ID: 452269
Cookbook: browseurl.jbs
Time: 02:51:32
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

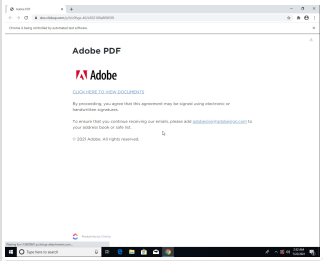
Windows Analysis Report https://doc.clickup.com/p/h/c…

Overview

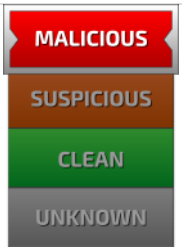
General Information

Sample URL:	http://https://doc.clickup.com/p/h/c0hgx-46/b302180a8f685f8
Analysis ID:	452269
Infos:	

Most interesting Screenshot:



Detection



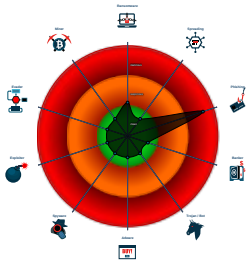
HTMLPhisher

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Phishing site detected (based on sh…
- Yara detected HtmlPhish10
- Yara detected HtmlPhish7
- Form action URLs do not match mai…
- Found iframes
- HTML body contains low number of …

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 5712 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://doc.clickup.com/p/h/c0hgx-46/b302180a8f685f8' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 3484 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1576,9348279836173803146,15535106751469244526,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1700 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:

Phishing site detected (based on shot template match)

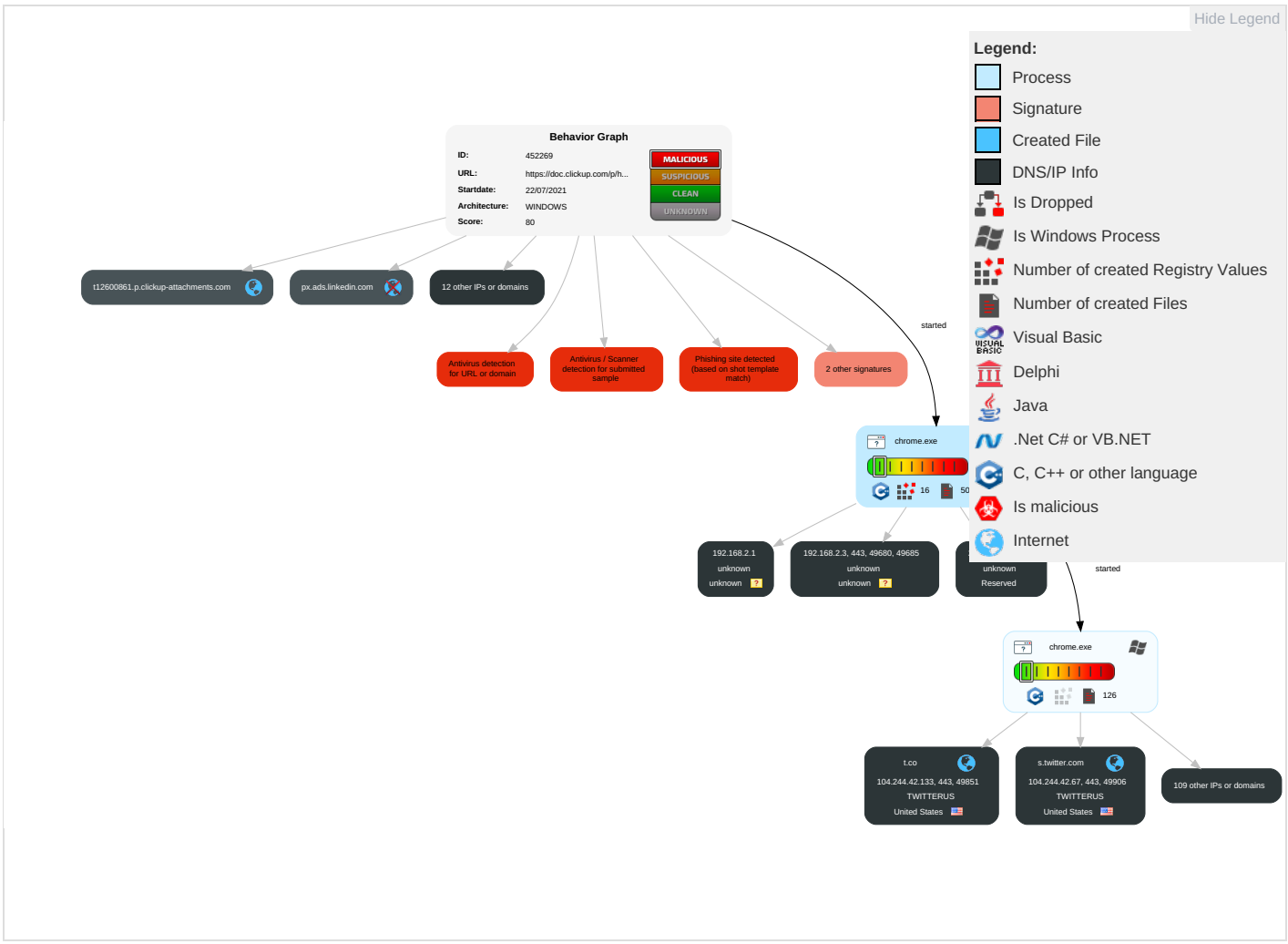
Yara detected HtmlPhish10

Yara detected HtmlPhish7

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
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
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 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
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 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap	

