ID: 358580
Cookbook: browseurl.jbs
Time: 21:41:31
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

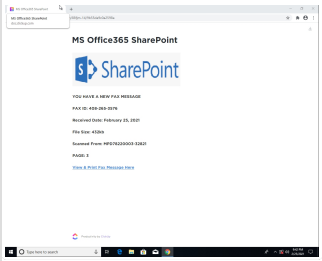
Analysis Report https://doc.clickup.com/d/h/88fjm-14/9b…

Overview

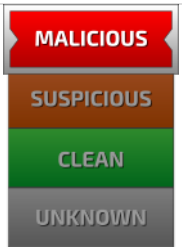
General Information

Sample URL:	http://https://doc.clickup.com/d/h/88fjm-14/9b55da9c0a2598a
Analysis ID:	358580
Infos:	

Most interesting Screenshot:



Detection



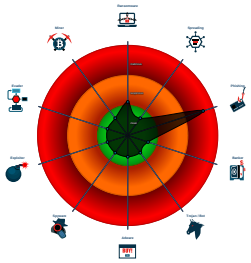
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Phishing site detected (based on fav…
- Yara detected HtmlPhish_10
- Phishing site detected (based on im…
- Phishing site detected (based on log…
- Found iframes
- HTML body contains low number of …
- HTML title does not match URL

Classification



Startup

- **System is w10x64**
- chrome.exe (PID: 4616 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://doc.clickup.com/d/h/88fjm-14/9b55da9c0a2598a' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 5368 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1612,2893176907998818176,3513762577707477399,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1672 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

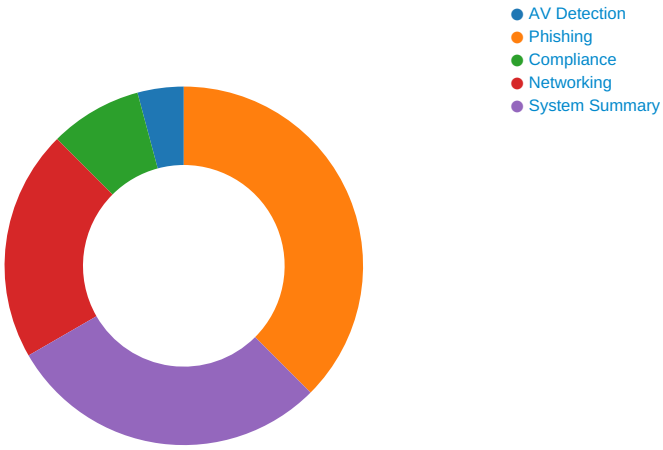
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Phishing:

Phishing site detected (based on favicon image match)

Yara detected HtmlPhish_10

Phishing site detected (based on image similarity)

Phishing site detected (based on logo template match)

Compliance:

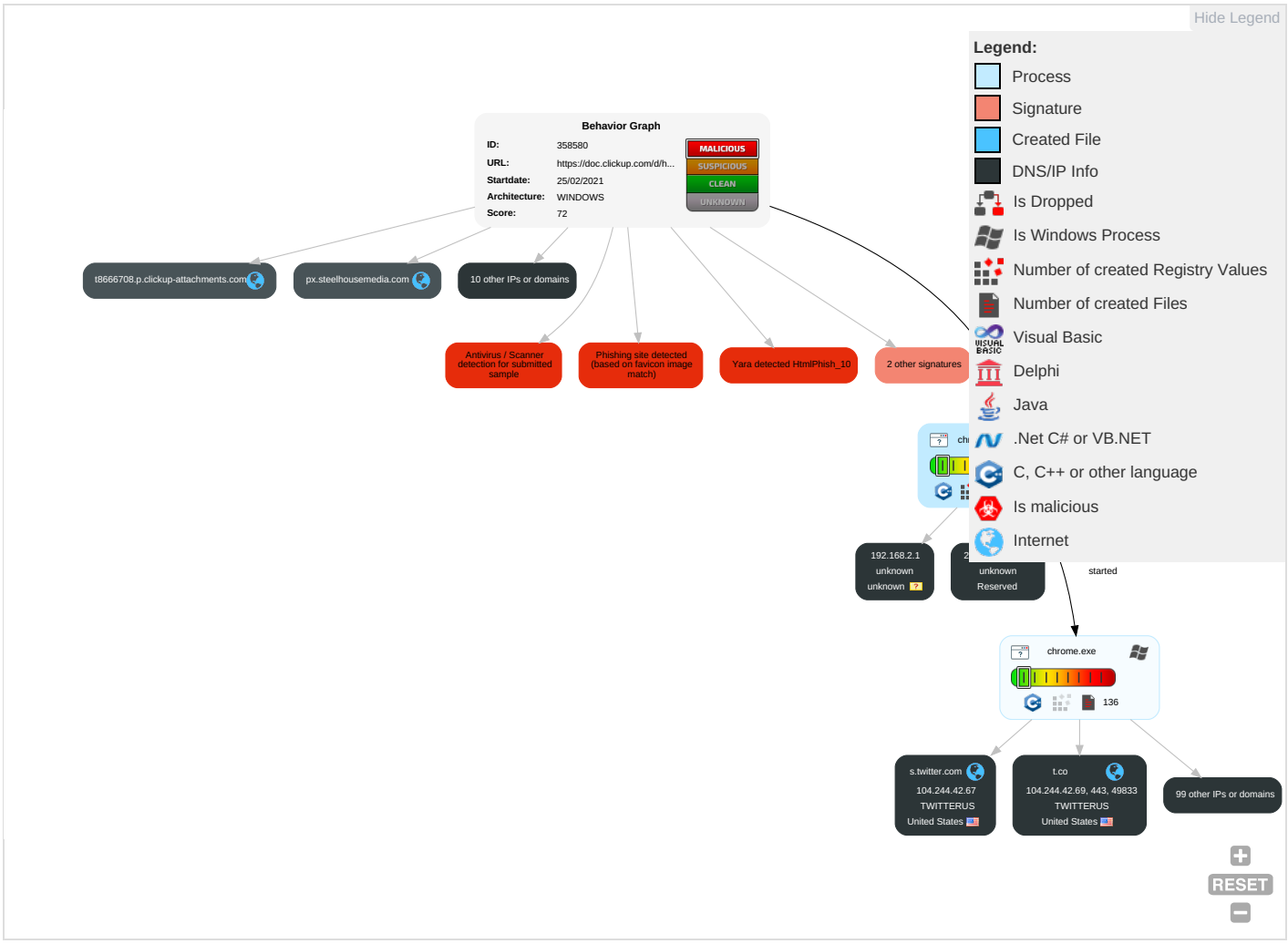
Creates a directory in C:\Program Files

Uses secure TLS version for HTTPS connections

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	I
Drive-by Compromise 1	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	M S F
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	D L
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	D D D

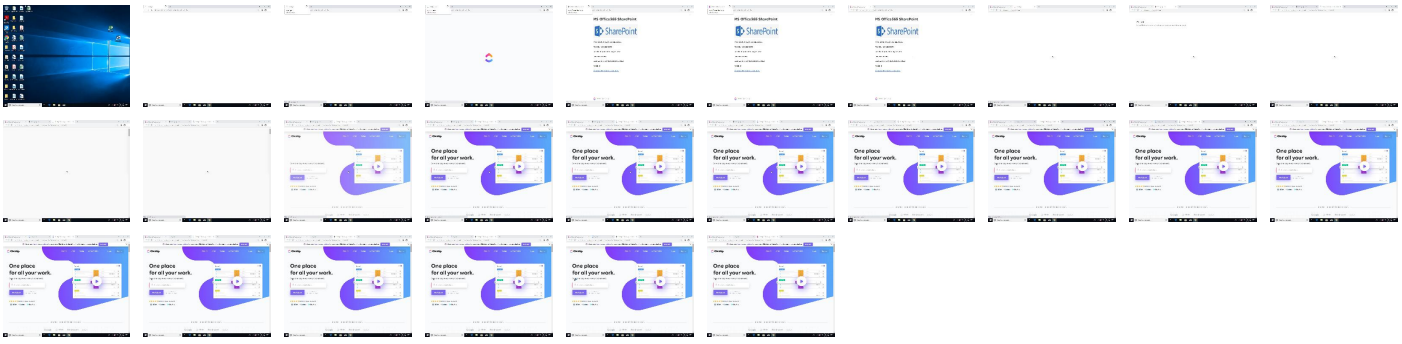
Behavior Graph

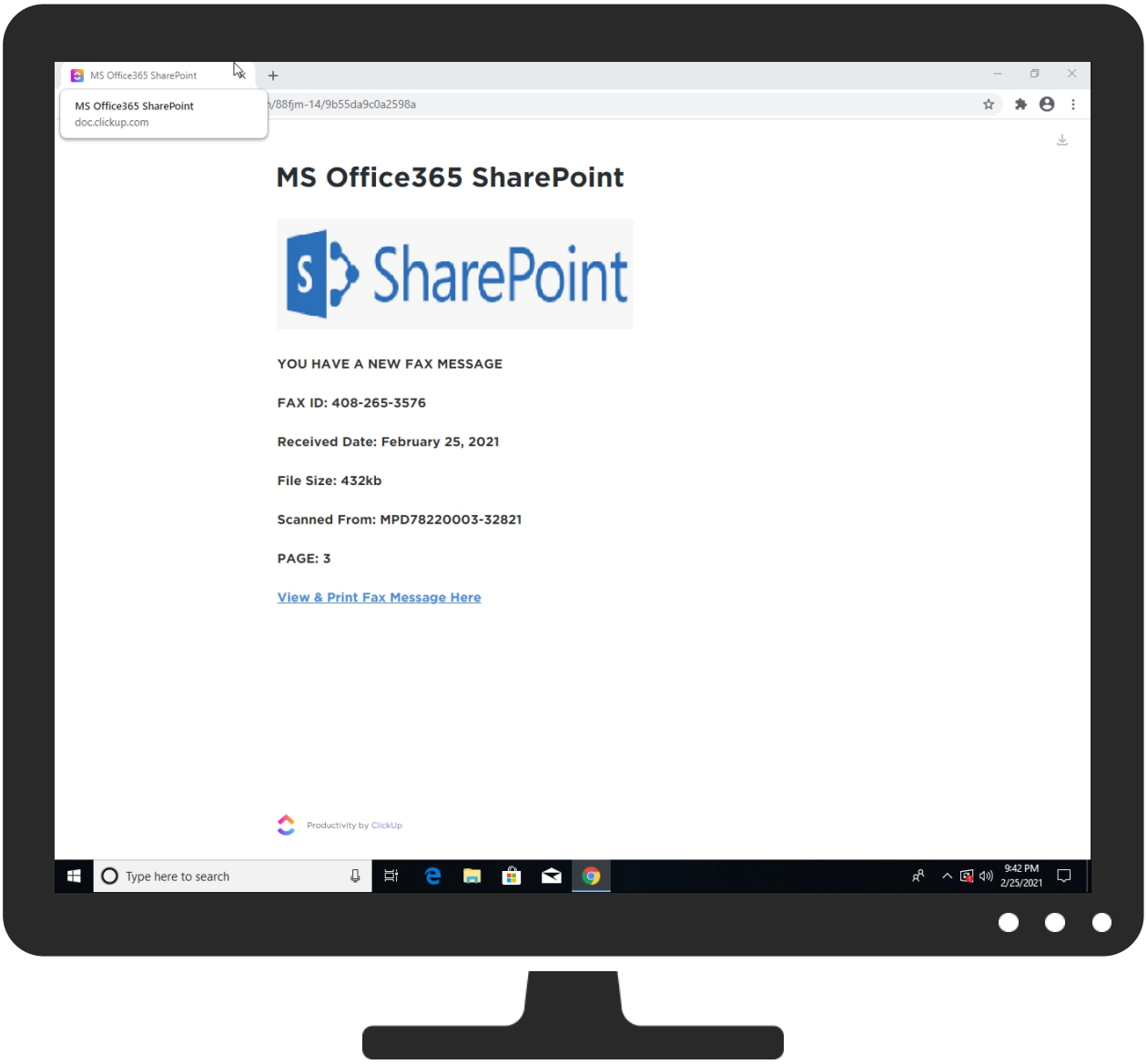


Screenshots

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://doc.clickup.com/d/h/88fjm-14/9b55da9c0a2598a	0%	Virustotal		Browse
http://https://doc.clickup.com/d/h/88fjm-14/9b55da9c0a2598a	0%	Avira URL Cloud	safe	
http://https://doc.clickup.com/d/h/88fjm-14/9b55da9c0a2598a	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
obs.cheqzone.com	0%	Virustotal		Browse
platform.twitter.map.fastly.net	0%	Virustotal		Browse
pixel2.cheqzone.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://client-registry.mutinycdn.com/	0%	Avira URL Cloud	safe	
http://https://clickup.comh	0%	Avira URL Cloud	safe	
http://https://js.hs-analytics.net/analytics/1614285600000/6613321.js	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://www.googleoptimize.com/	0%	Avira URL Cloud	safe	
http://https://client.mutinycdn.com/mutiny-client/4.1.1.5.js	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://x.clearbitjs.com/v1/pk_77a36b09108b9b80c547cddad434b648/clearbit.min.js	0%	Avira URL Cloud	safe	
http://https://www.googleoptimize.com/optimize.js?id=GTM-PBLF7VJ	0%	Avira URL Cloud	safe	
http://crl.securetrust.com/STCA.crl0	0%	URL Reputation	safe	
http://crl.securetrust.com/STCA.crl0	0%	URL Reputation	safe	
http://crl.securetrust.com/STCA.crl0	0%	URL Reputation	safe	
http://https://js.hscollectedforms.net/collectedforms.js	0%	URL Reputation	safe	
http://https://js.hscollectedforms.net/collectedforms.js	0%	URL Reputation	safe	
http://https://js.hscollectedforms.net/collectedforms.js	0%	URL Reputation	safe	
http://https://client-registry.mutinycdn.com/personalize/client/e970333877260fa7.js	0%	Avira URL Cloud	safe	
http://https://ob.cheqzone.com/clicktrue_invocation.js?id=3839	0%	Avira URL Cloud	safe	
http://https://cdn.pdst.fm/ping.min.js	0%	Avira URL Cloud	safe	
http://https://obs.cheqzone.com/ct?id=3839&url=https%3A%2F%2Fclickup.com%2F%3Futm_source%3Dclickup%26utm_me	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
t8666708.p.clickup-attachments.com	13.227.156.121	true	false		unknown
forms.hubspot.com	104.19.154.83	true	false		high
clickup.com	13.227.156.22	true	false		high
d10w4ikcrdu13z.cloudfront.net	13.227.156.61	true	false		high
obs.cheqzone.com	52.45.196.192	true	false	• 0%, Virustotal, Browse	unknown
platform.twitter.map.fastly.net	151.101.12.157	true	false	• 0%, Virustotal, Browse	unknown
pixel2.cheqzone.com	35.153.6.179	true	false	• 0%, Virustotal, Browse	unknown
client.mutinycdn.com	99.84.90.13	true	false		unknown
t.co	104.244.42.69	true	false		high
track.hubspot.com	104.19.155.83	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
js.hs-scripts.com	104.17.211.204	true	false		high
dx.steelhousemedia.com	44.241.10.203	true	false		high
tracking.g2crowd.com	104.18.27.190	true	false		high
match-1943069928.eu-west-1.elb.amazonaws.com	34.249.70.28	true	false		high
q.quora.com	50.17.2.180	true	false		high
quora.map.fastly.net	151.101.1.2	true	false		unknown
static-cdn.hotjar.com	99.84.90.83	true	false		high
d2ycxbs0cq3yaz.cloudfront.net	13.227.156.87	true	false		high
px.steelhousemedia.com	54.245.46.233	true	false		high
js.intercomcdn.com	99.84.90.89	true	false		high
js.hs-banner.com	104.18.21.191	true	false		unknown
star-mini.c10r.facebook.com	31.13.92.36	true	false		high
stats.l.doubleclick.net	74.125.71.157	true	false		high
pale-small-origami.glitch.me	18.215.10.11	true	false		high
s.twitter.com	104.244.42.67	true	false		high
ww.steelhousemedia.com	44.238.130.186	true	false		high
monetization-framework.bsa.netdna-cdn.com	108.161.189.78	true	false		high
edge.fullstory.com	35.201.112.186	true	false		high
api-iam.intercom.io	99.83.219.81	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.googleoptimize.com	142.250.184.78	true	false		unknown
insight-566961044.eu-west-1.elb.amazonaws.com	34.251.161.187	true	false		high
clockify.me	13.227.156.123	true	false		high
reddit.map.fastly.net	151.101.1.140	true	false		unknown
googleads.g.doubleclick.net	142.250.184.34	true	false		high
www.google.co.uk	142.250.184.67	true	false		unknown
acsbapp.com	167.172.136.187	true	false		unknown
atlas.c10r.facebook.com	31.13.92.2	true	false		high
calendly.com	104.20.248.116	true	false		high
cheqzone2.b-cdn.net	89.187.165.193	true	false		high
googlehosted.l.googleusercontent.com	142.250.184.33	true	false		high
d5txjkmyderx.cloudfront.net	13.227.156.8	true	false		high
forms.hsforms.com	104.16.88.5	true	false		unknown
global-v2.clearbit.com	18.134.247.58	true	false		high
pop-eda6.mix.linkedin.com	108.174.11.69	true	false		high
elb046299-1187644484.us-east-1.elb.amazonaws.com	54.225.168.201	true	false		high
js.hs-analytics.net	104.17.70.176	true	false		unknown
api.exchangeratesapi.io	172.67.74.213	true	false		unknown
x.clearbit.com	18.134.247.58	true	false		high
us-central1-adaptive-growth.cloudfunctions.net	216.239.36.54	true	false		unknown
scontent.xx.fbcdn.net	31.13.92.14	true	false		high
script.hotjar.com	99.84.90.20	true	false		high
cdn.pdst.fm	35.244.142.80	true	false		unknown
nexus-websocket-a.intercom.io	35.174.127.31	true	false		high
widget.intercom.io	99.84.90.9	true	false		high
fullstory.com	34.107.252.72	true	false		high
api.clickup.com	52.58.150.147	true	false		high
d279x8308vq8mj.cloudfront.net	99.84.90.85	true	false		high
gentle-meadow-3800.shrouded-lake-4691.herokuspace.com	34.210.168.131	true	false		unknown
vars.hotjar.com	99.84.90.32	true	false		high
rs.fullstory.com	35.186.194.58	true	false		high
api.getdrip.com	13.227.156.11	true	false		high
app.clickup.com	52.29.76.203	true	false		high
dlx6k0k2hv67n.cloudfront.net	99.84.90.17	true	false		high
js.hscollectedforms.net	104.17.130.171	true	false		unknown
alb.reddit.com	unknown	unknown	false		high
static.ads-twitter.com	unknown	unknown	false		unknown
app-cdn.clickup.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
static.hotjar.com	unknown	unknown	false		high
ob.cheqzone.com	unknown	unknown	false		unknown
match.adsrvr.org	unknown	unknown	false		high
www.redditstatic.com	unknown	unknown	false		high
cx.atdmt.com	unknown	unknown	false		high
doc.clickup.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
px.ads.linkedin.com	unknown	unknown	false		high
cdn.acsbapp.com	unknown	unknown	false		unknown
a.quora.com	unknown	unknown	false		high
tag.getdrip.com	unknown	unknown	false		high
x.clearbitjs.com	unknown	unknown	false		unknown
cdn.firstpromoter.com	unknown	unknown	false		high
insight.adsrvr.org	unknown	unknown	false		high
scripts.attributionapp.com	unknown	unknown	false		high
track.attributionapp.com	unknown	unknown	false		high
stackpath.bootstrapcdn.com	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
client-registry.mutinycdn.com	unknown	unknown	false		unknown
analytics.twitter.com	unknown	unknown	false		high
m.servedby-buysellads.com	unknown	unknown	false		unknown
snap.licdn.com	unknown	unknown	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
user-data.mutinycdn.com	unknown	unknown	false		unknown
api-v2.mutinyhq.io	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://clickup.com/?utm_source=clickup&utm_medium=doc&utm_campaign=8666708	false		high
http://https://pale-small-origami.glitch.me/	false		high
http://https://doc.clickup.com/d/h/88fjm-14/9b55da9c0a2598a	false		high

