2.6
May 12, 2021 21:22:03.783926964 CEST	59678	443	192.168.2.6	142.250.186.130
May 12, 2021 21:22:03.785523891 CEST	59678	443	192.168.2.6	142.250.186.130
May 12, 2021 21:22:03.785876036 CEST	59678	443	192.168.2.6	142.250.186.130
May 12, 2021 21:22:03.848486900 CEST	443	59678	142.250.186.130	192.168.2.6
May 12, 2021 21:22:03.849174023 CEST	59678	443	192.168.2.6	142.250.186.130
May 12, 2021 21:22:03.858432055 CEST	443	59678	142.250.186.130	192.168.2.6
May 12, 2021 21:22:03.858469009 CEST	443	59678	142.250.186.130	192.168.2.6
May 12, 2021 21:22:03.858968019 CEST	59678	443	192.168.2.6	142.250.186.130
May 12, 2021 21:22:04.351713896 CEST	65439	443	192.168.2.6	142.250.185.102
May 12, 2021 21:22:04.410711050 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:22:04.410996914 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:22:04.413630962 CEST	65439	443	192.168.2.6	142.250.185.102
May 12, 2021 21:22:04.429117918 CEST	65439	443	192.168.2.6	142.250.185.102
May 12, 2021 21:22:04.442087889 CEST	65439	443	192.168.2.6	142.250.185.102
May 12, 2021 21:22:04.490792036 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:22:04.500703096 CEST	55652	443	192.168.2.6	35.186.226.184
May 12, 2021 21:22:04.507894039 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:22:04.508059978 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:22:04.508344889 CEST	65439	443	192.168.2.6	142.250.185.102
May 12, 2021 21:22:04.555515051 CEST	443	55652	35.186.226.184	192.168.2.6
May 12, 2021 21:22:04.580976009 CEST	55652	443	192.168.2.6	35.186.226.184
May 12, 2021 21:22:04.614221096 CEST	55652	443	192.168.2.6	35.186.226.184
May 12, 2021 21:22:04.628092051 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:22:04.674086094 CEST	443	55652	35.186.226.184	192.168.2.6
May 12, 2021 21:22:04.689450979 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:22:04.689476967 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:22:04.689964056 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:22:04.699444056 CEST	55652	443	192.168.2.6	35.186.226.184
May 12, 2021 21:22:04.821419954 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:22:04.822494030 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:22:04.822768927 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:22:04.826589108 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:22:04.863347054 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:22:04.879514933 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:22:04.879614115 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:22:04.880827904 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:22:04.900630951 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:22:04.908174038 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:22:04.908212900 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:22:04.908338070 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:22:04.908544064 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:22:04.908711910 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:22:04.908792973 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:22:04.909101963 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:22:04.934998035 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:22:05.001405954 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:22:05.002511024 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:22:05.003865957 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:22:05.051054955 CEST	443	55650	142.250.186.99	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:22:05.064569950 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:22:05.064708948 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:22:05.064930916 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:22:05.065184116 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:22:05.065562010 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:22:05.066724062 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:22:05.066837072 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:22:05.067219973 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:22:05.067337990 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:22:05.205755949 CEST	60149	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:05.351624012 CEST	53	60149	8.8.8.8	192.168.2.6
May 12, 2021 21:22:05.574019909 CEST	62141	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:05.632910013 CEST	53	62141	8.8.8.8	192.168.2.6
May 12, 2021 21:22:06.449197054 CEST	49345	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:06.517174959 CEST	53	49345	8.8.8.8	192.168.2.6
May 12, 2021 21:22:06.564177036 CEST	64074	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:06.613183022 CEST	53	64074	8.8.8.8	192.168.2.6
May 12, 2021 21:22:07.570317984 CEST	55829	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:07.620795965 CEST	53	55829	8.8.8.8	192.168.2.6
May 12, 2021 21:22:08.577070951 CEST	62260	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:08.625617981 CEST	53	62260	8.8.8.8	192.168.2.6
May 12, 2021 21:22:09.562063932 CEST	64211	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:09.610723019 CEST	53	64211	8.8.8.8	192.168.2.6
May 12, 2021 21:22:10.456907988 CEST	52578	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:10.518783092 CEST	53	52578	8.8.8.8	192.168.2.6
May 12, 2021 21:22:11.521178007 CEST	50711	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:11.582889080 CEST	53	50711	8.8.8.8	192.168.2.6
May 12, 2021 21:22:12.054426908 CEST	61820	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:12.115766048 CEST	53	61820	8.8.8.8	192.168.2.6
May 12, 2021 21:22:12.701036930 CEST	57735	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:12.752612114 CEST	53	57735	8.8.8.8	192.168.2.6
May 12, 2021 21:22:13.692915916 CEST	55006	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:13.715645075 CEST	56061	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:13.751591921 CEST	53	55006	8.8.8.8	192.168.2.6
May 12, 2021 21:22:13.797235966 CEST	53	56061	8.8.8.8	192.168.2.6
May 12, 2021 21:22:14.446685076 CEST	63969	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:14.505467892 CEST	53	63969	8.8.8.8	192.168.2.6
May 12, 2021 21:22:17.244101048 CEST	56101	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:17.253599882 CEST	62167	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:17.303749084 CEST	53	56101	8.8.8.8	192.168.2.6
May 12, 2021 21:22:17.318757057 CEST	53	62167	8.8.8.8	192.168.2.6
May 12, 2021 21:22:17.433581114 CEST	58929	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:17.498491049 CEST	53	58929	8.8.8.8	192.168.2.6
May 12, 2021 21:22:17.616470098 CEST	64113	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:17.678775072 CEST	53	64113	8.8.8.8	192.168.2.6
May 12, 2021 21:22:17.860172987 CEST	63520	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:17.917500973 CEST	53	63520	8.8.8.8	192.168.2.6
May 12, 2021 21:22:18.787743092 CEST	59678	443	192.168.2.6	142.250.186.130
May 12, 2021 21:22:18.861766100 CEST	443	59678	142.250.186.130	192.168.2.6
May 12, 2021 21:22:19.354811907 CEST	65439	443	192.168.2.6	142.250.185.102
May 12, 2021 21:22:19.430747032 CEST	443	65439	142.250.185.102	192.168.2.6
May 12, 2021 21:22:19.629802942 CEST	55771	443	192.168.2.6	216.58.212.130
May 12, 2021 21:22:19.695694923 CEST	443	55771	216.58.212.130	192.168.2.6
May 12, 2021 21:22:20.003818035 CEST	55650	443	192.168.2.6	142.250.186.99
May 12, 2021 21:22:20.078286886 CEST	443	55650	142.250.186.99	192.168.2.6
May 12, 2021 21:22:30.366733074 CEST	57347	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:30.478171110 CEST	53	57347	8.8.8.8	192.168.2.6
May 12, 2021 21:22:32.349503994 CEST	51839	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:32.406697989 CEST	53	51839	8.8.8.8	192.168.2.6
May 12, 2021 21:22:33.004770041 CEST	59552	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:33.053529978 CEST	53	59552	8.8.8.8	192.168.2.6
May 12, 2021 21:22:33.830091953 CEST	51149	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:33.897099972 CEST	53	51149	8.8.8.8	192.168.2.6
May 12, 2021 21:22:34.353488922 CEST	65392	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 21:22:34.410660028 CEST	53	65392	8.8.8.8	192.168.2.6
May 12, 2021 21:22:34.878062010 CEST	56831	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:34.937927961 CEST	53	56831	8.8.8.8	192.168.2.6
May 12, 2021 21:22:35.336535931 CEST	58224	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:35.442503929 CEST	53	58224	8.8.8.8	192.168.2.6
May 12, 2021 21:22:35.674159050 CEST	63852	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:35.739763975 CEST	53	63852	8.8.8.8	192.168.2.6