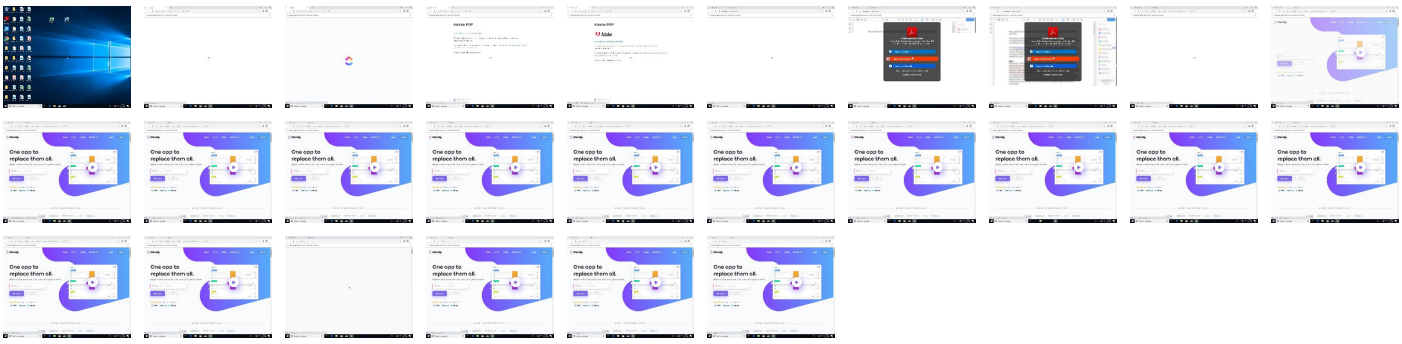
Behavior Graph

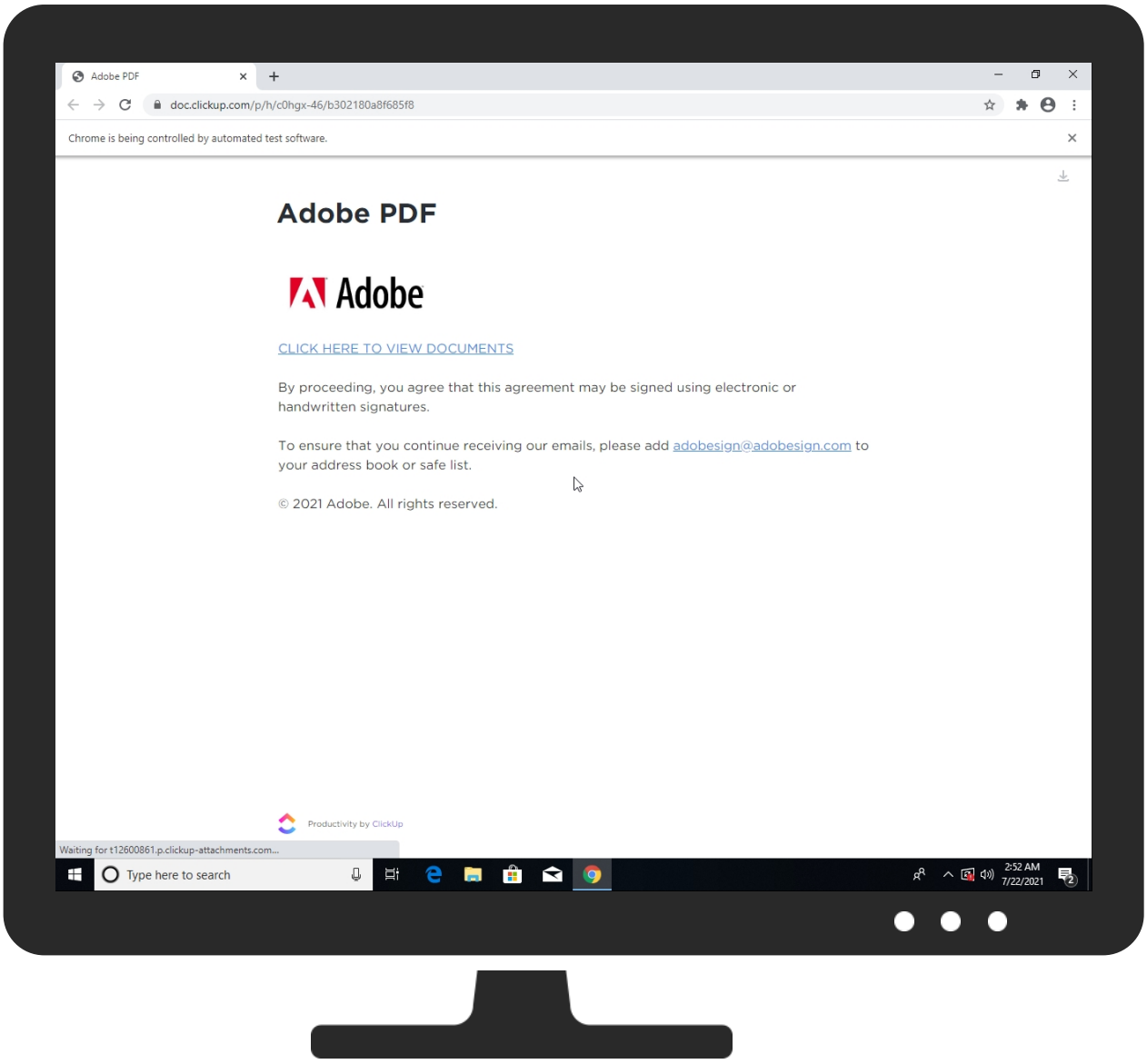


Screenshots

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/p/h/c0hgx-46/b302180a8f685f8	0%	Virustotal		Browse
http://https://doc.clickup.com/p/h/c0hgx-46/b302180a8f685f8	0%	Avira URL Cloud	safe	
http://https://doc.clickup.com/p/h/c0hgx-46/b302180a8f685f8	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://https://mega-sharedrives.club/data/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://mega-sharedrives.club/dataShare	0%	Avira URL Cloud	safe	
http://https://clickup.comh	0%	Avira URL Cloud	safe	
http://https://mega-sharedrives.club/	0%	Avira URL Cloud	safe	
http://https://js.hs-banner.com/6613321.js	0%	Avira URL Cloud	safe	
http://https://mega-sharedrives.club/data	0%	Avira URL Cloud	safe	
http://https://mega-sharedrives.club/dataShare	0%	Avira URL Cloud	safe	
http://https://js.hs-analytics.net/analytics/1626915000000/6613321.js	0%	Avira URL Cloud	safe	
http://https://www.intercom-reporting.com/sentry/index.html	0%	Avira URL Cloud	safe	
http://https://www.googleoptimize.com/optimize.js?id=GTM-PBLF7VJ	0%	Avira URL Cloud	safe	
http://https://surveystats.hotjar.io/hit	0%	URL Reputation	safe	
http://https://surveystats.hotjar.io/hit	0%	URL Reputation	safe	
http://https://surveystats.hotjar.io/hit	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://mega-sharedrives.club/cQ	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	
http://https://www.intercom-reporting.com	0%	Avira URL Cloud	safe	
http://https://client.mutinycdn.com/mutiny-client/8.2.1.0.js	0%	Avira URL Cloud	safe	
http://app.intercom.test	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	172.217.168.3	true	false		high
forms.hubspot.com	104.19.155.83	true	false		high
clickup.com	13.224.99.47	true	false		high
d10w4ikcrdu13z.cloudfront.net	13.224.99.21	true	false		high
obs.cheqzone.com	3.227.190.204	true	false		unknown
platform.twitter.map.fastly.net	199.232.136.157	true	false		unknown
client.mutinycdn.com	13.224.99.6	true	false		unknown
t.co	104.244.42.133	true	false		high
track.hubspot.com	104.19.154.83	true	false		high
cdnjs.cloudflare.com	104.16.18.94	true	false		high
js.hs-scripts.com	104.17.212.204	true	false		high
dx.steelhousemedia.com	52.11.37.91	true	false		high
ob.cheqzone.com	13.224.99.100	true	false		unknown
tracking.g2crowd.com	104.18.27.190	true	false		high
www.google.com	172.217.168.68	true	false		high
q.quora.com	3.224.194.150	true	false		high
usage.trackjs.com	158.69.52.117	true	false		high
static-cdn.hotjar.com	13.224.99.122	true	false		high
quora.map.fastly.net	151.101.1.2	true	false		unknown
d2ycxbs0cq3yaz.cloudfront.net	13.224.99.29	true	false		high
px.steelhousemedia.com	52.10.121.135	true	false		high
js.intercomcdn.com	13.224.99.12	true	false		high
js.hs-banner.com	104.18.20.191	true	false		unknown
star-mini.c10r.facebook.com	157.240.17.35	true	false		high
fluffy-alpaca-j1w7zdv61tmqz86b33z4c6tl.herokudns.com	52.45.121.249	true	false		unknown
stats.l.doubleclick.net	108.177.126.156	true	false		high
s.twitter.com	104.244.42.67	true	false		high
ww.steelhousemedia.com	44.238.216.23	true	false		high
monetization-framework.bsa.netdna-cdn.com	108.161.189.78	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
edge.fullstory.com	35.201.112.186	true	false		high
api-iam.intercom.io	99.83.219.81	true	false		high
www.googleoptimize.com	142.250.203.110	true	false		unknown
insight-566961044.eu-west-1.elb.amazonaws.com	52.50.64.214	true	false		high
t12600861.p.clickup-attachments.com	13.224.99.60	true	false		unknown
clockify.me	13.224.99.4	true	false		high
in-live.live.eks.hotjar.com	63.32.233.146	true	false		high
reddit.map.fastly.net	151.101.1.140	true	false		unknown
googleads.g.doubleclick.net	172.217.168.2	true	false		high
prod.appnexus.map.fastly.net	151.101.1.108	true	false		unknown
clients.l.google.com	142.250.185.142	true	false		high
calendly.com	104.20.247.116	true	false		high
googlehosted.l.googleusercontent.com	142.250.203.97	true	false		high
d5txjkmyderx.cloudfront.net	13.224.99.77	true	false		high
forms.hsforms.com	104.16.86.5	true	false		unknown
a97adde81b00f2ca4.awsglobalaccelerator.com	13.248.242.197	true	false		unknown
global-v2.clearbit.com	18.168.223.221	true	false		high
js.hs-analytics.net	104.17.70.176	true	false		unknown
api.exchangeratesapi.io	104.26.8.91	true	false		unknown
x.clearbit.com	18.134.49.160	true	false		high
pop-edc2.mix.linkedin.com	108.174.11.85	true	false		high
us-central1-adaptive-growth.cloudfunctions.net	216.239.36.54	true	false		unknown
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
script.hotjar.com	13.224.99.26	true	false		high
cdn.pdst.fm	35.244.142.80	true	false		unknown
nexus-websocket-a.intercom.io	35.170.0.145	true	false		high
www.google.de	172.217.168.3	true	false		high
accounts.google.com	172.217.168.45	true	false		high
www-google-analytics.l.google.com	216.58.215.238	true	false		high
ws.zoominfo.com	104.16.168.82	true	false		high
www-googletagmanager.l.google.com	172.217.168.8	true	false		high
widget.intercom.io	13.224.99.107	true	false		high
api.clickup.com	3.124.156.213	true	false		high
mega-sharedrives.club	66.29.132.95	true	false		unknown
d279x8308vq8mj.cloudfront.net	13.224.99.54	true	false		high
doc-cdn.clickup.com	13.224.99.46	true	false		high
vars.hotjar.com	13.224.99.33	true	false		high
gentle-meadow-3800.shrouded-lake-4691.herokuspace.com	50.112.148.251	true	false		unknown
rs.fullstory.com	35.186.194.58	true	false		high
api.getdrip.com	13.224.99.3	true	false		high
app.clickup.com	3.125.16.43	true	false		high
ib.anycast.adnxs.com	185.33.220.244	true	false		high
js.hscollectedforms.net	104.17.129.171	true	false		unknown
alb.reddit.com	unknown	unknown	false		high
static.ads-twitter.com	unknown	unknown	false		unknown
ka-f.fontawesome.com	unknown	unknown	false		high
app-cdn.clickup.com	unknown	unknown	false		high
stats.g.doubleclick.net	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
static.hotjar.com	unknown	unknown	false		high
match.adsrvr.org	unknown	unknown	false		high
www.redditstatic.com	unknown	unknown	false		high
acdn.adnxs.com	unknown	unknown	false		high
kit.fontawesome.com	unknown	unknown	false		high
doc.clickup.com	unknown	unknown	false		high
px.ads.linkedin.com	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
a.quora.com	unknown	unknown	false		high
in.hotjar.com	unknown	unknown	false		high
tag.getdrip.com	unknown	unknown	false		high
x.clearbitjs.com	unknown	unknown	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.firstpromoter.com	unknown	unknown	false		high
insight.adsrvr.org	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
scripts.attributionapp.com	unknown	unknown	false		high
track.attributionapp.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

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.19.155.83	forms.hubspot.com	United States		13335	CLOUDFLARENETUS	false
216.58.215.238	www-google-analytics.l.google.com	United States		15169	GOOGLEUS	false
35.186.194.58	rs.fullstory.com	United States		15169	GOOGLEUS	false
104.18.20.191	js.hs-banner.com	United States		13335	CLOUDFLARENETUS	false
157.240.17.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.203.97	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
3.124.156.213	api.clickup.com	United States		16509	AMAZON-02US	false
13.224.99.29	d2ycxbs0cq3yaz.cloudfront.net	United States		16509	AMAZON-02US	false
151.101.1.2	quora.map.fastly.net	United States		54113	FASTLYUS	false
108.177.126.156	stats.l.doubleclick.net	United States		15169	GOOGLEUS	false
142.250.185.142	clients.l.google.com	United States		15169	GOOGLEUS	false
108.174.11.85	pop-edc2.mix.linkedin.com	United States		14413	LINKEDINUS	false
13.224.99.26	script.hotjar.com	United States		16509	AMAZON-02US	false
66.29.132.95	mega-sharedrives.club	United States		19538	ADVANTAGECOMUS	false
13.224.99.60	t12600861.p.clickup-attachments.com	United States		16509	AMAZON-02US	false
104.16.18.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
13.224.99.21	d10w4ikcrdu13z.cloudfront.net	United States		16509	AMAZON-02US	false
185.33.220.244	ib.anycast.adnxs.com	Netherlands		29990	ASN-APPNEXUS	false
18.168.223.221	global-v2.clearbit.com	United States		3	MIT-GATEWAYSUS	false
44.238.216.23	ww.steelhousemedia.com	United States		16509	AMAZON-02US	false
104.19.154.83	track.hubspot.com	United States		13335	CLOUDFLARENETUS	false
104.244.42.133	t.co	United States		13414	TWITTERUS	false
172.217.168.2	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
50.112.148.251	gentle-meadow-3800.shrouded-lake-4691.herokuspace.com	United States		16509	AMAZON-02US	false
63.32.233.146	in-live.live.eks.hotjar.com	United States		16509	AMAZON-02US	false
13.224.99.77	d5txjkmyderx.cloudfront.net	United States		16509	AMAZON-02US	false
13.224.99.33	vars.hotjar.com	United States		16509	AMAZON-02US	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
104.16.86.5	forms.hsforms.com	United States		13335	CLOUDFLARENETUS	false
216.239.36.54	us-central1-adaptive-growth.cloudfunctions.net	United States		15169	GOOGLEUS	false
18.184.109.158	unknown	United States		16509	AMAZON-02US	false
13.224.99.122	static-cdn.hotjar.com	United States		16509	AMAZON-02US	false
52.50.64.214	insight-566961044.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
158.69.52.117	usage.trackjs.com	Canada		16276	OVHFR	false
104.17.212.204	js.hs-scripts.com	United States		13335	CLOUDFLARENETUS	false
104.17.70.176	js.hs-analytics.net	United States		13335	CLOUDFLARENETUS	false
52.10.121.135	px.steelhousemedia.com	United States		16509	AMAZON-02US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.161.189.78	monetization-framework.bsa.netdna-cdn.com	United States		33438	HIGHWINDS2US	false
142.250.203.110	www.googleoptimize.com	United States		15169	GOOGLEUS	false
35.170.0.145	nexus-websocket-a.intercom.io	United States		14618	AMAZON-AESUS	false
52.11.37.91	dx.steelhousemedia.com	United States		16509	AMAZON-02US	false
13.248.242.197	a97adde81b00f2ca4.awsglobalaccelerator.com	United States		16509	AMAZON-02US	false
18.134.49.160	x.clearbit.com	United States		16509	AMAZON-02US	false
13.224.99.47	clickup.com	United States		16509	AMAZON-02US	false
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
172.217.168.68	www.google.com	United States		15169	GOOGLEUS	false
172.217.168.8	www-googletagmanager.l.google.com	United States		15169	GOOGLEUS	false
13.224.99.46	doc-cdn.clickup.com	United States		16509	AMAZON-02US	false
172.217.168.3	gstaticadssl.l.google.com	United States		15169	GOOGLEUS	false
3.224.194.150	q.quora.com	United States		14618	AMAZON-AESUS	false
104.26.8.91	api.exchangeratesapi.io	United States		13335	CLOUDFLARENETUS	false
3.227.190.204	obs.cheqzone.com	United States		14618	AMAZON-AESUS	false
52.45.121.249	fluffy-alpaca-j1w7zdv61tmqz86b33z4c6tl.herokudns.com	United States		14618	AMAZON-AESUS	false
104.17.129.171	js.hscollectedforms.net	United States		13335	CLOUDFLARENETUS	false
151.101.1.108	prod.appnexus.map.fastly.net	United States		54113	FASTLYUS	false
104.20.247.116	calendly.com	United States		13335	CLOUDFLARENETUS	false
104.244.42.67	s.twitter.com	United States		13414	TWITTERUS	false
13.224.99.6	client.mutinycdn.com	United States		16509	AMAZON-02US	false
99.83.219.81	api-iam.intercom.io	United States		16509	AMAZON-02US	false
151.101.1.140	reddit.map.fastly.net	United States		54113	FASTLYUS	false
13.224.99.3	api.getdrip.com	United States		16509	AMAZON-02US	false
13.224.99.107	widget.intercom.io	United States		16509	AMAZON-02US	false
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
13.224.99.12	js.intercomcdn.com	United States		16509	AMAZON-02US	false
35.201.112.186	edge.fullstory.com	United States		15169	GOOGLEUS	false
104.16.168.82	ws.zoominfo.com	United States		13335	CLOUDFLARENETUS	false
13.224.99.100	ob.cheqzone.com	United States		16509	AMAZON-02US	false
3.125.16.43	app.clickup.com	United States		16509	AMAZON-02US	false
35.244.142.80	cdn.pdst.fm	United States		15169	GOOGLEUS	false
13.224.99.54	d279x8308vq8mj.cloudfront.net	United States		16509	AMAZON-02US	false
104.18.27.190	tracking.g2crowd.com	United States		13335	CLOUDFLARENETUS	false
199.232.136.157	platform.twitter.map.fastly.net	United States		54113	FASTLYUS	false

Private

IP
192.168.2.1
192.168.2.3
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452269
Start date:	22.07.2021
Start time:	02:51:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 39s

Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://doc.clickup.com/p/h/c0hgx-46/b302180a8f685f8
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:	13
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:	mal80.phis.win@41/326@85/76
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: http://mega-sharedrives.club/data • Browse: https://clickup.com/?utm_source=clickup&utm_medium=doc&utm_campaign=12600861 • Browse: https://clickup.com/
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
02:52:25	API Interceptor	1x 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 GM DS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMDS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	Microsoft Cabinet archive data, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	61020
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	1536:IZ/FdeYPeFusuQszEfL0/NfXfdl5lNQbGxO4EBJE:0tdeYPiuWAVtlLBGm
MD5:	2902DE11E30DCC620B184E3BB0F0C1CB
SHA1:	5D11D14A2558801A2688DC2D6DFAD39AC294F222
SHA-256:	E6A7F1F8810E46A736E80EE5AC6187690F28F4D5D35D130D410E20084B2C1544
SHA-512:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2FA0
Malicious:	false
Reputation:	low
Preview:	MSCF....\.....,.....I.....l.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,.=.I.D.....3...3WW.....y...9..w..D.yM10....`.0.e.._.'..a0xN....)F.C..t .z.,.O20.1``L.....m?H..C..X>Oc..q.....%.!^v%<...O...-..@/.....H.J.W..... T...Fp..2.|$....._Y..Y`&..s.1.....s.{..,.":o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.` =*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...l.....D0.....Ba...Z.0.o..l.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)... .....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f|.*...'^K`\..e.....j/..|..)..&i...wEj.w...o..r<.$.....C.....}.x...L..&..).r..\...>....v.....7...^..L!.$..'m...*,*.....7F$..~..S.6$S.-y....|.!.....x ...~k...Q/.w.e...h.[...9<x...Q.x.[]}*_%Z..K.).3..'....M.6QkJ.N.....Y..Q.n.[.(.... ...Bg..33..[...S..[... .Z..<i.-.]...po.k.,...X6.....y3^.t[.Dw.]ts. R..L..`..ut_F....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.145340414441777
Encrypted:	false
SSDEEP:	6:kKn6PqdoW+N+SkQlPlEGYRMY9z+4KlDA3RUeIlD1Ut:P6O5kPlE99SNxAhUe0et
MD5:	557A64F4B2DC08222814031F6BFCC4C6
SHA1:	642FA2E5270F08DC456EC0CDC739C35AD9F05134
SHA-256:	1C4AD7915B874B1F65C109846CA7BEE2E2BFD5806AC952F5C5E7DB17F499719C
SHA-512:	67100CCA8D53B978354E7973412F6E8172D52840B3C9F04A2CF7EA45E2D8A2FCDF2D307100E51DC0D72595E08E90500CA0F8DFB046BA2A96C2DBF2901CC6A7
Malicious:	false
Reputation:	low
Preview:	p..... .....yXF.~..(..... .....T'._.....$.....\...h.t.t.p.:.//.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."..0.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...