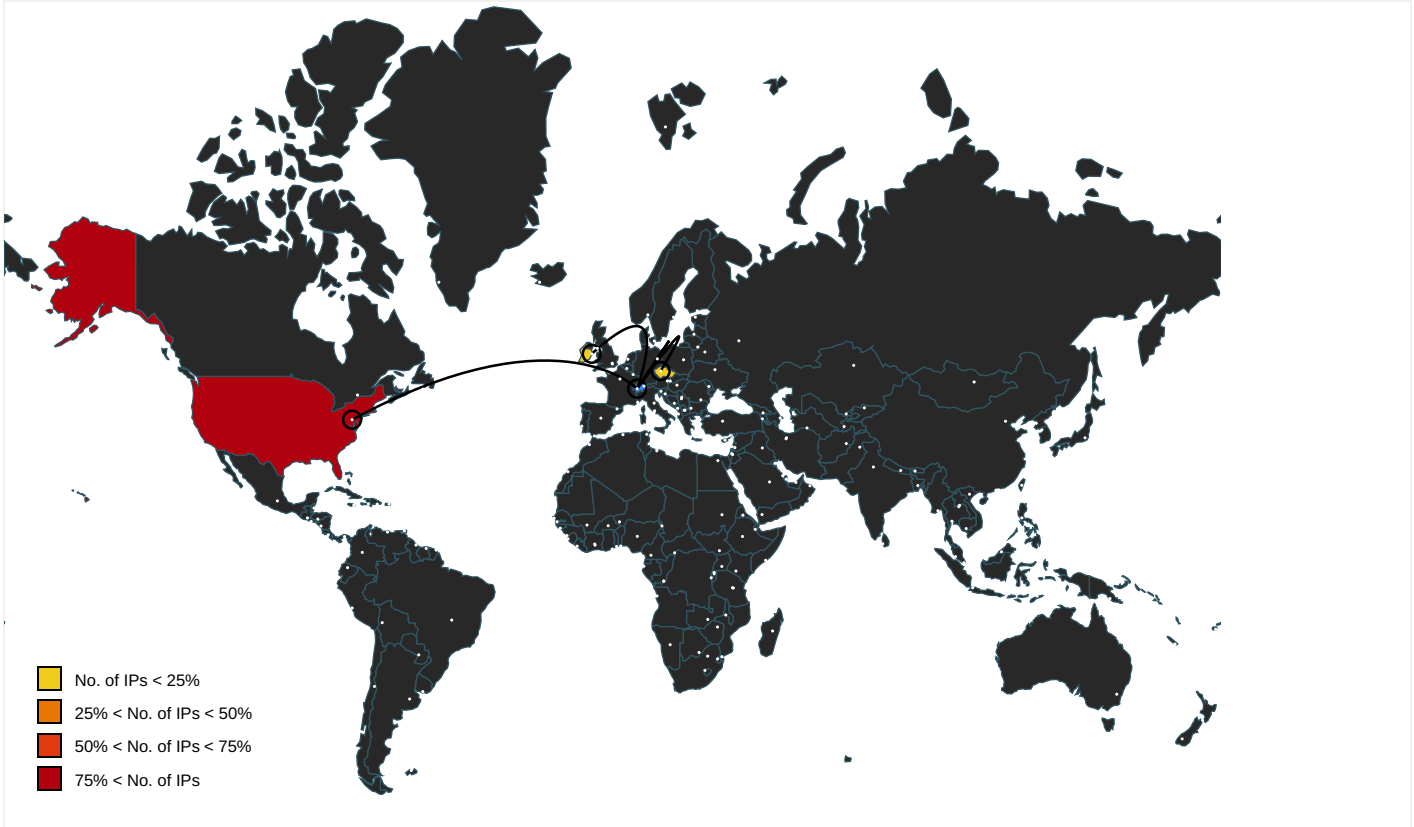
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js	f7fd71217955a417_0.0.dr	false		high
http://https://a.nel.cloudflare.com/report?s=O11DbKbToEDYU8BbPXLEMOvzLTbKNgfKv%2FYXb5hD6n5s5XyhWCSPrCk9kKob	Reporting and NEL.1.dr	false		high
http://https://client-registry.mutinycdn.com/	Network Action Predictor.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://px.steelhousemedia.com/st?ga_tracking_id=UA-87708648-1&ga_client_id=1304408799.1614318149&sh	bfbf5849650ec0d2_0.0.dr	false		high
http://https://clickup.com/I$	4071488f0118ba2c_0.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/617640813/?random=1614318166633&cv=	68fe4b04414a05eb_0.0.dr	false		high
http://https://www.redditstatic.com/ads/pixel.js	4589da573ea5c1c6_0.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/867030291/?random=1614318176081&cv=	7e26d863851b82b7_0.0.dr	false		high
http://https://clickup.com/landing/js/cssrelpreload.js	8fd5d1efccaacc9f_0.0.dr	false		high
http://https://clickup.comh	Current Session.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://doc.clickup.com/30-es2015.c8400463cbca5eefae05.js	d3f4ed42682742c9_0.0.dr	false		high
http://https://clickup.com/landing/favicons/favicon-32x32.pngB	Favicons.0.dr	false		high
http://https://doc.clickup.com/d/h/88fjm-14/9b55da9c0a2598a	Current Session.0.dr, History-journal.0.dr	false		high
http://https://px.ads.linkedin.com/collect?	ecba0530bad5195f_0.0.dr	false		high
http://https://pale-small-origami.glitch.me/Sign	History.0.dr	false		high
http://https://doc.clickup.com/8-es2015.572c4744fe272494ec6d.js	cae14352f97fb1aa_0.0.dr	false		high
http://https://clickup.com/?utm_source=clickup&utm_medium=doc&utm_campaign=8666708	Current Session.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/617640813/?random=1614318179820&cv=	7f8fede988c53756_0.0.dr	false		high
http://https://clickup.com/?	d3f4ed42682742c9_0.0.dr	false		high
http://https://connect.facebook.net/en_US/fbevents.js	293e5233d64a0a25_0.0.dr	false		high
http://https://clickup.com/E	7e26d863851b82b7_0.0.dr	false		high
http://https://js.hs-analytics.net/analytics/1614285600000/6613321.js	099b5e3dfcf45bcf_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://js.hs-scripts.com/6613321.js	4303153a6c225d91_0.0.dr	false		high
http://https://scripts.attributionapp.com/attribution.js	4071488f0118ba2c_0.0.dr	false		high
http://https://clickup.com//	4d623bcd069ac743_0.0.dr	false		high
http://https://doc.clickup.com/polyfills-es2015.74fd49d5fff3696d5809.js	c2c5635b1cb2c5d5_0.0.dr	false		high
http://https://pale-small-origami.glitch.me/2	History Provider Cache.0.dr	false		high
http://https://clickup.com/Y	438fcc93076e9e9c_0.0.dr	false		high
http://https://clickup.com/Z	668970570f5e454b_0.0.dr	false		high
http://https://dns.google	95097a95-8bab-45e6-a8f4-2a8c2bc140d5.tmp.1.dr, 9222b070-7287-4cdd-bb70-e35b6a9fe87f.tmp.1.dr, 9f0ba012-829b-4938-8dbf-fef5ec645bfd.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://doc.clickup.com/d/h/88fjm-14/9b55da9c0a2598aMS	History-journal.0.dr	false		high
http://https://js.intercomcdn.com/vendors~app-modern.257e5d56.js	9cf84dddf1420918_0.0.dr	false		high
http://https://a.nel.cloudflare.com/report?s=2qSDxEO%2Bl16iEO%2Fr9dXZQqGJD0MD0GfEkqEOr9zZJVapODq9dxMtkrwDYC	Reporting and NEL.1.dr	false		high
http://https://js.intercomcdn.com/shim.latest.js	71d60bb0bfb5747b_0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://doc.clickup.com	000003.log3.0.dr, Current Session.0.dr	false		high
http://https://clickup.com	Current Session.0.dr	false		high
http://https://clickup.com/H	ecba0530bad5195f_0.0.dr	false		high
http://https://vars.hotjar.com/	000003.log0.0.dr	false		high
http://https://clickup.com/J	f8a2aae8c7eea631_0.0.dr	false		high
http://https://www.googleoptimize.com/	Network Action Predictor.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clickup.com/L	060571bc15e680b3_0.0.dr	false		high
http://https://clickup.com/tJ	7f8fede988c53756_0.0.dr	false		high
http://https://doc.clickup.com/6-es2015.cba4f5449c46d437389a.js	438fcc93076e9e9c_0.0.dr	false		high
http://https://clickup.com/?utm_source=clickup&utm_medium=doc&utm_campaign=8666708&ClickUp	Current Session.0.dr	false		high
http://https://clickup.com/O	426f0f97b11e76c3_0.0.dr	false		high
http://https://client.mutinycdn.com/mutiny-client/4.1.1.5.js	90c36c75ff2a1ff6_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clickup.com/Q	cae14352f97fb1aa_0.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/617640813/?random=1614318166627&cv=	3783441f7181a3e9_0.0.dr	false		high
http://https://clickup.com/	372528a3f8712b40_0.0.dr, 099b5e3dfcf45bcf_0.0.dr, 000003.log3.0.dr, 4303153a6c225d91_0.0.dr, 73b471123e2428a3_0.0.dr, 8fd5d1efccaacc9f_0.0.dr, 000003.log0.0.dr	false		high
http://https://doc.clickup.com/d/h/88fjm-14/9b55da9c0a2598a2	History Provider Cache.0.dr	false		high
http://https://static.ads-twitter.com/uwt.js	86f3493414ae88e3_0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clickup.com/x	be2d99002a93a98a_0.0.dr	false		high
http://https://x.clearbitjs.com/v1/pk_77a36b09108b9b80c547cddad434b648/clearbit.min.js	a0836518de30683a_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clickup.com/z	4589da573ea5c1c6_0.0.dr	false		high
http://https://js.intercomcdn.com/vendor-modern.2ab434f6.js	a64461351d5f2a59_0.0.dr	false		high
http://https://www.linkedin.com/company/12949663	Current Session.0.dr	false		high
http://https://googleads.g.doubleclick.net/pagead/viewthroughconversion/617640813/?random=1614318166622&cv=	81950e9ecb9b5351_0.0.dr	false		high
http://https://clickup.com/landing/js/typed.min.js	73b471123e2428a3_0.0.dr	false		high
http://https://clickup.com/cu	afbc24eaef0bbeb7_0.0.dr	false		high
http://https://clickup.com/j	668970570f5e454b_0.0.dr	false		high
http://https://a.quora.com/qevents.js	4d623bcd069ac743_0.0.dr	false		high
http://https://app-cdn.clickup.com/assets/favicons/favicon-32x32.png	Favicons-journal.0.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js	b11f6c304de41b06_0.0.dr	false		high
http://https://feedback.googleusercontent.com	manifest.json0.0.dr	false		high
http://https://clickup.com/t	1408a718ac481827_0.0.dr	false		high
http://https://clickup.com/w	81950e9ecb9b5351_0.0.dr	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/bowser/1.9.4/bowser.min.js	31aa3190c5efd805_0.0.dr	false		high
http://https://pale-small-origami.glitch.me	Current Session.0.dr	false		high
http://https://www.googleoptimize.com/optimize.js?id=GTM-PBLF7VJ	4e268f2ebf5198c2_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://cdn.firstpromoter.com/fprom.js	d9133d4093e7cc49_0.0.dr	false		high
http://https://edge.fullstory.com/s/fs.js	a81f1b4d5a99dd1d_0.0.dr	false		high
http://https://js.intercomcdn.com/frame-modern.17b2a5c1.js	38aa030603a13736_0.0.dr	false		high
http://https://doc.clickup.com:443	73d613a0-1d9e-4787-b174-f6001c9eb0aa.tmp.0.dr	false		high
http://https://clickup.com/?utm_source=clickup&utm_medium=doc&utm_campaign=8666708ClickUp	History-journal.0.dr	false		high
http://https://calendly.com/assets/external/widget.js	701263a561b04671_0.0.dr	false		high
http://https://docs.clickup.com	000003.log3.0.dr	false		high
http://crl.securetrust.com/STCA.crl0	4CA77D36767B6202D4786BF3D1EC52420.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/WebPage	Current Session.0.dr	false		high
http://https://clickup.com/images/schema_org/image.png	Current Session.0.dr	false		high
http://schema.org	Current Session.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://js.hscollectedforms.net/collectedforms.js	0cf69c09debb1d32_0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://script.hotjar.com/modules.dbbd0f16dca02537aef0.js	372528a3f8712b40_0.0.dr	false		high
http://https://clickup.com/J:%	76094a390b8abd4a_0.0.dr	false		high
http://https://client-registry.mutinycdn.com/personalize/client/e970333877260fa7.js	8fbb15542bd0b54d_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://connect.facebook.net/signals/config/124630241461844?v=2.9.33&r=stable	f4e88cc7f3307961_0.0.dr	false		high
http://https://clickup.com/$M	f8a2aae8c7eea631_0.0.dr	false		high
http://https://pale-small-origami.glitch.me/	Current Session.0.dr	false		high
http://https://pale-small-origami.glitch.me/Waking	History-journal.0.dr	false		high
http://https://snap.licdn.com/li.lms-analytics/insight.min.jsaD	ecba0530bad5195f_0.0.dr	false		high
http://https://js.intercomcdn.com/app-modern.16409436.js	e62126747b8640fd_0.0.dr	false		high
http://https://ob.cheqzone.com/clicktrue_invocation.js?id=3839	1dfebe463549e1f9_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://doc.clickup.com/4-es2015.e012bd08670670cdbbee.js	399055e3fa3b678b_0.0.dr	false		high
http://https://vars.hotjar.com/box-469cf41adb11dc78be68c1ae7f9457a4.html	Current Session.0.dr	false		high
http://https://cdn.pdst.fm/ping.min.js	d6a93f49c5fe3a17_0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://doc.clickup.com/runtime-es2015.1e4c4eb7935977bacb85.js	21cda92b5a14b9f1_0.0.dr	false		high
http://https://calendly.com/	Network Action Predictor.0.dr	false		high
http://https://obs.cheqzone.com/ct?id=3839&url=https%3A%2F%2Fclickup.com%2F%3Futm_source%3Dclickup%26utm_me	396648a11d6cfbf5_0.0.dr	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
99.84.90.85	unknown	United States		16509	AMAZON-02US	false
104.19.155.83	unknown	United States		13335	CLOUDFLARENETUS	false
34.107.252.72	unknown	United States		15169	GOOGLEUS	false
99.84.90.89	unknown	United States		16509	AMAZON-02US	false
13.227.156.8	unknown	United States		16509	AMAZON-02US	false
35.186.194.58	unknown	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
31.13.92.36	unknown	Ireland		32934	FACEBOOKUS	false
161.35.15.77	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
35.174.127.31	unknown	United States		14618	AMAZON-AESUS	false
18.215.10.11	unknown	United States		14618	AMAZON-AESUS	false
151.101.1.2	unknown	United States		54113	FASTLYUS	false
104.18.21.191	unknown	United States		13335	CLOUDFLARENETUS	false
50.17.2.180	unknown	United States		14618	AMAZON-AESUS	false
13.227.156.22	unknown	United States		16509	AMAZON-02US	false
167.172.136.187	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
104.16.18.94	unknown	United States		13335	CLOUDFLARENETUS	false
13.227.156.61	unknown	United States		16509	AMAZON-02US	false
99.84.90.83	unknown	United States		16509	AMAZON-02US	false
18.134.247.58	unknown	United States		16509	AMAZON-02US	false
104.17.211.204	unknown	United States		13335	CLOUDFLARENETUS	false
104.19.154.83	unknown	United States		13335	CLOUDFLARENETUS	false
13.227.156.123	unknown	United States		16509	AMAZON-02US	false
54.245.46.233	unknown	United States		16509	AMAZON-02US	false
99.84.90.13	unknown	United States		16509	AMAZON-02US	false
13.227.156.121	unknown	United States		16509	AMAZON-02US	false
34.251.161.187	unknown	United States		16509	AMAZON-02US	false
99.84.90.17	unknown	United States		16509	AMAZON-02US	false
44.238.130.186	unknown	United States		16509	AMAZON-02US	false
34.249.70.28	unknown	United States		16509	AMAZON-02US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
31.13.92.2	unknown	Ireland		32934	FACEBOOKUS	false
89.187.165.193	unknown	Czech Republic		60068	CDN77GB	false
216.239.36.54	unknown	United States		15169	GOOGLEUS	false
104.16.88.5	unknown	United States		13335	CLOUDFLARENETUS	false
13.227.156.11	unknown	United States		16509	AMAZON-02US	false
104.17.70.176	unknown	United States		13335	CLOUDFLARENETUS	false
151.101.12.157	unknown	United States		54113	FASTLYUS	false
104.17.130.171	unknown	United States		13335	CLOUDFLARENETUS	false
99.84.90.20	unknown	United States		16509	AMAZON-02US	false
142.250.184.67	unknown	United States		15169	GOOGLEUS	false
31.13.92.14	unknown	Ireland		32934	FACEBOOKUS	false
108.161.189.78	unknown	United States		33438	HIGHWINDS2US	false
54.225.168.201	unknown	United States		14618	AMAZON-AESUS	false
74.125.71.157	unknown	United States		15169	GOOGLEUS	false
99.84.90.9	unknown	United States		16509	AMAZON-02US	false
13.227.156.87	unknown	United States		16509	AMAZON-02US	false
108.174.11.69	unknown	United States		14413	LINKEDINUS	false
142.250.184.33	unknown	United States		15169	GOOGLEUS	false
142.250.184.78	unknown	United States		15169	GOOGLEUS	false
99.84.90.32	unknown	United States		16509	AMAZON-02US	false
35.153.6.179	unknown	United States		14618	AMAZON-AESUS	false
104.244.42.69	unknown	United States		13414	TWITTERUS	false
104.244.42.67	unknown	United States		13414	TWITTERUS	false
44.241.10.203	unknown	United States		16509	AMAZON-02US	false
99.83.219.81	unknown	United States		16509	AMAZON-02US	false
151.101.1.140	unknown	United States		54113	FASTLYUS	false
52.29.76.203	unknown	United States		16509	AMAZON-02US	false
52.58.150.147	unknown	United States		16509	AMAZON-02US	false
35.201.112.186	unknown	United States		15169	GOOGLEUS	false
104.20.248.116	unknown	United States		13335	CLOUDFLARENETUS	false
34.210.168.131	unknown	United States		16509	AMAZON-02US	false
52.45.196.192	unknown	United States		14618	AMAZON-AESUS	false
172.67.74.213	unknown	United States		13335	CLOUDFLARENETUS	false
35.244.142.80	unknown	United States		15169	GOOGLEUS	false
104.18.27.190	unknown	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
192.168.2.6
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358580
Start date:	25.02.2021
Start time:	21:41:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://doc.clickup.com/d/h/88fjm-14/9b55da9c0a2598a
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.phis.win@32/246@80/68
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://pale-small-origami.glitch.me/ • Browse: https://clickup.com/?utm_source=clickup&utm_medium=doc&utm_campaign=8666708

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe • TCP Packets have been reduced to 100 • Created / dropped Files have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.88.21.125, 204.79.197.200, 13.107.21.200, 51.104.144.132, 23.54.113.53, 104.43.193.48, 52.255.188.83, 104.43.139.144, 142.250.180.163, 216.58.208.142, 142.250.180.77, 216.58.205.78, 173.194.188.74, 173.194.187.230, 142.250.185.232, 8.253.207.121, 8.241.121.126, 67.27.235.126, 67.26.83.254, 8.253.207.120, 142.250.184.110, 216.58.206.36, 13.64.90.137, 151.101.2.217, 151.101.66.217, 151.101.130.217, 151.101.194.217, 216.58.208.170, 216.58.209.42, 142.250.184.42, 142.250.184.74, 142.250.184.106, 142.250.180.74, 142.250.180.106, 142.250.180.138, 142.250.180.170, 216.58.208.138, 184.30.21.40, 184.30.20.56, 142.250.184.34, 204.13.202.71, 209.197.3.15, 51.103.5.159, 216.58.208.131, 216.58.208.163, 173.194.188.6, 51.104.139.180 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, clientservices.googleapis.com, r5.sn-4g5ednsl.gvt1.com, fs-wildcard.microsoft.com.edgekey.net, clients2.google.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, update.googleapis.com, www.google.com, watson.telemetry.microsoft.com, www.gstatic.com, au-bg-shim.trafficmanager.net, c3.shared.global.fastly.net, www.google-analytics.com, www.bing.com, fs.microsoft.com, content-autofill.googleapis.com, dual-a-0001.a-msedge.net, ssl.trustwave.com, skypedataprdcolcus16.cloudapp.net, www.googleapis.com, skypedataprdcolcus15.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, clients.l.google.com, r1---sn-4g5ednly.gvt1.com, www.googleadservices.com, r1---sn-4g5edns7.gvt1.com, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, e9706.dscg.akamaiedge.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, redirector.gvt1.com, www.googletagmanager.com, bat.bing.com, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, firebasestorage.googleapis.com, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, accounts.google.com, www-google-analytics.l.google.com, r5---sn-4g5ednsl.gvt1.com, www-googletagmanager.l.google.com, r1.sn-4g5edns7.gvt1.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcoleus17.cloudapp.net, bat-bing-com.a-0001.a-msedge.net, a-0001.a-afdentry.net.trafficmanager.net, wildcard.licdn.com.edgekey.net, cds.j3z9t3p6.hwcdn.net, r1.sn-4g5ednly.gvt1.com, skypedataprdcolwus15.cloudapp.net • Report size exceeded maximum capacity and may have missing network information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtQueryVolumeInformationFile calls found. • Report size getting too big, too many NtWriteFile calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:42:27	API Interceptor	2x Sleep call for process: chrome.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\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
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\4CA77D36767B6202D4786BF3D1EC5242	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1912
Entropy (8bit):	7.3478006141797225
Encrypted:	false

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\4CA77D36767B6202D4786BF3D1EC5242	
SSDEEP:	24:t9vguPvg+7QqUESjQLscZ3Oywr9ICRo9vguPvg+7QqUESjQLscZ3Oywr9ICRk:/jPVQ842hV1i9IGkjPVQ842hV1i9IGk
MD5:	A4EECCAEF5148699F70ACB88F752247D
SHA1:	2A27D8A3FE60977EB4A68420378602F05BB8D4AC
SHA-256:	7C6C8AC621EDD346C6077ACD9904FECD2A992FFCF177330027966C8194401420
SHA-512:	BD9639FE6C833C343DBEF5CD46C48022A915F3CF51BA46E032044DC24426AF9866AF11295EFCDE23421273C79F75E4BF7D980C8F56285185C9C2FCF37DE8745
Malicious:	false
Reputation:	low
Preview:	0...0.....\....B...'.Y.0...*.H.....0H1.0...U....US1 0...U....SecureTrust Corporation1.0...U....SecureTrust CA0...061107193118Z..2912311940555Z0H1.0...U....US1 0 ...U....SecureTrust Corporation1.0...U....SecureTrust CA0.."0...*.H.....0.....O...x.X.A...@$.9.3f..b\...$[a....A..n.....H.....A>...).....m.g.W.....f%H...].....O. F..\..^..m.....o1BlR>h...4...V.&....o.....d.KD.....c.f.v.q..6.hzw..../.z.r..k.....Y?.r.D$..s...W/B&..t..R.K.S\|G.6..f....4W.f....pT...(.Y.....0..0...+.....7.....C.A0...U.....0...U.....0... .0...U.....B2.....]Kz...L@.ZC.04..U...-0+0).'.%.#http://crl.securetrust.com/STCA.crl0...+.....7.....0...*.H.....0.OJ.X:Rr[...e...Q;w...\.Ee{..[.pP.....I.A..s.~.#!....`.Zr.....z o].....iB..q..&....j.q....|!T+.X..W).....&.....i.....+.64{$.xL....&..dR6_`g...t..g#.....0.7~..2.-.D00l....4...@.K.fF.T..2.c&0k...G...b...g.x)c.o....L...7...(K...,h....10...0.....\....B... '.Y.0...*.H.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwElztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	low
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n- .....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..Ir.....I.I6/..d.].xIX<...&U...GD..Mn.y&. [<(tk.....%B.b;./..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5 X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xl@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/l\.cDB0.'.Y...r.[.....vM...o.=....zK..r.. I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\4CA77D36767B6202D4786BF3D1EC5242	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	480
Entropy (8bit):	2.9511345389404173
Encrypted:	false
SSDEEP:	6:kKXk3R+3N2veVtcE+IIn9clIFG5lOKXk3R+3N2veVtcE+IIn9clIFG5l1:LFZIn97G7NFZIn97G71
MD5:	BD8F0E136D75C5D702C39C2FD0295C4C
SHA1:	F3E2D34CDEF4EA83F1ED45A4BCA357CE10651358
SHA-256:	0950437501773900F7F74B148D3D581D836E0D7B155B28521347DF0D6D0ABA09
SHA-512:	EACED672CCB42EDE271BAD7D71709813EA909D273C20F8F37FB07CC84ED5E8AB39EE2C20BA9179E2EACFA778F6A64521D10089E7233B5CEA0C736957E9944E 60
Malicious:	false
Reputation:	low
Preview:	p..... ....T.....O....(..... ....9t.....(.....h.t.t.p.:././.s.s.l...t.r.u.s.t.w.a.v.e...c.o.m./.i.s.s.u.e.r.s./.S.T.C.A...c.r.t..."..3.b.c.-.5.b.8.1.c.4.f.e.b.c. 5.c.0."...p..... ....T.....O....(..... ....9t.....(.....h.t.t.p.:././.s.s.l...t.r.u.s.t.w.a.v.e...c.o.m./.i.s.s.u.e.r.s./.S.T.C.A...c.r.t..."..3.b.c.-.5.b.8.1.c. 4.f.e.b.c.5.c.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.0847546854849544
Encrypted:	false
SSDEEP:	6:kKzlXbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:pe3kPlE99SNxAhUeo+aKt
MD5:	4D80D25A5A6F20C007A00C4E88AA1C66
SHA1:	4F2D388734BE4B5DE0D763E4B288A684927F839B
SHA-256:	B77F6B55403DE7B5C1914F5A3A4D4790153FCBA7B998ED04ECDE35729501E45B
SHA-512:	50BD8DE0F65E8461E817F66CECC04F77062DB60D52E5AC95FE4816E26CDA4B482DC5ED24F6E15161650EEEE8514B2DBFB78CE13D5E7649BFDED4C15E7FD41 53

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Malicious:	false
Reputation:	low
Preview:	p..... .....+.x*....(..... .....&.....h.t.t.p.:./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\42c6b281-1f5f-4f5d-ab46-168c00e0294e.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):	355904
Entropy (8bit):	6.015625851039051
Encrypted:	false
SSDEEP:	6144:IflkhsXNZswa2bn8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBeo:lju2bUxzurRDn9nfNxF4ijZVtilBeo
MD5:	A4532C32FFCF0E84E2D12F8863A16075
SHA1:	3D156747FCA5D69303C7CBA0C33B33DCD1451CEB
SHA-256:	1AC641FC0178963DE622E75B4105302EE8CA5A152334BC3B5D3CF1527BAB5D26
SHA-512:	CC217D0EAC550A49BFF4D7A9B4F9B0BE51082EF29527CD3EF182626393AA1DDC04775FE837F55AE6048E3E7DFB6F51B3B6B564C2756D645C9633F467622ECD9 A
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":1.614318145316447e+12,"network":1.614285746e+12,"ticks":110260792.0,"uncertainty":2758566.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13258791742133

C:\Users\user\AppData\Local\Google\Chrome\User Data\4f893992-532e-4b71-8224-35f888e3c764.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):	355905
Entropy (8bit):	6.015626121837182
Encrypted:	false
SSDEEP:	6144:IflkhsXNZswa2bn8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBeo:lju2bUxzurRDn9nfNxF4ijZVtilBeo
MD5:	702E0DEC952B85BDE6CC7C781EB71FAB
SHA1:	664DC96F3F1798FB2E04070D73AB6448966636F6
SHA-256:	61E191CAC5EC313AD2A7BAB0C110ECC9BFE6A8E90B36D852991A81D221BD7AEF
SHA-512:	25757966B48ED58F053ADF97878C1CC241ACB1B81B1E0115D0D75EC406D2A2276B58643BE0C9489A697ADE3F67F3645D05E5AAB08369C0CB88234A739BF4A19
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":1.614318145316447e+12,"network":1.614285746e+12,"ticks":110260792.0,"uncertainty":2758566.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075265799"},"policy":{"last_statistics_update":"13258791742133