May 12, 2021 21:22:36.077120066 CEST	50342	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:36.134167910 CEST	53	50342	8.8.8.8	192.168.2.6
May 12, 2021 21:22:36.798407078 CEST	62748	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:36.858381033 CEST	53	62748	8.8.8.8	192.168.2.6
May 12, 2021 21:22:37.238198042 CEST	52084	53	192.168.2.6	8.8.8.8
May 12, 2021 21:22:37.301446915 CEST	53	52084	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 21:20:53.539518118 CEST	192.168.2.6	8.8.8.8	0x144a	Standard query (0)	page.adobe spark-assets.com	A (IP address)	IN (0x0001)
May 12, 2021 21:20:53.815376997 CEST	192.168.2.6	8.8.8.8	0x2769	Standard query (0)	use.typekit.net	A (IP address)	IN (0x0001)
May 12, 2021 21:20:54.627326012 CEST	192.168.2.6	8.8.8.8	0x12a3	Standard query (0)	s3.amazona ws.com	A (IP address)	IN (0x0001)
May 12, 2021 21:20:55.036526918 CEST	192.168.2.6	8.8.8.8	0x8582	Standard query (0)	p.typekit.net	A (IP address)	IN (0x0001)
May 12, 2021 21:20:57.725526094 CEST	192.168.2.6	8.8.8.8	0xd9b4	Standard query (0)	page.adobe spark-assets.com	A (IP address)	IN (0x0001)
May 12, 2021 21:20:58.492057085 CEST	192.168.2.6	8.8.8.8	0x433d	Standard query (0)	clients2.g oogleuserc ontent.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:13.439686060 CEST	192.168.2.6	8.8.8.8	0x1119	Standard query (0)	greycottage.ng	A (IP address)	IN (0x0001)
May 12, 2021 21:21:15.910207033 CEST	192.168.2.6	8.8.8.8	0x3df5	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:15.913331032 CEST	192.168.2.6	8.8.8.8	0x1a95	Standard query (0)	maxcdn.boo tstrapcdn.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:15.916712046 CEST	192.168.2.6	8.8.8.8	0xd008	Standard query (0)	kit.fontaw esome.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:17.374811888 CEST	192.168.2.6	8.8.8.8	0x5908	Standard query (0)	cdnjs.clou dflare.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:17.421921015 CEST	192.168.2.6	8.8.8.8	0xc4d9	Standard query (0)	ka-f.fonta wesome.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:19.203511953 CEST	192.168.2.6	8.8.8.8	0xad22	Standard query (0)	greycottage.ng	A (IP address)	IN (0x0001)
May 12, 2021 21:21:30.714517117 CEST	192.168.2.6	8.8.8.8	0x525a	Standard query (0)	static.ado belogin.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:30.799909115 CEST	192.168.2.6	8.8.8.8	0xbdc7	Standard query (0)	assets.ado bedtm.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:30.819286108 CEST	192.168.2.6	8.8.8.8	0x7131	Standard query (0)	cdn.cookie law.org	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.019823074 CEST	192.168.2.6	8.8.8.8	0xb8d5	Standard query (0)	adobe.tt.o mtrdc.net	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.254123926 CEST	192.168.2.6	8.8.8.8	0x3d86	Standard query (0)	geolocatio n.onetrust.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.427840948 CEST	192.168.2.6	8.8.8.8	0x3a27	Standard query (0)	dpm.demdex.net	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.554650068 CEST	192.168.2.6	8.8.8.8	0x29d1	Standard query (0)	ims-na1.ad obelogin.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:32.640019894 CEST	192.168.2.6	8.8.8.8	0x1a86	Standard query (0)	adobedc.de mdex.net	A (IP address)	IN (0x0001)
May 12, 2021 21:21:33.589492083 CEST	192.168.2.6	8.8.8.8	0xb086	Standard query (0)	api.demand base.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:33.981010914 CEST	192.168.2.6	8.8.8.8	0x5ddf	Standard query (0)	www.everes tjs.net	A (IP address)	IN (0x0001)
May 12, 2021 21:21:34.079061985 CEST	192.168.2.6	8.8.8.8	0x47b0	Standard query (0)	universal. iperceptions.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:34.110538960 CEST	192.168.2.6	8.8.8.8	0xf5f6	Standard query (0)	servedby.f lashtalking.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:34.208079100 CEST	192.168.2.6	8.8.8.8	0x6aa5	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:34.269778967 CEST	192.168.2.6	8.8.8.8	0x6f4b	Standard query (0)	scripts.de mandbase.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 21:21:34.282058954 CEST	192.168.2.6	8.8.8.8	0xe9ae	Standard query (0)	lasteventf-tm.everesttech.net	A (IP address)	IN (0x0001)
May 12, 2021 21:21:34.696458101 CEST	192.168.2.6	8.8.8.8	0xf0b0	Standard query (0)	d9.flashtalking.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:34.733449936 CEST	192.168.2.6	8.8.8.8	0x9381	Standard query (0)	9212252.fls.doubleclick.net	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.493350983 CEST	192.168.2.6	8.8.8.8	0x2581	Standard query (0)	static.ads-twitter.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.494102955 CEST	192.168.2.6	8.8.8.8	0x6c6a	Standard query (0)	pixel.everesttech.net	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.522293091 CEST	192.168.2.6	8.8.8.8	0x1e5b	Standard query (0)	sc-static.net	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.524754047 CEST	192.168.2.6	8.8.8.8	0xb0bc	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.595820904 CEST	192.168.2.6	8.8.8.8	0x98e5	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.651597977 CEST	192.168.2.6	8.8.8.8	0x3fe1	Standard query (0)	api.company-target.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.653215885 CEST	192.168.2.6	8.8.8.8	0x25a6	Standard query (0)	match.prod.bidr.io	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.656128883 CEST	192.168.2.6	8.8.8.8	0x6b8f	Standard query (0)	id.rlcdn.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:36.201260090 CEST	192.168.2.6	8.8.8.8	0xd511	Standard query (0)	tr.snapchat.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:36.209296942 CEST	192.168.2.6	8.8.8.8	0xe678	Standard query (0)	analytics.twitter.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:36.227003098 CEST	192.168.2.6	8.8.8.8	0x3afe	Standard query (0)	t.co	A (IP address)	IN (0x0001)
May 12, 2021 21:21:36.770916939 CEST	192.168.2.6	8.8.8.8	0xc6e5	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:36.772147894 CEST	192.168.2.6	8.8.8.8	0xb5db	Standard query (0)	segments.company-target.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:37.273519039 CEST	192.168.2.6	8.8.8.8	0x27e6	Standard query (0)	prod.adobeccstatic.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:38.109608889 CEST	192.168.2.6	8.8.8.8	0x9faa	Standard query (0)	bumper.adobeprojectm.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:40.420047045 CEST	192.168.2.6	8.8.8.8	0xc450	Standard query (0)	js-agent.newrelic.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:40.798075914 CEST	192.168.2.6	8.8.8.8	0xe32	Standard query (0)	bam.nr-data.net	A (IP address)	IN (0x0001)
May 12, 2021 21:21:40.998821020 CEST	192.168.2.6	8.8.8.8	0x9820	Standard query (0)	adservice.google.ch	A (IP address)	IN (0x0001)
May 12, 2021 21:21:41.539350986 CEST	192.168.2.6	8.8.8.8	0x4b60	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:42.082798004 CEST	192.168.2.6	8.8.8.8	0xcf6	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
May 12, 2021 21:21:43.539113045 CEST	192.168.2.6	8.8.8.8	0x717a	Standard query (0)	cm.everesttech.net	A (IP address)	IN (0x0001)
May 12, 2021 21:21:44.801426888 CEST	192.168.2.6	8.8.8.8	0xf7e9	Standard query (0)	adobe.demdex.net	A (IP address)	IN (0x0001)
May 12, 2021 21:21:44.859424114 CEST	192.168.2.6	8.8.8.8	0x85f1	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)
May 12, 2021 21:21:44.893419981 CEST	192.168.2.6	8.8.8.8	0x934d	Standard query (0)	api.iperceptions.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:46.439229965 CEST	192.168.2.6	8.8.8.8	0x77c	Standard query (0)	sd.iperceptions.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:46.526153088 CEST	192.168.2.6	8.8.8.8	0x279b	Standard query (0)	match.prod.bidr.io	A (IP address)	IN (0x0001)
May 12, 2021 21:21:46.539649963 CEST	192.168.2.6	8.8.8.8	0x9881	Standard query (0)	id.rlcdn.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:47.019771099 CEST	192.168.2.6	8.8.8.8	0x14be	Standard query (0)	segments.company-target.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:48.179645061 CEST	192.168.2.6	8.8.8.8	0x515b	Standard query (0)	aa.agkn.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:48.631136894 CEST	192.168.2.6	8.8.8.8	0xf766	Standard query (0)	sync.mathtag.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:48.733664989 CEST	192.168.2.6	8.8.8.8	0x3770	Standard query (0)	idsync.rlcdn.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:48.839030027 CEST	192.168.2.6	8.8.8.8	0x77e0	Standard query (0)	d.turn.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:48.940691948 CEST	192.168.2.6	8.8.8.8	0x4b36	Standard query (0)	pixel.tapad.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 21:21:49.056749105 CEST	192.168.2.6	8.8.8.8	0xe923	Standard query (0)	cm.g.doubleclick.net	A (IP address)	IN (0x0001)