C:\Users\user\AppData\Local\Google\Chrome\User Data\2e29a375-b9b7-4703-9beb-403bcdc54c19.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):	174419

C:\Users\user\AppData\Local\Google\Chrome\User Data\2e29a375-b9b7-4703-9beb-403bcdc54c19.tmp	
Entropy (8bit):	6.079206992770344
Encrypted:	false
SSDEEP:	3072:4g9kZExZKKJEuwA4x37SiHnDcWYKWFnFcbXafIB0u1GOJmA3iuRU:zsExzgRx37iWYFbaqfIlUOoSiuRU
MD5:	C5D638A6EEDE1F1917A715AE95110084
SHA1:	62BB7ECC14A8BCE266862DC121CD7C976E060E04
SHA-256:	F26B523173388ED5598645CC5F204039208F3A9F26E2FC9B209E90BB992B70D0
SHA-512:	B572BC2AAC977322B43370F830C6D647A7BA3648A27585B12A8A7647F2A26EB12149D8FD631D227EDFB45415B44193ED7FD5958FC6EF3C35086115B2A3D92655
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":1.626947542479471e+12,"network":1.626915145e+12,"ticks":4468045800.0,"uncertainty":4845367.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016364978"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\4df18817-4524-4966-8a12-f9c7d20136d4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	modified
Size (bytes):	97400
Entropy (8bit):	3.7441065633367727
Encrypted:	false
SSDEEP:	384:l/zEU25f55t68VxDg3N8rdv403XUGfH6zGzWrRmYylx3quqxr94mZFP1WE8onOWe:JKmBp2ugD0e3TY0eQPfC4KScElE
MD5:	3B11487A06F8213C79BD3F2BDD8960EF
SHA1:	7FA2085B4FAACF7B9949F521BF254B90653E480C
SHA-256:	100DEC82E82FC75819E202A10B65478AA34F0DDBEF5CF891946E35039244D4D5
SHA-512:	80365376B744C224D3127EFE0A48EB7CD4B31CD6C6B75B1D647F99EB3DAC1E622278EB22737D5B3ABAC50F706F0ACCC32154A81A05F58265034800AEE8DB014
Malicious:	false
Reputation:	low
Preview:	t|.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...{)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...i@8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\59028cee-9a6e-42dc-adeb-037dc8acf2ee.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):	165961
Entropy (8bit):	6.049431113972012
Encrypted:	false
SSDEEP:	3072:fmkZExZKKJEuwA4x37SiHnDcWYKWFnFcbXafIB0u1GOJmA3iuRU:tExzgRx37iWYFbaqfIlUOoSiuRU
MD5:	58218C489F134A806A162F3063B6BB7B
SHA1:	0D0E21468F2EEEB12A604C69861456FDAEB08540
SHA-256:	EEFE417EF41615A5C86B4C44693A49F0DB20487F9C5CED4B7AA9F3A1764631EA
SHA-512:	E73F4DA461E399CA61A60513E4FFC9A17A7AA0346B55DD2A07BD7969BBD8C1180090B2D97D1F32E23A4FCDE1C6F916C08FA45B8B8375FFA0C9445423FCD642C
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":1.626947542479471e+12,"network":1.626915145e+12,"ticks":4468045800.0,"uncertainty":4845367.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016364978"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\62b1e5d9-c33d-4e4f-a205-63e62e333cf6.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):	174419
Entropy (8bit):	6.079206186260387

C:\Users\user\AppData\Local\Google\Chrome\User Data\62b1e5d9-c33d-4e4f-a205-63e62e333cf6.tmp

Encrypted:	false
SSDEEP:	3072:w6ykZExZKKJEuwA4x37SiHnDcWYKWFnFcbXafIB0u1GOJmA3iuRU:JZExzgRx37iWYFbaqfIlUOoSiuRU
MD5:	EAF0602E0A3D2DEB1449176467F93977
SHA1:	F3AFDEF946C26E71605F685B536A2359806C56A6
SHA-256:	F58CC2F8606B3C281DF43B9F2A43DB124CEF2D9C76B9FD7430440B571757856D
SHA-512:	BECB5D4A6B912FB927B01A1EF845EB06C38095DE85A75375E62140B40FED4B91CAB0B6E15DCE29CF5032B6AFD541B6C3BBA744EC870C44721DE69C446C713A33
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":1.626947542479471e+12,"network":1.626915145e+12,"ticks":4468045800.0,"uncertainty":4845367.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\641073a3-ba45-4bff-9d3f-26ae4ebfa0b7.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):	174418
Entropy (8bit):	6.079207348160879
Encrypted:	false
SSDEEP:	3072:wFZkZExZKKJEuwA4x37SiHnDcWYKWFnFcbXafIB0u1GOJmA3iuRU:iAExzgRx37iWYFbaqfIlUOoSiuRU
MD5:	D4D1697E7CD00C2CE45C644438CE0514
SHA1:	7059865481C1C98FCCDF1398C75B890A3B553A01
SHA-256:	5353C707731B637A17D3566A2A23981FB8E856AD71D086692592EB4E6D725017
SHA-512:	DE2888FC3F8EEFC0D242B6A7CB5C14AF6A5EC1C4AE2B03296ED88B294A2ADEF551BE59ADFDF6ED9110B2F86761DA508B23F5301D0F85393AA7E4318DA4BAA36B
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":1.626947542479471e+12,"network":1.626915145e+12,"ticks":4468045800.0,"uncertainty":4845367.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\6fb18d10-e4a3-41dd-b3b4-29c2664a8939.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	96680
Entropy (8bit):	3.7440344447692553
Encrypted:	false
SSDEEP:	384:K/zEU25f55t68VxDg3N8rdv403XUGfH6zGzWrRmYylx3quqxr94mZO1WE8onOWax:HKmBp2uPD0e3TY0eQPfC4KScElG
MD5:	8422EBE855ABBF1C0FCDF8F8CE7DDC2C
SHA1:	56382F77AA15C58F1AA1644CC2E2D0C219C23652
SHA-256:	E3C4E135122B1F0B7BBFEA857808B8A5C36D9ECCF985ABDD34E6B83E5A8DCADD
SHA-512:	A66A906D5B7DF7D3FE0012C68347DF1DF9AFE90C607D795A68386F0DC156A2AB1DBB3E410B5FA11FCE1D8AB148B629A224AB9235B350132C7C3584F0EC6386F
Malicious:	false
Reputation:	low
Preview:	.y.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L..P!...[)...%.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .o.f.f.i.c.e.\.o.f.f.i.c.e.1.6.\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .2.0.1.6...*...M.i.c.r.o.s.o.f.t. .O.n.e.D.r.i.v.e. .f.o.r. .B.u.s.i.n.e.s.s. .E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.....*...C.:.\.P.R.O.G.R.A.~.1.\.M.I.C.R.O.S.~.1.\.O.f.f.i.c.e.1.6.\.G.R.O.O.V.E.E.X...D.L.L.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...i@8.D...C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.C.o.m.m.o.n. .F.i.l.e.s.\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\.O.F.F.I.C.E.1.6.\.m.s.o.s.h.e.x.t...d.l.l..@.....U/...%.c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%.\.m.i.c.r.o.s.o.f.t. .s.h.a.r.e.d.\.o.f.f.i.c.e.1.6.\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t. .O.f.f.i.c.e. .S.h.e.l.l. .E.x.t.e.n.s.i.o.n. .H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C.:.\.P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	120

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftlE1G1mkftlE1G1mkftlE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Reputation:	low
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\0f604b79-fe36-4cdf-9000-e13e5ba1bc5a.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22595
Entropy (8bit):	5.535342879426243
Encrypted:	false
SSDEEP:	384:dKXtTLl/7Xv1kXqKf/pUZNCgVLH2HfDmrUBHGNnTssfnI4A:ILlbv1kXqKf/pUZNCgVLH2HfCrU1GNng
MD5:	64A708D94DAA964D652F78B2AAD31477
SHA1:	812CF16D5FFC63905F96E2DB86FD0970D7CBFAEA
SHA-256:	1AFC550BA37E8DEED40D8307D8EE06356C0596030E95FB68DBAB753C39631F0B
SHA-512:	EC8F52066A011BD4C34BE4CD6D4E17821798DC799EF61C49D4740A97E11C4708A9D394111D3B999AA418B50C9F5F8B0B8FD9E11534572F8649F290765641A842
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":"13271421139333515","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1fd59d5f-de58-4f3e-87ea-0ae9bdd9b548.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22596
Entropy (8bit):	5.535331844744268
Encrypted:	false
SSDEEP:	384:dKXtTLl/7Xv1kXqKf/pUZNCgVLH2HfDmrUBHGMnTssPnI4r:ILlbv1kXqKf/pUZNCgVLH2HfCrU1GMnb
MD5:	69DCDDC6F1BFA6D98855911AA40820B2
SHA1:	4780FEA080B2BD13A56F686C63CB42667FDC3B89
SHA-256:	0F93F61D149E1185146F0909E1001E372AA04681AF93043AF9F9D2F65123E5C0
SHA-512:	AF3B08E9F5770FEE26672C4E7561E3F2A7FBFC88C50DC121C61E10C81146F11A58599DC546FA3E52D672CC0974BD1B9879FC7C934192A8B541042C8A75016912
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":"13271421139333515","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\51966cad-a714-4eae-803b-d8e1a4aca5e6.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):	6036
Entropy (8bit):	5.191347176545369
Encrypted:	false
SSDEEP:	96:nBCd6CMmyHZcKILok0JCKL8jkqq+zokCS17bOTQVuwn:nBCTMTHZcE4Kqkqqgokl9
MD5:	E42938809300DE201F9E419320FF1D27
SHA1:	F81BA42E6ED617753915F54516AE3208DCC69025
SHA-256:	6B85C849D682F4ADF06E4140D0BE219B8A2C71DDFCBB7C6888431AC01C8F05DC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\51966cad-a714-4eae-803b-d8e1a4aca5e6.tmp	
SHA-512:	A15729AFD45D5AE447E02A68834DA39359336296D8AE38BDF6A3B891FBDBBE693A56628463E1C20C953DFF296BAB978D1473381287AEB3ED689180E1CBEBEF6 7
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271421139586545","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\58276ada-d86f-4fd8-a3c2-e544dc21c025.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):	5764
Entropy (8bit):	5.180496708570775
Encrypted:	false
SSDEEP:	96:nBC7GCMmyHZcKIWok0JCKL8ukCS1SbOTQVuwn:nBClMTHZcH4KHklS
MD5:	D7CF805789E989926066EB02A00DB626
SHA1:	EF7C5404351A608712DD1C61D813D971D8D46771
SHA-256:	126826CF5AD28B2633B1398632144EDA5A61201F7197B39B6B96D63EBDD3769B
SHA-512:	8EDC73FFD5033BD7903E28E72EF8F37BFD41DF883F05D68AAEB672536C49E68ADB89818156A6A39D4329DCA898483F58660321FF3FDBFF6AB0420B8E86C45D7
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271421139586545","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\70a9ae32-ffc0-4a97-9e90-71b06bcd0542.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):	5118
Entropy (8bit):	4.98207301736042
Encrypted:	false
SSDEEP:	96:nBCeoXMpcKIfok0JCKL8ukCS1SbOTQVuwn:nBCbMpcM4KHklS
MD5:	0497A2395BF9C7EE9510A0EC2D388FAF
SHA1:	F06EA9B89821CAA630324BB1B2CD6A90774B0CA1
SHA-256:	FF7DA1CB20D72699C04208E253E73282F6B335611B6C06C836EAF045A7970FB7
SHA-512:	C24E6BA2996ABE55688556BDBC1876CEFCD76DDB9274E356B40B9720490F320A2B939C2EC89201F0577CAC6E0695EEF5130FAA27669D77D14AD30EE69058B55 B
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13271421139586545","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0","

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7a279dad-8eee-4900-b7d6-2a7d712f872f.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):	16745
Entropy (8bit):	5.576869561627101
Encrypted:	false
SSDEEP:	384:dKXtOLl/7Xv1kXqKf/pUZNCgVLH2HfDmrUts0I4f:jLlbv1kXqKf/pUZNCgVLH2HfCrUe0IY
MD5:	3A750B10894FA097F2F48E6FD510E58B
SHA1:	1B5BDA42F2503353574344E5DC409F09D4AF94C0
SHA-256:	11A53FE0715E229AEEB44B4C11CB6D3D56A73E5DE0096ABFCEFB646C47AB747F
SHA-512:	10200DFAA1D86323C5837F46BBD76E2A050CCD95E7C7D7E6892EC160FCFC9044CADAA313BF6B4BD00A62041EC7E4D335AE6EFF4710D9919D4D1B2010A87BE DF