C:\Users\user\AppData\Local\Google\Chrome\User Data\9c6d5fe8-d9a0-4de8-b00f-e6d32721552d.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):	359473
Entropy (8bit):	6.028188717015475
Encrypted:	false
SSDEEP:	6144:iflkhsXNZswa2bn8Acx6ZaurE5/EDnJpAl9SeefNqWF4iVx/9LPeq/1LHm/dBeo:iju2bUxzurRDn9nfNxF4ijZVtilBeo
MD5:	5289E6C763771956AF759AA6244B67A3
SHA1:	654405E672D5DC4ED8F3456F687B9E863F202E0A
SHA-256:	13F226AE71A9D3825A5F90617C344C3B6C0FBC1E74CCA152D07C1101EE1198D4
SHA-512:	586A169C7C86CF1B902D79792E28984D012764F4170EE67CBA0850CA92C5437611A7030BF0F2D9CDAA522224790E7826CA9EB6D021FDF75A19805CE413DEB4A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\9c6d5fe8-d9a0-4de8-b00f-e6d32721552d.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":1.614318145316447e+12,"network":1.614285746e+12,"ticks":110260792.0,"uncertainty":2758566.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABUPWY4cSyAQZRX3j8/SLmMAAAAAAIAAAAAABBmAAAAAQAAIAAAACC7lwCjByxIY/Ds1S6cdCxJW6iSr1QfjoKlVKoVEQ4EAAAAAA6AAAAAAgAAIAAAAD9PMfiGkWkdrfU+zeMpOLPS1eDxLpcgjYP2R/ndeCNxMAAAAK+RpovfP61NtB5nOpQgPMjPTyt2T1WPeru9i3yP05zNVEj0uCRDWfONruG9ricX1kAAAADB9KtQ9KY2z38GdfaF7dW2ZLcAMHOX2oEKBg8ZJG9lsuMexxChB4M8HFpyb0Bpr6axpi+zmMIXt76noTOxFzKN"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245950075217487"},"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:FkXYDu6cR9iTXYDu6cR9iTXYDu6cR9n:+Y66cR4TXY66cR4TXY66cR9
MD5:	569FA64ACAA310B1DE1A6250CC7356B0
SHA1:	14251450C245F8612958BF94779E8B72AE6D6213
SHA-256:	AEE20ADEBF2D35EB8A39BE2DC391B0E5966EFCB4AFDC971BB3A18115C929F563
SHA-512:	850914A053EF541046B29260266C17FEFF2466A87784394F9AB3B565D2EA1E656F61F02BDB78F9F9676E90365F837F3709BCC0856B3B844256848F477250E0C7
Malicious:	false
Reputation:	low
Preview:	sdPC.....................8...?E."..N_.sdPC.....................8...?E."..N_.sdPC.....................8...?E."..N_.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0edec198-978c-4e4f-9e6a-e581d064482a.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\20d03fbf-66f1-4450-9a8a-8c02511167cf.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):	5612
Entropy (8bit):	5.185521966662627
Encrypted:	false
SSDEEP:	96:nxBsC4QodCbSVLIk0JCKL8Sk411+bOTQVuwn:nxp4nCbSJC4KLk4c
MD5:	DB6D1CB79B743DB6CE5D8E5E71B7563C
SHA1:	DAFDD651213E3913E9C3BEF14E65EFA4D7718CCD
SHA-256:	AF88E62BD97F28EDF514461E43D1C29EE46E67DBF826035B5F5C160E579E02C4
SHA-512:	F84E5ED07AB3FDEA5A9B3E915C7C58E104654A4616A2F30A379A825CF8910658BE7C57E9A3A8C9A58DE70C8E7F7D25ABCA8039160501A44EB6E04AD9DAEFA2 43
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13258791742428435","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3796488d-6b3e-4709-9f80-9ecff221bc78.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3796488d-6b3e-4709-9f80-9ecff221bc78.tmp	
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5948
Entropy (8bit):	5.195019785011712
Encrypted:	false
SSDEEP:	96:nxj6C4QodCbSVLIk0JCKL88k4gDk4116bOTQVuwn:nxh4nCbSJC4Ktk4yk4g
MD5:	B8E195D7F2F8443003C8142EFAB21637
SHA1:	9F1CCC1226BAB4400F89F9B07D29D92C1CAD56FA
SHA-256:	A46A448F4CC2353464F53A9871641899C59CE0AFB5FF934686556CB07B01B6FA
SHA-512:	BA085A22E114CF31CC94260C45E394306EEDB6775BF3196815386E1379551DEED0DDAC9088803536006D7F6D27D3A285BB1FBC9B57607A1EEF01E563556DCA9
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13258791742428435","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\44a2bab6-bbad-4d92-b69d-75e5576372b1.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):	1539
Entropy (8bit):	5.5957411851683245
Encrypted:	false
SSDEEP:	48:YSeUOeieUw6UUhsUhUYOSDKUeAUeC/DwUtUeh:leUOeieU5UUOUhUYOSDKUlUH/sUtUc
MD5:	9251993F16D4B10EF97F1AABD5055765
SHA1:	17BD986761F6DE17EFA25906439EEF457D74C1ED
SHA-256:	57C462B6AF55D1CCC4A3ABC4972B4D3B38CB143F9E4EEF1A8AF61CB324AEC693
SHA-512:	A430811A73E9C76970875188DE94B14745CC1E777B324A013D9FCAB13B6B6DF2E540854EBF22D14507F8FF2191EC1A702EC00BAA246A86401FC122506072F686
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1625204579.055896,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614318179.055901},{"expiry":1645854147.095015,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614318147.09502},{"expiry":1633013028.822833,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601477028.822838},{"expiry":1630086179.679578,"host":"UDjGJndGVqgg3BowfS8jfsQuAhj6k4rmKzYJoI3cvaE=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614318179.679583},{"expiry":1625204547.940113,"host":"fJjUrPqhktMfiTHJX3Q0pJi/P12Q72DBgzzJqjlNC4o=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614318147.940117},{"expiry":1633013028.743725,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_obse

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4f69affb-682e-471f-818c-e26c49168cec.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16763
Entropy (8bit):	5.578521263012893
Encrypted:	false
SSDEEP:	384:pQStfLlzaXl1kXqKf/pUZNCgVLH2HfD0rUo+044C:PLlcl1kXqKf/pUZNCgVLH2HfYrUp0zC
MD5:	942ED4D7D8859F1A63749E2AB80C145D
SHA1:	B50FB7D01D8615CF48C5877354627027CE5954BC
SHA-256:	797C6369A1BF4D46EFE230A009C9E54392CEF0B98E4DDC16F19374306832789E
SHA-512:	0778460B8D8C329716E15038760A3BF8E39957C66EBC6DE29CC5B893686B6EA07CDB07C6DB7DB7A344AC274F91D5825B2D08FEA3551E8CE41A10533B6176800
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":"13258791742207240","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\6205782d-01aa-4254-9579-56dda41950ef.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6205782d-01aa-4254-9579-56dda41950ef.tmp	
Size (bytes):	4215
Entropy (8bit):	5.59378401769018
Encrypted:	false
SSDEEP:	96:a7UhUgUfUBeUOneieUBUUlU6UAUvUbUADKU0cUBuU8UlPUOApUNlU/UH/sUgjgU7:a7UhUgUfUBeUOKUBUUlU6UAUvUbUADKc
MD5:	9F35495CA40A8826535124E3328C16BB
SHA1:	B471F1C6A3C15C164962594119A3EFC1F879D0AD
SHA-256:	1958175C80FE85DDD6EA9D9552F2C311A6058A50541F3E0801ED25EB2F2C1AB5
SHA-512:	36CA5274D72C51FC78778F791BC6336DD94342BE21FB4B8309F08244C1CBB9662121C5C4E790891667836DA2286224160A4AAD2C10ECA7F4C6EB23128405239F
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1645854196.784695,"host":"B33dNWuWc3elp/rqxbaViYp8VufHqjSms9l6Z0xI7lk=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614318196.784699},{"expiry":1645854190.654243,"host":"DZojSgKWXqymKhdrkb0V9PlsJoovVUGWsPWVArl/V48=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614318190.654247},{"expiry":1630098186.97321,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1614318186.973214},{"expiry":1645854191.486396,"host":"K3wA0vSiWGfORMgxvNmP2zylcmDMsG1B1uS7fKBX/Z0=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1614318191.486398},{"expiry":1625204579.055896,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614318179.055901},{"expiry":1645854205.502491,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\73d613a0-1d9e-4787-b174-f6001c9eb0aa.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):	4968
Entropy (8bit):	4.96813346427016
Encrypted:	false
SSDEEP:	48:Yc4kPklqL2cBqAJRqTlYclQuoTw0J81aPc8C1Nfct/9BhUJo3KhmeSnpSk4Jb5G7:nxBoG4pSV7Ik0JCKL8Sk411+bOTQVuwn
MD5:	39A78A4CA4429A7EFD332691C2511CC3
SHA1:	2889D469B6E4D76383845DC34E4541BEAD93E296
SHA-256:	17A6964C7BC8DE8C534B8E242ED039136E242ED27278C5A886378821F5D4A6BB
SHA-512:	5BF7069B34373C9485C93F5C263747F283D7D1B8AE55F71A364F3DE71181BD84FFEB14A79BB1B5CC1F9DB976F50642D89FED5B8EEB762F9F7293B1B7CAD9707
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13258791742428435","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","1538886"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\79d46b30-2361-4a59-91f6-b84123e72ffd.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):	4383
Entropy (8bit):	5.595741829703213
Encrypted:	false
SSDEEP:	96:a7UhU+UKkUBeUOneieUcNZUOUUlU6UAUvUbUADKU0cUBuU8UlPUOApUNlU/UH/sd:a7UhU+UhUBeUOKUIZUOUUlU6UAUvUbUU
MD5:	80D298A1027C6EAF1E09CF9061E820B1
SHA1:	47223694A664FB4B0717A2728BE245BB77EC90FA
SHA-256:	8932519506EE610496B82551D8A6565D2F38F930E0800F411D926B2C8615EA08
SHA-512:	5EC6046BB8A39AD5943355E16011E4BFC79BC714B155DE44D3C91B142A3654E04CCFE89673961AE17990DF69A7B7005EFC9F4E7955C98FDF877B9E21D874C01
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1645854196.784695,"host":"B33dNWuWc3elp/rqxbaViYp8VufHqjSms9l6Z0xI7lk=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614318196.784699},{"expiry":1645854190.654243,"host":"DZojSgKWXqymKhdrkb0V9PlsJoovVUGWsPWVArl/V48=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614318190.654247},{"expiry":1630098268.427291,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1614318268.427295},{"expiry":1645854191.486396,"host":"K3wA0vSiWGfORMgxvNmP2zylcmDMsG1B1uS7fKBX/Z0=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1614318191.486398},{"expiry":1625204579.055896,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1614318179.055901},{"expiry":1645854205.502491,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_ob

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8137b773-227f-4420-abbb-1f7e94c3355b.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):	5830
Entropy (8bit):	5.194064446141401

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8137b773-227f-4420-abbb-1f7e94c3355b.tmp	
Encrypted:	false
SSDEEP:	96:nxB1C4QodCbSVLIk0JCKL8EkJ6dk411IbOTQVuwn:nxW4nCbSJC4K1kJik4q
MD5:	5E7215D62E0FF8ED1384151CCA0CCAE6
SHA1:	0AD73A42A440AFF642F8ECC8870B1E83A701D403
SHA-256:	F01F8BF362BDBBE6013734EF485121CD44A32CB17896C35A8DCA70F774C0D7E3
SHA-512:	4FBC985146A64D0C7F88886917D88657D65E8C80139A13028D9A9C5DEE0D567C50C3CED6D7369F64DA0A2FA7B7181A32D8DDD517FA3E6ADB02FAEEC2C5E30 8
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13258791742428435","alternate_error_pages":{"backup":true},"announcement_notification_ser vice_first_run_time":"13245950583260338","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"has_seen_welcom e_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":1 0,"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","1538886"],"daily_received_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8b83f8ec-2aab-43ab-a21b-9528ca2a9204.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22614
Entropy (8bit):	5.535875993657626
Encrypted:	false
SSDEEP:	384:pQSteLlzaXl1kXqKf/pUZNCgVLH2HfD0rUxHGUnTko2R04d:uLlcl1kXqKf/pUZNCgVLH2HfYrUlGUnm
MD5:	A69906464CBFC7BAB4010B49C8B5093D
SHA1:	9F63C2DB1E5E8BEA536953C7E5A0907668D3FE86
SHA-256:	E63FEF844B075B615BCAE4342E5B675B5ED9DBC5532EAA94401C016E8C0C28EB
SHA-512:	0A6E14EC5D54D3E2D429E2F6B94FD956AD4DACB2E4B55BAD83EBDB5034AFA5A0B78046A9D907F2861EEFE811032863CD0054975907E2813911CA04F7631816D E
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.cpu","system.memory","system.network"],"manifest_permissions":[]},"app_launcher_ordinal":"t","commands":{},"content_settings":[],"creation_flags":1,"events": [],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":[],"incognito_preferences":{},"install_time":"13258791742207240","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVG ijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9222b070-7287-4cdd-bb70-e35b6a9fe87f.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	2693
Entropy (8bit):	4.871599185186076
Encrypted:	false
SSDEEP:	48:YXs2MHRzsoMHT5s0MHyKsTMHksrDys4Csb7synWsQItFsym6zs6zMHWLsZMH5YhV:+GDGTHGmGHDW1/nOIbmOGlGGhVD
MD5:	829D5654ADF098AD43036E24C47F2A94
SHA1:	506C8BA397509BA0357787950C538C1879047DF3
SHA-256:	4D0B852D18FCA5C1A712904CF6DB3811FB905E86D8A7508A2D42F9C8D68E2211
SHA-512:	D9B18E6B0AD1E8E4BECF9E84BBE30D64730CFEC2CBEAF96D5DF52E28B907B03EADF22F020FBE0A56D137A52F4F09798031BC6CA026CFA8A979A608B3445DB CAA
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600883925","port":443,"protocol_str":"quic"}],"isolation": [],"network_stats":{"srtt":40156},"server":"https://www.googleapis.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"1324854 2628822803","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":30856},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{ "advertised_versions":[],"expiration":"13248542600893104","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":25300},"server":"https://clients2.goog leusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248542600872791","port":443,"protocol_str":"quic"}],"isolation": [],"network_stats":{"srtt":34789},"server":"https://clients2.google.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"exp

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9c4c784c-2d21-49c4-8f5e-083d854d27a3.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):	22613
Entropy (8bit):	5.5358219155557675
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9c4c784c-2d21-49c4-8f5e-083d854d27a3.tmp	
SSDEEP:	384:pQSteLlzaXl1kXqKf/pUZNCgVLH2HfD0rUxHGfnTk+R041:uLlcl1kXqKf/pUZNCgVLH2HfYrUlGfnh
MD5:	D2B8A8F731E73AD0A72F674045CDCE43
SHA1:	6C22805BA296577F2687018B24168470624805F6
SHA-256:	46C3F90E175095EA9FE8587D1487B025208023908444FA492E71301A2BCBA631
SHA-512:	A473F9742EDDC2355A9C0C04A7C77616CE730364CBB89507302E9518835FD8A178EFF4B1C14523B38DC952CDD5B5FD4D34A4B5FF2CEE7199E67426459C00AB6
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":"13258791742207240","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/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	333
Entropy (8bit):	5.20085964792948
Encrypted:	false
SSDEEP:	6:mN23iN+q2P923iKKdK9RXXTZIFUtpe2MGN2WZmwPe2MGN9VkwO923iKKdK9RXX5d:C+v45Kk7XT2FUtpcXW/PciV5L5Kk7XVJ
MD5:	DE55CED5C12AF86E9D3315B53A6DD977
SHA1:	985AC1489EA012EBD0E45E43284E1688428AF3F2
SHA-256:	67853A108D23E47563016C7CA737BECA2BC58A526F96F455678438729790C7A7
SHA-512:	02193B2BBBF51F7AC5C74F84F05C1B15C0140EB3B29EEAB4E5B0AAD9998BDE8EDD63B6D5CCA233433DB72BC72EB155619DB9FFD6D0557338C9212D3C84D9F2C
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:42:38.955 9ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/02/25-21:42:38.958 9ec Recovering log #3.2021/02/25-21:42:38.958 9ec 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):	317
Entropy (8bit):	5.226904140308762
Encrypted:	false
SSDEEP:	6:mN234+q2P923iKKdKyDZIFUtpe232ZZmwPe2UnVkwO923iKKdKyJLJ:dv45Kk02FUtpy/PA5L5KkWJ
MD5:	B68581C18C4294793343 16B22ECFDF11
SHA1:	4985C19D233894BE5A712BA070450ADD0CB184FD
SHA-256:	4159605DF2BB1F179E3390F015102264AF42CA57C91B2C0CFBF5FBCCCAE4D29C
SHA-512:	AFF5AF1DA98788EC82C002FFCD99906B834DEA667F12372297956D21D50764BCC9C4923CFA7682BFAAFA3386CC120890ED8ECCF96E6C7EC38235F4A65A39697
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:42:38.947 608 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/02/25-21:42:38.949 608 Recovering log #3.2021/02/25-21:42:38.950 608 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\060571bc15e680b3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	259
Entropy (8bit):	5.820277521457073
Encrypted:	false
SSDEEP:	6:m+nYGL+MORm/b8fK0WVRxjIR/siLgITG2WqfhcDK6t:LDpQS9jSsKqqm1
MD5:	4F147DF73C491996E85BD16483258212
SHA1:	8C3289C46BBB052FBF43452A6D29F1C745ED43E5
SHA-256:	B5CD8E5DC34985098414D0270BE6CBC74F24BE2AC73B239F95649C2EA6D4D620
SHA-512:	9978A40B11FCA5260F71F929E32DBE2FE987945D705565B2129F3CA8E92B361BA87F4F2E5304FF072AF2A9327D115EDE89B6A980CC53D4118BF0A7F82B51E32A
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\060571bc15e680b3_0	
Reputation:	low
Preview:	0\r..m.....6#Be...._keyhttps://www.google-analytics.com/gtm/js?id=GTM-PBLF7VJ&t=gtag_UA_87708648_1&cid=1304408799.1614318149 .https://clickup.com/L./.../.. .....+.....MH.*x.k....;.2..[.P.1AY..l-.x.X.A..Eo.....K^.H.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\099b5e3dfcf45bcf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.543917491712945
Encrypted:	false
SSDEEP:	6:m/llVYfDMtvpURXAITgnVlom1tg+/nyX+y2xY3zrN0llhK6t:sllIQtv6RwITmym15/yX+y2Sjh0T
MD5:	6F6FBB0D40C816A621E815FE792C6AA6
SHA1:	FA3E6FF39B3A57086F9D6D145E6E33D690AE504A
SHA-256:	AFDA9AE1F88F22782ADECE8B17D800BF5266EA7C911983F9032A89075D1ADED4
SHA-512:	385ACD73859222FAABC592CC7E6C9AA45CE502CCB14F898A2569C3D06854D742437A9DC5341228B648168C8966A7CBEC668194358D54BAF871209C95CF3D2CF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X...*....._keyhttps://js.hs-analytics.net/analytics/1614285600000/6613321.js .https://clickup.com/ .'.../.....UB@.....c.n.i.,....p>...;...A..Eo.....o... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0cf69c09debb1d32_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.324931235934071
Encrypted:	false
SSDEEP:	6:mqV4EYjQYLbJAlYLM1tg1nLIOUrrP50hK6t:SzQYZwY41enLIOUe7
MD5:	80ABA149D5F32744C4153F6EC1A1C72F
SHA1:	E80F14567F94C4705E305310B7215925C3BC0786
SHA-256:	0C8C59EED0077BB07E6D0748C3D346CD57E2D89E180D781460C99C1FD6E5096F
SHA-512:	50AB786EC5C80AB7B1ED6650E48BA1577E7214D40775265CFAE7EBF1F33B0FDAAFE479ED8CC4F84CB7A8E903C7ADD7A3055CECACABE6BAD391E79CC9C3E1 AB7B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K.....0....._keyhttps://js.hscollectedforms.net/collectedforms.js .https://clickup.com/..%.../.....CK6i/m....d....u.P|IY.j...}...(.A..Eo.....Cs.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1408a718ac481827_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.513733703694862
Encrypted:	false
SSDEEP:	3:m+le/mlt6OA8RzYIXTzgJST7MsRlNRP9LYC9//lHCTlaBZed/9S0G5mkom5mJYtB:mgY+7bRXV/Fguedgdmkom4JCK6t
MD5:	E73C6B7D46BEF111EA5DB561C5E126D6
SHA1:	260479641F37E2D5F73F832E372BF9727D649BF0
SHA-256:	318CD700B1CAE89BA534BC20E4CC2FECAAE08578EA498796B79D6636755B7354
SHA-512:	01F1FD4568FF5D655A56DD3913EC000E17236070A99CACCFD8F86F8E6A148623D73DD5DA6B3797A8E5ACD9AD60D0FD15D7F8DD3EB581AAC2EEF67250BE713 67
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N....q....._keyhttps://m.servedby-buysellads.com/monetization.it.js .https://clickup.com/t.*.../....._.....dG.+.X).Zp8.....z...Q.3.Z....A..Eo.....E{^.....A..E o.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1dfebe463549e1f9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	213
Entropy (8bit):	5.5367170732763915

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1dfebe463549e1f9_0	
Encrypted:	false
SSDEEP:	6:molYmymJMBKTXK3FsUug5l8d99M1k4TnK6t:gKTXKFsUOVOhp
MD5:	1119D0B6ACB41218E990124070652076
SHA1:	BC6AE283579CD1630F15FC7EDD052B7153669414
SHA-256:	30F0B421A69B57AB757C7E7E070E548B891F1B7497DFD11D60B14504075E6992
SHA-512:	557D6F48F8117B36F4D456CD108C7D0F45350C352AF9A13284C49A7E4F0D9711306F975D36414781D4F0DCE42DAFFDFB300CBC635729375D4BB14166227D7BE4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://ob.cheqzone.com/clicktrue_invocation.js?id=3839 .https://clickup.com/..+.../.....W.....nNF..d....A...c.}=.....A..Eo.....<..x.....A. .Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\21cda92b5a14b9f1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.617057072837059
Encrypted:	false
SSDEEP:	3:m+lfrLA8RzYKceMGOQVLQOIRpXvWZQwP9LLU/Kt/lHCvlX4IL1DN0yIg4mfq5pK+:mYRYKIOIPDUougvlXh5p31fqvK6t
MD5:	7D5B5E9FF8546841D3A69CC138A14468
SHA1:	427B24197BF28B17BA3EDF5914B5943785A1C4D6
SHA-256:	CBA5AD4E9A6ADB389D3BC8A7AB333165D4410E09E12D9E90EC7B8FF3A38EDA4D
SHA-512:	2F49DD7DE58F3AB676159348B168CFBCFF42E87C2D7258B987AA93944D6DA57711EFB101D2EA0C0451DCBC59E6FA1C621084F283B1743045F4207649B62F2D6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X....QR....._keyhttps://doc.clickup.com/runtime-es2015.1e4c4eb7935977bacb85.js .https://clickup.com/.N8.../.....P.....l...T.....{..h.....&...,&..A..Eo.....<..*.... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\293e5233d64a0a25_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.396772508868376
Encrypted:	false
SSDEEP:	6:mulXYAWQf257UCsugDA//98xb5ljlZK6t:tHe54CFelZT
MD5:	0CD74B0ECC8997A0A0390FC21F24A1C0
SHA1:	742AB8EB70CE657074C0F3A3194856128CE7DC51
SHA-256:	7B514C707F733C841A4C224034D0C908DF3B449DF3651D8ECD40EBFC8EDC5B7C
SHA-512:	C73614129030CAAFC602EAC2CBD24A066C0BB071C8116B304B1690493C69333B4B0066A6FF8E7255D713408A484CA1D6010DF8211AC2F5DCE86391F5E3EE6D4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H...e....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://clickup.com/...../.....T.y.*.E....H.....E....J.5..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\302386b6e7db3ed0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	212
Entropy (8bit):	5.65953441465977
Encrypted:	false
SSDEEP:	6:mdl/VYGLSmXZCLRQID3/ugUS6Tx4l57bb/VlDK6t:E/11e3qvel5H5r
MD5:	AF638A0A400A3E67197DC66CF3264C1A
SHA1:	17285188615D112C02324C38CA4AFB692A86498B
SHA-256:	FABB21DD5AB97213B484883D859120045E72D9DC29660C4C439AB2F994EEA270
SHA-512:	1BAF7289A6D02D3933EAE75B9B287EFB2D5BCA13D67863A350719F6A2C99C57B953CD9CDB30E2E735A17EFF76E0FE242601405A75A372EFBA31E55B56CB39C D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...C..R...._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-W9LSCFD .https://clickup.com/.u.../.....b?..>...:e+.....-.M..*.+qr..&.A..Eo.....vN{ .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\31aa3190c5efd805_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	5.588865488211218
Encrypted:	false
SSDEEP:	6:mnYET08NgDQOQo8XzJTKsngKiqnVZ/yARARK6t:ug8NkQo8FOsHBL60Ar
MD5:	5407CE3B30B55EED55E5A61928CE4225
SHA1:	FEB736A6FEF5877E958236E75DCB7C163851EFF0
SHA-256:	A9A4F5DD3C3755667F1D4F210C3F71C950011D7CABAB0D1A37B1010845D06341
SHA-512:	17BB54D65E70DB2BA37FDFF951EA76380FD8BE6F54923E63A7268EDCA8F6BCC8A7ACF983519C2840F86A27473D5654E040C6B8A47D65D9820895B543012BA0C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I...."`....._keyhttps://cdnjs.cloudflare.com/ajax/libs/bowser/1.9.4/bowser.min.js .https://pale-small-origami.glitch.me/t.../.....I.$n...5>..T.>{W.S.Qg.K..3Z.. ..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\372528a3f8712b40_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.519305017116318
Encrypted:	false
SSDEEP:	3:m+lxYtla8RzYzYXXAJnBB6TxV+pcRP9LPL/Kl//lHCXltFi/9jRBYa576P5m8q5Z:msYnYMHAJn36TKpqotgXIlbk4NnK6t
MD5:	72F819E7C17B677C1ABE14692B7663EC
SHA1:	FCDE25648477DA7B800C59F2C96BB1AFEB87E2E9
SHA-256:	57B174B04049BD0F3EAC00C176D77999D15045C8610CACEA7D33B2A8FCFA8C74
SHA-512:	2C200BFBB8587FE37EAF7F1EE9159E4CED2AF18362D3328CCB9D2908CF3DDE7D25CAFA717566225DF7A0CA7F15A03E9C07B82B8043766D31DD181F79E368DF 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...5.|....._keyhttps://script.hotjar.com/modules.dbbd0f16dca02537aef0.js .https://clickup.com/.a'.../.....*. ..`. $p..A.....$.e...G.N..A..Eo....."/..... A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3783441f7181a3e9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	691
Entropy (8bit):	5.76303424351716
Encrypted:	false
SSDEEP:	12:1qrE31zIA6W1Smoux2pHgyyyJ3CMxzDPdXSNL8mz4oMGxa1DEChE7ED1zGA:WElz9jguyAyyASuD414oza1DEChE7EB
MD5:	1895462BD82DF222D28A06530EFC7AEF
SHA1:	D2871C01E342A5E08C987F1941F6FBD6DDA8A832
SHA-256:	F4F73BF06F35C82D50976C16C0477196C59839950024E116B71BFDBDD945C86B
SHA-512:	2109BAB5208645EF7E612F5B1D493CB4820FC706F8CF0337841F1EE585B0F9B80230C6615D542645BCC9CAFF38FD497D82A5ED6110AB8039B56FBF2D3D2505C
Malicious:	false
Reputation:	low
Preview:	0\r..m...../...F,.U...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/617640813/?random=1614318166627&cv=9&fst=1614318166627&nu m=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-480&u_java=false&u_nplug=1& u_nmime=2&gtm=2oa2h0&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fclickup.com%2F%3Futm_source%3Dclickup%26utm_med ium%3Ddoc%26utm_campaign%3D8666708&tiba=ClickUp%E2%84%A2%20%7C%20One%20app%20to%20replace%20them%20all&hn=www.googleadservices.com &async=1&rfmt=3&fmt=4 .https://clickup.com/..2.../.....@....."..?.....G.j.f7...F..&dG.o|.....A..Eo.....n.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\38aa030603a13736_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.602647828696006
Encrypted:	false
SSDEEP:	6:mexJPYOXdTAqxAXLXXYUwVUngfOYu3HcH01K4UbK6t:pFXBuXKUkHis
MD5:	0003BF4C49C9EC8128BA591FCABEEC1F
SHA1:	5A50BFF62A42CF94761C108F7A4248998CE890B9