May 12, 2021 21:21:49.220597029 CEST	192.168.2.6	8.8.8.8	0xdb25	Standard query (0)	rtd.tubemogul.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:49.319024086 CEST	192.168.2.6	8.8.8.8	0x7186	Standard query (0)	p.rfihub.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:49.421844959 CEST	192.168.2.6	8.8.8.8	0xf569	Standard query (0)	match.adsrvr.org	A (IP address)	IN (0x0001)
May 12, 2021 21:21:49.430138111 CEST	192.168.2.6	8.8.8.8	0xb35d	Standard query (0)	rtd-tm.everesttech.net	A (IP address)	IN (0x0001)
May 12, 2021 21:21:49.542217970 CEST	192.168.2.6	8.8.8.8	0xddab	Standard query (0)	pixel.quantserve.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:52.770406961 CEST	192.168.2.6	8.8.8.8	0xf4e7	Standard query (0)	adobe-sync.dotomi.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:54.634258032 CEST	192.168.2.6	8.8.8.8	0x8ad1	Standard query (0)	a.tribalfusion.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:58.431173086 CEST	192.168.2.6	8.8.8.8	0x52ec	Standard query (0)	ml314.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:58.632989883 CEST	192.168.2.6	8.8.8.8	0x2a40	Standard query (0)	s.tribalfusion.com	A (IP address)	IN (0x0001)
May 12, 2021 21:21:59.618535042 CEST	192.168.2.6	8.8.8.8	0x8c75	Standard query (0)	bttrack.com	A (IP address)	IN (0x0001)
May 12, 2021 21:22:00.505672932 CEST	192.168.2.6	8.8.8.8	0x2ff3	Standard query (0)	ds-aksb-a.akamaihd.net	A (IP address)	IN (0x0001)
May 12, 2021 21:22:00.564548016 CEST	192.168.2.6	8.8.8.8	0xa358	Standard query (0)	pix-us.revjet.com	A (IP address)	IN (0x0001)
May 12, 2021 21:22:01.516689062 CEST	192.168.2.6	8.8.8.8	0x38c9	Standard query (0)	sync-tm.everesttech.net	A (IP address)	IN (0x0001)
May 12, 2021 21:22:05.205755949 CEST	192.168.2.6	8.8.8.8	0xbb8c	Standard query (0)	pixel.rubiconproject.com	A (IP address)	IN (0x0001)
May 12, 2021 21:22:05.574019909 CEST	192.168.2.6	8.8.8.8	0xfaaf	Standard query (0)	dsum-sec.casalemedia.com	A (IP address)	IN (0x0001)
May 12, 2021 21:22:06.564177036 CEST	192.168.2.6	8.8.8.8	0x4ab7	Standard query (0)	ib.adnxs.com	A (IP address)	IN (0x0001)
May 12, 2021 21:22:07.570317984 CEST	192.168.2.6	8.8.8.8	0x4a41	Standard query (0)	us-u.openx.net	A (IP address)	IN (0x0001)
May 12, 2021 21:22:08.577070951 CEST	192.168.2.6	8.8.8.8	0xbbc7	Standard query (0)	image2.pubmatic.com	A (IP address)	IN (0x0001)
May 12, 2021 21:22:09.562063932 CEST	192.168.2.6	8.8.8.8	0xfee1	Standard query (0)	sync.search.spotxchange.com	A (IP address)	IN (0x0001)
May 12, 2021 21:22:11.521178007 CEST	192.168.2.6	8.8.8.8	0xa20	Standard query (0)	g2.gumgum.com	A (IP address)	IN (0x0001)
May 12, 2021 21:22:12.701036930 CEST	192.168.2.6	8.8.8.8	0xa2a1	Standard query (0)	s.thebrightag.com	A (IP address)	IN (0x0001)
May 12, 2021 21:22:13.692915916 CEST	192.168.2.6	8.8.8.8	0xf85b	Standard query (0)	partner.mediawallahscript.com	A (IP address)	IN (0x0001)
May 12, 2021 21:22:14.446685076 CEST	192.168.2.6	8.8.8.8	0xb9e7	Standard query (0)	use.typekit.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 21:20:52.097846985 CEST	8.8.8.8	192.168.2.6	0x394a	No error (0)	spark.adobeprojectm.com		13.225.74.123	A (IP address)	IN (0x0001)
May 12, 2021 21:20:52.097846985 CEST	8.8.8.8	192.168.2.6	0x394a	No error (0)	spark.adobeprojectm.com		13.225.74.35	A (IP address)	IN (0x0001)
May 12, 2021 21:20:52.097846985 CEST	8.8.8.8	192.168.2.6	0x394a	No error (0)	spark.adobeprojectm.com		13.225.74.22	A (IP address)	IN (0x0001)
May 12, 2021 21:20:52.097846985 CEST	8.8.8.8	192.168.2.6	0x394a	No error (0)	spark.adobeprojectm.com		13.225.74.86	A (IP address)	IN (0x0001)
May 12, 2021 21:20:53.600004911 CEST	8.8.8.8	192.168.2.6	0x144a	No error (0)	page.adobespark-assets.com		13.224.193.29	A (IP address)	IN (0x0001)
May 12, 2021 21:20:53.600004911 CEST	8.8.8.8	192.168.2.6	0x144a	No error (0)	page.adobespark-assets.com		13.224.193.122	A (IP address)	IN (0x0001)
May 12, 2021 21:20:53.600004911 CEST	8.8.8.8	192.168.2.6	0x144a	No error (0)	page.adobespark-assets.com		13.224.193.81	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 21:20:53.600004911 CEST	8.8.8.8	192.168.2.6	0x144a	No error (0)	page.adobe spark-asse ts.com		13.224.193.108	A (IP address)	IN (0x0001)
May 12, 2021 21:20:53.875915051 CEST	8.8.8.8	192.168.2.6	0x2769	No error (0)	use.typekit.net	use-stls.adobe.com.edgesuite .net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:20:54.680233002 CEST	8.8.8.8	192.168.2.6	0x12a3	No error (0)	s3.amazona ws.com		52.217.103.94	A (IP address)	IN (0x0001)
May 12, 2021 21:20:55.090486050 CEST	8.8.8.8	192.168.2.6	0x8582	No error (0)	p.typekit.net	p.typekit.net-v3.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:20:57.789710045 CEST	8.8.8.8	192.168.2.6	0xd9b4	No error (0)	page.adobe spark-asse ts.com		13.224.193.122	A (IP address)	IN (0x0001)
May 12, 2021 21:20:57.789710045 CEST	8.8.8.8	192.168.2.6	0xd9b4	No error (0)	page.adobe spark-asse ts.com		13.224.193.108	A (IP address)	IN (0x0001)
May 12, 2021 21:20:57.789710045 CEST	8.8.8.8	192.168.2.6	0xd9b4	No error (0)	page.adobe spark-asse ts.com		13.224.193.81	A (IP address)	IN (0x0001)
May 12, 2021 21:20:57.789710045 CEST	8.8.8.8	192.168.2.6	0xd9b4	No error (0)	page.adobe spark-asse ts.com		13.224.193.29	A (IP address)	IN (0x0001)
May 12, 2021 21:20:58.564223051 CEST	8.8.8.8	192.168.2.6	0x433d	No error (0)	clients2.g oogleuserc ontent.com	googlehosted.l.googleuse rcontent.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:20:58.564223051 CEST	8.8.8.8	192.168.2.6	0x433d	No error (0)	googlehost ed.l.googl euserconte nt.com		216.58.212.129	A (IP address)	IN (0x0001)
May 12, 2021 21:21:13.488878965 CEST	8.8.8.8	192.168.2.6	0x1119	No error (0)	greycottage.ng		162.241.7.225	A (IP address)	IN (0x0001)
May 12, 2021 21:21:15.963061094 CEST	8.8.8.8	192.168.2.6	0x3df5	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:15.973402023 CEST	8.8.8.8	192.168.2.6	0x1a95	No error (0)	maxcdn.boo tstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
May 12, 2021 21:21:15.973402023 CEST	8.8.8.8	192.168.2.6	0x1a95	No error (0)	maxcdn.boo tstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
May 12, 2021 21:21:15.986399889 CEST	8.8.8.8	192.168.2.6	0xd008	No error (0)	kit.fontaw esome.com	kit.fontawesome.com.cdn. cloudflare.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:17.434900999 CEST	8.8.8.8	192.168.2.6	0x5908	No error (0)	cdnjs.clou dflare.com		104.16.18.94	A (IP address)	IN (0x0001)
May 12, 2021 21:21:17.434900999 CEST	8.8.8.8	192.168.2.6	0x5908	No error (0)	cdnjs.clou dflare.com		104.16.19.94	A (IP address)	IN (0x0001)
May 12, 2021 21:21:17.485511065 CEST	8.8.8.8	192.168.2.6	0xc4d9	No error (0)	ka-f.fonta wesome.com	ka-f.fontawesome.com.cdn.cl oudflare.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:19.252346992 CEST	8.8.8.8	192.168.2.6	0xad22	No error (0)	greycottage.ng		162.241.7.225	A (IP address)	IN (0x0001)
May 12, 2021 21:21:30.795042038 CEST	8.8.8.8	192.168.2.6	0x525a	No error (0)	static.ado belogin.com	adobelogin-static.prod.ims.adobejanu s.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:30.795042038 CEST	8.8.8.8	192.168.2.6	0x525a	No error (0)	adobelogin-static.pr od.ims.ado bejanus.com	dd20fzx9mj46f.cloudfront. net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:30.795042038 CEST	8.8.8.8	192.168.2.6	0x525a	No error (0)	dd20fzx9mj 46f.cloudf ront.net		13.224.187.69	A (IP address)	IN (0x0001)
May 12, 2021 21:21:30.858906984 CEST	8.8.8.8	192.168.2.6	0xbdc7	No error (0)	assets.ado bedtm.com	cn-assets.adobedtm.com.ed gekey.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:30.879559994 CEST	8.8.8.8	192.168.2.6	0x7131	No error (0)	cdn.cookie law.org		104.16.149.64	A (IP address)	IN (0x0001)