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7a279dad-8eee-4900-b7d6-2a7d712f872f.tmp	
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":"13271421139333515","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\7d94b1be-ab7e-4f32-86da-b23b4210567c.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):	4712
Entropy (8bit):	5.608256445664752
Encrypted:	false
SSDEEP:	96:b7UJUrUUeUUieUkNZUJUU6UbKU/gU2SzU4UsUmKUScU+uUmv3UrPU5gYpUeWPeUB:b7UJUrUUeUEUQZUJUU6UeU/gU2SzU4Ue
MD5:	DAC8985F8895C5A51389625C20DFA6CE
SHA1:	FE939881620C5C392E8EE69FC5085E6D1AEEC42D
SHA-256:	C2F36BC8365696AB68AB0894DF8C506285E394084F63DA0DA20F73DCF739246E
SHA-512:	1A46417CFC4F4A55C566E2DFD8594ACC66853E815030354C4D78193549828210BAF966588956A5F8FE95CE5E81B3742A7C13BDEA2E0C9B5D792CBF579BEED06
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1658483600.800176,"host":"B33dNWuWc3elp/rqxbaViYp8VufHqjSms9l6Z0xI7lk=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626947600.800182},{"expiry":1658483593.85775,"host":"DZojSgKWXqymKhdrkb0V9PlsJoovVUGWsPWVArl/V48=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626947593.857757},{"expiry":1642727589.336034,"host":"E10e7Gwg5+phsYD4E8qNYFsQySXnIHPAfo4zloUPESc=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1626947589.33604},{"expiry":1637834000.058222,"host":"LAZkYS46RVRcFiZAzmUJrz6TJHBd4nwE6VxPWfPLYHs=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626947600.058228},{"expiry":1658483603.963533,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626947603.963541},{"expiry":1658483609.221069,"host":"NlMbAACeZ6GFqgYKbWFINnSsfFM9gCcHh+OP80Q98ts=","mode":"force-https","sts_include_subdomains":true,"sts_obser

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9058b2bd-cf5f-403a-967c-cfcc538fb35a.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):	24055
Entropy (8bit):	5.532961096036103
Encrypted:	false
SSDEEP:	384:dKXtTLl/7Xv1kXqKf/pUZNCgVLH2HfDmrU+HGcHGenTssuFnI4Lw:ILlbv1kXqKf/pUZNCgVLH2HfCrUuGQGm
MD5:	AE83CA060CD47B3E25B4E5C3E7CBEBF9
SHA1:	6FB4F1E51CBDB1355C8FBBF16A7A81F5D42DC3AF
SHA-256:	CC021D2A12142F582449377E5E4F5E283A1721534E8CAD75E09334DBD4321540
SHA-512:	BAC192CA20BEF1261E7B19E3BC113592A5006B40967E09A6F39A5B86E27853C69467ECDCDD9F16BF672AE8EA0F35DC48E3CB085564BB93C46FC96EA4F6DDEA06
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":"13271421139333515","location":5,"manifest":{"app":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9849adaf-94b7-4b00-99f6-d60f899e280e.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):	1203
Entropy (8bit):	5.578414184722949
Encrypted:	false
SSDEEP:	24:Yn9RAeUaI6H0UhVsTG1KUerkq/HeUeXby2qUeXvE7wURRUenHQ:Y9ieUaI6UUhVseKUewqPeUer2UefSwUG
MD5:	B60F1A7BD2A9C773993D6FE0C399C064
SHA1:	DF32AFAF7A5340A32041C7DF8CD8AB05E4D3D11C
SHA-256:	C74ED12A9D6D928FD4B703D06F1B57FEBDD87B03F63B4423B1A0C4711E205A7C
SHA-512:	BEA2B0C3EA10611731FD6A75D5DBE1D6CB5DF73B95F8C928E73EEF025AC1D3348BECA4740028ACAFED7DAE80697E445262ED0474E1B25ED00C8B1A8AC9F81F9B

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\9849adaf-94b7-4b00-99f6-d60f899e280e.tmp	
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1658483545.29506,"host":"M4bfUnCmQAi4PNb3B8aI/2+SVJhHKsMfMMT7fzi6ij4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1626947545.295065},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1658483544.2635,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_observe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.207298935776468
Encrypted:	false
SSDEEP:	6:mCF6Iq2PWXp+N23iKKdK9RXXTZIFUtpbF6ZZmwPUYkwOWXp+N23iKKdK9RXX5LJ:dEIva5Kk7XT2FUtpQZ/P95f5Kk7XVJ
MD5:	FDCCC1FC4BDB6E9399E831CD2EE0BDEE
SHA1:	D682B28EDCE904CA8B849CE958E316ACCDEA3BF4
SHA-256:	953F2AC8175027E28C78E5992AF05D5BE047B614D80D9248B8DA9205E24C395E
SHA-512:	CD5E27C369829EDEA8830F9E0F435CF3BD1AFE5499911D3899DE09B6C5FDCBED16EAEC0BC297A02B907ABA62E719E5A4341C54747CF5822B02E8269836CB7D32
Malicious:	false
Reputation:	low
Preview:	2021/07/22-02:52:39.000 15e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/07/22-02:52:39.060 15e4 Recovering log #3.2021/07/22-02:52:39.061 15e4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.253302039696301
Encrypted:	false
SSDEEP:	6:mLLq2PWXp+N23iKKdKyDZIFUtpcuZmwPVMFkwOWXp+N23iKKdKyJLJ:eLva5Kk02FUtpB/PVMF5f5KkWJ
MD5:	3168C1E16FEEDF52D28E0C6C02D5C70A
SHA1:	8296908FBEE671405DC3FAE3423E6514EB91822E
SHA-256:	7E05CC532A71163293F7FBF29D89482EE0B05D64DEFD82E559006D73CF679965
SHA-512:	4EC4640BD15EDF82DF33435A509360DB603C27F19EEB86B225A5F194A8D295B81C620243FD15B512721B013C00860B5EB3D9E929E699AAB30D5700F118397F7F
Malicious:	false
Reputation:	low
Preview:	2021/07/22-02:52:38.976 15e4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/07/22-02:52:38.978 15e4 Recovering log #3.2021/07/22-02:52:38.979 15e4 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\092d86524c03659b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	595
Entropy (8bit):	5.902054373799083
Encrypted:	false
SSDEEP:	12:EDtnAKm34b/ux2pHgyye3CMxucLStyChxkN:aSKm3+uyAyyeSHWCh+
MD5:	E6D86C6BEA0B1863D008E77F3A230AAE
SHA1:	5E53809889AE31ED5701AF688CB01D80C2A7F7E2
SHA-256:	A19B5E31877D9DB45816BF73E52ECAB8B8C00F75A3D261BDE78532FB05E277EA
SHA-512:	42413DCF38C5E9D3AFAD0D304DC1ED5863B742E5823B88E3C63C90FF9D84BC2A6E15D51D709F08AFE5EA4AE1EF7D38D3A662EC0BF50462C52EA6E4F54A0CF0D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....E....._keyhttps://www.googleadservices.com/pagead/conversion/867030291/?random=1626947602807&cv=9&fst=1626947602807&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=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa7j0&sendb=1&ig=1&data=event%3Dconversion&frm=1&url=https%3A%2F%2Fclickup.com%2F&auid=1951469803.1626947567&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://clickup.com/..>.I&/.....e.....".`PW.A..r..lyU..y..J.=...'...A..Eo.....%.....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):	414
Entropy (8bit):	5.362721357330515
Encrypted:	false
SSDEEP:	12:SzQYZwY4A9XLIOUc70zQYZwY4mnLIOUt:SEnR0lz0EnRMly
MD5:	5AAED66CA7B4F530C7517E2AC8DB34B1
SHA1:	CCA84E1ADE186404B6A545879DC096227042CDD2
SHA-256:	E97725B75938049ECEBD7070448F2DEB7C061D0499A50A2A8261FE6461A8A74D
SHA-512:	3C6B9F6B1A16DBE3E44DFA6B48AAEABA6D35BDE100B1E66EDE7EE34EAE3009AA848BBD720583E1A5D8F67EF1A2D0E6F18D2C5408FBD45BB24B3310D5D2B35DBA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K.....0....._keyhttps://js.hscollectedforms.net/collectedforms.js .https://clickup.com/....I&/.....CK6i/m....d....u.P|IY.j...}...(.A..Eo...../t.....A..Eo.....0\r..m.....K.....0....._keyhttps://js.hscollectedforms.net/collectedforms.js .https://clickup.com/....I&/.....1^.....CK6i/m....d....u.P|IY.j...}...(.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0d60e00d6ac12ad5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	352
Entropy (8bit):	5.84004825524572
Encrypted:	false
SSDEEP:	6:mKwnYmXHUj8TKU6t3z0WDEXTQ1SNL8mprp7SWRAXJwY6ugntdNLb4HK6t:en5P6ZdXSNL8mn4XJwbndNLbm
MD5:	E330480A6672DC67789D97B205F6673A
SHA1:	31FE487CC45F2468D24E16DF264C52DBAFC187EB
SHA-256:	C46F105C7C144C0E4CA6163F424F4E4837969D6D108574604D96EC2F9012A024
SHA-512:	73E9CBA02FE79240865D7F52382BF878085EA760D3908BCB2E8350DFB3A99D4F7ACBE5BD1F4E172C96B3B2D4DC17296F53BB40C1E6F829B196DD2C306BE1C38
Malicious:	false
Reputation:	low
Preview:	0\r..m....._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%3D12600861&cb=1456956481810523term=value .https://clickup.com/:...I&/....."`..jx.T..r^...G..}.'.X.w.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1069df37f59e7f2a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	692
Entropy (8bit):	5.773794504938955
Encrypted:	false
SSDEEP:	12:1E31zIAhISoux2pHgyye3CMxuDPdXSNL8maMGxa1DEChsh7WoQv4Q:1Elz9hIbuyAyyeSHD44za1DEChQ0
MD5:	B898E9B5EA6FDCF25C224FA42DFFB6A4
SHA1:	63B38333D3C142A30DBA40A86C5304748C4AC58C
SHA-256:	59F1058AAED6CB9D7D06CAA7F76B7FE70190FDA97093C60DBF3EAFBE8CDF75D6
SHA-512:	2D55F171FC6CB0F35CB44EB05C7EDF5AB3C672149F5A57A18D39BD4B76734E118B3D930C315BFFADC67D463422B93E9264D7DDF1DD42AB3BBA77DDE2B1FFF20
Malicious:	false
Reputation:	low
Preview:	0\r..m.....0....r.R...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/617640813/?random=1626947567938&cv=9&fst=1626947567938&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=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa7j0&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fclickup.com%2F%3Futm_source%3Dclickup%26utm_medium%3Ddoc%26utm_campaign%3D12600861&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/d%..I&/.....+.2^..j.^x#..M..d.l..+t..j....7.A..Eo.....M.....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):	5798
Entropy (8bit):	5.541124016034105
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1408a718ac481827_0	
SSDEEP:	96:THh3OOfMo1b6TPI1awmlmxBBflkn1J39CeO7K8pLU/0MTE:BDIA1rmlmxBBNkFC57XLMFI
MD5:	41B2B780591B3C9F051DA9CA54802B10
SHA1:	07C74A49B2E0B8AB78018154E81EEBCC9D7B6D76
SHA-256:	C552F9EDC5AAFC87F458A1457D2FD850F3D5F2DB0D80191B68230F21956AA3D2
SHA-512:	86021781D6F26028F5EC59677C203041057AD238AA3BB396003EDFEFCD042F90A8594260C2B4FEF0672C8057039329632D3372672FC3E307A57EBFB4EDCF0F50
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N....q....._keyhttps://m.servedby-buysellads.com/monetization.it.js .https://clickup.com/8...I&/.....i.....dG.+.X).Zp8.....z...Q.3.Z....A..Eo.....#m.....A..Eo.....'..7....O....0...D8.....(S....`.....9.L`.....L`.....Qb./....._bsa..Qc.h4....._bsa_go.....ar.....Qb.m.S....initC..Qb..\?....srv.C..Qd...)....frequencyCapC. Qf..)}....appendQueryString...C..Qd.?.....clearQueue..C..QbB.....linkC..Qc..6....pixel...C..Qd.....findInQueue.C..Qb.a.l....dropC..Qcj.....callbackC..Qb.....hideC..Qbr .E....showC..Qc.G.....close...C..Qc.t.....hasClassC..Qc":.....addClassC..Qd.Y.....removeClass.C..Qe.....removeElement...C..Qd..Q.....emptyElementC..QcB.s....reload..C..Qc.O.....isHex...C..QcJD.....isMobileC..Qc.....extend..C..QcVHBC....isset...C..QcV>.s....exists..C..Qd..'.....objExists...C..Qc..z/....getAttr.C..QdZ.....getURLVar...C..Qd..cj....htmlEncode..C.(S.....Pd....._bs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\14889cf1e33a62c3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	234
Entropy (8bit):	5.6926118633783265
Encrypted:	false
SSDEEP:	6:mU/VYKf4YvAP7FTkGsMngUycuWNzhQK6t:/sYYzFAGsM2cuqY
MD5:	9D2C4071698ED8E8E4A6FC16C55C1C5C
SHA1:	46FEFCFEEE2809E0CC5816A9F926E3ECC1D250E2
SHA-256:	C5FDAE1C33E48A47A1E1B59F565B097ADC5CA9C4F46B9BD489F5E3697A1828D2
SHA-512:	B13D91B9266EE2CD9D89DB167D5483B8656F91D5FB454A4B344275D6F326F0E310F3BC8FAE8609F084FE58FEDCBE33153FD5A0EE3A365F88693EF3A02847CC4D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f....._keyhttps://doc-cdn.clickup.com/intl-displaynames-es2015.4b62ff9df40330a137a6.js .https://clickup.com/...I&/.....=.....s....{_..)3...<...q.\z.G).."O..A..Eo.....+.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\157c30be0bd7c29b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	470
Entropy (8bit):	5.655428490025617
Encrypted:	false
SSDEEP:	12:QdTC315vrukpGLCTWdTC315vrhC7pGLx1:oKxr/8+TqKxri8T
MD5:	0A83ADB6D04A017D7C0987702A533AAD
SHA1:	C1601CCB37AF910FEEADA5B26B61CF7699B5BA3C
SHA-256:	60F754C589D6ED6CB9DF073A6539B0F4F5348E70EB5D6C1E0F70F0B149ABC4B9
SHA-512:	F42BBDFFDD522BD24A762BC1E0B21CFF0200D7DE0EA3202990DAA45267CF5993F3842608B3E44D06001EAA592C74167CC7C0F9644A8E03FA8187D05A249BF1F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g...._R....._keyhttps://connect.facebook.net/signals/config/124630241461844?v=2.9.43&r=stable .https://clickup.com/&...I&/.....1.....s.Z..TL.|.S.6*..a.~Y.Kp.L@...A..Eo.....2.....A..Eo.....0\r..m.....g...._R....._keyhttps://connect.facebook.net/signals/config/124630241461844?v=2.9.43&r=stable .https://clickup.com/....I&/.....].....s.Z..TL.|.S.6*..a.~Y.Kp.L@...A..Eo.....).....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\18b50005768776d1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.623009764995856
Encrypted:	false
SSDEEP:	6:mM69YKf4PVl/+l7BWV5gjuM2X+0mGu5yFzLrzfEK6t:zNl/+TWVXX+TAFzK
MD5:	B135B54E2D9A7AF3A37FD05D6441C705
SHA1:	B2F70BCA984AF5CF819EA8B499B41EAF5D620299
SHA-256:	2FA836F10F813D83BA5BF7E873AB6C223515C31EDAE433DA760679B2C267ABA8
SHA-512:	5685023603A73AD1E121D2981A6446133427C562B2AA4BC508E0A88956CC065B307304AF2BC97F225185665E95842F3AA1F5F38569D3AD142F67903B8903B7A9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\18b50005768776d1_0	
Preview:	0\r..m.....g....._keyhttps://doc-cdn.clickup.com/attachments-viewer-es2015.c4028c36d8cb64626cd8.js .https://clickup.com/...I&/.....Y9.8.9.+F...C..O.G...d%.....\.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\195df249e37e8246_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	224
Entropy (8bit):	5.5663116732186
Encrypted:	false
SSDEEP:	6:myRYKf4bOIPLGqFU3s4kPWtgnBs3mlDK6t:XIbnP49KV
MD5:	BB414E9E949BBFC6D2C27C7A287AC950
SHA1:	4FFE4527AD1E617AE1970D9B97A5E34837929A89
SHA-256:	ACF713C0B0FC8A6DB1E6EE6803ADD7FB8524DC86F9179147AE57FB61CBA92038
SHA-512:	0B208389EC0A868A771D3A7E60119ADFDF939C489CBAE7BCF9D3C37C399F3973BFDA6F2DA500C634582C97EA555E41CBAF7725350159D8B8722E3276B0E13B7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....\....V.f...._keyhttps://doc-cdn.clickup.com/runtime-es2015.886bc0e678ccf257da8f.js .https://clickup.com/....I&/.....e...../0.....l.i.w].~.-.s..(.L/..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1a2096b9bef1f056_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	780
Entropy (8bit):	5.803387856215599
Encrypted:	false
SSDEEP:	24:UwElz9bYHLuyAyyeSHIyZd4za1DEChYsg7:UwElxOurfVj+sg7
MD5:	E60986143031BB16F4DA1D322B08DF95
SHA1:	57CA00BAD81C9A103E58ACC297C9BECA080B430B
SHA-256:	5391C9C6933922C6133DBCF7A855090AAA4B369DD075F7533000D0175B373146
SHA-512:	F8754E6519875EC6CECAA2D3B9AE01C5795415C46FEE317E0886FADA002F77CC6FCF2B50632414D138315E6C750879C9AC92095964615F7B055774D5A259FDD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....6]....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/617640813/?random=1626947570973&cv=9&fst=1626947570973&num=1&value=0&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=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa7j0&sendb=1&ig=1&data=event%3DInvalid_Users%3Bevent_category%3DCHEQ%3Bevent_label%3DInvalid_Users%3BnonInteraction%3Dtrue&frm=0&url=https%3A%2F%2Fclickup.com%2F%3Futm_source%3Dclickup%26utm_medium%3Ddoc%26utm_campaign%3D12600861&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/J.p.I&/.....g.}&..... 9.Y....1j.V9.....A..Eo.....ZI.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1aaafb503b581d84_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	624
Entropy (8bit):	5.8367296606161485
Encrypted:	false
SSDEEP:	12:iE31zIAnHUmoux2pHgyye3CMxuDwdXSNL8mD2ChxFN3V3:iElz9n0/uyAyyeSHDpJ2Chx/t
MD5:	5427DA17A3CE7B6C9D38448749AD83D1
SHA1:	005463DE6E8374DBCF716B16A4ECEF4890FD03C0
SHA-256:	E479F930B46C53DCCCB15E5BDFABEFD26D3C976C5192AD76D4C8CD1B491874C4
SHA-512:	58C0C3AB49D4714D7B133166A5B20F7AFAB831A52D6071B8DB8C5D9293A9E4BF1B32073145BDBE0E2F0889F7BE2574C425873F3EA8ADD91744D4CE4F5B68E9F0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]"K...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/617640813/?random=1626947574245&cv=9&fst=1626947574245&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=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa7j0&sendb=1&ig=1&data=event%3Dgtag.config&frm=1&url=https%3A%2F%2Fclickup.com%2F%3Futm_source%3Dclickup%26utm_medium%3Ddoc%26utm_campaign%3D12600861&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://clickup.com/DM..I&/.....Pm^..].`.Mi4.....[#+.A..Eo.....C.*j.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1dca4e1f9dd820a9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1dca4e1f9dd820a9_0	
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.703046179625093
Encrypted:	false
SSDEEP:	6:mQvq9YKf49o0mFlVFHgHl/VVy6vLEGIghlbK6t:PqU9oVqVNVVpvoahlN
MD5:	9ED6BB9CFB6DEC36032B9915E8332374
SHA1:	7C7AABB41B795CBA4E0CE6C93B2B48552176A7FA
SHA-256:	6EA67DBDFD004C43A057B144313FA27E87D048CB17AF14C79735581FFC49E435
SHA-512:	E171CC3E12D2BDE3F410FFF27E01C3518CE08A1AC64344CC0342E7FE0465FCE5BC65338507F878A7A1D31254A17CCC2D665A3C062D752F1D26FA6B6CB1F4EC0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....^...I.n....._keyhttps://doc-cdn.clickup.com/polyfills-es2015.7015662f3125b17981a8.js .https://clickup.com/:..I&/....."".....v..p.NW..V'....x.....#K$.w....A. .Eo.....%.....A..Eo.....