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\38aa030603a13736_0	
SHA-256:	D508C2FEEA75B07C124BE7C011F3DB5920E9CD1D9005F6A05105852AD12F5A98
SHA-512:	222C71F9AF048FB30A97BCCBE0D7CA404961CD89EAACABAC39ECEFC118BC6ABFA1B7E3433D81D7C44416E4F3A3FD8A0C6D9B984EEB46BC5072EAC444BC5A 4C47
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M.....l*...._keyhttps://js.intercomcdn.com/frame-modern.17b2a5c1.js .https://clickup.com/...../.....9..G.].z..U.j.8v...;..^....Q..A..Eo.....$..#.....A..Eo... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\396648a11d6cfbf5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4033
Entropy (8bit):	5.792922171531528
Encrypted:	false
SSDEEP:	48:AUDh1bN0Sw9ZrRm1QGk2+c3zyQBqMylLQMy4wtjZ1wF32SOtsIOCQHP5I6vl4r2I:v9RPw93tf2+c3z9AtlLs139tsrdl/N
MD5:	F5903ED51F3496D93AF52CCDAB897BCD
SHA1:	5553903422ED66A72DA4AC3EBA96A79DB6CC853C
SHA-256:	14FAA9A970839D7B93CE11666366F1777DEC32AB7AD6F4E12DB9021526F4A714
SHA-512:	1827249C977B0648EF8096C451A1AE8675C384F39B3FFBA91B515E0524F6B921ADB57A3F3C08C5F715A74FBA3069D7AD8DFE83A52EF3DEA39E262021432037BC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....=..... ...._keyhttps://obs.cheqzone.com/ct?id=3839&url=https%3A%2F%2Fclickup.com%2F%3Futm_source%3Dclickup%26utm_medium%3Ddoc%2 6utm_campaign%3D8666708&sf=0&tpi=&ch=&tsf=0&tsfmi=&tsfu=&cb=1614318167789&hl=1&op=0&ag=3098761112&rand=5489551918186810150871986796 7 62127516590915072591182781072691758996 0&fs=1280x913&fst=1280x913&np=win32&nv=google%20inc.&ref=&ss=1280x1024&nc=0&at=&di=W1siZWYiL DEwMV0sWyJjYiIsIjAsMCwwLDAsMiwwLDAsMCwwLDMsMSwwLDAsNCwwLDAsMCwwLDAsMCwwLDAsMCwwLDEsMCwxLDAsMCwwLDAsMCw wLDAsMCwwLDAsMCwwLDEsMCwwLDAsMCwwLDEsMSwwLDAsNSwwLDEsMCwwLDAsMCwwLDAsMSwwLDAsMCwxIl0sWy0xLCItIl0sWy0yLCIxOCx2MElrMkt2VmZ BaG1JM1dHS2lzVVFUbzhhYUdHdlVUeE9OK2hrVGpZbkdpaTJXb0lsSzFLalJHTVVTQlFzZ1JRU0JwU3hzblpsenpsdi82emt6WjNkWVFmMzhsMnV2bVowdDdKIl0sWy0zL CJbXCJpbnRlcm5hbC1uYWNsLXBsdWdpblwiXSJdLFstNCwiLSJdLFstNSwiLSJdLFstNiwie1wid1wiOltcImRhdGFMYXllclwiLFwibG9hZENTU1wiLFwibXV0aW55V3B Kc29ucFwiLFwic2V0SW1tZWRpYXRlXCIsXCJjbGVhcklltbWVkaWF0ZVwiLFwiMmYxYWNjNmMzYTYwNmIwODJlNWVlZjVlNTQ0MTRmZmJcIixcI

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\399055e3fa3b678b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.586850486750155
Encrypted:	false
SSDEEP:	3:m+lL6tla8RzYKceMGOQVLqUf+XHB3eVTxBlSFvDP9LMlH/lHCbeMca/T07vRmF7w:mMaXYKiUwBeVRIraHgbeMc5AFUnK6t
MD5:	C55FA7A05EF37FEE23A6BDFCBA1A1F1D
SHA1:	D7994E7ABA78B1D1D16F531759B1768A66CAE7E0
SHA-256:	0AEAB8062EFEE13A163393390932EC092E602D2BB050C5234567FE03C680CCD0
SHA-512:	DB6105E8299855D27B9958DF8F6C9FB25D6DDF153F9675D2D35FBD465E38B8131B029741B17ACF8E2D8CD628FE221E07C4477106A48A882C761D81DB2899C97
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....._keyhttps://doc.clickup.com/4-es2015.e012bd08670670cdbbee.js .https://clickup.com/..K.../.....G...]..4.n.v...&..,.]H.)C5.P...A..Eo..... A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4071488f0118ba2c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.444239756573873
Encrypted:	false
SSDEEP:	3:m+ljHlC8RzYzYtMHeE/yJkP9LKZT//lHCskltl3ceU3ftMMmsRyl//lpK5kt:mklPYM++E/yJ4slgsscVMnwwK6t
MD5:	1CCE9B7F2DB8924BC33A6E6313EE6582
SHA1:	E5957644ECFB35D87B2256338D9D5BAE477825DD
SHA-256:	84699D22E982262C30746F94DB7DAC95BC66CC7E5973D068EA5B8A7D6C118E58
SHA-512:	B8D97B7E609414095C00D44305886B004340FC530104A2FAC9845E866EA794C28C4302959B630F69C9E67E9A4779ADDB340CC706416BE5994D588F5FB3253DD2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K...H.3I...._keyhttps://scripts.attributionapp.com/attribution.js .https://clickup.com/I$..../.....)M..D=.^.;.v.W....O....U.....A..Eo.....4.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\426f0f97b11e76c3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.490269690019324
Encrypted:	false
SSDEEP:	3:m+l5PZ/LA8RzYKceMGOQVLvlkrVq1LoP9LMShLH/lHCTltOJdnT0rE+Vm5mB//pD:m+B/VYKSrAOqAgTXOTTKY4B/hK6t
MD5:	4F93A0C8F0EC2FEC708740ADCFC154DD
SHA1:	EE0939C85462F8A652F7047F3AACA6DC6CC9DF0E
SHA-256:	E33ACFA538EE9589397EC2D56C27EA5A7B773ED8933C80FE42CD9C5B8C0532C3
SHA-512:	BCF30C36302E5B75DC8364FAC27E4D488E7B71519AEE821C1CD88BC10C1B261E18A3AF653582E9BF2CB6FB4D71942A962CEE221A48FE49A330CCBC9768B56C 45
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....._keyhttps://doc.clickup.com/5-es2015.5bc3006d8825d1f0c7fe.js .https://clickup.com/O.B.../.....OD.,.Y..l8i.=.1.5~.....n.0...A..Eo.....p).....A..E o.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4303153a6c225d91_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	194
Entropy (8bit):	5.420195767966578
Encrypted:	false
SSDEEP:	3:m+lKs1A8RzYGAGcVUIKHWXUSnRP9Liq//lHCPA/1jlfDxKNLOQ/BRmf8l/tpK5kt:mEYNGcVUXW3nV06gPA//DUOQif0DK6t
MD5:	46DD78043C25EFDD5AB52C67B4E6B672
SHA1:	6A67D44D5DC4CBFA21D81560382D78751C236023
SHA-256:	2E4990DCF1B37F7CAB5D29F09165DEC9B4829972D67719E5B2B34EF7DAE6313C
SHA-512:	7FC806FA3A83758E9FE0650AC047146CD257EC920D2F3F36EAE923584C042AD7504F6D9AB9BBD6F31AE222C61B2972DA33B4D689FAB7157D131DDD311BF8E1 2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....>....._keyhttps://js.hs-scripts.com/6613321.js .https://clickup.com/,...../.....b..z.t)..Tbno.v.....M...A..Eo.....m.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\43724727b15723b9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	623
Entropy (8bit):	5.772127167684403
Encrypted:	false
SSDEEP:	12:mwE31zIAbOYDoux2pHgyyyJ3CMxzDwdXSNL8mz4EChTlA+:mwElz9b0uyAyyASuDp14EChTlb
MD5:	A60A4AB0C88D7478A9877AB0EC9CBF33
SHA1:	E5A0FB1F95E024AA96739D90439E000F85DE88C6
SHA-256:	6D7812AC8D667AE635FCE0029CF3660CCEDB50F473B58B935F2F7A190F84F6EE
SHA-512:	6FC4253FF5C47DA1C19D9A1CDD90324B9F7738BDC74D53FBD67B8E193F78182D98CECA98CE7BB0126175294E4D1BDC83A835D4F51A7FB529D502A0279538A4 A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....F....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/617640813/?random=1614318176073&cv=9&fst=1614318176073&nu m=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-480&u_java=false&u_nplug=1& u_nmime=2&gtm=2oa2h0&sendb=1&ig=1&data=event%3Dgtag.config&frm=1&url=https%3A%2F%2Fclickup.com%2F%3Futm_source%3Dclickup%26utm_med ium%3Ddoc%26utm_campaign%3D8666708&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://clickup.com/.y..../.....*.....\..<.....6).....6.... .spu.A..Eo.....ll.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\438fcc93076e9e9c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.580924318132676
Encrypted:	false
SSDEEP:	6:mEMlPYK0+aQRV7NV8MggstlXHJoY4K6t:ojaQRV7rFMpod
MD5:	DD66F3ED49237B641FEEB1876624A604