May 12, 2021 21:21:30.879559994 CEST	8.8.8.8	192.168.2.6	0x7131	No error (0)	cdn.cookie law.org		104.16.148.64	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 21:21:31.079431057 CEST	8.8.8.8	192.168.2.6	0xb8d5	No error (0)	adobe.tt.omtrdc.net		54.75.9.158	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.079431057 CEST	8.8.8.8	192.168.2.6	0xb8d5	No error (0)	adobe.tt.omtrdc.net		34.252.156.174	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.079431057 CEST	8.8.8.8	192.168.2.6	0xb8d5	No error (0)	adobe.tt.omtrdc.net		52.212.164.82	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.079431057 CEST	8.8.8.8	192.168.2.6	0xb8d5	No error (0)	adobe.tt.omtrdc.net		52.213.168.74	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.079431057 CEST	8.8.8.8	192.168.2.6	0xb8d5	No error (0)	adobe.tt.omtrdc.net		52.18.150.20	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.079431057 CEST	8.8.8.8	192.168.2.6	0xb8d5	No error (0)	adobe.tt.omtrdc.net		34.252.166.160	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.079431057 CEST	8.8.8.8	192.168.2.6	0xb8d5	No error (0)	adobe.tt.omtrdc.net		52.212.193.208	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.079431057 CEST	8.8.8.8	192.168.2.6	0xb8d5	No error (0)	adobe.tt.omtrdc.net		18.203.205.32	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.094820976 CEST	8.8.8.8	192.168.2.6	0x74f3	No error (0)	services.prod.ims.adobejanus.com		52.213.176.171	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.094820976 CEST	8.8.8.8	192.168.2.6	0x74f3	No error (0)	services.prod.ims.adobejanus.com		52.209.27.136	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.094820976 CEST	8.8.8.8	192.168.2.6	0x74f3	No error (0)	services.prod.ims.adobejanus.com		54.76.80.163	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.094820976 CEST	8.8.8.8	192.168.2.6	0x74f3	No error (0)	services.prod.ims.adobejanus.com		63.32.113.5	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.094820976 CEST	8.8.8.8	192.168.2.6	0x74f3	No error (0)	services.prod.ims.adobejanus.com		99.81.92.132	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.094820976 CEST	8.8.8.8	192.168.2.6	0x74f3	No error (0)	services.prod.ims.adobejanus.com		54.73.76.208	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.313230991 CEST	8.8.8.8	192.168.2.6	0x3d86	No error (0)	geolocation.onetrust.com		104.20.185.68	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.313230991 CEST	8.8.8.8	192.168.2.6	0x3d86	No error (0)	geolocation.onetrust.com		104.20.184.68	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.491921902 CEST	8.8.8.8	192.168.2.6	0x3a27	No error (0)	dpm.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:31.491921902 CEST	8.8.8.8	192.168.2.6	0x3a27	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:31.491921902 CEST	8.8.8.8	192.168.2.6	0x3a27	No error (0)	edge-irl1.demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:31.491921902 CEST	8.8.8.8	192.168.2.6	0x3a27	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.246.133.154	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.491921902 CEST	8.8.8.8	192.168.2.6	0x3a27	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.30.135.179	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.491921902 CEST	8.8.8.8	192.168.2.6	0x3a27	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		18.200.233.208	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.491921902 CEST	8.8.8.8	192.168.2.6	0x3a27	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		3.250.252.43	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.491921902 CEST	8.8.8.8	192.168.2.6	0x3a27	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.48.201.185	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 21:21:31.491921902 CEST	8.8.8.8	192.168.2.6	0x3a27	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		18.203.106.177	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.491921902 CEST	8.8.8.8	192.168.2.6	0x3a27	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.31.176.223	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.491921902 CEST	8.8.8.8	192.168.2.6	0x3a27	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.170.210.188	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.616642952 CEST	8.8.8.8	192.168.2.6	0x29d1	No error (0)	ims-na1.adobelogin.com	adobelogin.prod.ims.adobejanus.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:31.616642952 CEST	8.8.8.8	192.168.2.6	0x29d1	No error (0)	adobelogin.prod.ims.adobejanus.com	adobelogin-origin.prod.ims.adobejanus.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:31.616642952 CEST	8.8.8.8	192.168.2.6	0x29d1	No error (0)	adobelogin-origin.prod.ims.adobejanus.com		63.32.113.5	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.616642952 CEST	8.8.8.8	192.168.2.6	0x29d1	No error (0)	adobelogin-origin.prod.ims.adobejanus.com		52.209.27.136	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.616642952 CEST	8.8.8.8	192.168.2.6	0x29d1	No error (0)	adobelogin-origin.prod.ims.adobejanus.com		54.76.80.163	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.616642952 CEST	8.8.8.8	192.168.2.6	0x29d1	No error (0)	adobelogin-origin.prod.ims.adobejanus.com		54.73.76.208	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.616642952 CEST	8.8.8.8	192.168.2.6	0x29d1	No error (0)	adobelogin-origin.prod.ims.adobejanus.com		52.213.176.171	A (IP address)	IN (0x0001)
May 12, 2021 21:21:31.616642952 CEST	8.8.8.8	192.168.2.6	0x29d1	No error (0)	adobelogin-origin.prod.ims.adobejanus.com		99.81.92.132	A (IP address)	IN (0x0001)
May 12, 2021 21:21:32.654850960 CEST	8.8.8.8	192.168.2.6	0x8bb9	No error (0)	adobe.com.ssl.d1.sc.omtrdc.net		15.237.136.106	A (IP address)	IN (0x0001)
May 12, 2021 21:21:32.654850960 CEST	8.8.8.8	192.168.2.6	0x8bb9	No error (0)	adobe.com.ssl.d1.sc.omtrdc.net		15.237.76.117	A (IP address)	IN (0x0001)
May 12, 2021 21:21:32.654850960 CEST	8.8.8.8	192.168.2.6	0x8bb9	No error (0)	adobe.com.ssl.d1.sc.omtrdc.net		35.181.18.61	A (IP address)	IN (0x0001)
May 12, 2021 21:21:32.705813885 CEST	8.8.8.8	192.168.2.6	0x1a86	No error (0)	adobedc.demdex.net	demdex.net.ssl.sc.omtrdc.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:32.705813885 CEST	8.8.8.8	192.168.2.6	0x1a86	No error (0)	demdex.net.ssl.sc.omtrdc.net		15.237.136.106	A (IP address)	IN (0x0001)
May 12, 2021 21:21:32.705813885 CEST	8.8.8.8	192.168.2.6	0x1a86	No error (0)	demdex.net.ssl.sc.omtrdc.net		15.237.76.117	A (IP address)	IN (0x0001)
May 12, 2021 21:21:32.705813885 CEST	8.8.8.8	192.168.2.6	0x1a86	No error (0)	demdex.net.ssl.sc.omtrdc.net		35.181.18.61	A (IP address)	IN (0x0001)
May 12, 2021 21:21:33.652601957 CEST	8.8.8.8	192.168.2.6	0xb086	No error (0)	api.demandbase.com		13.225.74.124	A (IP address)	IN (0x0001)
May 12, 2021 21:21:33.652601957 CEST	8.8.8.8	192.168.2.6	0xb086	No error (0)	api.demandbase.com		13.225.74.112	A (IP address)	IN (0x0001)
May 12, 2021 21:21:33.652601957 CEST	8.8.8.8	192.168.2.6	0xb086	No error (0)	api.demandbase.com		13.225.74.37	A (IP address)	IN (0x0001)
May 12, 2021 21:21:33.652601957 CEST	8.8.8.8	192.168.2.6	0xb086	No error (0)	api.demandbase.com		13.225.74.58	A (IP address)	IN (0x0001)
May 12, 2021 21:21:34.043633938 CEST	8.8.8.8	192.168.2.6	0x5ddf	No error (0)	www.everestjs.net	www.everestjs.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 21:21:34.147519112 CEST	8.8.8.8	192.168.2.6	0x47b0	No error (0)	universal.iperceptions.com	iperceptions01.azureedge.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:34.147519112 CEST	8.8.8.8	192.168.2.6	0x47b0	No error (0)	scdn1.wpc.2ba63.deltacdn.net	sni1gl.wpc.deltacdn.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:34.147519112 CEST	8.8.8.8	192.168.2.6	0x47b0	No error (0)	sni1gl.wpc.deltacdn.net		152.199.21.175	A (IP address)	IN (0x0001)
May 12, 2021 21:21:34.159473896 CEST	8.8.8.8	192.168.2.6	0xf5f6	No error (0)	servedby.flashtalking.com	cds.f7f2q8c3.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:34.268110037 CEST	8.8.8.8	192.168.2.6	0x6aa5	No error (0)	snap.licdn.com	wildcard.licdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:34.331413031 CEST	8.8.8.8	192.168.2.6	0x6f4b	No error (0)	scripts.demandbase.com		13.224.193.108	A (IP address)	IN (0x0001)
May 12, 2021 21:21:34.331413031 CEST	8.8.8.8	192.168.2.6	0x6f4b	No error (0)	scripts.demandbase.com		13.224.193.116	A (IP address)	IN (0x0001)
May 12, 2021 21:21:34.331413031 CEST	8.8.8.8	192.168.2.6	0x6f4b	No error (0)	scripts.demandbase.com		13.224.193.53	A (IP address)	IN (0x0001)
May 12, 2021 21:21:34.331413031 CEST	8.8.8.8	192.168.2.6	0x6f4b	No error (0)	scripts.demandbase.com		13.224.193.78	A (IP address)	IN (0x0001)
May 12, 2021 21:21:34.341939926 CEST	8.8.8.8	192.168.2.6	0xe9ae	No error (0)	lasteventf-tm.everesttech.net	lasteventf.tubemogul.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:34.341939926 CEST	8.8.8.8	192.168.2.6	0xe9ae	No error (0)	lasteventf.tubemogul.com	h2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:34.756037951 CEST	8.8.8.8	192.168.2.6	0xf0b0	No error (0)	d9.flashtalking.com	ft.device9.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:34.756037951 CEST	8.8.8.8	192.168.2.6	0xf0b0	No error (0)	ft.device9.com	tag.device9.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:34.756037951 CEST	8.8.8.8	192.168.2.6	0xf0b0	No error (0)	tag.device9.com		52.17.98.114	A (IP address)	IN (0x0001)
May 12, 2021 21:21:34.756037951 CEST	8.8.8.8	192.168.2.6	0xf0b0	No error (0)	tag.device9.com		34.247.239.226	A (IP address)	IN (0x0001)
May 12, 2021 21:21:34.756037951 CEST	8.8.8.8	192.168.2.6	0xf0b0	No error (0)	tag.device9.com		34.249.65.165	A (IP address)	IN (0x0001)
May 12, 2021 21:21:34.756037951 CEST	8.8.8.8	192.168.2.6	0xf0b0	No error (0)	tag.device9.com		52.49.199.119	A (IP address)	IN (0x0001)