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):	426
Entropy (8bit):	5.538746585225292
Encrypted:	false
SSDEEP:	6:molYmymJMBKTXK3FQzHg0d99M1k41enK6tWolYmymJMBKTXK3FUsyg5l8d99M1kq:gKTXKFQjVO6WKTXKF1Tl8VOT/T
MD5:	AD08ACF6CAFE3B88B770A88B7F2DD30A
SHA1:	8F195ACC0FF2917768BFC1EB376144EA2DC807C6
SHA-256:	24C193274442D0CB3D3341CB9C6C80C78DD8A99EFFBD70A6A004CE8D6E08908E
SHA-512:	09EF372639F16EE8CD2ADB585B7712C5F8CEAB3E853884481DC6416C5343C24299758EA5B39C0171D37C188AD03086B7D79AF3E051D861FEAEF05AC0998116
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Q....._keyhttps://ob.cheqzone.com/clicktrue_invocation.js?id=3839 .https://clickup.com/. ..I&/.....'.....nNF..d....A...c.}=.....A..Eo.....p.{.....A. .Eo.....0\r..m.....Q....._keyhttps://ob.cheqzone.com/clicktrue_invocation.js?id=3839 .https://clickup.com/.u..I&/....._.....nNF..d....A...c.}=.....A..Eo..... {.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2396c899aa8f61f3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3670
Entropy (8bit):	5.801531263384456
Encrypted:	false
SSDEEP:	48:wD64AgwCMstAuuKDQP2Dybhy3E4n4pGJB/E6djQMy4wZa31bk0zhOtsIOCQhg1eN:wm47whg2Vyr4AThUC40ctsrvc/
MD5:	30995F9D2A9832D01A7C9CA232E8C294
SHA1:	2E988390E4172FCD3B890594F6ED75C370218917
SHA-256:	283BC80EB256DA6BDC7B3AA22A85ECC244826D6A65D7E201281663BCC6513498
SHA-512:	FE4EC699FBFFFC0E5BC5194050C84688DEF9F321FA059212DF970DCADE7039CE3D7B3AD42A0441DD126EF5C678B59324CF6939D3AB9E00D40CC7F6156A24167
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L)....._keyhttps://obs.cheqzone.com/ct?id=3839&url=https%3A%2F%2Fclickup.com%2F&sf=0&tpi=&ch=cheq4ppc&tsf=0&tsfmi=&tsfu=&cb=1626947601866&hl=1&op=0&ag=3098761112&rand=0460667770407500782867690001970958502286780219110865782099802609557 9&fs=1280x869&fst=1280x869&np=win32&nv=google%20inc.&ref=&ss=1280x1024&nc=0&at=&di=W1siZWYiLDQ0NTddLFsiY2IiLCIwLDAsMCwwLDMsMCwwLDEsMCw1LDAsMCwwLDUsMCwxLDAsMCwwLDAsMCwwLDAsMCwwLDAsMSwwLDAsMCwxLDAsMCwwLDAsMCwwLDEsMCwwLDAsMSwwLDAsMCwxLDAsMCwwLDAsMCwwLDEsMCwwLDAsMSwwLDAiXSxbLTEsIi0iXSxbLTIsIjE3LHYwSWsyS3ZWZkFobUkzV0dLaXNVUVRvOGFhR0d2VVR4T04raGtUalluR2lpMldvSWxLMUtqUkdNVVNCUXNnUlFTQnBTeHNuWmx6emx2LzZ6a3paM2RZUWYzOGwydXZtWjB0N0oiXSxbLTMsIltcImludGVybmFsLW5hY2wtcGx1Z2luXCJdIl0sWy00LCItIl0sWy01LCItIl0sWy02LCJ7XCJ3XCI6W1wiZGF0YUxheWVyXCIsXCJsb2FkQ1NTXCIsXCJoamlkXCIsXCJoalwiLFwiX2hqU2V0dGluZ3NcIixcImd0YWdcIixcImdvb2dsZV90YWdfbWFuYWdlclwiLFwiZ29vZ2xlX29wdGltaXplXCIsXCJtdXRpbnlXcEpzb25wXCIsXCJzZXRJbW1lZGlhdGVVcIixcImNsZWFySW1tZW