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\438fcc93076e9e9c_0	
SHA1:	A690525CCC3E41610FABDF1B7A673198063D5D1A
SHA-256:	4AAB9314FB465BDD4AA211E66EC95365DB186E0887A1CA22CC2B6802A562FDDE
SHA-512:	3FA0F866E26F55DD4E4C2B1BCA0609510C7561BAB0582EC02DCAE2852E261C1B46E1A76AD0E0B1C4471D56C555B532013BEAE97A3666BF59BC5CDBE2A79603A5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....|.3...._keyhttps://doc.clickup.com/6-es2015.cba4f5449c46d437389a.js .https://clickup.com/Y.B.../.....U.....,$...K.?.RG../.....Uy.O..A..Eo.....d.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4589da573ea5c1c6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	199
Entropy (8bit):	5.407262371863988
Encrypted:	false
SSDEEP:	3:m+lwNgcK8RzYrSLQzRE9LduVcvVDP9LQom//lHC4jJj+AGD/DMm+cz/lpK5kt:m3ycnYGLQmpd9VfWgmgD/TVbK6t
MD5:	50CED39A66A5DE04521CF37EC81BFAC5
SHA1:	4DEF04D00944709499EC425649B06067E109C3E7
SHA-256:	8CFB44C32F217DA499E29CEF3E85F8E82D7F157008349CD4B7704CF66B0B39EE
SHA-512:	24E3806B6D242C243C37C578C8133000D569E1453499AF2B918655AF45FFC23C84D2129DB22EF0CEF83C623206330E24C1F24BC30A0816B5827B74C2FEAFFFE5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....C...c.E...._keyhttps://www.redditstatic.com/ads/pixel.js .https://clickup.com/z.*.../.....X.!..lf.k..*+|..T.;h.'..S..C..A..Eo.....y.Y.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4a2623481b433f65_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	635
Entropy (8bit):	5.884597039793996
Encrypted:	false
SSDEEP:	12:7tnAvzIANSAgWux2pHgyyyJ3CMxzcLSdXSNL8mz4EChpdMzRpg:7Svz9NSauyAyyASuu14EChKi
MD5:	A0BB0C8B513C85A5A5243FDF6990F3FC
SHA1:	8D5381E790624CD96AD163AA206F8C3E8CD6D58A
SHA-256:	1E4AD0CB0EA6816273E24936014AEBDD1F5952218DCADF30208FC75795D57109
SHA-512:	514C3AAA71770395D5AC3DAAE0B9A698D43A4A6C29552D0C2F3BF49245B789B49632903F70CADCABFC806E5B273711809BD91D93AD125E9EA9F8C9D58644A38
Malicious:	false
Reputation:	low
Preview:	0\r..m..... ....._keyhttps://www.googleadservices.com/pagead/conversion/617640813/?random=1614318176075&cv=9&fst=1614318176075&num=1&label=2fF3CPOynuUBEO3mwaYC&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-480&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa2h0&sendb=1&ig=1&data=event%3Dconversion&frm=1&url=https%3A%2F%2Fclickup.com%2F%3Futm_source%3Dclickup%26utm_medium%3Ddoc%26utm_campaign%3D8666708&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://clickup.com/.t.../.....*.....".C.....E;.n]..1!.....Y..H..2.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4d623bcd069ac743_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	188
Entropy (8bit):	5.376598011146418
Encrypted:	false
SSDEEP:	3:m+llyELA8RzY9iRbwP9LRi+//lHClk1rF4Olt1VVZ/VK3W9kRmivpK5kt:mrVY9i9Uvg+1r2O3fVlgXAiRK6t
MD5:	3DDFBB4ABC26076F3FF4527932DFB099
SHA1:	C47273A52E51F08A05FAC69E43FB353AFBEDDF4F
SHA-256:	355ABD6DB4D73F44EBE8E5595C587E3D7C91AB02D7B7502FC2BB912E9B63ED77
SHA-512:	64CD53C63F59C74195D13F45870453648C9679C282D7C81D17FE499250B84D05469E5E69731344EE0EC8192443C67286B2F8726C309954A406862ACA48654689
Malicious:	false
Reputation:	low
Preview:	0\r..m.....8.....)...._keyhttps://a.quora.com/qevents.js .https://clickup.com//...../.....F..V=..p...#...N.....og...b..r.A..Eo.....U;I.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4e268f2ebf5198c2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4e268f2ebf5198c2_0	
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.546445753077007
Encrypted:	false
SSDEEP:	6:msPMYGLfjsVgWPWRb6D1+Hgob5WJaIlt04ERO/hK6t:BeDSkoq+7
MD5:	3F0E131FB60DA33DCF90C2481AA7EEC1
SHA1:	9323BC647B7EC2B4C4488A0D39572B67BC3C97E3
SHA-256:	5253AC382C0561E1ED602020C5B63D58BDA4E4129A9D113919612D4BC6CDE11B
SHA-512:	75006710E21D510377AB01139B5DBF923C701B415A187C5581ECBFA2768B92A5DF2E5728C08082E9967E241B515D5A16437AAFB2D87635B62D0220CF9AFC0A24
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S....Vc"...._keyhttps://www.googleoptimize.com/optimize.js?id=GTM-PBLF7VJ .https://clickup.com/.G.../.....`....>.z....?T.j.s.....d9 ...A..Eo.....w.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\668970570f5e454b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	370
Entropy (8bit):	5.384339324156118
Encrypted:	false
SSDEEP:	6:m2JXYW+wVWg1ijTvun9oRK6tW2JXYW+wVMugV/sjTvungK6t:nhVy3vuorphVMbs3vf
MD5:	B3D4C1F93CA526F66F13CAA18A985BCE
SHA1:	8B4EC44D1440019F8F00400FCE8617FB4345A599
SHA-256:	F0DF3598CFAB6E1E23EEF7C503008CA46AB20F1F935BDF6B781F0350814C2EF9
SHA-512:	2817CE8F6C71E2650240033FE1207E680669C4E47D812FD4C4C3379A0DE28BF8A12B78FB3BEED76375513AEB9A0DB7A79834349C254D2C5B8B3A33F474996799
Malicious:	false
Reputation:	low
Preview:	0\r..m.....5.....0...._keyhttps://bat.bing.com/bat.js .https://clickup.com/j.*.../.....j.5)6..0-ka...f.....']..r.'4..A..Eo....._eiX.....A..Eo.....0\r..m.....5.....0...._key https://bat.bing.com/bat.js .https://clickup.com/Z.L.../.....#.....j.5)6..0-ka...f.....']..r.'4..A..Eo.....4.H.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\689332e427d15ae4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.5037278598442905
Encrypted:	false
SSDEEP:	3:m+lx8v8RzYKceMGOQVL4LpAGJA0DP9LaoCF/lHC+eMlBhUNRPcb3L6AmutpK5kt:ms8EYKALuSA0rMoWgSHKybWoK6t
MD5:	7E87CC0B7E520A9465D3F7093EE42B4F
SHA1:	B355302D3DB6BB2281E0E7F6860322E7EE756E14
SHA-256:	B931C4F9CC0F03DEF449E8DE7BF93335FEF7535A77A92AFD11D7FCFCAD774AB0
SHA-512:	26FE69493E8F28057F7065E696DC349F1D99D9B743F6496794AECA0F0C9F06C7F4D621DDA475A7BB7EDE4A955C55FCD8463EA316C1A68E4F0A0D249D02A13E3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...M.)...._keyhttps://doc.clickup.com/20-es2015.666b0fb40ec673ec73d7.js .https://clickup.com/..B.../.....%..ZL.F..q.._h...~.7..~.^..uS..A..Eo.....Hj. .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\68fe4b04414a05eb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	787
Entropy (8bit):	5.75370633259891
Encrypted:	false
SSDEEP:	24:9Elz9SbuyAyyASuHoRJ14oza1DEChaYzm:9ElxyurxHRJ1nIm
MD5:	3318D776A2C89F5A64703DD1B0546A6E
SHA1:	D39FBFF8F5F721C85C2EA47ED61BED3EA4A12D86
SHA-256:	F8EFF83972525B8973730E13673751178664F25C295ED77956759187567BB68A
SHA-512:	EDFB842BB2C14C88A286D34916B734BA734D6D24F73910A27C39C4BA0BD14E143B7C34EE5EE2FC2B604A1A31B793653AFE3E6E0551F78D590BBAAB715E5B2776
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\68fe4b04414a05eb_0	
Reputation:	low
Preview:	0\r..m.....?....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/617640813/?random=1614318166633&cv=9&fst=1614318166633&num=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-480&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa2h0&sendb=1&ig=1&data=event%3DClearbitSegmentMatch%3Bevent_category%3DSegmentMatches%3Bevent_label%3Dab357ba2-b241-4d61-8de5-d5bbf7707f7c&frm=0&url=https%3A%2F%2Fclickup.com%2F%3Futm_source%3Dclickup%26utm_medium%3Ddoc%26utm_campaign%3D8666708&tiba=ClickUp%E2%84%A2%20%7C%20One%20app%20to%20replace%20them%20all&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://clickup.com/..2.../.....7.....z/f..r..?..e.t.].c...?..m)_oe..A..Eo.....s.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\701263a561b04671_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.418386631409548
Encrypted:	false
SSDEEP:	3:m+loOLA8RzYBJuB5hE/0AyRP9LNK9//lHCLjlltZHBO5OgllzFMhm5mtw1lpK5kt:mmY2B5hV+FgLjlX501uH4twRK6t
MD5:	9FE94101820F2E98362630CD040011A1
SHA1:	6E17088C95CD8A237AF74EAD0EDD059E1B5781E7
SHA-256:	6F2E399FA49772BEB8C127C777780A635F9D656360D5F123EFF39B15E74A884E
SHA-512:	86E9D9138FB22306E7CC760010BC403413C812181780E451A6DFF67C9F772224DFD4167083F3D67E8965253A27AD36D4FEC98F8FA649D41506A5D00B7ABFF2F9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H....:;(...._keyhttps://calendly.com/assets/external/widget.js .https://clickup.com/.<..../.....e..L9E..}.8.....>.W.Z.`.5;v.Y{..A..Eo.....y.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7188dd9bfd300813_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.771363444211716
Encrypted:	false
SSDEEP:	12:5E3Ym6B1LfPux2pHgyyyJ3CMxhHdXSNL8mz4oMGxa1DEChWmRLzWk+q:5EImwVPuyAyyASn14oza1DEChWmHW8
MD5:	811A784EB0567D65C795728A21F29FC7
SHA1:	8071F384E00274E937AAE2F7E1D99C2A6EF73DD8
SHA-256:	A42160D9F01E6E71FE5CC039B0407145C3CBC64F7203E1B5B3D1C8E73087DE65
SHA-512:	FE209B0CE0B66941D83F977CE1C6CE23202FB022E1A1E4D6670BBC6C19C34A017611A9A23B0356F7E707444294EB112E3296333A20F9C278612C12FA1A234561
Malicious:	false
Reputation:	low
Preview:	0\r..m.....0....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/867030291/?random=1614318166635&cv=9&fst=1614318166635&num=1&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-480&u_java=false&u_nplug=1&u_nmime=2&gtm=2wg2h0&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fclickup.com%2F%3Futm_source%3Dclickup%26utm_medium%3Ddoc%26utm_campaign%3D8666708&tiba=ClickUp%E2%84%A2%20%7C%20One%20app%20to%20replace%20them%20all&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://clickup.com/..2.../.....=.....%R.t.P:../..=X...I=.....A..Eo.....s.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\71d60bb0bfb5747b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	199
Entropy (8bit):	5.3751993547403485
Encrypted:	false
SSDEEP:	6:mVJVYOXdTmNgR7sVjugfnH68adZnkDK6t:CX0WRwVp686Zw
MD5:	4F4F257E4E5269F55C3ADF7D5DE6465B
SHA1:	70BCEC972982EACFFFEEAD4358697E39E1E549ED
SHA-256:	85F167DE9F5C07C487A28D19EAC77FFF8AC943A3617D19F47BEA298AD68D017E
SHA-512:	BBC24D8AEDC2C489C04843720629292F03044CD974E740BF777A08D9FD22224EC10E33183CBF410A49C0D9279BD005414C2F2A6554A42F40FA7BECA4537044E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....C....,....._keyhttps://js.intercomcdn.com/shim.latest.js .https://clickup.com/.E..../.....5.V3}.d...|._;5..x2X...1..Br_+.P.A..Eo.....~.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\73b471123e2428a3_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\73b471123e2428a3_0	
Size (bytes):	201
Entropy (8bit):	5.297071001980314
Encrypted:	false
SSDEEP:	3:m+lt588RzYM9Lc1MRPd2FvDP9LKl1l//lHC0k1+/U90ZqNpmGioMmLvaxpK5kt:mctYMK1MJqkFg0k1HQoI9onLCnK6t
MD5:	8A0A350C32F36E389402A90A0F7ED763
SHA1:	916D532E13E596AA11446C8E0D171B641D5CACF1
SHA-256:	336A6D26DDC21437EF2886DB05FE0DE5D04736BED4EBE416E4B3F9B28C333CBB
SHA-512:	9993DCA544088D1198165CDD6845E88A32F18177A2B343B40395E656736AF2947682DD2140BDC47B546C9585B63B82D8738F4A0C06DE4BBE3375C631A8AFF43D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....E.....A....._keyhttps://clickup.com/landing/js/typed.min.js .https://clickup.com/...../.....^!.j|.^0.8...Q..O.....qhF....^..A..Eo.....n0.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\76094a390b8abd4a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	201
Entropy (8bit):	5.314803999333689
Encrypted:	false
SSDEEP:	6:m1PYMHE/dKmu4ga1tgyFjbe/o2lnIZK6t:eE/3/BVbewrT
MD5:	A7714DB70C6CD75F4E57CD7AE458E0CB
SHA1:	CEBE568F77A87D0C5EF361BF135A04305ED81766
SHA-256:	A8588EE8A515BD91B296E7FF5F26D8E0B7CA6E0C3648D77CD0BFF2DA9F15BFEE
SHA-512:	87E7A0C827D70FF357E776CC9C24A9E84A6A70096D38FB509D8B45DDA53DD3B3ED7876926FF36D207841C832EC17C920CAEDF9242790C99E3CEE33212A2586
Malicious:	false
Reputation:	low
Preview:	0\r..m.....E.....D....._keyhttps://acsbapp.com/apps/app/dist/js/app.js .https://clickup.com/J:%.../.....a.{.4.{x.W.R.w...z-.GH....A..Eo.....b.[.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7e26d863851b82b7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	623
Entropy (8bit):	5.762961146880617
Encrypted:	false
SSDEEP:	12:sE3YmLO+Doux2pHgyyyJ3CMxzDwdXSNL8mz4EChYY9Et+w:sEImK+EuyAyyASuDp14EChYQE1
MD5:	A9A7293CBBE4310E7297B057C279BBFD
SHA1:	70B268BA634B14EF2FA1261EC05A12073DD5145F
SHA-256:	4124CBB285C57A6CCC23441C1DC0373B34FC129BDC5C571F870645A2501D2DB9
SHA-512:	450309FDC9221E72C4D3842D97E9C4126D6B9A4C4998C286EA3E6F0097E6A99EFBBCE06586649AA1AD36ADC7184EA39C5954CED5B35AC319B9ACC7B1B25767 4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....&....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/867030291/?random=1614318176081&cv=9&fst=1614318176081&nu m=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-480&u_java=false&u_nplug=1& u_nmime=2&gtm=2oa2h0&sendb=1&ig=1&data=event%3Dgtag.config&frm=1&url=https%3A%2F%2Fclickup.com%2F%3Futm_source%3Dclickup%26utm_med ium%3Ddoc%26utm_campaign%3D8666708&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://clickup.com/E..../.....*.....KK.I..qo..i.....|..h$....].= ,.=y.A..Eo.....&.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7f8fede988c53756_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	697
Entropy (8bit):	5.804355011733886
Encrypted:	false
SSDEEP:	12:b+E31zIAwAoux2pHgyyyJ3CMxzonJdXSNL8mz4oMGxa1DEChQN8IN:KElz9w5uyAyyASuz14oza1DEChQN8k
MD5:	20085F7003226050F6DEC9BA3ED8B9E4
SHA1:	47BE0C6A09BAED295FD8CF2B2214FCDEFA882625
SHA-256:	C9A2690CCAE4296149B704186797663EB320CC8C2117BA54844E319A2CCD9F8B
SHA-512:	50144CC88ED84D9BACD23FC79FE70F984E2058B9ECEC5DC45EAB69576C3F53F0E3602944BD37FD7B56A06F9EE4A8131AD3AB3EB0F5A9D01A9615993FDC5B3 1D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7f8fede988c53756_0	
Preview:	0\r..m.....5....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/617640813/?random=1614318179820&cv=9&fst=1614318179820&num=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-480&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa2h0&sendb=1&ig=1&data=event%3Doptimize.callback&frm=0&url=https%3A%2F%2Fclickup.com%2F%3Futm_source%3Dclickup%26utm_medium%3Ddoc%26utm_campaign%3D8666708&tiba=ClickUp%E2%84%A2%20%7C%20One%20app%20to%20replace%20them%20all&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://clickup.com/tJ..../.....7.....W...Y.2Ha5.....|.....#.G./.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\81950e9ecb9b5351_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.75580793068263
Encrypted:	false
SSDEEP:	12:voE31zIA6517ux2pHgyyyJ3CMxhHdXSNL8mz4oMGxa1DEChOnPrR:voElz949uyAyyASn14oza1DEChArR
MD5:	5F20783BF9E01D38B4D16BACC5786D4B
SHA1:	EF81960FFF4E7054F9B2F9B8577B94E383FBD40F
SHA-256:	42F3A10FC30475AD4B93528678C37FA53D3B08DDFA193FF2CEA9DD51034A6BA4
SHA-512:	5BDEF34A717690CEB773F0782F991F17B70B044856C86CA1C1AAB9D320CBED60844C150137521233B57BA96D4480B05019F9797A264CBD0B30C8979D7A1E6698
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/617640813/?random=1614318166622&cv=9&fst=1614318166622&num=1&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-480&u_java=false&u_nplug=1&u_nmime=2&gtm=2wg2h0&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fclickup.com%2F%3Futm_source%3Dclickup%26utm_medium%3Ddoc%26utm_campaign%3D8666708&tiba=ClickUp%E2%84%A2%20%7C%20One%20app%20to%20replace%20them%20all&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://clickup.com/w.2.../.....C.....-.+F.z..L*..=.p.f....y4mUj/...A..Eo.....[j.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\86f3493414ae88e3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	195
Entropy (8bit):	5.39939432222461
Encrypted:	false
SSDEEP:	3:m+l3Fdqv8RzYkwLLIK7CVRP9L80oC9//lHCQFlz/yqusbA0yRmqqrlpK5kt:mcdnYk+OVK0FgilTyIlyAqAK6t
MD5:	2903BCC6F7433FF29D1F2549AEE4C5A3
SHA1:	6AB27417EEE87551D753EEE9B3D0BE1809C7A348
SHA-256:	710EBC0684C8EE438A284F03E43BE330B8FBAA367BBFEB337D58CD2986C0DC44
SHA-512:	C90B1526E39B13CD530F5595A71D20E5EEEDE38E6D18BD74B576F5ED1309FEEB4146C1F5D2FF8EC49AC657875065A02A72303207B54217997A05E39025244AEE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....?....;....._keyhttps://static.ads-twitter.com/uwt.js .https://clickup.com/...../.....,.~...".W.W.!.....>.....'|.A..Eo.....B.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8fbb15542bd0b54d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	234
Entropy (8bit):	5.608007055270972
Encrypted:	false
SSDEEP:	3:m+l2Cf/C8RzYMeMNqdIOAXvXGJMA2mWRd3LuRP9LjS9//lHC//IcDcEjPtrtOz4w:mQ/YMdqdaX2shRd7MoFg//luxkn/K6t
MD5:	6AFE7785738986419CD0CF20A2701EB3
SHA1:	E0D2E3697E4C651707B916FA0407D7C485A1581B
SHA-256:	7122EE891C0D375C165FF54CEE662F5BD1DDB164A85A7E1DED49E8A05E00ED00
SHA-512:	B2C08156CC68C75D55D72C005A79529188BA2CBDA5A1BC7E11FEE643C4C3D1FB87932064F3FF30C004CFDCAF063F78DA3893FD4696EA4CFF1CD76F7B3C5D82
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f....)....._keyhttps://client-registry.mutinycdn.com/personalize/client/e970333877260fa7.js .https://clickup.com/...../.....`.,...-F.Sy..C].Z.t...c..D..A..Eo.....~.B.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8fd5d1efccaacc9f_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\8fd5d1efccaacc9f_0	
Size (bytes):	205
Entropy (8bit):	5.368848937193374
Encrypted:	false
SSDEEP:	6:mJJ/VYMK1MGeVAtU1Wg6FZ8y6FbdVt5K6t:+JtRPAtU1IFl61dj
MD5:	E74E41246AA77D9F55049303000E3DA3
SHA1:	C95E81943AC2784D93686B84E7938C99A662B5F3
SHA-256:	4867DA9A39B4560F2F26FB169FEB12C27480080D3E767E9A12372B1DC4F4C12F
SHA-512:	2BFDA0B74EAEAD7E441C8360F25666CD016BE3C294E780FB1BFDC47ACED23199F7C4304D45A7310E66332B871BB891C199F1572ED2130FEC95F70AA4F2291BE 5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I....._keyhttps://clickup.com/landing/js/cssrelpreload.js .https://clickup.com/^...../.....^.....(..U…#.<.I..n.....C…DL....A..Eo.....h@Vh.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\90c36c75ff2a1ff6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	211
Entropy (8bit):	5.357878573021865
Encrypted:	false
SSDEEP:	3:m+ly5/lta8RzYMwtdITRYBKgTwP9Ld+//lHCTn//TBajKbnK5mv9w/llpK5kt:m1hnYM+d4Rrvugb9VO4v9whK6t
MD5:	76CD2E09158D9ED935D3B52DA28D2E6E
SHA1:	6AFED2087DAE8332CB38013256088113A8D3ABDA
SHA-256:	ABDD96E8D4854C3A74B6D34DCA39C11DBAEDFC95283EF8A003C88D097927355F
SHA-512:	5D0BBBFFC94C85494518A5196DA16FA6E5728C63A8FA350F2704F664904475E778B96961A1E95D704E6F689BA912A270A53D94BF180AA47BDF5F4857F9E5494E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O....\....._keyhttps://client.mutinycdn.com/mutiny-client/4.1.1.5.js .https://clickup.com/.4-.../.....uIm.c.0..J...m..".8-..... F1.A..Eo.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9229dca696207896_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	406
Entropy (8bit):	5.48346424430649
Encrypted:	false
SSDEEP:	6:mw4YGL+MIwJJyDAKlHgPH/SD/iK6tWw4YGL+MIwJJyIrvtgvx/SD/P7/bK6t:dwlwvyUHqonwlwvy0Kq7zN
MD5:	F38E4E4CF653DBB203B96A3260E8A854
SHA1:	5BE79290F22850723868BA654F2133DF2420DD7F
SHA-256:	454F2F7ADBE1F75CEFDAC00C0DAA021CC8ABA3B8627266B1A73D508A9B84CA17
SHA-512:	293A00C0FB0796D6DB5BFE817A1A9A339FBC87B11DE298CD195EC726859DDCAFEBA112435B3705F2FB481D72453FA1500DE45DC440258D41C9E7E4CC499B18 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G...O....._keyhttps://www.google-analytics.com/analytics.js .https://clickup.com/.$I.../.....g...3..$<-,.s...].....KU...D.A..Eo.....CN.....A..Eo.....0 \r..m.....G...O....._keyhttps://www.google-analytics.com/analytics.js .https://clickup.com/.a.../.....g...3..$<-,.s...].....KU...D.A..Eo.....&.k6.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9cf84dddf1420918_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.589780934246679
Encrypted:	false
SSDEEP:	6:msBlVYOXdTKKW+mLuVA3HgEqXNYx5ItYJK6t:BThXwKW+8MZXNYx5Iq
MD5:	36A689D860F36F6FB7251EDB2919F2DA
SHA1:	9A41BD45625E39B3E26E06822E09C4A62F731FFA
SHA-256:	4C16ED7AFCBBC2C9E58B2591547BD92773C53254C7F56CA09D5953DE1D25C1B1
SHA-512:	3D5D1B9E84C6D940BB6F93CE1006EA3D3F767CDDA648824807B5FE0F8D3E7BA1124D75E786951625F361C31833BB9456595F00983E03211F7F03F5C29AE49218
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9cf84dddf1420918_0	
Preview:	0\r..m.....S...a.D3...._keyhttps://js.intercomcdn.com/vendors~app-modern.257e5d56.js .https://clickup.com/..}.../.....0..v.g.$@..x..]F.E=..&8y...&q*..A..Eo..... .}#.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a0836518de30683a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	237
Entropy (8bit):	5.604890859373339
Encrypted:	false
SSDEEP:	6:mFOY+pegkz7K9MINgiZ0/1GqYs/lhK6t:2Xg4KyILE8w/N
MD5:	67CBF2AEA61435E003C363253BE55326
SHA1:	EB76A84880722F434CD2D469E390BD52B18A2352
SHA-256:	F43699482D1B14720A2C79ED8FA48028D363535E94926804A2365AC84643CE35
SHA-512:	F1594D7D034B806AC89BF98A71D9D7FDDD2CBC8BFAA64D453060083D72A94A2F772EC779C6DA5B7003876A2EBAF359CE8AB29AF3C79A3AB69E8E5C60903F85 5C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i..../.g...._keyhttps://x.clearbitjs.com/v1/pk_77a36b09108b9b80c547cddad434b648/clearbit.min.js .https://clickup.com/...../.....u.W.I.....Fl...JJ..y...A. .Eo.....+.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a64461351d5f2a59_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.507694918855754
Encrypted:	false
SSDEEP:	3:m+leY/C8RzYGKAXGK7oKIIOKl4E8P9Lvn+1t/lHCBtnXhK5pmMsRlLeb2vg4m0YP:mSYOXdTKKlDw9ugBVumMGk3rrK6t
MD5:	49A75CDBC55DAC34F51CD6BE022FB0A4
SHA1:	7AD0E5BF84A456529A7A7338F281DE36BE3BF880
SHA-256:	8DDFB9368F280A0A50F7AF60FD992B70ADDEC179BAE2EB609EBAEA38933018FE
SHA-512:	1EA94A586B70F530D57A236D939CA66E8035880CAF43D471D3257A8076C82EA1B8D2304C81EDDEDDB264249BE992CC8ACEADEF1F3ED2162DD906D8916F7821 7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N....g...._keyhttps://js.intercomcdn.com/vendor-modern.2ab434f6.js .https://clickup.com/...../.....$.....S.o.....g.....u..].q...~..A..Eo.....z.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a81f1b4d5a99dd1d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	192
Entropy (8bit):	5.335922300557006
Encrypted:	false
SSDEEP:	3:m+l8Vjv8RzYm4WMctwLoP9L/2a1l//lHCtll6F1XApS04liRkP5mNUztpK5kt:mGYHWd+LM0+tgPwIST4NCbK6t
MD5:	EB99BE928D138D29D89A81A765DC1B09
SHA1:	B676DA34C186403C6B525505223DA7039A899506
SHA-256:	A1985E2A03DA7567786E822A886333690902DA83613A458B288D05E51DAA61AB
SHA-512:	A0D8C8629282880488B1B5FABA78196E64EF97AB1172B1AF4E40CECE3DCDA628789FE3BFA09DB609E06E7F79009048A997351FB089276AA3D3E28B9528C73E8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<...|...._keyhttps://edge.fullstory.com/s/fs.js .https://clickup.com/.?..../.....>..Lwc.....J..?..7....D...7....A..Eo.....B.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\afbc24eaef0bbeb7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	635
Entropy (8bit):	5.857452270066682
Encrypted:	false
SSDEEP:	12:mtnAKmp1PIj/ux2pHgyyyJ3CMxzcLSdXSNL8mz4ECh/csZ:mSKmp1PITuyAyyASuu14EChLZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\afbc24eaef0bbeb7_0	
MD5:	03E6B4C150C533B106034B0D4D3F5D50
SHA1:	0D04FF59FFF70130D907F91ED7ED687A58FAF8F8
SHA-256:	1FA442DAB3561B488483DEFCE2B8EE0FA05A6299E7A1EAECD062CA5DC1B1DB96
SHA-512:	574B16BE2315AFE9814E60C45B3B0F63AC593A40CA7FE777FA4E65A295C91A5A5A36A85363295FBFDF80C9AE6850EA6DDAA33ADF829CDA57EC0C2C840712AC57
Malicious:	false
Reputation:	low
Preview:	0\r..m.....u....._keyhttps://www.googleadservices.com/pagead/conversion/867030291/?random=1614318176082&cv=9&fst=1614318176082&num=1&label=sFHSCLa0k-UBEJOqt50D&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-480&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa2h0&sendb=1&ig=1&data=event%3Dconversion&frm=1&url=https%3A%2F%2Fclickup.com%2F%3Futm_source%3Dclickup%26utm_medium%3Ddoc%26utm_campaign%3D8666708&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://clickup.com/cu..../.....*.....|.].d]...!.q&1..A.f../.7`RK.A..Eo.....R.1.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b11f6c304de41b06_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	5.534134538587187
Encrypted:	false
SSDEEP:	6:mo/yEYET08NWQAgt8XzJTK6VugX03L9sGePqn9Y0LK6t:c0g8NWQht8FOdh9R
MD5:	02C81A6183B3BC93D13581A2B8608A0E
SHA1:	C58D0DA37AB4B0F147C14593B2E98E6A0FAA4CA4
SHA-256:	A4AF2412E5E81820C63DADCAE38CBD42E635A2BED9D0CC061F8187CF9743E00C
SHA-512:	6F9B16F18EB7A97C2297909B5AF0120548A98B6EB2028976680D5FC7434884F3E53EEA9A386C2DD72B54D0599242B1A30E1D49010AF3FD42AAA447CF2C15CC51
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I...D.a....._keyhttps://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js .https://pale-small-origami.glitch.me/..#.../.....2.....z..X{W.!.2..mX}..._.O..f}.....A..Eo.....At.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b482e01c93094c80_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.490150251820392
Encrypted:	false
SSDEEP:	6:mm3PYMK1ME/JA4FgxXlYBYe68x6AdXnK6t:hREhpuWBqmZ
MD5:	8A2012A24C30FF9C6AC60B5DD282925B
SHA1:	8FDE5DB7B93C2134D26D086D67C7AAE854728923
SHA-256:	2703F6731F397A5E5A7DC254DED093BDFFF6F1FCD4D7F805991B72FF714CBE34
SHA-512:	C77E3D8F5816D41DEDF02B4E21FB11361D83B2270E03A6FE0804B14F4DC9E74D502C5877DBB89BCCDE5D68BF8CE4D17EE757647EF561116879DC67662CEA53F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L...m.*....._keyhttps://clickup.com/landing/js/app.min.120a1dff.js .https://clickup.com/...../.....@."=..zL.....j.J@Y..ei...A..Eo.....EKI.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bceb1bf92d92d13e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.392596725655373
Encrypted:	false
SSDEEP:	3:m+ljULls8RzYkwLYR8X6pF/L9LEcomv//lHCNvlltqyGHUml1DFmmAxlpK5kt:mTnYk+z6pFD2cLHgNvlXq6S14NK6t
MD5:	EEFC8B6444948FAD07F461BB18D055C6
SHA1:	3A7B041DE36AC5CCC3BC4F4A7A3532804ABC2F35
SHA-256:	F635F2C4DA63B06DA488EEF8D82BE8DF9BA4B716AC5E199D630C72A891580635
SHA-512:	D8D595EC5EA1A366DD778AC410EC5D1C474EC8988CE026F18FABDD4431DF9FD6907CB749ACD057E48E98307E34948FECD3200990010199F0C6C5115E4641E7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K....d....._keyhttps://static.hotjar.com/c/hotjar-779854.js?sv=6 .https://clickup.com/...../.....(.....-t.S.....+[..../..j.....w.'.'.A..Eo.....'.x.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\be2d99002a93a98a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	88626
Entropy (8bit):	6.136944441107465
Encrypted:	false
SSDEEP:	1536:Iqeb1WThkE8tA+JH4E21qeU1+/4B6wCj4cJH4YIi:IqmWNwA+6b1qP+WIj36ni
MD5:	3D732AAC3ECA7231B2C758F487DEE44A
SHA1:	79B553E97348EBD703679C14B8BDB9E0ECA041C7
SHA-256:	34CA9D2AE8DCFE72C33EAD58231E40445AB0AFA0EF7A2CADBF4D8BCF282B4DBE
SHA-512:	6D27CDF6A3A7150FA79188FE75C01F5BD79375CC1EDE6FEB44CEEE4FF7E96864A302CF5E4F0B7C87C2AA0453CF39CA89378AC10F0DE144BE9E5285EFAD427 70
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U....._keyhttps://www.googleadservices.com/pagead/conversion_async.js .https://clickup.com/x...../.....~^.xY_..{....a2.9V;...K.H.....A..Eo.....E.w..... ...A..Eo.....'.O|....O.... ...$c.^.....,.....(S.<..`2....L`.....(S...`.....L`r.....Rc~.....6....Qb..=....aa....Qb..h.....l... ..Qb...#....ca....Qb.....da....Qb.....p.....QbF.....v.....Qb.a3c....w.....Qb.....ea....Qb..u.....fa....Qb.:.O....B.....Qb.....ha....QbVt.....ia....Qbb.....ja....Qb.....ka....Qb..q.. ...pa....Qb.r.....F.....Qb:`.b....H.....Qbv.....l.....Qb.K.S....sa....Qb.W.....ta....Qbz.....ua....Qb.%<.....va....Qb.N.'....wa.....Qb..ch....xa....Qb.....ya....Qb.J.....J.....Qb.b.N....za... .Qb.z....Aa....Qb:.....Ba....Qb.....K.....Qb&.....Ca....Qb.....Da....Qb.s18....Fa....Qb.qt....Ga....Qb.....Ea....Qb.....Ha....Qb.h.....Ja....Qb.....Ka.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\be4f8f8a4aeaa100_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	192
Entropy (8bit):	5.405031749018736
Encrypted:	false
SSDEEP:	3:m+l8bBlll08RzY0IDXMVLdgdyLPWnRP9LMKvl//lHCZjeqq2Q2udy9kvg4mHRMtB:m5llVY0IX1qPWnVLgZVmLU6grH8K6t
MD5:	8FD27E3D930D1DF310FDDC6CF10CC9A4
SHA1:	5BEEEBC2CCFAAD0793B67EF0E0475B60552F2E06
SHA-256:	BF9BCE9455CDFD10008D887D73AB9AC976DC8D56A771BC9B43339E4420A27443
SHA-512:	383346CE0F17B2E37B99DD10D097DC5166D4EAB161A9A148B9617153941B12D08AA29BFDC837B5D34E8ABF51DAD2F3BC0AD0F0337FEE78DF5DA311E0C46CC FE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<...0.g....._keyhttps://tag.getdrip.com/4818331.js .https://clickup.com/...../.....<.....).,(....a.....s.5.m..Y.q...A..Eo.....M.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bfbf5849650ec0d2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1406
Entropy (8bit):	5.401094391522958
Encrypted:	false
SSDEEP:	24:OlaOdIljGza1DHPZFGOen44zjOVza1FZfiSk3LKjYXPkYX7XZv+iYX2kYXnvYXBz:ZjrZ8744zCwZfiSkbakPkk7XZvJk2kke
MD5:	68C3A06E14D6DD5915F450D7B71967F7
SHA1:	E890D77503A780BFFF504D8272753129C1C443D9
SHA-256:	08093916F2A1AD6AD5D73BC6DA14CFCD73A94A5C2E6F0E73BB298C7384B5991A
SHA-512:	9E8A2881A1AA62C86D7A67D5D219895AC2F811AD5C28439E367197F8EF9EA76BC9B17C4ED35613B5C3A64094035787CDB39C7D07130AF895B7BF7FE3C00C97C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....?...._keyhttps://px.steelhousemedia.com/st?ga_tracking_id=UA-87708648-1&ga_client_id=1304408799.1614318149&shpt=ClickUp%E2%84%A2%20% 7C%20One%20app%20to%20replace%20them%20all&ga_info=%7B%22status%22%3A%22OK%22%2C%22ga_tracking_id%22%3A%22UA-87708648-1% 22%2C%22ga_client_id%22%3A%221304408799.1614318149%22%2C%22shpt%22%3A%22ClickUp%E2%84%A2%20%7C%20One%20app%20to%20replac e%20them%20all%22%2C%22dcm_cid%22%3A%22undefined.undefined%22%2C%22dcm_gid%22%3A%221852786573.1614318149%22%2C%22execution_workflo w%22%3A%7B%22iteration%22%3A3%2C%22getTrackingIdByGA%22%3A%22FAILED%22%2C%22getTrackingIdByOther1%22%3A%22FAILED%22%2C%2 2getTrackingIdByOther2%22%3A%22OK%22%2C%22getClientIdByGA%22%3A%22OK%22%2C%22getClientIdByTracker%22%3A%22FAILED%22%2C%22getClient IdByGAData%22%3A%22FAILED%22%2C%22getClientIdByCookie%22%3A%22FAILED%22%2C%22shpt%22%3A%22OK%22%2C%22dcm_gid%22%3A%22OK% 22%7D%2C%22message%22%3A%7B%7D%7D&dcm_cid=undefined.undefined&dcm_gid=1852786573.1614318149&dxver=4.0.0&shaid

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c2829b54881167c2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.705144102305208