May 12, 2021 21:21:34.756037951 CEST	8.8.8.8	192.168.2.6	0xf0b0	No error (0)	tag.device9.com		54.171.117.141	A (IP address)	IN (0x0001)
May 12, 2021 21:21:34.756037951 CEST	8.8.8.8	192.168.2.6	0xf0b0	No error (0)	tag.device9.com		52.211.172.236	A (IP address)	IN (0x0001)
May 12, 2021 21:21:34.756037951 CEST	8.8.8.8	192.168.2.6	0xf0b0	No error (0)	tag.device9.com		52.48.136.43	A (IP address)	IN (0x0001)
May 12, 2021 21:21:34.756037951 CEST	8.8.8.8	192.168.2.6	0xf0b0	No error (0)	tag.device9.com		34.251.104.84	A (IP address)	IN (0x0001)
May 12, 2021 21:21:34.801822901 CEST	8.8.8.8	192.168.2.6	0x9381	No error (0)	9212252.fls.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:34.801822901 CEST	8.8.8.8	192.168.2.6	0x9381	No error (0)	dart.l.doubleclick.net		142.250.185.102	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.543649912 CEST	8.8.8.8	192.168.2.6	0x2581	No error (0)	static.ads-twitter.com	platform.twitter.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:35.543649912 CEST	8.8.8.8	192.168.2.6	0x2581	No error (0)	platform.twitter.map.fastly.net		199.232.136.157	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.572267056 CEST	8.8.8.8	192.168.2.6	0x6c6a	No error (0)	pixel.everesttech.net	tp00.everesttech.net.akadns.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 21:21:35.575242043 CEST	8.8.8.8	192.168.2.6	0xb0bc	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:35.575242043 CEST	8.8.8.8	192.168.2.6	0xb0bc	No error (0)	scontent.xx.fbcdn.net		185.60.216.19	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.582792997 CEST	8.8.8.8	192.168.2.6	0x1e5b	No error (0)	sc-static.net		13.225.74.57	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.582792997 CEST	8.8.8.8	192.168.2.6	0x1e5b	No error (0)	sc-static.net		13.225.74.54	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.582792997 CEST	8.8.8.8	192.168.2.6	0x1e5b	No error (0)	sc-static.net		13.225.74.126	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.582792997 CEST	8.8.8.8	192.168.2.6	0x1e5b	No error (0)	sc-static.net		13.225.74.36	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.654547930 CEST	8.8.8.8	192.168.2.6	0x98e5	No error (0)	px.ads.linkedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:35.654547930 CEST	8.8.8.8	192.168.2.6	0x98e5	No error (0)	mix.linkedin.com	glb-na.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:35.654547930 CEST	8.8.8.8	192.168.2.6	0x98e5	No error (0)	glb-na.mix.linkedin.com	pop-esv5.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:35.654547930 CEST	8.8.8.8	192.168.2.6	0x98e5	No error (0)	pop-esv5.mix.linkedin.com		108.174.11.37	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.713948011 CEST	8.8.8.8	192.168.2.6	0x3fe1	No error (0)	api.company-target.com		13.225.74.55	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.713948011 CEST	8.8.8.8	192.168.2.6	0x3fe1	No error (0)	api.company-target.com		13.225.74.24	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.713948011 CEST	8.8.8.8	192.168.2.6	0x3fe1	No error (0)	api.company-target.com		13.225.74.88	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.713948011 CEST	8.8.8.8	192.168.2.6	0x3fe1	No error (0)	api.company-target.com		13.225.74.42	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.714782953 CEST	8.8.8.8	192.168.2.6	0x25a6	No error (0)	match.prod.bidr.io		52.19.106.86	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.714782953 CEST	8.8.8.8	192.168.2.6	0x25a6	No error (0)	match.prod.bidr.io		52.210.44.111	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.714782953 CEST	8.8.8.8	192.168.2.6	0x25a6	No error (0)	match.prod.bidr.io		52.215.139.246	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.714782953 CEST	8.8.8.8	192.168.2.6	0x25a6	No error (0)	match.prod.bidr.io		52.49.40.147	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.714782953 CEST	8.8.8.8	192.168.2.6	0x25a6	No error (0)	match.prod.bidr.io		52.209.246.140	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.714782953 CEST	8.8.8.8	192.168.2.6	0x25a6	No error (0)	match.prod.bidr.io		52.48.151.83	A (IP address)	IN (0x0001)
May 12, 2021 21:21:35.715301991 CEST	8.8.8.8	192.168.2.6	0x6b8f	No error (0)	id.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
May 12, 2021 21:21:36.250025988 CEST	8.8.8.8	192.168.2.6	0xd511	No error (0)	tr.snapchat.com		35.186.226.184	A (IP address)	IN (0x0001)
May 12, 2021 21:21:36.258224010 CEST	8.8.8.8	192.168.2.6	0xe678	No error (0)	analytics.twitter.com	ads.twitter.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:36.258224010 CEST	8.8.8.8	192.168.2.6	0xe678	No error (0)	ads.twitter.com	s.twitter.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:36.258224010 CEST	8.8.8.8	192.168.2.6	0xe678	No error (0)	s.twitter.com		104.244.42.3	A (IP address)	IN (0x0001)
May 12, 2021 21:21:36.258224010 CEST	8.8.8.8	192.168.2.6	0xe678	No error (0)	s.twitter.com		104.244.42.67	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 21:21:36.258224010 CEST	8.8.8.8	192.168.2.6	0xe678	No error (0)	s.twitter.com		104.244.42.131	A (IP address)	IN (0x0001)
May 12, 2021 21:21:36.258224010 CEST	8.8.8.8	192.168.2.6	0xe678	No error (0)	s.twitter.com		104.244.42.195	A (IP address)	IN (0x0001)
May 12, 2021 21:21:36.278764963 CEST	8.8.8.8	192.168.2.6	0x3afe	No error (0)	t.co		104.244.42.5	A (IP address)	IN (0x0001)
May 12, 2021 21:21:36.278764963 CEST	8.8.8.8	192.168.2.6	0x3afe	No error (0)	t.co		104.244.42.197	A (IP address)	IN (0x0001)
May 12, 2021 21:21:36.278764963 CEST	8.8.8.8	192.168.2.6	0x3afe	No error (0)	t.co		104.244.42.69	A (IP address)	IN (0x0001)
May 12, 2021 21:21:36.278764963 CEST	8.8.8.8	192.168.2.6	0x3afe	No error (0)	t.co		104.244.42.133	A (IP address)	IN (0x0001)
May 12, 2021 21:21:36.830018997 CEST	8.8.8.8	192.168.2.6	0xc6e5	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:36.830018997 CEST	8.8.8.8	192.168.2.6	0xc6e5	No error (0)	star-mini.c10r.facebook.com		185.60.216.35	A (IP address)	IN (0x0001)
May 12, 2021 21:21:36.835088015 CEST	8.8.8.8	192.168.2.6	0xb5db	No error (0)	segments.company-target.com		13.225.74.27	A (IP address)	IN (0x0001)
May 12, 2021 21:21:36.835088015 CEST	8.8.8.8	192.168.2.6	0xb5db	No error (0)	segments.company-target.com		13.225.74.112	A (IP address)	IN (0x0001)
May 12, 2021 21:21:36.835088015 CEST	8.8.8.8	192.168.2.6	0xb5db	No error (0)	segments.company-target.com		13.225.74.75	A (IP address)	IN (0x0001)
May 12, 2021 21:21:36.835088015 CEST	8.8.8.8	192.168.2.6	0xb5db	No error (0)	segments.company-target.com		13.225.74.92	A (IP address)	IN (0x0001)
May 12, 2021 21:21:37.336332083 CEST	8.8.8.8	192.168.2.6	0x27e6	No error (0)	prod.adobeccstatic.com		13.224.193.20	A (IP address)	IN (0x0001)
May 12, 2021 21:21:37.336332083 CEST	8.8.8.8	192.168.2.6	0x27e6	No error (0)	prod.adobeccstatic.com		13.224.193.53	A (IP address)	IN (0x0001)
May 12, 2021 21:21:37.336332083 CEST	8.8.8.8	192.168.2.6	0x27e6	No error (0)	prod.adobeccstatic.com		13.224.193.78	A (IP address)	IN (0x0001)
May 12, 2021 21:21:37.336332083 CEST	8.8.8.8	192.168.2.6	0x27e6	No error (0)	prod.adobeccstatic.com		13.224.193.51	A (IP address)	IN (0x0001)
May 12, 2021 21:21:38.180305958 CEST	8.8.8.8	192.168.2.6	0x9faa	No error (0)	bumper.adobeprojectm.com	sparkbumper-production1-va6.cloud.adobe.io		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:38.180305958 CEST	8.8.8.8	192.168.2.6	0x9faa	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 12, 2021 21:21:38.180305958 CEST	8.8.8.8	192.168.2.6	0x9faa	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 12, 2021 21:21:38.180305958 CEST	8.8.8.8	192.168.2.6	0x9faa	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 12, 2021 21:21:38.180305958 CEST	8.8.8.8	192.168.2.6	0x9faa	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 12, 2021 21:21:40.468736887 CEST	8.8.8.8	192.168.2.6	0xc450	No error (0)	js-agent.newrelic.com	f4.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:40.846952915 CEST	8.8.8.8	192.168.2.6	0xe32	No error (0)	bam.nr-data.net		162.247.242.18	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 21:21:40.846952915 CEST	8.8.8.8	192.168.2.6	0xe32	No error (0)	bam.nr-data.net		162.247.242.21	A (IP address)	IN (0x0001)
May 12, 2021 21:21:40.846952915 CEST	8.8.8.8	192.168.2.6	0xe32	No error (0)	bam.nr-data.net		162.247.242.20	A (IP address)	IN (0x0001)
May 12, 2021 21:21:40.846952915 CEST	8.8.8.8	192.168.2.6	0xe32	No error (0)	bam.nr-data.net		162.247.242.19	A (IP address)	IN (0x0001)
May 12, 2021 21:21:41.065072060 CEST	8.8.8.8	192.168.2.6	0x9820	No error (0)	adservice.google.ch	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:41.065072060 CEST	8.8.8.8	192.168.2.6	0x9820	No error (0)	pagead46.l.doubleclick.net		172.217.23.98	A (IP address)	IN (0x0001)
May 12, 2021 21:21:41.568351984 CEST	8.8.8.8	192.168.2.6	0x543a	No error (0)	spark.adobeprojectm.com		13.225.74.123	A (IP address)	IN (0x0001)