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\261b48a28679694c_0	
SHA1:	E05725103B6B4879676085C1A4C94CF9033F7ADB
SHA-256:	C1EA7F653E667D649A66223BF7AE782758B4CB07CE6052D8566B578B5BBF9E9C
SHA-512:	F8EF06A5736261807FEB313CC991B65ECC9FE0FFAA3D1C84AAE95E7F21249FFDB5B33A4EFDA1A50F2B86E3752592B4B216A644D00696625730431467E0B36802
Malicious:	false
Reputation:	low
Preview:	0\r..m.....R....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/867030291/?random=1626947567936&cv=9&fst=1626947567936&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=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2wg7j0&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fclickup.com%2F%3Futm_source%3Dclickup%26utm_medium%3Ddoc%26utm_campaign%3D12600861&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/X,..I&/.....;k-..i5.(F.HZ.^...k.G.....A..Eo.....Q.....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):	408
Entropy (8bit):	5.441102403480548
Encrypted:	false
SSDEEP:	6:mulXYAWQf257UoKvtgVh8xbVblbK6tWulXYAWQf257UsgBA8xboMnK6t:tHe54cMlNLHe54RVp
MD5:	7F26F34FC9C5CA29A1E60D32D2BA3A24
SHA1:	0892DD0167AB94CA3D7A865565F25BFDE8C7EB70
SHA-256:	EE73B03E411CBB83DD39AB9D19DC994DEA80C1B1061BDECDA14A485E7C1D8103
SHA-512:	CB0A8ACA32B4F7FDE44487C780686E1FCD42C0CEE1DFDAA505A4BA58D8B694A65AFA1869F122E2DF9076528B478DC3269770258C9C1D46D62DF42F5ECA4701C9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H...e....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://clickup.com/M..I&/.....T.y.*.E....H.....E....J.5..A..Eo.....E.....A..Eo..... .0\r..m.....H...e....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://clickup.com/L...I&/.....W.....T.y.*.E....H.....E....J.5..A..Eo.....A..Eo..... ...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2d8e6e750fdb8441_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.499320681764836
Encrypted:	false
SSDEEP:	3:m+lxyl/08RzYGKAXGK7oKIIOKGh2bcsPsDP9LpJji1l//lHCpt/U2EmnaA+5mdzP:ms2/VYOXdTKKW+cuUBWtgDS/B4dnK6t
MD5:	815847FF526F04F1E450A2589620B772
SHA1:	5914594907EB204AC131D3203E4164E446C10129
SHA-256:	6C7ACDA8ED682FFA8185507B83415AA73EC386E3FE460D9232C1F130A855947B
SHA-512:	2215B7B06992C841B6012586A5353B45239B66E1E79FE9EBEA26C1DE19E5BCFF858EE9E1CBC2100515EC13DF05683017421C8AF6523B186FEB5AD3A03504D67A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S....._keyhttps://js.intercomcdn.com/vendors~app-modern.8ef9459b.js .https://clickup.com/..4.I&/.....!.....!....._.c..>..*..y.!H.....Y!..+...IF.A..Eo.....4..... 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):	424
Entropy (8bit):	5.680052752050936
Encrypted:	false
SSDEEP:	6:mdl/VYGLSmXZCLRQIDWvtgaw6Tx4l57bb/doZK6tWdl/VYGLSmXZCLRQID8XgA61:E/11eWvXel5HB0i/11e8Ael5HWp
MD5:	5806562614C221C2650CC52FB1B46664
SHA1:	9E52DE65B634C1FEC6A1F59A3BBEC49DB18D88C5
SHA-256:	076A41F59693FB66A6BFFBBCA2541504BFCD8D5CC9E58DA4307CDB27574BCFED
SHA-512:	50CC55AD08598F30B954B0F280DB0D23E5A24A38B1360DF49F0DB93C3435C99DAE8914559A3E9D1A8EAA63D015586B78BD823633C01E084678D8E0BF8773784E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....P...C..R...._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-W9LSCFD .https://clickup.com/?[.I&/.....b?..>...:e+.....-.M..*.+qr..&.A..Eo..... .....A..Eo.....0\r..m.....P...C..R...._keyhttps://www.googletagmanager.com/gtm.js?id=GTM-W9LSCFD .https://clickup.com/Fe..I&/.....HX.....b?..>...:e+.....- .M..*.+qr..&.A..Eo.....rF.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\305e5b9f98f34560_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	440
Entropy (8bit):	5.581427184372988
Encrypted:	false
SSDEEP:	6:m2rtXYfDMtvp2QgnVigcl98Y7nIM7P4RgDK6tW2rtXYfDMtvp2QgnVqrpiugh8YB:6Qtvfm+LJ7nD74MwQtvfmQoJ7nD7n
MD5:	69F648923C02022EACB1D3FB15C22556
SHA1:	9AA7EB7453CAEB1F6BFC79A979813D1EF16DB337
SHA-256:	4027FE13D23F50E55AC6714C4F797142D3BE59A6C1730CDEA1390E16DB930EE7
SHA-512:	89F9A14C3D017C9F7CED96B9E3AA72BD04B258837D2443F1C5035E00DC8B633EF3E3D86D7C6402D34E83133D6FA1909D504FCD36B53F92A96068F2A3A0CA50E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....X...Ik.4...._keyhttps://js.hs-analytics.net/analytics/1626915000000/6613321.js .https://clickup.com/....I&/.....9.....o(Z..._..(.'%..`..A..("....".A..Eo.....u.....A..Eo.....0\r..m.....X...Ik.4...._keyhttps://js.hs-analytics.net/analytics/1626915000000/6613321.js .https://clickup.com/`...I&/.....^.....o(Z..._..(.'%..`..A..("....".A..Eo.....B.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\31dcfb74895d0a6d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	595
Entropy (8bit):	5.838754065017037
Encrypted:	false
SSDEEP:	12:E1tnAvzIAs6gWux2pHgyye3CMxucLStyChmLN:YSvz9sEuyAyyeSHWChG
MD5:	84FB468F19150B639279489E68EBF213
SHA1:	263036EC793662579197FB560F68D0A744B41594
SHA-256:	BDB6F170C4A71C7BC02E51D981DBB0A33A24AB4E1327C74851A47EA7C5B2E1DA
SHA-512:	9FC75564EDA3E39733C505C050708981B47F965140454B1A1977356EF70A72109A732EDD2CFEC21E6A78E4D552FA2F9C515824BDF141AEEC6228A7454D839A18
Malicious:	false
Reputation:	low
Preview:	0\r..m.....OC...._keyhttps://www.googleadservices.com/pagead/conversion/617640813/?random=1626947602792&cv=9&fst=1626947602792&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=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa7j0&sendb=1&ig=1&data=event%3Dconversion&frm=1&url=https%3A%2F%2Fclickup.com%2F&auid=1951469803.1626947567&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://clickup.com/..=.I&/.....e.....Zpp...GP../....3>.Z.H.....M.h.A..Eo.....Gf.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\373e2e2976297dec_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	624
Entropy (8bit):	5.809986588094224
Encrypted:	false
SSDEEP:	12:R+E31zIAggoux2pHgyye3CMxuDPoqMGxa1DEChM8mO8co:kElz9gZuyAyyeSHDQqza1DEChM84
MD5:	76CB8183BA75EC0C78A45B17A69F897D
SHA1:	272CF8A1A9A1DA63A16784EB096648F1586E5FF1
SHA-256:	EDF1796F0D5D49E3D622A07A8A033EDDEA29F40A27AE88E160A57C946CC29DEB
SHA-512:	A5E19F58303475D3DB6E93653104DEB8948BA8B02B4D79172C8B138D0FF0459ADAE6C16ED466ED3296ADD370E00BD3DE9630BB46C489D780C1F442DDC9F576B
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h..@...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/617640813/?random=1626947601252&cv=9&fst=1626947601252&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=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa7j0&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fclickup.com%2F&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/.&.I&/.....r_.....<.8MGPw.....G.,/.$.....9.A..Eo.....(.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3bd725209635ff13_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	720
Entropy (8bit):	5.797589261976477
Encrypted:	false
SSDEEP:	12:VgE31zIArwmoux2pHgyye3CMxuHoynHn0YoqMGxa1DEChbt1zYX1:VgElz9rIuyAyyeSHHoynHoqza1DECh7S

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3bd725209635ff13_0	
MD5:	917D6431FEC0ECFA65F5D2C291E296AA
SHA1:	248B0DC9E64851CFC911F0D8771EEC6A891F1B10
SHA-256:	ED7B3C5493CB93E0F2E4F7871FA74BFD3F00EC31F2E2613A164CFE6FFBF74FD4
SHA-512:	5D7EF7E164808A6401105AEBFFA0D57E1625620816022C3106B1F2D3F698F743F0875EB2764C2D6F7686E7129A7CE5AB4FB845B28FA19B4C5FD6D6197F6AA3A5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L.....+....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/617640813/?random=1626947601257&cv=9&fst=1626947601257&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=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa7j0&sendb=1&ig=1&data=event%3DClearbitSegmentMatch%3Bevent_category%3DSegmentMatches%3Bevent_label%3D2840f98e-0865-4a90-a1e3-ad66bcadd1ec&frm=0&url=https%3A%2F%2Fclickup.com%2F&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/J.&.I&/.....w_.....z.e.....Avn..0.88...4..{y....).A..Eo.....g.>.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4079c17c4ab0c17a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	341
Entropy (8bit):	5.860549397465913
Encrypted:	false
SSDEEP:	6:metYOXdTAqxAXL7PsrsYpFgz/ExOfBQ/0K6tcmh2qhubdTnq1YEQC04d0fBQ/T/:xXBuLUsY6y4QOKmEqIbdGmEb4Q7/
MD5:	DBB0D1C328D9C344A1D7BA443AA1350F
SHA1:	21619E82577289176920CEA395120F0372306161
SHA-256:	D8C6048D3F2E611C630F5DAB7F770A5100C746B86C48092FA921D68601E3D659
SHA-512:	F9D5B89F9B37E3182019654E948EAD56BED99515D1F1D2FBF9D0B8FFA09EE76B2E7C625098131CA27E02A7D9E892796AD7452FD4CFBFD4E65FD62450671CF83
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M....._keyhttps://js.intercomcdn.com/frame-modern.f4b23b0e.js .https://clickup.com/...I&/.....P.....*c.y.....8...l\qi..iS.~.F0....A..Eo.....A..Eo.....I&/.....0FD77AA65AA6586DB5AB54456C6A0F3028FDE8F355F5A8FF8273C9D8BBFF91D3*c.y.....8...l\qi..iS.~.F0....A..Eo.....b=L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\427bba514c5223f8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	698
Entropy (8bit):	5.774143832072966
Encrypted:	false
SSDEEP:	12:NUt2E31zIAQ9moux2pHgyye3CMxuonJdXSNL8maMGxa1DEChV24gXO1:NUgElz9Q9/uyAyyeSHz4za1DEChVi6
MD5:	494DDE2D1477C9B83F2F8B9FCA0ECD9D
SHA1:	153E74B8AAFDD97CE9A18A5E828D200814F770E6
SHA-256:	FF5A3DB172C3C9625DC1FE74497CD4D369654AE15C538F7A0C12DA1CB898FEC6
SHA-512:	A90A7DB596367963906BDA48ED382B43A149CDA55CF96B5616927D152E5720221145EB0DEEA440FDD275E2EF1BD449696293347D12B9F47FA8A9B4DF67DA0BEA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....6....Yj....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/617640813/?random=1626947574815&cv=9&fst=1626947574815&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=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa7j0&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%3D12600861&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/y..I&/.....j.....A..x....."$.r.....r#H.i6.....A..Eo.....&t}.....A..Eo.....

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):	388
Entropy (8bit):	5.451346791167001
Encrypted:	false
SSDEEP:	6:mEYNGcVUXW3nVH0gfllnDUOQimK6tWEYNGcVUXW3nVDLHgJFDUOQi1K6t:GDFAEVwDFDgFEm
MD5:	5CEDE45ECEB986B11E05C2F181B7BBD8
SHA1:	706D1F61EE2F7CC36C714150E5CA273FCED4DBDE
SHA-256:	26C44FEE6237A62F1CFF7BB0F862405E93D45AEC8EE1C1E6355631DDA7DA6F20
SHA-512:	CA341C4AF3A7D3160EEB393FAFAB5A972116184ED7E583D267C1F44C6993889055C189EAFFD97D09B0D440D439A8A3367C24ECDF490B2273043A01E1C58E74C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4303153a6c225d91_0	
Preview:	0\r..m.....>....._keyhttps://js.hs-scripts.com/6613321.js .https://clickup.com/.x.I&/.....b..z.t)..Tbno.v.....M...A..Eo.....p.....A..Eo.....0\r..m.. ....>....._keyhttps://js.hs-scripts.com/6613321.js .https://clickup.com/....I&/.....NX.....b..z.t)..Tbno.v.....M...A..Eo.....).....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\445bbf35774a7481_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	657
Entropy (8bit):	5.8084146686434
Encrypted:	false
SSDEEP:	12:OE31zIAVGux2pHgyye3CMxyHdXSNL8maMGxa1DECh+WAd:OElz9VGuyAyyeS5w4za1DEChDo
MD5:	F3E8280DDB167C04EB83FE2BC2C11B88
SHA1:	A3205145151A41EB5429A17FE4111FBE6E09F510
SHA-256:	D8E5B761E25098CC0749C71FE53E71C09630FCE64675F57F261BA84968EC8F25
SHA-512:	16987B5CD3F3C468A2BC7EC4ADD141255BFF3FE02FE8F424CE2CE495817C8018928135946968EC653871E01E5ED9D36038ADA166C2092540B29CEAFA0942B31
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/617640813/?random=1626947567931&cv=9&fst=1626947567931&nu m=1&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2& gtm=2wg7j0&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fclickup.com%2F%3Futm_source%3Dclickup%26utm_medium%3Ddoc%26utm_campaign%3D12600861 &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/. !..I&/.....'../...awU&.+HC..y..A..Eo.....O.....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):	398
Entropy (8bit):	5.472653908419169
Encrypted:	false
SSDEEP:	6:m3ycnYGLQmpd9VKsDugGSgD/TpRK6tW3ycnYGLQmpd9VPpi+HgwhgD/TzK6t:APTp7VzbsNrCPTp7VY+vhsR
MD5:	1FE0B1920328320363BC6B343C315B5B
SHA1:	011DB43A96FEB403108ACC5DCBF99C752F2AC585
SHA-256:	B01D149509B2667AD36A636564977F45EC629A5AF043BCEC71899A8A44926C76
SHA-512:	5CBEFE9E66D0C0923EB29B1831025F488C8D765DA3286640E7957CAFB5DDD1632794F201F298DC850D66CD246A601BC26C9180D8924C2AE3BABF047F1CEE8E 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....C...c.E....._keyhttps://www.redditstatic.com/ads/pixel.js .https://clickup.com/>...I&/.....[.....X.!..lf.k..*+|..T.;h.'..S..C..A..Eo.....D@.....A..Eo.....0\r. .m.....C...c.E....._keyhttps://www.redditstatic.com/ads/pixel.js .https://clickup.com/....I&/....._.....X.!..lf.k..*+|..T.;h.'..S..C..A..Eo.....~P.....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):	376
Entropy (8bit):	5.440608225529668
Encrypted:	false
SSDEEP:	6:mrVY9i9UyNi1tgXYb2O3fVlgXAKK6tWrVY9i9UAiHgs12O3fVlgXAWhZK6t:kMiiDvBvfyTSMiiAuBvfytT
MD5:	DB73D0F29BC3A0069AD3A9AD7FA83189
SHA1:	AEAC921B3869B29B00509B754A1AF0F941F6729D
SHA-256:	9C8F12A4D45A96CB887480F2DE18D313DC56F5290550FB1DD18753C42D441B42
SHA-512:	5D136125A16ADE725488886431CA0B4DE99D2562D8C6CE0FDC728A8C7EC812EC054483F042911425DEC4CE36F87825CB36D38C4FCB48B753F2C6ECEFB8F1F0 E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....8.....)...._keyhttps://a.quora.com/qevents.js .https://clickup.com/x..I&/.....F..V=..p...#...N.....og...b..r.A..Eo.....|.....A..Eo.....0\r..m.....8.. ...)...._keyhttps://a.quora.com/qevents.js .https://clickup.com/....I&/.....X.....F..V=..p...#...N.....og...b..r.A..Eo.....-.....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
File Type:	data
Category:	dropped
Size (bytes):	430