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c2829b54881167c2_0	
Encrypted:	false
SSDEEP:	6:mjVYGLSmXZCkMTwpCGNFV3Fn/KtgpdqAoq4uK6t:2HMMpDVnlPoq7
MD5:	09E4138A98236BEE7F02143F2C5447EB
SHA1:	B5999DA500B4ED670E8F950197987C0C3FA33718
SHA-256:	9B0E6DE989694AB8ECD8225912B1454FE8A62FCB5FA202BC244B2862997CB6C6
SHA-512:	B4633DA39162085900F220630A7DAE7BCAC5D06478EDF5E9157C0C2ED75793906EAEACC1BFD816DA6660DA40B2835014148E61B01369F76591B8E0777185C73
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c.....I....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-617640813&l=dataLayer&cx=c .https://clickup.com/...../.....z....J....<Y...O...^.i...My..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c2c5635b1cb2c5d5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	222
Entropy (8bit):	5.542519635745779
Encrypted:	false
SSDEEP:	3:m+lKhs/l08RzYKceMGOQVLmZWIzFCRwBM7wP9LXS9/lHC0llIrsNwhSxk6DjRmiW:mkVYK+o0rBUUE9gUlo+hgkEjAfK6t
MD5:	04FFAA5E8028D10B8664F9D80E4BC44E
SHA1:	9548BF98B616A526074B0DA83346063EEA99712C
SHA-256:	F6A56370D3DD30CC64C736F4167FF375F8BEB083C1A9B68E0760419D30B792EB
SHA-512:	2275ABF8950E8C17BBA2384DF091B7BA2B387E0623718E0158C78BE4E4C3024DC712978B6E9505122DCE8B2D6EFD2B35BEFC2B4C5283461510E646ACD3B896D4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z.....D...._keyhttps://doc.clickup.com/polyfills-es2015.74fd49d5fff3696d5809.js .https://clickup.com/..7.../.....S.....U.....c`.B."....O.[.J.A..Eo.....#O.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c7327b2c27d4aad8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.478564677012896
Encrypted:	false
SSDEEP:	3:m+lgu/lla8RzYKceMGOQVLvWDDAcjKFnC7P9Li9H/lHCPltXsxsdC06Dg4m2jl/B:mu//XYKGDcVnCDQ9gPXcxs4CMK6t
MD5:	9153E65950A7E847ACF5512F85F5BB7F
SHA1:	6F2F76ECCF529A978C9E2FB4DE62278C3CBE075A
SHA-256:	FBDC09ED67DC2FE9A6A3DA443BFC83DCE346F11D2EBF41220C085A86D55C3D0E
SHA-512:	BA8A8F63CA447C21928AAD42E731CA0497F6162FC839300BA616D9375FDDF296C846EBCA59C2886B47054839B3B3BD7C8C38E8168ED5FBAD1D42FEDE3F13A07
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R...2....._keyhttps://doc.clickup.com/2-es2015.80c13cde974ec82050f9.js .https://clickup.com/.B.../.....l.....is&.Kc(.g.gr...-.:.}>...".1Q...A..Eo.....y\8.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cae14352f97fb1aa_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.629281867411164
Encrypted:	false
SSDEEP:	3:m+lJKw1A8RzYKceMGOQVLBWh1XSQvDP9LS79H/lHCKkl+n50N/aYq39WmBh5lXlB:mOxYKoDCQD0xgKkl+5rnNhBh5lDK6t
MD5:	0AA5A304AF54B4FB52448D56E968BBBE
SHA1:	965C00B215F261666FA840BAAAC17F7E3440C5EB
SHA-256:	05B72713DC6003048E0D998FAC6414318E69CB8707FC2778001D1BC60D98F6DE
SHA-512:	4650203C58F3DBA9DA25E4C60EA65284A63A65C1DD6B4BEE48DF1C3AF4BC87982FF1C86AF420E455439A63EA4A0886A3174F1DF3D693E9EDBBF686F5D06038B4
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cae14352f97fb1aa_0	
Preview:	0\r..m.....R...[oM....._keyhttps://doc.clickup.com/8-es2015.572c4744fe272494ec6d.js .https://clickup.com/Q.B.../.....I.3.bZ.....}..<....,..j...A..Eo.....g.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\cc7c77a27c21d11b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	214
Entropy (8bit):	5.641459918330729
Encrypted:	false
SSDEEP:	3:m+lGlFFlIOA8RzYrSLSELDXZCCcTDXcUn3F9LyLmv//lHCWGnlXO42z6EbTDd5vK:m+EYGLSmXZCCS3FoqgDCekd5vhcZK6t
MD5:	0CDA53C8BB13BFDF062688EB64EC7211
SHA1:	9746864976271548F12B19EA5581EC9AF9181B79
SHA-256:	77374C26AD547E7D362FBC435732CE09A1DD8153F02560CF4420AA985AEE996E
SHA-512:	853051A58B8640891F9461711CA8D59951D386F40C027374BC0695E9716E4ECCA0B4357E875C7CCEA441E84823A93B00651EC6E6355DC0490B5F7C988DB246A7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....@....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-867030291 .https://clickup.com/..L.../.....#.....2..^..{.-....!v[.k,.\1-....`..(.A..Eo.....<.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d1e77cef7d85a72b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.6277661632511276
Encrypted:	false
SSDEEP:	6:msT/PYGLSmXZCC5c7RF3ugZ4Xs3hmyA3+/ZK6tWsT/PYGLSmXZCC5c7RFOliug2x:BTXs7RFj4XQW+rLTXs7RFOlix0x
MD5:	D2237A274429BE31A64FE5BDA1F9CED5
SHA1:	10C3F124A1BB784DE29524C0B72B7C1F7F97B109
SHA-256:	61EAA0AE72306AE1B54A6CA7422156887089C0267BAE9B1E6C7DC2707C83416C
SHA-512:	AE9E677F0E129AB7022F1F7AA47AD9BB4A25ABABED713091C202E9C8BAFD2DEB729847F039CEFA979B1B3ABB57E26ECD10D3759D6A23A1A2D71884291F209EA6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S.....w....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-87708648-1 .https://clickup.com/..<.../.....f.s..e.....CN7`...S[...A..Eo.....#.?.....A..Eo.....0\r..m.....S.....w....._keyhttps://www.googletagmanager.com/gtag/js?id=UA-87708648-1 .https://clickup.com/...../.....f.s..e.....CN7`...S[...A..Eo.....$.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d3f4ed42682742c9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.519708050928847
Encrypted:	false
SSDEEP:	6:msf6EYKoIzXVuUEl7srQ9goiM6JcxnfnK6t:BXFudeQpd/
MD5:	0E5C9AA410DC620F12B433C2D40B4FA5
SHA1:	A0F681FC052368B2F8F2B0D2955DAB2DB5933A76
SHA-256:	614DD49422799249E50BFD00AC64080DB011BCE79734615371DFC39DDDCD8D53
SHA-512:	CBF5D32FDF35D276850F362A2BE1E33A2FCF8B6A5A9C2DFF75470B1A78285A47D2B1C6C9C37019A6917A94507D70020431536E0B2ABA712F3F15656DB016155E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...{....._keyhttps://doc.clickup.com/30-es2015.c8400463cbca5eefae05.js .https://clickup.com/?>B.../.....U.....}h..:..j..Qj.....]a.d..g.&....A..Eo.....4..w.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d6a93f49c5fe3a17_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	189
Entropy (8bit):	5.416854644057722
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d6a93f49c5fe3a17_0	
SSDEEP:	3:m+lB/l08RzYEDC3mWPWFvDP9L4Plv//lHCxXOEKXexXz4mhcl//pK5kt:mIYEDC3RUedHgBlXexXzrhcDK6t
MD5:	C9AC4BD72713761822F89059C844271A
SHA1:	8BFBC5B9E338B6A9B26B7DB3985650846E9F9CC6
SHA-256:	D2B512F3BA5886115F34757DDA760C14B34360AE8DA0CF054A58F45E555C227A
SHA-512:	CCEBDBC77E580527D9917DD11897C9D3D710A5B54A86E2E9F8E0E26056A2E2400F895BC10B3630836C0852F5DD05B483ECF8F10BBBFEB64024599A7EC1DB3FB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....9...T`.,...._keyhttps://cdn.pdst.fm/ping.min.js .https://clickup.com/..+.../.....]C_..5!....d.D..@.....U.J.A..Eo.....e.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d9133d4093e7cc49_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	196
Entropy (8bit):	5.314274125979985
Encrypted:	false
SSDEEP:	3:m+l6g2o8RzYEpGguoCVRP9LK+1l//lHCGt91cYozAgAFZmrTXpK5kt:miCYENbsV5HgGtsXCYrdK6t
MD5:	1A03E88E752D2698A74CF4F8CE2CED1A
SHA1:	06DFFE913E4F68EFB04A1CBAEC9162EBB151FCF4
SHA-256:	3E24FAF0705BD39F8F9D4FB4ED82A7660727566B18F7C6651A7B15C6AC3E2F35
SHA-512:	4FB00907FB259DCB089FAF9142BD27C619150BD29B92AC91B9510052FC1453E48305A46ECD9E27E3C81D924D0F43CD435FFBA247BE5954289506A2E4AD093B1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....._keyhttps://cdn.firstpromoter.com/fprom.js .https://clickup.com/...../.....A.....b.N.....C.r..H1.6....eo&...%.I..A..Eo.....(.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\d914bd0e979d4799_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	217
Entropy (8bit):	5.554825107073328
Encrypted:	false
SSDEEP:	3:m+ltyyta8RzYKceMGOQVLoWXgReQ7WFvDP9L7IBt/lHCOTEllluNKUhvKj5UbkgV:mkYKDXUjWVrqLg8EtCKjSkgrhK6t
MD5:	C8725A277768DABD3CD4F71106DE47E1
SHA1:	4D8C212F86863465B012D403F1B45288CC9CE4DC
SHA-256:	119E86C378B844220262B537BC3BBB8B0E7D9D2615A6268B07E58BBEA0C4A81B
SHA-512:	05C11CBDF85DD995A24342B597F8C44485E1021B1004C1685ED44A5460D32977E5A84C9F9CDA488DC8E21B9A724BB04868702842F20423741E3B065B8EF90550
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U...(.,m...._keyhttps://doc.clickup.com/main-es2015.8cfd6901e25e8624f9e5.js .https://clickup.com/.q8.../.....,.>(hYB..q.....vC&.....Fn...?t.A..Eo.....).....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\da27c87340da77ca_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	351
Entropy (8bit):	5.758848346529444
Encrypted:	false
SSDEEP:	6:mC9YmXHUj8TKU6t3z0WDEXTQ1SNL8mz4GE3wSgfYbc5OqGDK6t:JR5P6ZdXSNL8mz4GE3wWbc5U
MD5:	C26B22B45FE1A26433BF57C6C5871F09
SHA1:	4BF2F32A2F80D35CB8944D091D56A8212C02A5E0
SHA-256:	31A1D11836300EACC9CCB8200603C4C9121AA99B1D4D2B894125DD171888AC7D
SHA-512:	4B5B8FF48028B4167AF6CCABC782D2877764B32547679B349A242672A60506FF81D297CFB2B687155A64A88D1372E1D8187381FCEC3CE2BC5003E59E8E9E5087
Malicious:	false
Reputation:	low
Preview:	0\r..m.....D.O...._keyhttps://dx.steelhousemedia.com/spx?dxver=4.0.0&shaid=31571&tdr=&plh=https%3A%2F%2Fclickup.com%2F%3Futm_source%3Dclickup%26utm_medium%3Ddoc%26utm_campaign%3D8666708&cb=8118011296867045term=value .https://clickup.com/...../.....~.]..otmB7hLB."3.wf.t.Z...W...A..Eo.....c.|.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e62126747b8640fd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e62126747b8640fd_0	
File Type:	data
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.574859605085451
Encrypted:	false
SSDEEP:	3:m+lj///a8RzYGKAXGK7oKIf42bW2SK7P9LP+/lHC9/tCDSf87s9/6RmIct/pK5kt:munYOXdT04+vcgN8D0qG/6ABhK6t
MD5:	32F662F01451CC2639A80DAE4FB10682
SHA1:	6E100C7A39EAF399F3A56C196F5298D64DC29253
SHA-256:	CC16A8E401E5E451CDAF65ABA47F4D1580441CC95E5D292B87DA73AC5FF8D0F8
SHA-512:	48B3B3ABE16C57DA2FE4794B110C61AA54FDF82F1F2FC36933C3E5F3FFA56B0FEEA1E47D9B37CEFA647698426503D26CAE246D3626577AF3088A9A317203952
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K.....\...._keyhttps://js.intercomcdn.com/app-modern.16409436.js .https://clickup.com/L.}.../.....z.....7a....?Q.....EY/b+^....A..Eo.....x.T.....A..Eo.... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\e65c83fcefffa33a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1417
Entropy (8bit):	5.376610934344604
Encrypted:	false
SSDEEP:	24:OaOdIljGza1DHPZFGOen44zjOVza1FZfiSk3LKjYXPkYX7XZv+iYX2kYXnvYXBfb:/jrZ8744zCwZfiSkbakPkk7XZvJk2kkc
MD5:	EA0B63DBF74B062DF2FB8482276397D7
SHA1:	5F5E095A5347931FD5E783EFFDB29511AE7068EF
SHA-256:	48442BF1C03CBBC3675DB594A7F374D2BCA1784CD6E565B6154322927B3AEB42
SHA-512:	0BB53EB06537C11CB46966C7EFC4C2BF5ECC03903662F3CA325C8BF1333E86C138C37748EF16D0B1AEE1437BE8EE593EC9835CAA7ECBF26BAAE202C73B9A2 23
Malicious:	false
Reputation:	low
Preview:	0\r..m.....w.!...._keyhttps://px.steelhousemedia.com/st?ga_tracking_id=UA-87708648-1&ga_client_id=1304408799.1614318149&shpt=ClickUp%E2%84%A2%20 %7C%20One%20app%20to%20replace%20them%20all&ga_info=%7B%22status%22%3A%22OK%22%2C%22ga_tracking_id%22%3A%22UA-87708648-1 %22%2C%22ga_client_id%22%3A%221304408799.1614318149%22%2C%22shpt%22%3A%22ClickUp%E2%84%A2%20%7C%20One%20app%20to%20repla ce%20them%20all%22%2C%22dcm_cid%22%3A%22undefined.undefined%22%2C%22dcm_gid%22%3A%221852786573.1614318149%22%2C%22execution_workfl ow%22%3A%7B%22iteration%22%3A3%2C%22getTrackingIdByGA%22%3A%22FAILED%22%2C%22getTrackingIdByOther1%22%3A%22FAILED%22%2C% 22getTrackingIdByOther2%22%3A%22OK%22%2C%22getClientIdByGA%22%3A%22OK%22%2C%22getClientIdByTracker%22%3A%22FAILED%22%2C%22getClien tIdByGAData%22%3A%22FAILED%22%2C%22getClientIdByCookie%22%3A%22FAILED%22%2C%22shpt%22%3A%22OK%22%2C%22dcm_gid%22%3A%22OK %22%7D%2C%22message%22%3A%7B%7D%7D&dcm_cid=undefined.undefined&dcm_gid=1852786573.1614318149&dxver=4.0.0&shaid

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ecba0530bad5195f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7960
Entropy (8bit):	5.93060457504845
Encrypted:	false
SSDEEP:	192:99CyAAIJXjCy/6H+slx2ljbgy5xbNedAEY3F:yn1tyH1xPHNedxYV
MD5:	7FC9D70FF2E660E4EBE5C3E0829974DC
SHA1:	42FA13E02E9C0130FBDC1D3676EF680248DD956A
SHA-256:	A632DB62049290D29C394A1E04A900484790AC09A8AC3CD41E5BF80577EEAEF8
SHA-512:	71DE15FE7A411CF04F97F707F2A5BBFBCA9B037E5CEFCD8582AB2436D3379240C9BB946CCE05CAFD5208F5A6B8A5491A0E21181DC9CE18BB4339C84D984536 E7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P....._keyhttps://snap.licdn.com/li.lms-analytics/insight.min.js .https://clickup.com/H...../.....CT8.\..... .S.n.F.{m./b.}.I.WW,.A..Eo.....+f.....A..Eo..... .....'.....O.....MZ.....(S.0..`.....L`.....(S....`.....L`J.....Rc`.....(.....Qb..h.....l.....Qb&.S....._.....Qb.....t.....QbF.....s.....Qb.....r.....Qb..... ..c.....QbF.....v.....Qb.....p.....Qb.N.....f.....Qb.a3c....w.....Qb.....h.....Qb.E.....R.....Qb.ER.....C.....Qb.....U.....O...Qb..?.....E.....Qb*.j.....x.....Qb.)iG....D.....Qb.-.H....L. ....Qb2.].....T...s.....I`....Da.....!...(S.<.`.....L`.....Y...Qc2..{....getTime...K`....Di.....&.e....&.(...&.X.....,Rc.....Qb .a.c....n...`....DaF.....a.....c.....P.....@.-....DP.....6...https://snap.licdn.com/li.lms-analytics/insight.min.js..a....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f4e88cc7f3307961_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.619201627974647

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f4e88cc7f3307961_0	
Encrypted:	false
SSDEEP:	6:mnclVYAWGUJ3TC3aUQFvNFCqg8/EVQsxJP4tDK6t:QcludTC31QvrD/tCP01
MD5:	F666D90651A018549B9C7EF4C54F69F1
SHA1:	C99A6FB4973C224F24E32F5CE49882509BC96150
SHA-256:	B0619FE1CBD9A07569E1596F090A363979F463D2E6F46C5778AFC26F4C8E0BF5
SHA-512:	78FE2377C444792708F765D8178A72EA7034763C552100E3EB693B92076AAE81392CE3A7978AB92AC10A9C5C4A088A7BD5C2974937B5E9C1D605793A7B4424B7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g...W.h7...._keyhttps://connect.facebook.net/signals/config/124630241461844?v=2.9.33&r=stable .https://clickup.com/.8#.../.....=.....?...r...pq...;]..f...4... _us...A..Eo.....a.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f7bde544f5eb53fd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	231
Entropy (8bit):	5.647004717500298
Encrypted:	false
SSDEEP:	6:mwxlPYGLSmXZCCrpCGNFV3FRKtgN7/cHwv51I/0grqK6t:hxlfBrpDVcmzSq5e/0gw
MD5:	0C72D79332D1652DC85C1B6C1FF17643
SHA1:	8C2D099C3B27DBB5F362A7F6B1F54CF48BDF6198
SHA-256:	BDC16B0305289B2A207B2FA39FD8C91427264BD14BB44BC03E9C9695A8792C4A
SHA-512:	C589AED324E849089A17B1AC6FB3759D6D0AA58D90E5FBF97390FCD0D4E6AA414AC73380E9F7A0D2E3F5D97AD3A5CB3075D063288C76FB724AF11FDD14D27A AA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....c.....8....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-867030291&l=dataLayer&cx=c .https://clickup.com/...../.....(&.....<cvKu.....c.....?.5...u..... P.A..Eo.....).....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f7fd71217955a417_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	245
Entropy (8bit):	5.420635267385283
Encrypted:	false
SSDEEP:	6:mil9Ykb8E9xEZPWfEro8XzJTK2vLgTJWMzP4JJhK6t:PvQQ8FOI8kJ7
MD5:	423DAEC6ADF8AFB22115729059A5EA74
SHA1:	DE4775C3395C31715C155B6DEBDCC49A36BA8ECB
SHA-256:	0DC06DD467A7FC17E422E2590B83A0F0E02C7C5D3D0B59CBE9DE59A88EC8C849
SHA-512:	3ED13E37C46EA727237D573575BA42CB54D607E48BE50A9749A29ACE895F9183A4A3A8815D2A12F8DDBAB6D7209F535B09F7495751732BDE051A4B3CF83121F7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....q.....%`...._keyhttps://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js .https://pale-small-origami.glitch.me/...../.....8.VD.L.3../.I.?.. xa.ZW.....I.I0.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\f8a2aae8c7eea631_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	428
Entropy (8bit):	5.670387594619526
Encrypted:	false
SSDEEP:	6:msAXYGLSmXZCkMnRF0MHgheJgBK0hv31CYJRK6tWsAXYGLSmXZCkMnRFMiLgXYe3:yHMnP0BeJEK0hvrQHMnPMiNeJEK0hCr
MD5:	CA9AA2D5BE301012969DD3F1054A36EA
SHA1:	4A08D97093E9FF9C1A278CF286FB5AFD01B9DF04
SHA-256:	C9AF4916F2888AB2B817FFC5505E329826F45EBEAAB25ABF673584D6EA2A3180
SHA-512:	F048EAF871A7A4DFFFB1454EACC1A5259CA74B8900CF123AA445A1FC9E4CE881D4E034873C985B49603877E714DBFFA21D296D0CC00732E57A2E24080B43995
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R.....K....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-617640813 .https://clickup.com/J...../.....}...,E...DU|k...as+...A..Eo.....,.....A.. Eo.....0\r..m.....R.....K....._keyhttps://www.googletagmanager.com/gtag/js?id=AW-617640813 .https://clickup.com/.$M.../.....#.....}...,E...DU|k...as+ ...A..Eo.....l.j.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	36864
Entropy (8bit):	3.8508482907745307
Encrypted:	false
SSDEEP:	384:HhTwXBGAVeYxaMguj4XadnFT4yBxVYQxGjsji4h750s+mn8:BTwXBDfgiFT4yBx6A5HV8
MD5:	2ED3018B11ED5376FA2473C6DB30672C
SHA1:	8F0F340820D698EECAD1C2A6F9E96DAF13D127BF
SHA-256:	F70AF0B9405B40AD898A824A5E2B64FB929D95705E158C693BDDB90E8241C45E
SHA-512:	85967C20DD89C20047C6126EB42814880AFFDC9A4935BA47CCAB070BE31D3DF1A788F121D972761E2BBBF5BC25B7F5C651D0AF3F50D57A7A009CC81F398321F
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	29776
Entropy (8bit):	2.5781385850267178
Encrypted:	false
SSDEEP:	192:2FcuMIMhTwWlBGAVeYxqLMg0Ls6CnOxmu7:wKrhTwWlBGAVeYxaMguj4W3
MD5:	732FF0C75B45BDA038202102A6DECA39
SHA1:	7A2626CC18AAABEE1BDF95764ED17B6E84D77FA9
SHA-256:	66EC00DFEA0949462B2AF902CA504686D0C5A24F6464CBD4525909781DCB7744
SHA-512:	ADB6EF8909628307454CD15A4DB3E5240E995D6DD041FFFFCA16B438E543C47A6B8F2FC1360DCF02B88A77885089B1476D8EA3D9843533E10FA2D5E4F45C7C3
Malicious:	false
Reputation:	low
Preview:	.....j1..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	46322
Entropy (8bit):	3.255531793077023
Encrypted:	false
SSDEEP:	384:Jaj4TwGvSECeym4fXlcJ46Qlh9BYym4fXlcJ46BRH14rZF:Jaj4TwG6F5PfXlG2lh9lPfXlGTdyrj
MD5:	E0E840D72C43E01FDF56F88AB177CB23
SHA1:	0342EFACEF0E5EDA0F9571E5884C936D3A2E9038
SHA-256:	B05D7D670CCB2C5875AF89496CFE68440BB0FE6E8DDCA6F2CEC2D4323400A607
SHA-512:	55C55D4402B24BAE3D158BA81F33A55CD78AB3F2FAA95EC656B76B7792B69FB4BCF2D5D6C67F1DB9A7F91B7AB852F90345074B383F77C3D47ADDD90F5ADB59 3D
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...ea7de982_a207_4ceb_97d2_0848c0f4bd55.....@e..... .....5..0.....&...{2F4F8386-A58B-4B0C-A17B-2FAAF764E551}.....4...https://doc.clickup.com/d/h/88fjm-14/9b55da9c0a2598a... .C.l.i.c.k.U.p. .f.o.r.m.s.....h.....`.....6.....6...@.....X.....X.....p...4...h.t.t.p.s.:././.d.o.c...c.l.i.c.k.u .p...c.o.m./.d./.h./.8.8.f.j.m.-.1.4./.9.b.5.5.d.a.9.c.0.a.2.5.9.8.a..... .....o".navigationIdI.{.....8.....0.....8..... ....https://doc.clickup.com.....4...https://doc.clickup.c

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	1.8112781244591325
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
SSDEEP:	3:3Dtn:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
Reputation:	low
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491 A
Malicious:	false
Reputation:	low
Preview:	.f.5................i.Wd...............Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F..................F................

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.107016886928751
Encrypted:	false
SSDEEP:	6:mN2F9+q2P923iKKdK8aPrqIFUtpe2C2WZmwPe2v9VkwO923iKKdK8amLJ:F9+v45KkL3FUtpyJ/Pf9V5L5KkQJ
MD5:	08C938137ADA1C08C2D9C7B6B23DBDAC
SHA1:	EA10E22E6D84FC9B31EAF3C7D8E64B721B2247A1
SHA-256:	D7BFDD4878366E172400CA5DC34F6C47462713D58899D1D12ACA6D9E55346377
SHA-512:	11E85E9B2FD979F9020CEFE36200567DA40EAB27A1E9E6F0F65F47B561777CB872428477F1EF0DE27BE055FD236137091E62F5826E98B497E0A715D5694536D4
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:42:22.454 150c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/02/25-2 1:42:22.455 150c Recovering log #3.2021/02/25-21:42:22.456 150c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Reputation:	low
Preview:	.f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f. 5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5................f.5.. ....f.5................f.5................f.5...............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	322
Entropy (8bit):	5.100222742147057
Encrypted:	false
SSDEEP:	6:mN2IpR4q2P923iKKdK8NIFUtpe2I5OJZmwPe2IVDkwO923iKKdK8+eLJ:5v45KkpFUtpSI/PC5L5KkqJ
MD5:	6AB0124799AB8DBEA8EBD6147D8C17B5
SHA1:	58AC1F0D866D629A142B69F6CC97937FB3F7B549
SHA-256:	FBC7F9CBD06B3F3D7A61DD811FA0B56718081575B61CD9D9012776741568B589
SHA-512:	5F018C20BF168E6220A957A10BF2CB2E950595B2617C2B9E4156AA24D2FC483F6F3B6C4960AC5381324A6C705ECF4330043205AFEFFF280353A42723A30F5680
Malicious:	false
Reputation:	low
Preview:	2021/02/25-21:42:25.540 1600 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/02/25-21:42:25.541 1600 Recovering log #3.2021/02/25-21:42:25.542 1600 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\computed_hashes.json	
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):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXltmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMBN2jrtUtLgsCefvuceTpAatmLvuI11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FFFY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=","yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=","3mBGNAiRITANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAFMms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