May 12, 2021 21:21:41.568351984 CEST	8.8.8.8	192.168.2.6	0x543a	No error (0)	spark.adobeprojectm.com		13.225.74.35	A (IP address)	IN (0x0001)
May 12, 2021 21:21:41.568351984 CEST	8.8.8.8	192.168.2.6	0x543a	No error (0)	spark.adobeprojectm.com		13.225.74.22	A (IP address)	IN (0x0001)
May 12, 2021 21:21:41.568351984 CEST	8.8.8.8	192.168.2.6	0x543a	No error (0)	spark.adobeprojectm.com		13.225.74.86	A (IP address)	IN (0x0001)
May 12, 2021 21:21:41.588181973 CEST	8.8.8.8	192.168.2.6	0x4b60	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:42.132499933 CEST	8.8.8.8	192.168.2.6	0xcf6	No error (0)	googleads.g.doubleclick.net		216.58.212.130	A (IP address)	IN (0x0001)
May 12, 2021 21:21:43.613306046 CEST	8.8.8.8	192.168.2.6	0x717a	No error (0)	cm.everesttech.net	cm.everesttech.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:44.864471912 CEST	8.8.8.8	192.168.2.6	0xf7e9	No error (0)	adobe.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:44.864471912 CEST	8.8.8.8	192.168.2.6	0xf7e9	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:44.864471912 CEST	8.8.8.8	192.168.2.6	0xf7e9	No error (0)	edge-irl1.demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:44.864471912 CEST	8.8.8.8	192.168.2.6	0xf7e9	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.214.120.236	A (IP address)	IN (0x0001)
May 12, 2021 21:21:44.864471912 CEST	8.8.8.8	192.168.2.6	0xf7e9	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.243.47.58	A (IP address)	IN (0x0001)
May 12, 2021 21:21:44.864471912 CEST	8.8.8.8	192.168.2.6	0xf7e9	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.30.200.197	A (IP address)	IN (0x0001)
May 12, 2021 21:21:44.864471912 CEST	8.8.8.8	192.168.2.6	0xf7e9	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.31.176.223	A (IP address)	IN (0x0001)
May 12, 2021 21:21:44.864471912 CEST	8.8.8.8	192.168.2.6	0xf7e9	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.154.123.210	A (IP address)	IN (0x0001)
May 12, 2021 21:21:44.864471912 CEST	8.8.8.8	192.168.2.6	0xf7e9	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.76.54.153	A (IP address)	IN (0x0001)
May 12, 2021 21:21:44.864471912 CEST	8.8.8.8	192.168.2.6	0xf7e9	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.212.101.97	A (IP address)	IN (0x0001)
May 12, 2021 21:21:44.864471912 CEST	8.8.8.8	192.168.2.6	0xf7e9	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.48.201.185	A (IP address)	IN (0x0001)
May 12, 2021 21:21:44.911204100 CEST	8.8.8.8	192.168.2.6	0x85f1	No error (0)	www.google.ch		142.250.186.99	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 21:21:44.950849056 CEST	8.8.8.8	192.168.2.6	0x934d	No error (0)	api.iperceptions.com	api-traffic01.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:46.500052929 CEST	8.8.8.8	192.168.2.6	0x77c	No error (0)	sd.iperceptions.com	d1gs6rlbmzcurc.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:46.500052929 CEST	8.8.8.8	192.168.2.6	0x77c	No error (0)	d1gs6rlbmzcurc.cloudfront.net		13.224.193.115	A (IP address)	IN (0x0001)
May 12, 2021 21:21:46.500052929 CEST	8.8.8.8	192.168.2.6	0x77c	No error (0)	d1gs6rlbmzcurc.cloudfront.net		13.224.193.20	A (IP address)	IN (0x0001)
May 12, 2021 21:21:46.500052929 CEST	8.8.8.8	192.168.2.6	0x77c	No error (0)	d1gs6rlbmzcurc.cloudfront.net		13.224.193.85	A (IP address)	IN (0x0001)
May 12, 2021 21:21:46.500052929 CEST	8.8.8.8	192.168.2.6	0x77c	No error (0)	d1gs6rlbmzcurc.cloudfront.net		13.224.193.60	A (IP address)	IN (0x0001)
May 12, 2021 21:21:46.596760988 CEST	8.8.8.8	192.168.2.6	0x9881	No error (0)	id.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
May 12, 2021 21:21:46.617319107 CEST	8.8.8.8	192.168.2.6	0x279b	No error (0)	match.prod.bidr.io		52.49.40.147	A (IP address)	IN (0x0001)
May 12, 2021 21:21:46.617319107 CEST	8.8.8.8	192.168.2.6	0x279b	No error (0)	match.prod.bidr.io		52.209.246.140	A (IP address)	IN (0x0001)
May 12, 2021 21:21:46.617319107 CEST	8.8.8.8	192.168.2.6	0x279b	No error (0)	match.prod.bidr.io		52.210.44.111	A (IP address)	IN (0x0001)
May 12, 2021 21:21:46.617319107 CEST	8.8.8.8	192.168.2.6	0x279b	No error (0)	match.prod.bidr.io		52.48.151.83	A (IP address)	IN (0x0001)
May 12, 2021 21:21:46.617319107 CEST	8.8.8.8	192.168.2.6	0x279b	No error (0)	match.prod.bidr.io		52.19.106.86	A (IP address)	IN (0x0001)
May 12, 2021 21:21:46.617319107 CEST	8.8.8.8	192.168.2.6	0x279b	No error (0)	match.prod.bidr.io		52.215.139.246	A (IP address)	IN (0x0001)
May 12, 2021 21:21:47.079744101 CEST	8.8.8.8	192.168.2.6	0x14be	No error (0)	segments.company-target.com		13.225.74.112	A (IP address)	IN (0x0001)
May 12, 2021 21:21:47.079744101 CEST	8.8.8.8	192.168.2.6	0x14be	No error (0)	segments.company-target.com		13.225.74.27	A (IP address)	IN (0x0001)
May 12, 2021 21:21:47.079744101 CEST	8.8.8.8	192.168.2.6	0x14be	No error (0)	segments.company-target.com		13.225.74.92	A (IP address)	IN (0x0001)
May 12, 2021 21:21:47.079744101 CEST	8.8.8.8	192.168.2.6	0x14be	No error (0)	segments.company-target.com		13.225.74.75	A (IP address)	IN (0x0001)
May 12, 2021 21:21:48.229043007 CEST	8.8.8.8	192.168.2.6	0x515b	No error (0)	aa.agkn.com	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:48.229043007 CEST	8.8.8.8	192.168.2.6	0x515b	No error (0)	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com		52.29.225.117	A (IP address)	IN (0x0001)
May 12, 2021 21:21:48.229043007 CEST	8.8.8.8	192.168.2.6	0x515b	No error (0)	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com		52.58.248.2	A (IP address)	IN (0x0001)
May 12, 2021 21:21:48.229043007 CEST	8.8.8.8	192.168.2.6	0x515b	No error (0)	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com		3.120.52.200	A (IP address)	IN (0x0001)
May 12, 2021 21:21:48.229043007 CEST	8.8.8.8	192.168.2.6	0x515b	No error (0)	aa-agkn-com-https-2145740884.eu-central-1.elb.amazonaws.com		3.127.52.31	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 21:21:48.680860043 CEST	8.8.8.8	192.168.2.6	0xf766	No error (0)	sync.mathtag.com	pixel-origin.mathtag.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:48.680860043 CEST	8.8.8.8	192.168.2.6	0xf766	No error (0)	pixel-origin.mathtag.com		185.29.133.52	A (IP address)	IN (0x0001)
May 12, 2021 21:21:48.680860043 CEST	8.8.8.8	192.168.2.6	0xf766	No error (0)	pixel-origin.mathtag.com		185.29.135.226	A (IP address)	IN (0x0001)
May 12, 2021 21:21:48.680860043 CEST	8.8.8.8	192.168.2.6	0xf766	No error (0)	pixel-origin.mathtag.com		185.29.135.190	A (IP address)	IN (0x0001)
May 12, 2021 21:21:48.680860043 CEST	8.8.8.8	192.168.2.6	0xf766	No error (0)	pixel-origin.mathtag.com		185.29.135.234	A (IP address)	IN (0x0001)
May 12, 2021 21:21:48.785264969 CEST	8.8.8.8	192.168.2.6	0x3770	No error (0)	idsync.rlcdn.com		35.244.174.68	A (IP address)	IN (0x0001)
May 12, 2021 21:21:48.927777052 CEST	8.8.8.8	192.168.2.6	0x77e0	No error (0)	d.turn.com	d.turn.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:49.000449896 CEST	8.8.8.8	192.168.2.6	0x4b36	No error (0)	pixel.tapad.com		35.227.248.159	A (IP address)	IN (0x0001)
May 12, 2021 21:21:49.123723030 CEST	8.8.8.8	192.168.2.6	0xe923	No error (0)	cm.g.doubleclick.net		142.250.186.130	A (IP address)	IN (0x0001)
May 12, 2021 21:21:49.277978897 CEST	8.8.8.8	192.168.2.6	0xdb25	No error (0)	rtd.tubemogul.com	h2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:49.394958019 CEST	8.8.8.8	192.168.2.6	0x7186	No error (0)	p.rfihub.com	a.rfihub.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:49.394958019 CEST	8.8.8.8	192.168.2.6	0x7186	No error (0)	a.rfihub.com	a.rfihub.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:49.482047081 CEST	8.8.8.8	192.168.2.6	0xf569	No error (0)	match.adsrvr.org	match-aga.adsrvr.org		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:49.482047081 CEST	8.8.8.8	192.168.2.6	0xf569	No error (0)	match-aga.adsrvr.org	a97adde81b00f2ca4.awsglobalaccelerator.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:49.482047081 CEST	8.8.8.8	192.168.2.6	0xf569	No error (0)	a97adde81b00f2ca4.awsglobalaccelerator.com		76.223.111.131	A (IP address)	IN (0x0001)
May 12, 2021 21:21:49.482047081 CEST	8.8.8.8	192.168.2.6	0xf569	No error (0)	a97adde81b00f2ca4.awsglobalaccelerator.com		13.248.242.197	A (IP address)	IN (0x0001)
May 12, 2021 21:21:49.487586975 CEST	8.8.8.8	192.168.2.6	0xb35d	No error (0)	rtd-tm.everesttech.net	rtd.tubemogul.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:49.487586975 CEST	8.8.8.8	192.168.2.6	0xb35d	No error (0)	rtd.tubemogul.com	h2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:49.601685047 CEST	8.8.8.8	192.168.2.6	0xddab	No error (0)	pixel.quantserve.com	global.px.quantserve.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:21:49.601685047 CEST	8.8.8.8	192.168.2.6	0xddab	No error (0)	global.px.quantserve.com		91.228.74.134	A (IP address)	IN (0x0001)