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4e268f2ebf5198c2_0	
Entropy (8bit):	5.57119401717866
Encrypted:	false
SSDEEP:	6:msPMYGLfjsVgWPWRb6DgFgp/Fb5WJaIlt04ECDK6tWsPMYGLfjsVgWPWRb6DAxFq:BeDSgU9oVLeDSAdoL
MD5:	2CEB3E310A2D20BABD876540EC6E16A7
SHA1:	4C8FDB576925EA425176AA8DD46965BFD1A27D28
SHA-256:	349E350A620C68809127CDA2F4489456C3D1BA47CBF2B68088796F025D286622
SHA-512:	EA6A79AE8E58AD87FDADB7A355FE04F7B115372F09ABE93EEF1D0D7FADBA4DE6015D425A440BCB8B712EEC4D1844EA9691A9F03698C29D7227A94967691885C2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S....Vc"...._keyhttps://www.googleoptimize.com/optimize.js?id=GTM-PBLF7VJ .https://clickup.com/:..I&/.....`....>.z....?T.j.s.....d9 ...A..Eo.....%la.....A..Eo.....0\r..m.....S....Vc"...._keyhttps://www.googleoptimize.com/optimize.js?id=GTM-PBLF7VJ .https://clickup.com/....I&/.....nS.....`....>.z....?T.j.s.....d9 ...A..Eo.....E.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4ea3db30097f22d2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	221
Entropy (8bit):	5.565314493740346
Encrypted:	false
SSDEEP:	3:m+lzfDA8RzYKfG9HuVLkj+tH26XE2U9LPwP9L6y/lHCElzvZH1xXTZTaoyg4mKkD:mafNYKf4Lj+1xGpPULgEvbVnhnK6t
MD5:	73428B3105402E9B0DB24D659F74F1D1
SHA1:	6F1533B74A3EC5E359A25F9C7B95C1B4BB21CE96
SHA-256:	B1F3EC6E662586157AAB762E87C3AD5E61D52B3516247EEC76DF1ECA0CE5C937
SHA-512:	8833B6DD55C8E539F558B003EA2FED685AE9FEAAAA93B8D7BFEA2D1295EBD0D5705267DB2A1DF400808613194341CCF7B557349C3AF3AC273CDDADA4811E9ED
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Y...].%M...._keyhttps://doc-cdn.clickup.com/7856-es2015.122e92b45bfc22109102.js .https://clickup.com/"..I&/.....R.....l....@g.\2.md.`...2q~.Lo...8..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\52022017b76089e8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12607
Entropy (8bit):	5.437099851520041
Encrypted:	false
SSDEEP:	192:Dag+phgmeFMle5G4BB5UaSZFI4bLFhVIiOD+16y:DkfgjFMkvBztSU8hkFun
MD5:	C3E40E727D36BEE72CEF44512238DC23
SHA1:	888F391859CAA026F2591F8B1D60DD8BF34E292E
SHA-256:	D0A6BFE608A62C55AD5F3580E3DDE28752C105464C52E76E3447E2B55B03F3D5
SHA-512:	BB297B2C6E572802487601ED1CBECCADC3620772E8523E2EE690CEF397057E566928E7DC860F40A7AD6EABC06A6E9863A2564B88C65F25AADFD3013793258D45
Malicious:	false
Reputation:	low
Preview:	0\r..m.....O....._keyhttps://client.mutinycdn.com/mutiny-client/8.2.1.0.js .https://clickup.com/._#.I&/.....2.....C.s&)..S...ReP.6.J.(.....AY.A..Eo.....A..Eo.....'.}*....O...../.....P.....(S....`.....(L`.....Q.@.....window....Q.`.h-.....mutinyWpJsonp.....Qbj..U....push.....`.....L`.....`.....Ma.....`.....(..b.....C`....C`....C`.....(S...`.....(L`.....XRc(.....QbB. .....r.....Qb...q....o.....S....M...Qb.....c.....R..e.....Qb.....64..`.....Pc.....push.64.a.....(S.....Ia....B.....d.....@.*.....d.....@.....q.....@.-....DP.....5...https://client.mutinycdn.com/mutiny-client/8.2.1.0.js...a.....D`....D`....D`.....`....&...&....&.(S.....Iam...y...I.....d.....@.....&.(S...Ia.....I..d.....@.....&..A..D&.(S.....IaL.....d.....@.....R.....d.....@.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5349ba7143b2fdb1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	221
Entropy (8bit):	5.597572976932554
Encrypted:	false
SSDEEP:	6:ma19YKf4NhGVqgRNRKDGKcugct/fZ0h6AplK6t:+NhGVxIDG3a/o
MD5:	60AEF0C4915EA6B2C188D7B04E173364
SHA1:	5CFB0425869313DCAD1C8C92B5DA219B0AB79658
SHA-256:	0F3FE54641DD1EE64F37E50DE55CA435352CB572C401FF9E00751F8295739B60
SHA-512:	07B9DAAF81F57CB8120E04850B5775ADD96021ACF702A3A12BB56029DAC338334DFB894C7A703AA80AB90C429C43A2A0593EA28F21591DC4702E5DFF8708F5A

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5349ba7143b2fdb1_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Y.....mx...._keyhttps://doc-cdn.clickup.com/9062-es2015.b426bdbe8d7d844cc44f.js .https://clickup.com/...I&/.....|.....S.>Kvi...P./..vH;..+5..>.6]....A..Eo... ...w.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\546e83495969be22_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	630
Entropy (8bit):	5.745304689568595
Encrypted:	false
SSDEEP:	12:7/twE31zIA15oux2pHgyye3CMxuonJoqMGxa1DEChqKoDuP:T+Elz91SuyAyyeSHDqza1DEChqnm
MD5:	0A23A8BCC02A0D9494291F5D9C5EB33C
SHA1:	E89F4FF22CDCE1E06A5F45CB6B41604326E618BA
SHA-256:	4A7436F5D42CDC676EE9B20ACDFD481A0CEAE9F3FC17057105740021040FE742
SHA-512:	53415A4A4DB372CED80E3015346CE595D686D1ED1637E71D6058C409DE5B05162C6B38AC043F4CC08CD6E07BA6DDF355BD96E7BEF05CDF710B08FD96BFB08 79
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/617640813/?random=1626947602702&cv=9&fst=1626947602702&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=-420&u_java=false&u_nplug=1&u _nmime=2&gtm=2oa7j0&sendb=1&ig=1&data=event%3Doptimize.callback&frm=0&url=https%3A%2F%2Fclickup.com%2F&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/ p<.I&/.....e.....)2..j..p.. vw.p.N^G7-.CJi.f.@a..A..Eo.....a.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\594b85ba9e2c9367_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	347
Entropy (8bit):	5.909625587698374
Encrypted:	false
SSDEEP:	6:msmyEYMHAJnEPxV3iugElGKYWQZ4gOndDK6tMtnedxyhShFqVPQZ4gOnBt:B98OMxV3iyYwQZ4gOd1Q6xFYVPQZ4gOf
MD5:	F71727D4E39EBE342D67A4E360F65E8E
SHA1:	1DE0A10ED1E9487729A4631312957E25FCFD771C
SHA-256:	10DBA04B6D0D51E08768B544517FD8A159EB2FC64F42B074CFE8B4EC95C3DE0B
SHA-512:	0A8B7E33529B197E8E62BBAA9A1D698EF9DA8090C2CF8B4921A72566DFE6A6976B553A79A3B5FD49235D6B54798D22BF168285F61894EAD10214F4231BECC827
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S....XQ....._keyhttps://script.hotjar.com/modules.a6e08df3d112e629a598.js .https://clickup.com/....I&/.....Q.....=...h.>..u..D.f.T....^...A..Eo.....xu.,.....A. .Eo.....I&/. ...AD19B62093789652E5485A8E056E14777DACDFBDB37DF56B57B3A5480A265AD8....=...h.>..u..D.f.T....^...A..Eo.....L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5cb6e3852eaeee3e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	32422
Entropy (8bit):	5.082073737113371
Encrypted:	false
SSDEEP:	384:Dt974NfCHPNuRS8WWnSyxI5liwUvpHjcCkOF/gR/FbZ/0ehOJPDH5bIJIw7xAsVw:Dt9iERCFFER+jVH+pkLRj/HRncy
MD5:	6CD67BA441E69712AA79B7675954C2F7
SHA1:	2EF41151D4624C3258303E2E5C160CBCD2A75213
SHA-256:	5CD8235E6A205F9E3ABE0452644E13F5BCADF0622EF41CF57A175D0D68FC3177
SHA-512:	B65D0BDCB4EC32E555A77074984BFF18D62DB42E087FD3F9CBFB750B470A923A8C5C87542E3260805D9DF8B876599D7CA60AAFE72FEF2A8CBEDE2E655D0795 74
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N.....u....._keyhttps://js.intercomcdn.com/vendor-modern.0c2722c5.js .https://clickup.com/...I&/.....|....tn...~.B9.c.s...P..7..2...A..Eo.....1EKG.....A..Eo.. .....'.....O....}..}.....(...L...(.....(S...M...`N".....L`n.....Q.@.....window....Q.Pr%.T....webpackJsonp..Qbj..U....push..... `.....L`.....`.....Ma....^...`.....`....q.La4.....E`.....E`.....Ea.....E`.....Ea.....E`.....Ea.....Ea.....Eb.....E`.....Ec.....E`....Ea.....E`.....El..... .....E`.....E`.....Eo.....E`.....Ea.....Eq.....Ea.....E`.....E`.....Ek..... .....E.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\603911c3c110b630_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1435
Entropy (8bit):	5.3294959905833945
Encrypted:	false
SSDEEP:	24:JaOdIYNbza1DHPZFGOen44aVza1FUfYk3LKjYXPkYX7XZv+iYX2kYXnvYXBzfpRs:U62Z8744awUfYkbakPkk7XZvJk2kkvki
MD5:	35FEF690A14DC0A36204D36A2B22403E
SHA1:	F8C429D16D2A1BC35443EF72C99FABBEF18CF7D5
SHA-256:	1BC94885222266873430D69B8731AD2D20D3820B18FEB148D91AAD2116E4DF08
SHA-512:	2B7EF0AC6A689BE143F14D1EDE801733536F1A48EDC8A2978B7689E6A2BE664210052DEA1D756651BA5B4D0D13533E0E88A1433EB5E3A5B2D8C999F4BB77C8E9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....E...._keyhttps://px.steelhousemedia.com/st?ga_tracking_id=UA-87708648-1&ga_client_id=468527249.1626947568&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%22468527249.1626947568%22%2C%22shpt%22%3A%22ClickUp%E2%84%A2%20%7C%20One%20app%20to%20replace%20them%20all%22%2C%22dcm_cid%22%3A%22468527249.1626947568%22%2C%22dcm_gid%22%3A%221227578407.1626947568%22%2C%22execution_workflow%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%22getClientIdByGAData%22%3A%22FAILED%22%2C%22getClientIdByCookie%22%3A%22FAILED%22%2C%22shpt%22%3A%22OK%22%2C%22dcm_cid%22%3A%22OK%22%2C%22dcm_gid%22%3A%22OK%22%7D%2C%22message%22%3A%7B%7D%7D&dcm_cid=468527249.1626947568&dcm_gid=1227578407.1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\637a935098941fba_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	216
Entropy (8bit):	5.6100052246557945
Encrypted:	false
SSDEEP:	3:m+lUSXa8RzYP2FycyGYWCULLuFvDM67LGeZxct/lHCSrJOwga4xEsoyP5mSilpK+:mWXXYerCUq7LGftgyAwEH4LK6t
MD5:	4D0D62E1141DEDB7C20B705353277F32
SHA1:	AB4525243D99C9FE1C8CE6E32931DB3EA59CF42D
SHA-256:	D1FE7EF5F58B0518FDE242222238DD87FB8493D281FC0C95DFB92585BDA1F1A7
SHA-512:	7446BE36A1714735713EA43CDB7FEA44B7B98F7C20A4D8319ABCA55E716645B01626BCC2F0447845110DB91FC5AFEC0F89954C18D3BF780C3D5265DDA5B2221
Malicious:	false
Reputation:	low
Preview:	0\r..m.....T....1....._keyhttps://code.jquery.com/jquery-3.2.1.slim.min.js .https://mega-sharedrives.club/G...I&/.....! M+.\.J....r..p.....vH..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6489d258291920b6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	788
Entropy (8bit):	5.799712783717595
Encrypted:	false
SSDEEP:	24:qElz92DXuyAyyeSHHoynHQ4za1DEChfFX:qElxyurfob5FX
MD5:	C0BED669CAC03164B55006150D34B66D
SHA1:	A2E00DA2B21D6115980AD96E57581A781A9F523C
SHA-256:	2268205D29DDA18481F4C4B09485EAB21FD5FEF77C3F6DDB19007253C6A5B407
SHA-512:	A81E3DA2C9640DB67953C923C2C272166B0F66CBF3C1EDB3D37853ECBBF5C42337A010B93013825D14C5949D2FA7B814F75273CA02D156998F008BB88580663A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....GV...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/617640813/?random=1626947567941&cv=9&fst=1626947567941&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=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa7j0&sendb=1&ig=1&data=event%3DClearbitSegmentMatch%3Bevent_category%3DSegmentMatches%3Bevent_label%3D2840f98e-0865-4a90-a1e3-ad66bcadd1ec&frm=0&url=https%3A%2F%2Fclickup.com%2F%3Futm_source%3Dclickup%26utm_medium%3Ddoc%26utm_campaign%3D12600861&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..I&/.....)O.2C).X.w.7.m....+...IB|T.....A..Eo.....1.3.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\64e1d7183b6658e9_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\64e1d7183b6658e9_0	
Size (bytes):	624
Entropy (8bit):	5.818988160353869
Encrypted:	false
SSDEEP:	12:VnE3YmiY1oux2pHgyye3CMxuDwdXSNL8mD2ChyNx17:VnEImiYuuyAyyeSHDpJ2Chs7
MD5:	A905499A3AA13556E0E8A80ED4FD13FF
SHA1:	7473C9444399EF887EB6E86216F9C7271D16468F
SHA-256:	EF670FA11600F6F52FCEA9A4EE3534BF86250DCBD5807CDC9E628A618E972B95
SHA-512:	504D97E53E2C269965AC4FC53597384EC44E484A063E686C7BFC2C8388D181C9649AC69E8663EABB9070A7B319DF9D63EE20FE695CE01553294EA6BD1ABDD08 A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....2....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/867030291/?random=1626947574206&cv=9&fst=1626947574206&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=-420&u_java=false&u_nplug=1&u_ nmime=2&gtm=2oa7j0&sendb=1&ig=1&data=event%3Dgtag.config&frm=1&url=https%3A%2F%2Fclickup.com%2F%3Futm_source%3Dclickup%26utm_mediu m%3Ddoc%26utm_campaign%3D12600861&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://clickup.com/Z...I&/.....I..^..A.J..|-..34...$.$].M.2 .x..A..Eo.....0.yW.....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):	41046
Entropy (8bit):	6.274583005701176
Encrypted:	false
SSDEEP:	768:PBuO2UYjiDqS6AWnjmCJV1ndafXeg0wiHdTzjbqIo5ZioxYd:PBgUYjiZjWmCL1ndafXegwdTzjOF7Yd
MD5:	DF3EBFA173DDE8D52178EABA4E637EC3
SHA1:	A28E37757A268C8589485964ADAE3FCE46A3559A
SHA-256:	39E34BB1BE00D33136D5695A7DFBC7269B17CD71EC00ADB21128BC3BD0C79ED2
SHA-512:	C26785E96814E204025770761555C2E01E1FF0B8212B581C928C7B523CCC2E4BBE0856DE22C35167C6E1DF8AF39DD601BB26A64CCA018BFF654EE0FD32FE379
Malicious:	false
Reputation:	low
Preview:	0\r..m.....5.....0...._keyhttps://bat.bing.com/bat.js .https://clickup.com/....I&/.....g.....j.5)6..0-ka...f.....']..r.'4..A..Eo.....A..Eo.....0\r..m.....5.....0...._ke yhttps://bat.bing.com/bat.js .https://clickup.com/....I&/....._.....j.5)6..0-ka...f.....']..r.'4..A..Eo.....U(.....A..Eo.....'.6w....O.....p..... .....|.....X.....(S.0..`.....L`..... L`.....(S.U..`^.....L`.....<Rc.....Qb...q....o.....Qb:.:.....n...b$.....Qb.....UET.`....Da....B....(S.4.`.....L`.....M...K`... .Dg.....%...(...&..j.....,Rc.....I`.....5.a.....!...a.....Qd.....stringExistsaT.....a ....b.....@...@.-....(P.....https://bat.bing.com/bat.js.a.....D`.... D`....D`.....`\|...&...&....&..."&.(S.}...`.....PL`$.....Qcn..F....document..Qb.E.i....body..Qd.....readyState....Qd6.....in