Static File Info

No static file info

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:42:26.238092899 CET	49717	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:26.238831043 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:26.288625956 CET	443	49717	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:26.288661003 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:26.288800955 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:26.288803101 CET	49717	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:26.289078951 CET	49717	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:26.289304972 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:26.340503931 CET	443	49717	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:26.340550900 CET	443	49718	99.84.90.17	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:42:26.343278885 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:26.343329906 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:26.343451977 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:26.343467951 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:26.343493938 CET	443	49717	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:26.343573093 CET	443	49717	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:26.343621969 CET	443	49717	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:26.343657017 CET	49717	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:26.346580029 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:26.346609116 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:26.346662045 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:26.347229004 CET	443	49717	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:26.347259045 CET	443	49717	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:26.347362041 CET	49717	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:26.386305094 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:26.391747952 CET	49717	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:26.525824070 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:26.526484013 CET	49717	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:26.526597977 CET	49717	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:26.526916027 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:26.527340889 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:26.575666904 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:26.575719118 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:26.575973034 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:26.576288939 CET	443	49717	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:26.576355934 CET	443	49717	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:26.576427937 CET	49717	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:26.576459885 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:26.576751947 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:26.576920033 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:26.617707968 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:26.626487017 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.204870939 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.204925060 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.204955101 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.205003977 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:27.246052027 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:27.265731096 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:27.266134977 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:27.266271114 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:27.266652107 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:27.315717936 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.315849066 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.315865993 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.317184925 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.317212105 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.317231894 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.317301989 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:27.318646908 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.318677902 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.318779945 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:27.320055008 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.320084095 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.320153952 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:27.321476936 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.321495056 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.321563959 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:27.322928905 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.322948933 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.323021889 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:27.324369907 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.324388027 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.324441910 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:27.325787067 CET	443	49718	99.84.90.17	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 21:42:27.325814009 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.325859070 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:27.327250957 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.327274084 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.327702045 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:27.328708887 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.328728914 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.328896999 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:27.330080986 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.330111027 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.330199003 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:27.330580950 CET	49726	443	192.168.2.5	99.84.90.85
Feb 25, 2021 21:42:27.331584930 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.331621885 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.331685066 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:27.333029032 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.333067894 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.333127022 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:27.334460974 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.334501028 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.334573984 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:27.335993052 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.336009026 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.336077929 CET	49718	443	192.168.2.5	99.84.90.17
Feb 25, 2021 21:42:27.337327003 CET	443	49718	99.84.90.17	192.168.2.5
Feb 25, 2021 21:42:27.337349892 CET	443	49718	99.84.90.17	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 21:42:26.172132015 CET	192.168.2.5	8.8.8.8	0xe856	Standard query (0)	doc.clickup.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:27.268398046 CET	192.168.2.5	8.8.8.8	0xc1e2	Standard query (0)	scripts.attributionapp.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:27.922401905 CET	192.168.2.5	8.8.8.8	0x1343	Standard query (0)	app.clickup.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:28.765005112 CET	192.168.2.5	8.8.8.8	0x2144	Standard query (0)	t8666708.p.clickup-attachments.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:29.481724024 CET	192.168.2.5	8.8.8.8	0x70eb	Standard query (0)	app-cdn.clickup.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:29.489041090 CET	192.168.2.5	8.8.8.8	0x9551	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:29.759882927 CET	192.168.2.5	8.8.8.8	0x7f40	Standard query (0)	www.google.co.uk	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:31.356863022 CET	192.168.2.5	8.8.8.8	0x4b3e	Standard query (0)	app-cdn.clickup.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:31.469993114 CET	192.168.2.5	8.8.8.8	0x3074	Standard query (0)	t8666708.p.clickup-attachments.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:31.474327087 CET	192.168.2.5	8.8.8.8	0x575c	Standard query (0)	doc.clickup.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:35.498269081 CET	192.168.2.5	8.8.8.8	0x2556	Standard query (0)	pale-small-origami.glitch.me	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:36.768311977 CET	192.168.2.5	8.8.8.8	0xfba5	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:39.013823032 CET	192.168.2.5	8.8.8.8	0x85b4	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:40.058558941 CET	192.168.2.5	8.8.8.8	0xe640	Standard query (0)	clickup.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:40.469245911 CET	192.168.2.5	8.8.8.8	0x45fc	Standard query (0)	calendly.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:40.469791889 CET	192.168.2.5	8.8.8.8	0xc805	Standard query (0)	client-registry.mutinycdn.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:40.470383883 CET	192.168.2.5	8.8.8.8	0x7de7	Standard query (0)	www.googleoptimize.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.023523092 CET	192.168.2.5	8.8.8.8	0x2325	Standard query (0)	user-data.mutinycdn.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 21:42:41.212405920 CET	192.168.2.5	8.8.8.8	0xb998	Standard query (0)	clockify.me	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.311317921 CET	192.168.2.5	8.8.8.8	0x7653	Standard query (0)	js.hs-scripts.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.313292980 CET	192.168.2.5	8.8.8.8	0x249d	Standard query (0)	static.hotjar.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.314359903 CET	192.168.2.5	8.8.8.8	0x75e8	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.315165043 CET	192.168.2.5	8.8.8.8	0x3e9c	Standard query (0)	tag.getdrip.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.316066027 CET	192.168.2.5	8.8.8.8	0x8aa4	Standard query (0)	a.quora.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.316667080 CET	192.168.2.5	8.8.8.8	0x7a47	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.401125908 CET	192.168.2.5	8.8.8.8	0xcc3f	Standard query (0)	cdn.firstpromoter.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.403110027 CET	192.168.2.5	8.8.8.8	0x2fc7	Standard query (0)	tracking.g2crowd.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.403772116 CET	192.168.2.5	8.8.8.8	0x6130	Standard query (0)	x.clearbitjs.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.758896112 CET	192.168.2.5	8.8.8.8	0x187	Standard query (0)	fullstory.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:43.454758883 CET	192.168.2.5	8.8.8.8	0xbfe6	Standard query (0)	api.clickup.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:43.492100000 CET	192.168.2.5	8.8.8.8	0xb61c	Standard query (0)	static.ads-twitter.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:43.492664099 CET	192.168.2.5	8.8.8.8	0xaaeb	Standard query (0)	acsbapp.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:43.493263960 CET	192.168.2.5	8.8.8.8	0x787a	Standard query (0)	dx.steelhousemedia.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:44.609813929 CET	192.168.2.5	8.8.8.8	0x9867	Standard query (0)	edge.fullstory.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.388189077 CET	192.168.2.5	8.8.8.8	0x7f3b	Standard query (0)	track.attributionapp.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.401561022 CET	192.168.2.5	8.8.8.8	0x82f	Standard query (0)	api-v2.mutinyhq.io	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.428700924 CET	192.168.2.5	8.8.8.8	0xa217	Standard query (0)	js.hscollectedforms.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.428769112 CET	192.168.2.5	8.8.8.8	0x1eb7	Standard query (0)	js.hs-analytics.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.428782940 CET	192.168.2.5	8.8.8.8	0xaae7	Standard query (0)	js.hs-banner.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.476499081 CET	192.168.2.5	8.8.8.8	0xb95f	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.479944944 CET	192.168.2.5	8.8.8.8	0xb80c	Standard query (0)	q.quora.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.484424114 CET	192.168.2.5	8.8.8.8	0xaab9	Standard query (0)	script.hotjar.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.542380095 CET	192.168.2.5	8.8.8.8	0x7ffe	Standard query (0)	api.exchangeratesapi.io	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.706135988 CET	192.168.2.5	8.8.8.8	0x48be	Standard query (0)	www.redditstatic.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.715708017 CET	192.168.2.5	8.8.8.8	0xb8b1	Standard query (0)	m.servedby-buysellads.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.718822956 CET	192.168.2.5	8.8.8.8	0xa1d1	Standard query (0)	cdn.pdst.fm	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.734823942 CET	192.168.2.5	8.8.8.8	0xf384	Standard query (0)	ob.cheqzone.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.774933100 CET	192.168.2.5	8.8.8.8	0x7470	Standard query (0)	api.getdrip.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.812557936 CET	192.168.2.5	8.8.8.8	0xfc63	Standard query (0)	client.mutinycdn.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.903232098 CET	192.168.2.5	8.8.8.8	0x6604	Standard query (0)	x.clearbit.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.969948053 CET	192.168.2.5	8.8.8.8	0xee48	Standard query (0)	vars.hotjar.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.175178051 CET	192.168.2.5	8.8.8.8	0x7cfd	Standard query (0)	rs.fullstory.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.198348999 CET	192.168.2.5	8.8.8.8	0xd660	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.216073036 CET	192.168.2.5	8.8.8.8	0x1af9	Standard query (0)	t.co	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.281024933 CET	192.168.2.5	8.8.8.8	0x622e	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 21:42:47.636872053 CET	192.168.2.5	8.8.8.8	0x934b	Standard query (0)	forms.hubspot.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.651365042 CET	192.168.2.5	8.8.8.8	0x4f31	Standard query (0)	alb.reddit.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.700424910 CET	192.168.2.5	8.8.8.8	0xa5da	Standard query (0)	us-central1-adaptive-growth.cloudfunctions.net	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:48.167447090 CET	192.168.2.5	8.8.8.8	0xaaed	Standard query (0)	px.steelhousemedia.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:48.462081909 CET	192.168.2.5	8.8.8.8	0xfb21	Standard query (0)	forms.hsforms.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:48.463416100 CET	192.168.2.5	8.8.8.8	0x42d5	Standard query (0)	obs.cheqzone.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:49.146811008 CET	192.168.2.5	8.8.8.8	0x5196	Standard query (0)	pixel2.cheqzone.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:52.031035900 CET	192.168.2.5	8.8.8.8	0x845e	Standard query (0)	ww.steelhousemedia.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:53.717416048 CET	192.168.2.5	8.8.8.8	0x845e	Standard query (0)	ww.steelhousemedia.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:53.723649025 CET	192.168.2.5	8.8.8.8	0x9f1f	Standard query (0)	cx.atdmt.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:56.845679998 CET	192.168.2.5	8.8.8.8	0x6416	Standard query (0)	match.adsrvr.org	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:56.845781088 CET	192.168.2.5	8.8.8.8	0xad0d	Standard query (0)	insight.adsrvr.org	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:00.147733927 CET	192.168.2.5	8.8.8.8	0x8ec1	Standard query (0)	cdn.acsbapp.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:10.670619011 CET	192.168.2.5	8.8.8.8	0x44e5	Standard query (0)	widget.intercom.io	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:11.371197939 CET	192.168.2.5	8.8.8.8	0x2d3d	Standard query (0)	analytics.twitter.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:11.373054028 CET	192.168.2.5	8.8.8.8	0xc8ef	Standard query (0)	track.hubspot.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:12.902142048 CET	192.168.2.5	8.8.8.8	0x7853	Standard query (0)	stackpath.bootstrapcdn.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:19.409336090 CET	192.168.2.5	8.8.8.8	0xd3d1	Standard query (0)	js.intercomcdn.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:22.003029108 CET	192.168.2.5	8.8.8.8	0x6258	Standard query (0)	api-iam.intercom.io	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:23.261621952 CET	192.168.2.5	8.8.8.8	0x4e96	Standard query (0)	nexus-websocket-a.intercom.io	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:31.875437021 CET	192.168.2.5	8.8.8.8	0x7998	Standard query (0)	clickup.com	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:42.798779964 CET	192.168.2.5	8.8.8.8	0x558	Standard query (0)	clockify.me	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.056185007 CET	192.168.2.5	8.8.8.8	0xcb9a	Standard query (0)	match.adsrvr.org	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.075527906 CET	192.168.2.5	8.8.8.8	0xcc3c	Standard query (0)	insight.adsrvr.org	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.546488047 CET	192.168.2.5	8.8.8.8	0x48c1	Standard query (0)	px.steelhousemedia.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:42:26.237025023 CET	8.8.8.8	192.168.2.5	0xe856	No error (0)	doc.clickup.com	dlx6k0k2hv67n.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:26.237025023 CET	8.8.8.8	192.168.2.5	0xe856	No error (0)	dlx6k0k2hv67n.cloudfront.net		99.84.90.17	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:26.237025023 CET	8.8.8.8	192.168.2.5	0xe856	No error (0)	dlx6k0k2hv67n.cloudfront.net		99.84.90.12	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:26.237025023 CET	8.8.8.8	192.168.2.5	0xe856	No error (0)	dlx6k0k2hv67n.cloudfront.net		99.84.90.74	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:26.237025023 CET	8.8.8.8	192.168.2.5	0xe856	No error (0)	dlx6k0k2hv67n.cloudfront.net		99.84.90.19	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:27.328743935 CET	8.8.8.8	192.168.2.5	0xc1e2	No error (0)	scripts.attributionapp.com	d279x8308vq8mj.cloudfront.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:42:27.328743935 CET	8.8.8.8	192.168.2.5	0xc1e2	No error (0)	d279x8308v q8mj.cloud front.net		99.84.90.85	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:27.328743935 CET	8.8.8.8	192.168.2.5	0xc1e2	No error (0)	d279x8308v q8mj.cloud front.net		99.84.90.75	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:27.328743935 CET	8.8.8.8	192.168.2.5	0xc1e2	No error (0)	d279x8308v q8mj.cloud front.net		99.84.90.20	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:27.328743935 CET	8.8.8.8	192.168.2.5	0xc1e2	No error (0)	d279x8308v q8mj.cloud front.net		99.84.90.17	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:27.984090090 CET	8.8.8.8	192.168.2.5	0x1343	No error (0)	app.clickup.com		52.29.76.203	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:27.984090090 CET	8.8.8.8	192.168.2.5	0x1343	No error (0)	app.clickup.com		3.124.219.249	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:27.984090090 CET	8.8.8.8	192.168.2.5	0x1343	No error (0)	app.clickup.com		3.121.50.36	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:28.825757980 CET	8.8.8.8	192.168.2.5	0x2144	No error (0)	t8666708.p .clickup-a ttachments.com		13.227.156.121	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:28.825757980 CET	8.8.8.8	192.168.2.5	0x2144	No error (0)	t8666708.p .clickup-a ttachments.com		13.227.156.57	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:28.825757980 CET	8.8.8.8	192.168.2.5	0x2144	No error (0)	t8666708.p .clickup-a ttachments.com		13.227.156.119	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:28.825757980 CET	8.8.8.8	192.168.2.5	0x2144	No error (0)	t8666708.p .clickup-a ttachments.com		13.227.156.33	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:29.545913935 CET	8.8.8.8	192.168.2.5	0x9551	No error (0)	stats.g.do ubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:29.545913935 CET	8.8.8.8	192.168.2.5	0x9551	No error (0)	stats.l.do ubleclick.net		74.125.71.157	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:29.545913935 CET	8.8.8.8	192.168.2.5	0x9551	No error (0)	stats.l.do ubleclick.net		74.125.71.156	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:29.545913935 CET	8.8.8.8	192.168.2.5	0x9551	No error (0)	stats.l.do ubleclick.net		74.125.71.155	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:29.545913935 CET	8.8.8.8	192.168.2.5	0x9551	No error (0)	stats.l.do ubleclick.net		74.125.71.154	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:29.546988964 CET	8.8.8.8	192.168.2.5	0x70eb	No error (0)	app-cdn.cl ickup.com	d5txjkmyderx.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:29.546988964 CET	8.8.8.8	192.168.2.5	0x70eb	No error (0)	d5txjkmyde rx.cloudfront.net		13.227.156.8	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:29.546988964 CET	8.8.8.8	192.168.2.5	0x70eb	No error (0)	d5txjkmyde rx.cloudfront.net		13.227.156.19	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:29.546988964 CET	8.8.8.8	192.168.2.5	0x70eb	No error (0)	d5txjkmyde rx.cloudfront.net		13.227.156.66	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:29.546988964 CET	8.8.8.8	192.168.2.5	0x70eb	No error (0)	d5txjkmyde rx.cloudfront.net		13.227.156.87	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:29.820343971 CET	8.8.8.8	192.168.2.5	0x7f40	No error (0)	www.google .co.uk		142.250.184.67	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:31.423640013 CET	8.8.8.8	192.168.2.5	0x4b3e	No error (0)	app-cdn.cl ickup.com	d5txjkmyderx.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:31.423640013 CET	8.8.8.8	192.168.2.5	0x4b3e	No error (0)	d5txjkmyde rx.cloudfront.net		13.227.156.19	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:31.423640013 CET	8.8.8.8	192.168.2.5	0x4b3e	No error (0)	d5txjkmyde rx.cloudfront.net		13.227.156.87	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:31.423640013 CET	8.8.8.8	192.168.2.5	0x4b3e	No error (0)	d5txjkmyde rx.cloudfront.net		13.227.156.8	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:42:31.423640013 CET	8.8.8.8	192.168.2.5	0x4b3e	No error (0)	d5txjkmyderx.cloudfront.net		13.227.156.66	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:31.524930000 CET	8.8.8.8	192.168.2.5	0x3074	No error (0)	t8666708.p.clickup-attachments.com		13.227.156.121	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:31.524930000 CET	8.8.8.8	192.168.2.5	0x3074	No error (0)	t8666708.p.clickup-attachments.com		13.227.156.119	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:31.524930000 CET	8.8.8.8	192.168.2.5	0x3074	No error (0)	t8666708.p.clickup-attachments.com		13.227.156.57	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:31.524930000 CET	8.8.8.8	192.168.2.5	0x3074	No error (0)	t8666708.p.clickup-attachments.com		13.227.156.33	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:31.539191008 CET	8.8.8.8	192.168.2.5	0x575c	No error (0)	doc.clickup.com	dlx6k0k2hv67n.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:31.539191008 CET	8.8.8.8	192.168.2.5	0x575c	No error (0)	dlx6k0k2hv67n.cloudfront.net		99.84.90.12	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:31.539191008 CET	8.8.8.8	192.168.2.5	0x575c	No error (0)	dlx6k0k2hv67n.cloudfront.net		99.84.90.74	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:31.539191008 CET	8.8.8.8	192.168.2.5	0x575c	No error (0)	dlx6k0k2hv67n.cloudfront.net		99.84.90.19	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:31.539191008 CET	8.8.8.8	192.168.2.5	0x575c	No error (0)	dlx6k0k2hv67n.cloudfront.net		99.84.90.17	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:35.557877064 CET	8.8.8.8	192.168.2.5	0x2556	No error (0)	pale-small-origami.glitch.me		18.215.10.11	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:35.557877064 CET	8.8.8.8	192.168.2.5	0x2556	No error (0)	pale-small-origami.glitch.me		34.196.60.73	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:35.557877064 CET	8.8.8.8	192.168.2.5	0x2556	No error (0)	pale-small-origami.glitch.me		52.22.118.126	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:35.557877064 CET	8.8.8.8	192.168.2.5	0x2556	No error (0)	pale-small-origami.glitch.me		54.237.41.217	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:36.822787046 CET	8.8.8.8	192.168.2.5	0xfba5	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:36.822787046 CET	8.8.8.8	192.168.2.5	0xfba5	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:39.081511021 CET	8.8.8.8	192.168.2.5	0x85b4	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:39.081511021 CET	8.8.8.8	192.168.2.5	0x85b4	No error (0)	googlehosted.l.googleusercontent.com		142.250.184.33	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:40.112551928 CET	8.8.8.8	192.168.2.5	0xe640	No error (0)	clickup.com		13.227.156.22	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:40.112551928 CET	8.8.8.8	192.168.2.5	0xe640	No error (0)	clickup.com		13.227.156.60	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:40.112551928 CET	8.8.8.8	192.168.2.5	0xe640	No error (0)	clickup.com		13.227.156.31	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:40.112551928 CET	8.8.8.8	192.168.2.5	0xe640	No error (0)	clickup.com		13.227.156.62	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:40.526144981 CET	8.8.8.8	192.168.2.5	0x45fc	No error (0)	calendly.com		104.20.248.116	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:40.526144981 CET	8.8.8.8	192.168.2.5	0x45fc	No error (0)	calendly.com		104.20.247.116	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:40.532510042 CET	8.8.8.8	192.168.2.5	0xc805	No error (0)	client-registry.mutinycdn.com	c3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:40.532982111 CET	8.8.8.8	192.168.2.5	0x7de7	No error (0)	www.googleoptimize.com		142.250.184.78	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:42:41.079873085 CET	8.8.8.8	192.168.2.5	0x2325	No error (0)	user-data.mutinycdn.com	c3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:41.282893896 CET	8.8.8.8	192.168.2.5	0xb998	No error (0)	clockify.me		13.227.156.123	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.282893896 CET	8.8.8.8	192.168.2.5	0xb998	No error (0)	clockify.me		13.227.156.21	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.282893896 CET	8.8.8.8	192.168.2.5	0xb998	No error (0)	clockify.me		13.227.156.62	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.282893896 CET	8.8.8.8	192.168.2.5	0xb998	No error (0)	clockify.me		13.227.156.86	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.360299110 CET	8.8.8.8	192.168.2.5	0x7653	No error (0)	js.hs-scripts.com		104.17.211.204	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.360299110 CET	8.8.8.8	192.168.2.5	0x7653	No error (0)	js.hs-scripts.com		104.17.214.204	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.360299110 CET	8.8.8.8	192.168.2.5	0x7653	No error (0)	js.hs-scripts.com		104.17.212.204	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.360299110 CET	8.8.8.8	192.168.2.5	0x7653	No error (0)	js.hs-scripts.com		104.17.213.204	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.360299110 CET	8.8.8.8	192.168.2.5	0x7653	No error (0)	js.hs-scripts.com		104.17.210.204	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.372653008 CET	8.8.8.8	192.168.2.5	0x75e8	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:41.372653008 CET	8.8.8.8	192.168.2.5	0x75e8	No error (0)	scontent.xx.fbcdn.net		31.13.92.14	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.373224974 CET	8.8.8.8	192.168.2.5	0x8aa4	No error (0)	a.quora.com	quora.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:41.373224974 CET	8.8.8.8	192.168.2.5	0x8aa4	No error (0)	quora.map.fastly.net		151.101.1.2	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.373224974 CET	8.8.8.8	192.168.2.5	0x8aa4	No error (0)	quora.map.fastly.net		151.101.65.2	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.373224974 CET	8.8.8.8	192.168.2.5	0x8aa4	No error (0)	quora.map.fastly.net		151.101.129.2	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.373224974 CET	8.8.8.8	192.168.2.5	0x8aa4	No error (0)	quora.map.fastly.net		151.101.193.2	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.378007889 CET	8.8.8.8	192.168.2.5	0x7a47	No error (0)	snap.licdn.com	wildcard.licdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:41.378295898 CET	8.8.8.8	192.168.2.5	0x3e9c	No error (0)	tag.getdrip.com	d10w4ikcrdu13z.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:41.378295898 CET	8.8.8.8	192.168.2.5	0x3e9c	No error (0)	d10w4ikcrdu13z.cloudfront.net		13.227.156.61	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.378295898 CET	8.8.8.8	192.168.2.5	0x3e9c	No error (0)	d10w4ikcrdu13z.cloudfront.net		13.227.156.60	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.378295898 CET	8.8.8.8	192.168.2.5	0x3e9c	No error (0)	d10w4ikcrdu13z.cloudfront.net		13.227.156.37	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.378295898 CET	8.8.8.8	192.168.2.5	0x3e9c	No error (0)	d10w4ikcrdu13z.cloudfront.net		13.227.156.72	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.380584955 CET	8.8.8.8	192.168.2.5	0x249d	No error (0)	static.hotjar.com	static-cdn.hotjar.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:41.380584955 CET	8.8.8.8	192.168.2.5	0x249d	No error (0)	static-cdn.hotjar.com		99.84.90.83	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.380584955 CET	8.8.8.8	192.168.2.5	0x249d	No error (0)	static-cdn.hotjar.com		99.84.90.51	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:42:41.380584955 CET	8.8.8.8	192.168.2.5	0x249d	No error (0)	static-cdn .hotjar.com		99.84.90.95	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.380584955 CET	8.8.8.8	192.168.2.5	0x249d	No error (0)	static-cdn .hotjar.com		99.84.90.16	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.462723017 CET	8.8.8.8	192.168.2.5	0x2fc7	No error (0)	tracking.g 2crowd.com		104.18.27.190	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.462723017 CET	8.8.8.8	192.168.2.5	0x2fc7	No error (0)	tracking.g 2crowd.com		104.18.26.190	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.464698076 CET	8.8.8.8	192.168.2.5	0x6130	No error (0)	x.clearbitjs.com	global-v2.clearbit.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:41.464698076 CET	8.8.8.8	192.168.2.5	0x6130	No error (0)	global-v2. clearbit.com		18.134.247.58	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.464698076 CET	8.8.8.8	192.168.2.5	0x6130	No error (0)	global-v2. clearbit.com		18.135.140.129	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.471133947 CET	8.8.8.8	192.168.2.5	0xcc3f	No error (0)	cdn.firstp romoter.com	d2ycxbs0cq3yaz.cloudfro nt.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:41.471133947 CET	8.8.8.8	192.168.2.5	0xcc3f	No error (0)	d2ycxbs0cq 3yaz.cloud front.net		13.227.156.87	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.471133947 CET	8.8.8.8	192.168.2.5	0xcc3f	No error (0)	d2ycxbs0cq 3yaz.cloud front.net		13.227.156.28	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.471133947 CET	8.8.8.8	192.168.2.5	0xcc3f	No error (0)	d2ycxbs0cq 3yaz.cloud front.net		13.227.156.13	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.471133947 CET	8.8.8.8	192.168.2.5	0xcc3f	No error (0)	d2ycxbs0cq 3yaz.cloud front.net		13.227.156.73	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:41.816119909 CET	8.8.8.8	192.168.2.5	0x187	No error (0)	fullstory.com		34.107.252.72	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:43.510915995 CET	8.8.8.8	192.168.2.5	0xbfe6	No error (0)	api.clickup.com		52.58.150.147	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:43.510915995 CET	8.8.8.8	192.168.2.5	0xbfe6	No error (0)	api.clickup.com		18.198.102.107	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:43.510915995 CET	8.8.8.8	192.168.2.5	0xbfe6	No error (0)	api.clickup.com		52.29.203.165	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:43.541543007 CET	8.8.8.8	192.168.2.5	0xaaeb	No error (0)	acsbapp.com		167.172.136.187	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:43.541543007 CET	8.8.8.8	192.168.2.5	0xaaeb	No error (0)	acsbapp.com		208.68.39.149	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:43.541543007 CET	8.8.8.8	192.168.2.5	0xaaeb	No error (0)	acsbapp.com		161.35.15.77	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:43.544558048 CET	8.8.8.8	192.168.2.5	0xb61c	No error (0)	static.ads- twitter.com	platform.twitter.map.fastly .net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:43.544558048 CET	8.8.8.8	192.168.2.5	0xb61c	No error (0)	platform.t witter.map .fastly.net		151.101.12.157	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:43.545532942 CET	8.8.8.8	192.168.2.5	0x787a	No error (0)	dx.steelho usemedia.com		44.241.10.203	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:43.545532942 CET	8.8.8.8	192.168.2.5	0x787a	No error (0)	dx.steelho usemedia.com		44.236.162.197	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:43.545532942 CET	8.8.8.8	192.168.2.5	0x787a	No error (0)	dx.steelho usemedia.com		52.11.37.91	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:43.545532942 CET	8.8.8.8	192.168.2.5	0x787a	No error (0)	dx.steelho usemedia.com		54.69.84.146	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:44.664314032 CET	8.8.8.8	192.168.2.5	0x9867	No error (0)	edge.fulls tory.com		35.201.112.186	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:42:46.447938919 CET	8.8.8.8	192.168.2.5	0x7f3b	No error (0)	track.attr ibutionapp.com	nara-9228.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:46.447938919 CET	8.8.8.8	192.168.2.5	0x7f3b	No error (0)	nara-9228. herokussl.com	elb046299-1187644484.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:46.447938919 CET	8.8.8.8	192.168.2.5	0x7f3b	No error (0)	elb046299-1187644484.us-east-1 .elb.amazo naws.com		54.225.168.201	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.447938919 CET	8.8.8.8	192.168.2.5	0x7f3b	No error (0)	elb046299-1187644484.us-east-1 .elb.amazo naws.com		54.225.178.50	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.447938919 CET	8.8.8.8	192.168.2.5	0x7f3b	No error (0)	elb046299-1187644484.us-east-1 .elb.amazo naws.com		54.243.135.228	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.453624964 CET	8.8.8.8	192.168.2.5	0x82f	No error (0)	api-v2.mut inyhq.io	gentle-meadow-3800.shrouded-lake-4691.herokuspace.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:46.453624964 CET	8.8.8.8	192.168.2.5	0x82f	No error (0)	gentle-meadow-3800.shrouded-lake-4691.he rokuspace.com		34.210.168.131	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.453624964 CET	8.8.8.8	192.168.2.5	0x82f	No error (0)	gentle-meadow-3800.shrouded-lake-4691.he rokuspace.com		52.24.29.205	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.477760077 CET	8.8.8.8	192.168.2.5	0x1eb7	No error (0)	js.hs-anal ytics.net		104.17.70.176	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.477760077 CET	8.8.8.8	192.168.2.5	0x1eb7	No error (0)	js.hs-anal ytics.net		104.17.67.176	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.477760077 CET	8.8.8.8	192.168.2.5	0x1eb7	No error (0)	js.hs-anal ytics.net		104.17.71.176	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.477760077 CET	8.8.8.8	192.168.2.5	0x1eb7	No error (0)	js.hs-anal ytics.net		104.17.68.176	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.477760077 CET	8.8.8.8	192.168.2.5	0x1eb7	No error (0)	js.hs-anal ytics.net		104.17.69.176	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.480170965 CET	8.8.8.8	192.168.2.5	0xaae7	No error (0)	js.hs-bann er.com		104.18.21.191	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.480170965 CET	8.8.8.8	192.168.2.5	0xaae7	No error (0)	js.hs-bann er.com		104.18.20.191	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.490906000 CET	8.8.8.8	192.168.2.5	0xa217	No error (0)	js.hscolle ctedforms.net		104.17.130.171	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.490906000 CET	8.8.8.8	192.168.2.5	0xa217	No error (0)	js.hscolle ctedforms.net		104.17.127.171	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.490906000 CET	8.8.8.8	192.168.2.5	0xa217	No error (0)	js.hscolle ctedforms.net		104.17.131.171	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.490906000 CET	8.8.8.8	192.168.2.5	0xa217	No error (0)	js.hscolle ctedforms.net		104.17.128.171	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.490906000 CET	8.8.8.8	192.168.2.5	0xa217	No error (0)	js.hscolle ctedforms.net		104.17.129.171	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.525245905 CET	8.8.8.8	192.168.2.5	0xb95f	No error (0)	px.ads.lin kedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:46.525245905 CET	8.8.8.8	192.168.2.5	0xb95f	No error (0)	mix.linkedin.com	glb-na.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:46.525245905 CET	8.8.8.8	192.168.2.5	0xb95f	No error (0)	glb-na.mix .linkedin.com	pop-eda6.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:46.525245905 CET	8.8.8.8	192.168.2.5	0xb95f	No error (0)	pop-eda6.m ix.linkedin.com		108.174.11.69	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:42:46.528635025 CET	8.8.8.8	192.168.2.5	0xb80c	No error (0)	q.quora.com		50.17.2.180	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.528635025 CET	8.8.8.8	192.168.2.5	0xb80c	No error (0)	q.quora.com		3.217.219.88	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.528635025 CET	8.8.8.8	192.168.2.5	0xb80c	No error (0)	q.quora.com		3.214.152.179	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.528635025 CET	8.8.8.8	192.168.2.5	0xb80c	No error (0)	q.quora.com		3.213.100.238	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.528635025 CET	8.8.8.8	192.168.2.5	0xb80c	No error (0)	q.quora.com		3.230.50.184	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.528635025 CET	8.8.8.8	192.168.2.5	0xb80c	No error (0)	q.quora.com		3.227.227.165	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.528635025 CET	8.8.8.8	192.168.2.5	0xb80c	No error (0)	q.quora.com		3.225.115.141	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.537035942 CET	8.8.8.8	192.168.2.5	0xaab9	No error (0)	script.hotjar.com		99.84.90.20	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.537035942 CET	8.8.8.8	192.168.2.5	0xaab9	No error (0)	script.hotjar.com		99.84.90.74	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.537035942 CET	8.8.8.8	192.168.2.5	0xaab9	No error (0)	script.hotjar.com		99.84.90.72	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.537035942 CET	8.8.8.8	192.168.2.5	0xaab9	No error (0)	script.hotjar.com		99.84.90.43	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.592859030 CET	8.8.8.8	192.168.2.5	0x7ffe	No error (0)	api.exchangeratesapi.io		172.67.74.213	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.592859030 CET	8.8.8.8	192.168.2.5	0x7ffe	No error (0)	api.exchangeratesapi.io		104.26.9.91	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.592859030 CET	8.8.8.8	192.168.2.5	0x7ffe	No error (0)	api.exchangeratesapi.io		104.26.8.91	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.766563892 CET	8.8.8.8	192.168.2.5	0xb8b1	No error (0)	m.servedby-buysellads.com	monetization-framework.bsa.netdna-cdn.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:46.766563892 CET	8.8.8.8	192.168.2.5	0xb8b1	No error (0)	monetization-framework.bsa.netdna-cdn.com		108.161.189.78	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.767903090 CET	8.8.8.8	192.168.2.5	0x48be	No error (0)	www.redditstatic.com	reddit.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:46.767903090 CET	8.8.8.8	192.168.2.5	0x48be	No error (0)	reddit.map.fastly.net		151.101.1.140	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.767903090 CET	8.8.8.8	192.168.2.5	0x48be	No error (0)	reddit.map.fastly.net		151.101.65.140	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.767903090 CET	8.8.8.8	192.168.2.5	0x48be	No error (0)	reddit.map.fastly.net		151.101.129.140	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.767903090 CET	8.8.8.8	192.168.2.5	0x48be	No error (0)	reddit.map.fastly.net		151.101.193.140	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.777945995 CET	8.8.8.8	192.168.2.5	0xa1d1	No error (0)	cdn.pdst.fm		35.244.142.80	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.798732042 CET	8.8.8.8	192.168.2.5	0xf384	No error (0)	ob.cheqzone.com	cheqzone2.b-cdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:46.798732042 CET	8.8.8.8	192.168.2.5	0xf384	No error (0)	cheqzone2.b-cdn.net		89.187.165.193	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.827244043 CET	8.8.8.8	192.168.2.5	0x7470	No error (0)	api.getdrip.com		13.227.156.11	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.827244043 CET	8.8.8.8	192.168.2.5	0x7470	No error (0)	api.getdrip.com		13.227.156.15	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:42:46.827244043 CET	8.8.8.8	192.168.2.5	0x7470	No error (0)	api.getdrip.com		13.227.156.95	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.827244043 CET	8.8.8.8	192.168.2.5	0x7470	No error (0)	api.getdrip.com		13.227.156.34	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.875288963 CET	8.8.8.8	192.168.2.5	0xfc63	No error (0)	client.mutinycdn.com		99.84.90.13	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.875288963 CET	8.8.8.8	192.168.2.5	0xfc63	No error (0)	client.mutinycdn.com		99.84.90.73	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.875288963 CET	8.8.8.8	192.168.2.5	0xfc63	No error (0)	client.mutinycdn.com		99.84.90.125	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.875288963 CET	8.8.8.8	192.168.2.5	0xfc63	No error (0)	client.mutinycdn.com		99.84.90.93	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.962918043 CET	8.8.8.8	192.168.2.5	0x6604	No error (0)	x.clearbit.com		18.134.247.58	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:46.962918043 CET	8.8.8.8	192.168.2.5	0x6604	No error (0)	x.clearbit.com		18.135.140.129	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.021878958 CET	8.8.8.8	192.168.2.5	0xee48	No error (0)	vars.hotjar.com		99.84.90.32	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.021878958 CET	8.8.8.8	192.168.2.5	0xee48	No error (0)	vars.hotjar.com		99.84.90.31	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.021878958 CET	8.8.8.8	192.168.2.5	0xee48	No error (0)	vars.hotjar.com		99.84.90.109	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.021878958 CET	8.8.8.8	192.168.2.5	0xee48	No error (0)	vars.hotjar.com		99.84.90.87	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.232671022 CET	8.8.8.8	192.168.2.5	0x7cfd	No error (0)	rs.fullstory.com		35.186.194.58	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.257849932 CET	8.8.8.8	192.168.2.5	0xd660	No error (0)	googleads.g.doubleclick.net		142.250.184.34	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.268121004 CET	8.8.8.8	192.168.2.5	0x1af9	No error (0)	t.co		104.244.42.69	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.268121004 CET	8.8.8.8	192.168.2.5	0x1af9	No error (0)	t.co		104.244.42.133	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.268121004 CET	8.8.8.8	192.168.2.5	0x1af9	No error (0)	t.co		104.244.42.5	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.268121004 CET	8.8.8.8	192.168.2.5	0x1af9	No error (0)	t.co		104.244.42.197	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.340432882 CET	8.8.8.8	192.168.2.5	0x622e	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:47.340432882 CET	8.8.8.8	192.168.2.5	0x622e	No error (0)	star-mini.c10r.facebook.com		31.13.92.36	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.689523935 CET	8.8.8.8	192.168.2.5	0x934b	No error (0)	forms.hubspot.com		104.19.154.83	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.689523935 CET	8.8.8.8	192.168.2.5	0x934b	No error (0)	forms.hubspot.com		104.19.155.83	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.701195955 CET	8.8.8.8	192.168.2.5	0x4f31	No error (0)	alb.reddit.com	reddit.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:47.701195955 CET	8.8.8.8	192.168.2.5	0x4f31	No error (0)	reddit.map.fastly.net		151.101.1.140	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.701195955 CET	8.8.8.8	192.168.2.5	0x4f31	No error (0)	reddit.map.fastly.net		151.101.65.140	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.701195955 CET	8.8.8.8	192.168.2.5	0x4f31	No error (0)	reddit.map.fastly.net		151.101.129.140	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:42:47.701195955 CET	8.8.8.8	192.168.2.5	0x4f31	No error (0)	reddit.map.fastly.net		151.101.193.140	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:47.766119003 CET	8.8.8.8	192.168.2.5	0xa5da	No error (0)	us-central1-adaptive-growth.cloudfunctions.net		216.239.36.54	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:48.218941927 CET	8.8.8.8	192.168.2.5	0xaaed	No error (0)	px.steelhousemedia.com		54.245.46.233	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:48.218941927 CET	8.8.8.8	192.168.2.5	0xaaed	No error (0)	px.steelhousemedia.com		52.10.121.135	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:48.218941927 CET	8.8.8.8	192.168.2.5	0xaaed	No error (0)	px.steelhousemedia.com		44.237.157.168	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:48.218941927 CET	8.8.8.8	192.168.2.5	0xaaed	No error (0)	px.steelhousemedia.com		54.244.159.189	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:48.218941927 CET	8.8.8.8	192.168.2.5	0xaaed	No error (0)	px.steelhousemedia.com		44.225.29.129	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:48.519324064 CET	8.8.8.8	192.168.2.5	0xfb21	No error (0)	forms.hsforms.com		104.16.88.5	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:48.519324064 CET	8.8.8.8	192.168.2.5	0xfb21	No error (0)	forms.hsforms.com		104.16.85.5	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:48.519324064 CET	8.8.8.8	192.168.2.5	0xfb21	No error (0)	forms.hsforms.com		104.16.87.5	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:48.519324064 CET	8.8.8.8	192.168.2.5	0xfb21	No error (0)	forms.hsforms.com		104.16.89.5	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:48.519324064 CET	8.8.8.8	192.168.2.5	0xfb21	No error (0)	forms.hsforms.com		104.16.86.5	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:48.531253099 CET	8.8.8.8	192.168.2.5	0x42d5	No error (0)	obs.cheqzone.com		52.45.196.192	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:48.531253099 CET	8.8.8.8	192.168.2.5	0x42d5	No error (0)	obs.cheqzone.com		34.199.234.25	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:48.531253099 CET	8.8.8.8	192.168.2.5	0x42d5	No error (0)	obs.cheqzone.com		35.172.245.152	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:48.531253099 CET	8.8.8.8	192.168.2.5	0x42d5	No error (0)	obs.cheqzone.com		3.227.190.204	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:48.531253099 CET	8.8.8.8	192.168.2.5	0x42d5	No error (0)	obs.cheqzone.com		50.16.211.97	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:48.531253099 CET	8.8.8.8	192.168.2.5	0x42d5	No error (0)	obs.cheqzone.com		54.83.110.109	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:49.198055029 CET	8.8.8.8	192.168.2.5	0x5196	No error (0)	pixel2.cheqzone.com		35.153.6.179	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:49.198055029 CET	8.8.8.8	192.168.2.5	0x5196	No error (0)	pixel2.cheqzone.com		52.22.143.94	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:49.198055029 CET	8.8.8.8	192.168.2.5	0x5196	No error (0)	pixel2.cheqzone.com		52.20.231.122	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:52.102123976 CET	8.8.8.8	192.168.2.5	0x845e	No error (0)	ww.steelhousemedia.com		44.238.130.186	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:52.102123976 CET	8.8.8.8	192.168.2.5	0x845e	No error (0)	ww.steelhousemedia.com		44.238.216.23	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:53.775063992 CET	8.8.8.8	192.168.2.5	0x9f1f	No error (0)	cx.atdmt.com	atlas.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:53.775063992 CET	8.8.8.8	192.168.2.5	0x9f1f	No error (0)	atlas.c10r.facebook.com		31.13.92.2	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:53.776973009 CET	8.8.8.8	192.168.2.5	0x845e	No error (0)	ww.steelhousemedia.com		44.238.216.23	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:42:53.776973009 CET	8.8.8.8	192.168.2.5	0x845e	No error (0)	ww.steelhousemedia.com		44.238.130.186	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:56.897015095 CET	8.8.8.8	192.168.2.5	0x6416	No error (0)	match.adsrvr.org	match-1943069928.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:56.897015095 CET	8.8.8.8	192.168.2.5	0x6416	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		34.249.70.28	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:56.897015095 CET	8.8.8.8	192.168.2.5	0x6416	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		54.228.21.183	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:56.897015095 CET	8.8.8.8	192.168.2.5	0x6416	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		54.228.114.223	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:56.897015095 CET	8.8.8.8	192.168.2.5	0x6416	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		54.154.164.132	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:56.897015095 CET	8.8.8.8	192.168.2.5	0x6416	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.209.120.242	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:56.897015095 CET	8.8.8.8	192.168.2.5	0x6416	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.51.224.103	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:56.897015095 CET	8.8.8.8	192.168.2.5	0x6416	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		34.252.253.152	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:56.897015095 CET	8.8.8.8	192.168.2.5	0x6416	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.214.43.215	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:56.897135973 CET	8.8.8.8	192.168.2.5	0xad0d	No error (0)	insight.adsrvr.org	insight-566961044.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:42:56.897135973 CET	8.8.8.8	192.168.2.5	0xad0d	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		34.251.161.187	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:56.897135973 CET	8.8.8.8	192.168.2.5	0xad0d	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		34.251.61.210	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:56.897135973 CET	8.8.8.8	192.168.2.5	0xad0d	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		52.208.188.183	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:56.897135973 CET	8.8.8.8	192.168.2.5	0xad0d	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		52.50.124.20	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:56.897135973 CET	8.8.8.8	192.168.2.5	0xad0d	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		18.202.193.52	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:56.897135973 CET	8.8.8.8	192.168.2.5	0xad0d	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		54.77.184.190	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:42:56.897135973 CET	8.8.8.8	192.168.2.5	0xad0d	No error (0)	insight-56 6961044.eu-west-1.el b.amazonaw s.com		52.51.124.53	A (IP address)	IN (0x0001)
Feb 25, 2021 21:42:56.897135973 CET	8.8.8.8	192.168.2.5	0xad0d	No error (0)	insight-56 6961044.eu-west-1.el b.amazonaw s.com		18.200.151.216	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:00.198312044 CET	8.8.8.8	192.168.2.5	0x8ec1	No error (0)	cdn.acsbap p.com	acsbapp.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:43:00.198312044 CET	8.8.8.8	192.168.2.5	0x8ec1	No error (0)	acsbapp.com		161.35.15.77	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:00.198312044 CET	8.8.8.8	192.168.2.5	0x8ec1	No error (0)	acsbapp.com		167.172.136.187	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:00.198312044 CET	8.8.8.8	192.168.2.5	0x8ec1	No error (0)	acsbapp.com		208.68.39.149	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:10.732172966 CET	8.8.8.8	192.168.2.5	0x44e5	No error (0)	widget.int ercom.io		99.84.90.9	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:10.732172966 CET	8.8.8.8	192.168.2.5	0x44e5	No error (0)	widget.int ercom.io		99.84.90.99	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:10.732172966 CET	8.8.8.8	192.168.2.5	0x44e5	No error (0)	widget.int ercom.io		99.84.90.53	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:10.732172966 CET	8.8.8.8	192.168.2.5	0x44e5	No error (0)	widget.int ercom.io		99.84.90.63	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:11.422032118 CET	8.8.8.8	192.168.2.5	0xc8ef	No error (0)	track.hubs pot.com		104.19.155.83	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:11.422032118 CET	8.8.8.8	192.168.2.5	0xc8ef	No error (0)	track.hubs pot.com		104.19.154.83	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:11.422446012 CET	8.8.8.8	192.168.2.5	0x2d3d	No error (0)	analytics. twitter.com	ads.twitter.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:43:11.422446012 CET	8.8.8.8	192.168.2.5	0x2d3d	No error (0)	ads.twitter.com	s.twitter.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:43:11.422446012 CET	8.8.8.8	192.168.2.5	0x2d3d	No error (0)	s.twitter.com		104.244.42.67	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:11.422446012 CET	8.8.8.8	192.168.2.5	0x2d3d	No error (0)	s.twitter.com		104.244.42.195	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:11.422446012 CET	8.8.8.8	192.168.2.5	0x2d3d	No error (0)	s.twitter.com		104.244.42.3	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:11.422446012 CET	8.8.8.8	192.168.2.5	0x2d3d	No error (0)	s.twitter.com		104.244.42.131	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:12.950604916 CET	8.8.8.8	192.168.2.5	0x7853	No error (0)	stackpath. bootstrapc dn.com	cds.j3z9t3p6.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:43:19.469897985 CET	8.8.8.8	192.168.2.5	0xd3d1	No error (0)	js.interco mcdn.com		99.84.90.89	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:19.469897985 CET	8.8.8.8	192.168.2.5	0xd3d1	No error (0)	js.interco mcdn.com		99.84.90.42	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:19.469897985 CET	8.8.8.8	192.168.2.5	0xd3d1	No error (0)	js.interco mcdn.com		99.84.90.68	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:19.469897985 CET	8.8.8.8	192.168.2.5	0xd3d1	No error (0)	js.interco mcdn.com		99.84.90.5	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:22.054267883 CET	8.8.8.8	192.168.2.5	0x6258	No error (0)	api-iam.in tercom.io		99.83.219.81	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:22.054267883 CET	8.8.8.8	192.168.2.5	0x6258	No error (0)	api-iam.in tercom.io		75.2.88.188	A (IP address)	IN (0x0001)