May 12, 2021 21:21:49.601685047 CEST	8.8.8.8	192.168.2.6	0xddab	No error (0)	global.px.quantserve.com		91.228.74.226	A (IP address)	IN (0x0001)
May 12, 2021 21:21:49.601685047 CEST	8.8.8.8	192.168.2.6	0xddab	No error (0)	global.px.quantserve.com		91.228.74.133	A (IP address)	IN (0x0001)
May 12, 2021 21:21:49.601685047 CEST	8.8.8.8	192.168.2.6	0xddab	No error (0)	global.px.quantserve.com		91.228.74.198	A (IP address)	IN (0x0001)
May 12, 2021 21:21:49.601685047 CEST	8.8.8.8	192.168.2.6	0xddab	No error (0)	global.px.quantserve.com		91.228.74.189	A (IP address)	IN (0x0001)
May 12, 2021 21:21:52.853352070 CEST	8.8.8.8	192.168.2.6	0xf4e7	No error (0)	adobe-sync.dotomi.com	afp.dotomi.weighted.com.akadns.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 21:21:52.853352070 CEST	8.8.8.8	192.168.2.6	0xf4e7	No error (0)	ams02-usadmm-ds.dotomi.com		64.158.223.137	A (IP address)	IN (0x0001)
May 12, 2021 21:21:54.693624020 CEST	8.8.8.8	192.168.2.6	0x8ad1	No error (0)	a.tribalfusion.com		104.18.13.5	A (IP address)	IN (0x0001)
May 12, 2021 21:21:54.693624020 CEST	8.8.8.8	192.168.2.6	0x8ad1	No error (0)	a.tribalfusion.com		104.18.12.5	A (IP address)	IN (0x0001)
May 12, 2021 21:21:54.943655014 CEST	8.8.8.8	192.168.2.6	0xd36d	No error (0)	spark.adobeprojectm.com		13.225.74.35	A (IP address)	IN (0x0001)
May 12, 2021 21:21:54.943655014 CEST	8.8.8.8	192.168.2.6	0xd36d	No error (0)	spark.adobeprojectm.com		13.225.74.123	A (IP address)	IN (0x0001)
May 12, 2021 21:21:54.943655014 CEST	8.8.8.8	192.168.2.6	0xd36d	No error (0)	spark.adobeprojectm.com		13.225.74.86	A (IP address)	IN (0x0001)
May 12, 2021 21:21:54.943655014 CEST	8.8.8.8	192.168.2.6	0xd36d	No error (0)	spark.adobeprojectm.com		13.225.74.22	A (IP address)	IN (0x0001)
May 12, 2021 21:21:58.520167112 CEST	8.8.8.8	192.168.2.6	0x52ec	No error (0)	ml314.com		52.49.20.76	A (IP address)	IN (0x0001)
May 12, 2021 21:21:58.520167112 CEST	8.8.8.8	192.168.2.6	0x52ec	No error (0)	ml314.com		52.31.168.5	A (IP address)	IN (0x0001)
May 12, 2021 21:21:58.520167112 CEST	8.8.8.8	192.168.2.6	0x52ec	No error (0)	ml314.com		34.247.104.176	A (IP address)	IN (0x0001)
May 12, 2021 21:21:58.520167112 CEST	8.8.8.8	192.168.2.6	0x52ec	No error (0)	ml314.com		52.211.195.119	A (IP address)	IN (0x0001)
May 12, 2021 21:21:58.695900917 CEST	8.8.8.8	192.168.2.6	0x2a40	No error (0)	s.tribalfusion.com		104.18.12.5	A (IP address)	IN (0x0001)
May 12, 2021 21:21:58.695900917 CEST	8.8.8.8	192.168.2.6	0x2a40	No error (0)	s.tribalfusion.com		104.18.13.5	A (IP address)	IN (0x0001)
May 12, 2021 21:21:59.670203924 CEST	8.8.8.8	192.168.2.6	0x8c75	No error (0)	bttrack.com		192.132.33.46	A (IP address)	IN (0x0001)
May 12, 2021 21:22:00.567595959 CEST	8.8.8.8	192.168.2.6	0x2ff3	No error (0)	ds-aksb-a.akamaihd.net	ds-aksb-a.akamaihd.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:22:00.631513119 CEST	8.8.8.8	192.168.2.6	0xa358	No error (0)	pix-us.revjet.com		147.135.65.170	A (IP address)	IN (0x0001)
May 12, 2021 21:22:00.631513119 CEST	8.8.8.8	192.168.2.6	0xa358	No error (0)	pix-us.revjet.com		72.251.232.132	A (IP address)	IN (0x0001)
May 12, 2021 21:22:00.631513119 CEST	8.8.8.8	192.168.2.6	0xa358	No error (0)	pix-us.revjet.com		51.81.46.107	A (IP address)	IN (0x0001)
May 12, 2021 21:22:00.631513119 CEST	8.8.8.8	192.168.2.6	0xa358	No error (0)	pix-us.revjet.com		51.81.46.161	A (IP address)	IN (0x0001)
May 12, 2021 21:22:00.631513119 CEST	8.8.8.8	192.168.2.6	0xa358	No error (0)	pix-us.revjet.com		51.81.245.131	A (IP address)	IN (0x0001)
May 12, 2021 21:22:00.631513119 CEST	8.8.8.8	192.168.2.6	0xa358	No error (0)	pix-us.revjet.com		107.6.93.89	A (IP address)	IN (0x0001)
May 12, 2021 21:22:00.631513119 CEST	8.8.8.8	192.168.2.6	0xa358	No error (0)	pix-us.revjet.com		147.135.65.58	A (IP address)	IN (0x0001)
May 12, 2021 21:22:00.631513119 CEST	8.8.8.8	192.168.2.6	0xa358	No error (0)	pix-us.revjet.com		51.81.46.116	A (IP address)	IN (0x0001)
May 12, 2021 21:22:00.631513119 CEST	8.8.8.8	192.168.2.6	0xa358	No error (0)	pix-us.revjet.com		74.217.31.249	A (IP address)	IN (0x0001)
May 12, 2021 21:22:00.631513119 CEST	8.8.8.8	192.168.2.6	0xa358	No error (0)	pix-us.revjet.com		23.92.178.246	A (IP address)	IN (0x0001)
May 12, 2021 21:22:00.631513119 CEST	8.8.8.8	192.168.2.6	0xa358	No error (0)	pix-us.revjet.com		147.135.105.7	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 21:22:00.631513119 CEST	8.8.8.8	192.168.2.6	0xa358	No error (0)	pix-us.revjet.com		51.81.109.166	A (IP address)	IN (0x0001)
May 12, 2021 21:22:00.631513119 CEST	8.8.8.8	192.168.2.6	0xa358	No error (0)	pix-us.revjet.com		74.217.31.247	A (IP address)	IN (0x0001)
May 12, 2021 21:22:00.631513119 CEST	8.8.8.8	192.168.2.6	0xa358	No error (0)	pix-us.revjet.com		147.135.105.5	A (IP address)	IN (0x0001)
May 12, 2021 21:22:00.631513119 CEST	8.8.8.8	192.168.2.6	0xa358	No error (0)	pix-us.revjet.com		72.251.235.230	A (IP address)	IN (0x0001)
May 12, 2021 21:22:00.631513119 CEST	8.8.8.8	192.168.2.6	0xa358	No error (0)	pix-us.revjet.com		107.6.88.54	A (IP address)	IN (0x0001)
May 12, 2021 21:22:00.631513119 CEST	8.8.8.8	192.168.2.6	0xa358	No error (0)	pix-us.revjet.com		51.81.67.84	A (IP address)	IN (0x0001)
May 12, 2021 21:22:00.631513119 CEST	8.8.8.8	192.168.2.6	0xa358	No error (0)	pix-us.revjet.com		51.81.109.164	A (IP address)	IN (0x0001)
May 12, 2021 21:22:00.631513119 CEST	8.8.8.8	192.168.2.6	0xa358	No error (0)	pix-us.revjet.com		74.201.172.216	A (IP address)	IN (0x0001)
May 12, 2021 21:22:01.575823069 CEST	8.8.8.8	192.168.2.6	0x38c9	No error (0)	sync-tm.everesttech.net	sync.tubemogul.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:22:01.575823069 CEST	8.8.8.8	192.168.2.6	0x38c9	No error (0)	sync.tubemogul.com	syncf.tubemogul.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:22:01.575823069 CEST	8.8.8.8	192.168.2.6	0x38c9	No error (0)	syncf.tubemogul.com	h2.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:22:05.351624012 CEST	8.8.8.8	192.168.2.6	0xbb8c	No error (0)	pixel.rubiconproject.com	pixel.rubiconproject.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:22:05.632910013 CEST	8.8.8.8	192.168.2.6	0xfaaf	No error (0)	dsum-sec.casalemedia.com	dsum-sec.casalemedia.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:22:06.613183022 CEST	8.8.8.8	192.168.2.6	0x4ab7	No error (0)	ib.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:22:06.613183022 CEST	8.8.8.8	192.168.2.6	0x4ab7	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:22:06.613183022 CEST	8.8.8.8	192.168.2.6	0x4ab7	No error (0)	ib.anycast.adnxs.com		185.33.220.145	A (IP address)	IN (0x0001)
May 12, 2021 21:22:06.613183022 CEST	8.8.8.8	192.168.2.6	0x4ab7	No error (0)	ib.anycast.adnxs.com		185.33.221.14	A (IP address)	IN (0x0001)
May 12, 2021 21:22:06.613183022 CEST	8.8.8.8	192.168.2.6	0x4ab7	No error (0)	ib.anycast.adnxs.com		185.33.221.88	A (IP address)	IN (0x0001)
May 12, 2021 21:22:06.613183022 CEST	8.8.8.8	192.168.2.6	0x4ab7	No error (0)	ib.anycast.adnxs.com		185.33.221.13	A (IP address)	IN (0x0001)
May 12, 2021 21:22:06.613183022 CEST	8.8.8.8	192.168.2.6	0x4ab7	No error (0)	ib.anycast.adnxs.com		185.33.220.244	A (IP address)	IN (0x0001)
May 12, 2021 21:22:06.613183022 CEST	8.8.8.8	192.168.2.6	0x4ab7	No error (0)	ib.anycast.adnxs.com		185.33.221.53	A (IP address)	IN (0x0001)
May 12, 2021 21:22:06.613183022 CEST	8.8.8.8	192.168.2.6	0x4ab7	No error (0)	ib.anycast.adnxs.com		185.33.220.241	A (IP address)	IN (0x0001)
May 12, 2021 21:22:06.613183022 CEST	8.8.8.8	192.168.2.6	0x4ab7	No error (0)	ib.anycast.adnxs.com		185.33.221.52	A (IP address)	IN (0x0001)
May 12, 2021 21:22:07.620795965 CEST	8.8.8.8	192.168.2.6	0x4a41	No error (0)	us-u.openx.net		34.98.64.218	A (IP address)	IN (0x0001)
May 12, 2021 21:22:07.620795965 CEST	8.8.8.8	192.168.2.6	0x4a41	No error (0)	us-u.openx.net		35.244.159.8	A (IP address)	IN (0x0001)
May 12, 2021 21:22:08.625617981 CEST	8.8.8.8	192.168.2.6	0xbbc7	No error (0)	image2.pubmatic.com	pug-lhrc.pubmatic.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 21:22:08.625617981 CEST	8.8.8.8	192.168.2.6	0xbbc7	No error (0)	pug-lhrc.pubmatic.com	pug-lhr.pubmatic.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:22:08.625617981 CEST	8.8.8.8	192.168.2.6	0xbbc7	No error (0)	pug-lhr.pubmatic.com		185.64.190.80	A (IP address)	IN (0x0001)
May 12, 2021 21:22:09.610723019 CEST	8.8.8.8	192.168.2.6	0xfee1	No error (0)	sync.search.spotxchange.com	sync.search-gtm.spotxchange.com.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:22:09.610723019 CEST	8.8.8.8	192.168.2.6	0xfee1	No error (0)	ams01.sync.search.spotxchange.com		185.94.180.126	A (IP address)	IN (0x0001)
May 12, 2021 21:22:09.610723019 CEST	8.8.8.8	192.168.2.6	0xfee1	No error (0)	ams01.sync.search.spotxchange.com		185.94.180.125	A (IP address)	IN (0x0001)
May 12, 2021 21:22:11.582889080 CEST	8.8.8.8	192.168.2.6	0xa20	No error (0)	g2.gumgum.com		52.208.210.171	A (IP address)	IN (0x0001)
May 12, 2021 21:22:11.582889080 CEST	8.8.8.8	192.168.2.6	0xa20	No error (0)	g2.gumgum.com		54.247.114.64	A (IP address)	IN (0x0001)
May 12, 2021 21:22:11.582889080 CEST	8.8.8.8	192.168.2.6	0xa20	No error (0)	g2.gumgum.com		54.77.19.59	A (IP address)	IN (0x0001)
May 12, 2021 21:22:11.582889080 CEST	8.8.8.8	192.168.2.6	0xa20	No error (0)	g2.gumgum.com		52.208.41.69	A (IP address)	IN (0x0001)
May 12, 2021 21:22:11.582889080 CEST	8.8.8.8	192.168.2.6	0xa20	No error (0)	g2.gumgum.com		34.254.122.11	A (IP address)	IN (0x0001)
May 12, 2021 21:22:11.582889080 CEST	8.8.8.8	192.168.2.6	0xa20	No error (0)	g2.gumgum.com		54.77.47.243	A (IP address)	IN (0x0001)
May 12, 2021 21:22:11.582889080 CEST	8.8.8.8	192.168.2.6	0xa20	No error (0)	g2.gumgum.com		34.251.173.19	A (IP address)	IN (0x0001)
May 12, 2021 21:22:11.582889080 CEST	8.8.8.8	192.168.2.6	0xa20	No error (0)	g2.gumgum.com		52.212.126.234	A (IP address)	IN (0x0001)
May 12, 2021 21:22:12.752612114 CEST	8.8.8.8	192.168.2.6	0xa2a1	No error (0)	s.thebrightag.com		34.248.208.147	A (IP address)	IN (0x0001)
May 12, 2021 21:22:12.752612114 CEST	8.8.8.8	192.168.2.6	0xa2a1	No error (0)	s.thebrightag.com		54.195.251.142	A (IP address)	IN (0x0001)
May 12, 2021 21:22:12.752612114 CEST	8.8.8.8	192.168.2.6	0xa2a1	No error (0)	s.thebrightag.com		46.137.100.162	A (IP address)	IN (0x0001)
May 12, 2021 21:22:12.752612114 CEST	8.8.8.8	192.168.2.6	0xa2a1	No error (0)	s.thebrightag.com		54.228.243.159	A (IP address)	IN (0x0001)
May 12, 2021 21:22:13.751591921 CEST	8.8.8.8	192.168.2.6	0xf85b	No error (0)	partner.mediawallahscript.com	mwsyncpixel.eu-west-1.elasticbeanstalk.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 21:22:13.751591921 CEST	8.8.8.8	192.168.2.6	0xf85b	No error (0)	mwsyncpixel.eu-west-1.elasticbeanstalk.com		34.240.86.127	A (IP address)	IN (0x0001)
May 12, 2021 21:22:13.751591921 CEST	8.8.8.8	192.168.2.6	0xf85b	No error (0)	mwsyncpixel.eu-west-1.elasticbeanstalk.com		52.51.73.37	A (IP address)	IN (0x0001)
May 12, 2021 21:22:14.505467892 CEST	8.8.8.8	192.168.2.6	0xb9e7	No error (0)	use.typekit.net	use-stls.adobe.com.edgesuite.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 21:20:54.951432943 CEST	52.217.103.94	443	192.168.2.6	49731	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 12, 2021 21:20:56.384743929 CEST	52.217.103.94	443	192.168.2.6	49734	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 12, 2021 21:21:19.585820913 CEST	162.241.7.225	443	192.168.2.6	49796	CN=greycottage.ng 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	Tue May 04 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Tue Aug 03 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 12, 2021 21:21:19.586581945 CEST	162.241.7.225	443	192.168.2.6	49797	CN=greycottage.ng 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	Tue May 04 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Tue Aug 03 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 12, 2021 21:21:31.209677935 CEST	54.75.9.158	443	192.168.2.6	49841	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 12, 2021 21:21:31.220031977 CEST	52.213.176.171	443	192.168.2.6	49843	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 12, 2021 21:21:31.629048109 CEST	34.246.133.154	443	192.168.2.6	49845	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 12, 2021 21:21:32.759622097 CEST	54.75.9.158	443	192.168.2.6	49849	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 12, 2021 21:21:34.907823086 CEST	52.17.98.114	443	192.168.2.6	49878	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		
May 12, 2021 21:21:35.683969975 CEST	199.232.136.157	443	192.168.2.6	49890	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 12, 2021 21:21:35.994436979 CEST	52.19.106.86	443	192.168.2.6	49898	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 12, 2021 21:21:36.028701067 CEST	52.19.106.86	443	192.168.2.6	49900	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 12, 2021 21:21:36.298549891 CEST	108.174.11.37	443	192.168.2.6	49896	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 12, 2021 21:21:36.381352901 CEST	104.244.42.3	443	192.168.2.6	49905	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 12, 2021 21:21:36.412411928 CEST	104.244.42.5	443	192.168.2.6	49906	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

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 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 12, 2021 21:21:41.149513006 CEST	162.247.242.18	443	192.168.2.6	49929	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 12, 2021 21:21:41.656066895 CEST	13.225.74.123	443	192.168.2.6	49936	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 12, 2021 21:21:41.658328056 CEST	13.225.74.123	443	192.168.2.6	49935	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 12, 2021 21:21:44.996623993 CEST	52.214.120.236	443	192.168.2.6	49952	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 12, 2021 21:21:46.699768066 CEST	35.244.174.68	443	192.168.2.6	49981	CN=*.rlcdn.com CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Feb 25 01:00:00 CET 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Tue Mar 29 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
May 12, 2021 21:21:48.315258026 CEST	52.29.225.117	443	192.168.2.6	50001	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 12, 2021 21:21:48.804269075 CEST	185.29.133.52	443	192.168.2.6	50003	CN=*.mathtag.com, O="MediaMath, Inc.", L=New York, ST=New York, C=US CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed Apr 15 02:00:00 CEST 2020 Fri Mar 08 13:00:00 CET 2013	Fri Apr 22 14:00:00 CEST 2022 Wed Mar 08 13:00:00 CET 2023	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 08 13:00:00 CET 2013	Wed Mar 08 13:00:00 CET 2023		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 12, 2021 21:21:49.590759993 CEST	76.223.111.131	443	192.168.2.6	50017	CN=*.adsrvr.org CN=GlobalSign GCC R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	CN=GlobalSign GCC R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3 CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Thu Mar 18 23:45:32 CET 2021 Tue Jul 28 02:00:00 CEST 2020 Wed Mar 18 11:00:00 CET 2009	Wed Apr 20 00:45:32 CEST 2022 Sun Mar 18 01:00:00 CET 2029 Sun Mar 18 11:00:00 CET 2029	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GlobalSign GCC R3 DV TLS CA 2020, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Tue Jul 28 02:00:00 CEST 2020	Sun Mar 18 01:00:00 CET 2029		
					CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Mar 18 11:00:00 CET 2009	Sun Mar 18 11:00:00 CET 2029		
May 12, 2021 21:21:49.698468924 CEST	91.228.74.134	443	192.168.2.6	50018	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 12, 2021 21:21:52.976815939 CEST	64.158.223.137	443	192.168.2.6	50026	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 Wed Nov 21 01:00:00 CET 2018	Tue Aug 31 09:59:59 CEST 2021 Tue Nov 21 01:00:00 CET 2028	771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0	b32309a26951912be7dba376398abc3b
					CN=GlobalSign RSA OV SSL CA 2018, O=GlobalSign nv-sa, C=BE	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3	Wed Nov 21 01:00:00 CET 2018	Tue Nov 21 01:00:00 CET 2028		
May 12, 2021 21:21:58.696523905 CEST	52.49.20.76	443	192.168.2.6	50052	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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 12, 2021 21:21:58.716738939 CEST	13.225.74.123	443	192.168.2.6	50053	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 12, 2021 21:21:59.938827991 CEST	192.132.33.46	443	192.168.2.6	50057	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		
May 12, 2021 21:22:04.933022022 CEST	13.225.74.123	443	192.168.2.6	50100	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		

Code Manipulations

Statistics

Behavior

chrome.exe
chrome.exe

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6064 Parent PID: 2880

General

Start time:	21:20:48
Start date:	12/05/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://spark.adobe.com/page/3qeDIVcjdwWVx/'
Imagebase:	0x7ff7c15e0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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: 5892 Parent PID: 6064

General

Start time:	21:20:49
Start date:	12/05/2021
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=1568,11667160178596294028,15359971514153105505,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1772 /prefetch:8
Imagebase:	0x7ff7c15e0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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