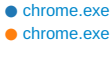
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:43:23.310368061 CET	8.8.8.8	192.168.2.5	0x4e96	No error (0)	nexus-websocket-a.intercom.io		35.174.127.31	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:23.310368061 CET	8.8.8.8	192.168.2.5	0x4e96	No error (0)	nexus-websocket-a.intercom.io		35.170.0.145	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:23.310368061 CET	8.8.8.8	192.168.2.5	0x4e96	No error (0)	nexus-websocket-a.intercom.io		34.237.73.95	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:31.924320936 CET	8.8.8.8	192.168.2.5	0x7998	No error (0)	clickup.com		13.227.156.22	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:31.924320936 CET	8.8.8.8	192.168.2.5	0x7998	No error (0)	clickup.com		13.227.156.60	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:31.924320936 CET	8.8.8.8	192.168.2.5	0x7998	No error (0)	clickup.com		13.227.156.31	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:31.924320936 CET	8.8.8.8	192.168.2.5	0x7998	No error (0)	clickup.com		13.227.156.62	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:42.893318892 CET	8.8.8.8	192.168.2.5	0x558	No error (0)	clockify.me		13.227.156.123	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:42.893318892 CET	8.8.8.8	192.168.2.5	0x558	No error (0)	clockify.me		13.227.156.21	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:42.893318892 CET	8.8.8.8	192.168.2.5	0x558	No error (0)	clockify.me		13.227.156.86	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:42.893318892 CET	8.8.8.8	192.168.2.5	0x558	No error (0)	clockify.me		13.227.156.62	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.104943991 CET	8.8.8.8	192.168.2.5	0xcb9a	No error (0)	match.adsrvr.org	match-1943069928.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 21:43:47.104943991 CET	8.8.8.8	192.168.2.5	0xcb9a	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		54.228.114.223	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.104943991 CET	8.8.8.8	192.168.2.5	0xcb9a	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		34.246.156.173	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.104943991 CET	8.8.8.8	192.168.2.5	0xcb9a	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		54.216.86.107	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.104943991 CET	8.8.8.8	192.168.2.5	0xcb9a	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.16.108.17	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.104943991 CET	8.8.8.8	192.168.2.5	0xcb9a	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		99.80.71.186	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.104943991 CET	8.8.8.8	192.168.2.5	0xcb9a	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		54.72.52.19	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.104943991 CET	8.8.8.8	192.168.2.5	0xcb9a	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		63.32.128.23	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.104943991 CET	8.8.8.8	192.168.2.5	0xcb9a	No error (0)	match-1943069928.eu-west-1.elb.amazonaws.com		52.209.120.242	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.124418974 CET	8.8.8.8	192.168.2.5	0xcc3c	No error (0)	insight.adsrvr.org	insight-566961044.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 21:43:47.124418974 CET	8.8.8.8	192.168.2.5	0xcc3c	No error (0)	insight-56 6961044.eu-west-1.el b.amazonaw s.com		54.77.184.190	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.124418974 CET	8.8.8.8	192.168.2.5	0xcc3c	No error (0)	insight-56 6961044.eu-west-1.el b.amazonaw s.com		18.200.151.216	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.124418974 CET	8.8.8.8	192.168.2.5	0xcc3c	No error (0)	insight-56 6961044.eu-west-1.el b.amazonaw s.com		52.49.200.205	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.124418974 CET	8.8.8.8	192.168.2.5	0xcc3c	No error (0)	insight-56 6961044.eu-west-1.el b.amazonaw s.com		52.208.188.183	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.124418974 CET	8.8.8.8	192.168.2.5	0xcc3c	No error (0)	insight-56 6961044.eu-west-1.el b.amazonaw s.com		52.50.124.20	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.124418974 CET	8.8.8.8	192.168.2.5	0xcc3c	No error (0)	insight-56 6961044.eu-west-1.el b.amazonaw s.com		34.251.61.210	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.124418974 CET	8.8.8.8	192.168.2.5	0xcc3c	No error (0)	insight-56 6961044.eu-west-1.el b.amazonaw s.com		34.251.161.187	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.124418974 CET	8.8.8.8	192.168.2.5	0xcc3c	No error (0)	insight-56 6961044.eu-west-1.el b.amazonaw s.com		52.51.124.53	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.600156069 CET	8.8.8.8	192.168.2.5	0x48c1	No error (0)	px.steelho usemedia.com		44.237.157.168	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.600156069 CET	8.8.8.8	192.168.2.5	0x48c1	No error (0)	px.steelho usemedia.com		54.244.159.189	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.600156069 CET	8.8.8.8	192.168.2.5	0x48c1	No error (0)	px.steelho usemedia.com		54.245.46.233	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.600156069 CET	8.8.8.8	192.168.2.5	0x48c1	No error (0)	px.steelho usemedia.com		44.225.29.129	A (IP address)	IN (0x0001)
Feb 25, 2021 21:43:47.600156069 CET	8.8.8.8	192.168.2.5	0x48c1	No error (0)	px.steelho usemedia.com		52.10.121.135	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 4616 Parent PID: 3560

General

Start time:	21:42:21
Start date:	25/02/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized 'https://doc.clickup.com/d/h/88fjm-14/9b55da9c0a2598a'
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: chrome.exe PID: 5368 Parent PID: 4616

General

Start time:	21:42:23
Start date:	25/02/2021
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=1612,2893176907998818176,3513762577707477399,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1672 /prefetch:8
Imagebase:	0x7ff677c70000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

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

Disassembly