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6c5995e5e9020eaa_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.90209719784889
Encrypted:	false
SSDEEP:	12:IwtnAKmCIIFH/ux2pHgyye3CMxucLSdXSNL8m2yChlssEe:7SKmCIIFfuyAyyeSHuBChlsle
MD5:	43147101AB46840C218070A670C9E6AD
SHA1:	00204CC32EBE0CB1EE6ACA110234117C7B81FA62
SHA-256:	BFE539882333FFF2D987126D101103514EB7116EC1D00A11495922B9E6EF059C
SHA-512:	F02A4DBAEE0635D3E96B0D70C02B7C051EA44553CF63298D3682D028E859FE95E8E867725F6616E8446983C781009F5BA59A40FED9D7D5A007D48D839B3E2068
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i.....keyhttps://www.googleadservices.com/pagead/conversion/867030291/?random=1626947574208&cv=9&fst=1626947574208&num=1&label=sFHSC La0k-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=-420&u_java=fals e&u_nplug=1&u_nmime=2&gtm=2oa7j0&sendb=1&ig=1&data=event%3Dconversion&frm=1&url=https%3A%2F%2Fclickup.com%2F%3Futm_source%3Dclicku p%26utm_medium%3Ddoc%26utm_campaign%3D12600861&auid=1951469803.1626947567&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://clickup. com/....I&/.....B.....^E.m..[...k.N0.g....!5.@`...).A..Eo.....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):	408
Entropy (8bit):	5.465818134162609
Encrypted:	false
SSDEEP:	6:mmY2B5hVTBtg1v01uH4SK6tWmY2B5hVKHgfq01uH4CK6t:9rVTB8NHzLrVKlNHv
MD5:	1B7618725AD9CBE4830FF541A63AD160

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\701263a561b04671_0	
SHA1:	0AB0182873653A923430CADC32B053E4368D242F
SHA-256:	506EBECD6A885AA128B50B60F33DBD6AF01AB4AFF38E94260B825AB263A39DC8
SHA-512:	EFD73188FFD4DC0288711BCEC1E8E57FFF786F79AB1CD99BE74F44EDE6A330C5E5E9A2C74D16D2BD93ED1D35D6ED930B05DA5B3C60DE984DD027AD38C7D27A4
Malicious:	false
Reputation:	low
Preview:	0\r..m.....H....:;(...._keyhttps://calendly.com/assets/external/widget.js .https://clickup.com/..I&/.....e..L9E..}.8.....>.W.Z.`.5;v.Y{..A..Eo.....A..Eo..... 0\r..m.....H....:;(...._keyhttps://calendly.com/assets/external/widget.js .https://clickup.com/.1..I&/.....:W.....e..L9E..}.8.....>.W.Z.`.5;v.Y{..A..Eo.....|.....A..Eo..... ...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\70fbd66c3b329f27_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	163784
Entropy (8bit):	5.964409971274706
Encrypted:	false
SSDEEP:	3072:vhnVjRrRidcKu+P562+QqeKC+c/B+gMda+qehQ:vhlRlNCkTeBn+gMd6T
MD5:	40A685DB700A8212172D78D5AEB1655F
SHA1:	00C40ECEE2010B94C4DDCBBB7C3AAFB4FDDF3C9E
SHA-256:	C14271CD25F603807B0C0E2B61018E014CC6CA8D722DA62DF765A49535D2700C
SHA-512:	64D06B5F7B0D2C546F67C6CB3C9720B705525CC88656BD35BAE768214DC6CBE21A92EFAC2F587315F0839D52CCA9D6573FA7246213203A872F1CE0734094B25
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.../.fn....AD19B62093789652E5485A8E056E14777DACDFBDB37DF56B57B3A5480A265AD8.....'.@T....O5... ~....~.....`.....x...0.... .....(S.9...`.....L`.....(S...`.....LL`"....@Rc.....Qb..s....e.....Qb~..u... .t.....Qb:.:.....n...b$.....I`....Da.... ....(S...`.....L`.....Q.@.(.....exports..$..a.....S.C..Qb.7d....I...H..!....a.....Qb...0....call... ..K`....D}8.....&.%.*.....&.%.*..&.( .....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&.(...&...&.'..W.....-...(.....,Rc.....`....Da@...8....!.....e..... P.....@....@.-....HP.....9...https://script.hotjar.com /modules.a6e08df3d112e629a598.js...a.....D`....D`....D`.....a....`,...&...&....&....&...(S.X..`.I....L`.....Qb...q....o.....e.....a.....G...C..

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):	283
Entropy (8bit):	5.495562324594493
Encrypted:	false
SSDEEP:	6:mVJVYOXdTmNgR7sVKTgR68adZnt/lbK6tILgTt68adZns:CX0WRwVKM686ZF+4686Zs
MD5:	A0AD914267EAE0B1C7B70628B022CC12
SHA1:	EC53FF8E55769E48EE1A19736EBC36EA9C048859
SHA-256:	46516D0B7EF1A2F22B33D26C5B1CCC9889175B6A6B6371DAF691E8ABAB0BAC32
SHA-512:	DF9D83A6CF6DA3709BBDF3D4A388C061DEC9E4342A658D0F48DFA9A3B23286DCAA5BA5397199F42F4915C712CE606A3827633C41465F523DDCC5C40CAAAE7E0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....C....,.....,_keyhttps://js.intercomcdn.com/shim.latest.js .https://clickup.com/vH..I&/.....5.V3}.d...|._;5..x2X...1..Br_+.P.A..Eo.....A..Eo.....Q.. .I&/.....}.....5.V3}.d...|._;5..x2X...1..Br_+.P.A..Eo.....9kF.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\72a529d08e0ccb34_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	221
Entropy (8bit):	5.61547051896625
Encrypted:	false
SSDEEP:	6:maXEYKf44yJVIrFgYLbSTA4whoP4nfTlDK6t:L4yJuVLWs4co0Tl1
MD5:	C74041F613D35F70F0A4BE24A257FA15
SHA1:	7D96828858EF7D3FA5D295D9797857C95BB1A296
SHA-256:	D5C31A982DA5AEB4E6A38FCF1C3FA1719C002E3020FD767E176E5B2B2CE4412E
SHA-512:	7154BE219F2EFE03E6BD403DFF6401F08CE497911D1F9264CC64CF92B70103C18294D1BF24EBA0553FFE348BED49A52EE8242B50CE6ADFB0BF5AB0E9FBF47186
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Y....D.....,_keyhttps://doc-cdn.clickup.com/9154-es2015.ee4d66b014ebd86b4425.js .https://clickup.com/...I&/.....>...B...>l....<b.....n..=.A..Eo..... ..wz.....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
Size (bytes):	11781
Entropy (8bit):	5.51018568317737
Encrypted:	false
SSDEEP:	192:iyv5zn5I4K/JcbDAzfITjhkGpJ0IEc/+h6kjITqocUvUk/IHLSPgzhH6r1nr+:78jibDCoq6HB/+h1jxBUcFrUOkr1nq
MD5:	12777C7D6874DB24DE42507B8F681A6B
SHA1:	4E8D45E7A55EA49880D28F5298376631B5652AE3
SHA-256:	1D4660D0FB83C85803FACA6F3616960B2C222310EA7A02A053F901331BCC6824
SHA-512:	70DB5E680B998DD0465AEFE924503BB0603ACE4C8477A19046566A54E884BCE1657195270634618F9976C44EB37DEB3BD2DECC68613C17560298744C69207FD9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....E.....A....._keyhttps://clickup.com/landing/js/typed.min.js .https://clickup.com/sX.I&/.....^!.j|.^0.8...Q..O.....qhF....^..A..Eo.....|.....A..Eo.....'..-....O.....,..R.....$.....(S.<..`2....L`.....(S...`.....L`.....Q.@.(.....exports...Q.@.A.....module....Q.@n.a.....define....Qb..`.....amd...Q.@.....Typed.....K`....D}.....s.....s.....&.\..&.-...%..H...s.....&.(.....&.\|.&.^.....&...s.....&.\..&.-...%...\..&.-...%.....(Rc.....I`....Da..... ..f.....`...p...0.....@.-....8P....+...https://clickup.com/landing/js/typed.min.js.a.....D`....D`V...D`.....-....`....&...&....&.(S.d.`..... L`.....(S.`.`x.... L`.....@Rc.....Qb~..u....t....Qb..s....e.....Qb..\|.....s...b$.....I`....DaP.....(S...`.....L`.....!..$..a.....a.....Qb..%.....id..C..Qcv.....loaded..H.....Qb...0....call.....K`....D}8.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\744090898999c899_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	221
Entropy (8bit):	5.630331209080025
Encrypted:	false
SSDEEP:	3:m+lzsA8RzYKfG9HuVLReUrHxEar137WFvNRP9LE5cu/lHCDktllSJkVFdidxAK5e:maSYKf4RUVhpLsNV2ng4XlEdB49K6t
MD5:	68A8B973F75A723E7BD0295CE342B48B
SHA1:	8F2C875727F24C92044D644601411B3C73EACC67
SHA-256:	3002D461797AD270AF4D85674413613DE68383C178B4B9CB867BA36D021931C0
SHA-512:	66EF85AFF731C73839AD603A18BE597E238A3CA425941E3B6391D82A205117E0DC048F9FD31F1FE0A16F30AD687893806A41D5FB42A2C231FD784C620872EAAE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Y.....Y...._keyhttps://doc-cdn.clickup.com/2536-es2015.2ef417be10301f0ddf7a.js .https://clickup.com/-n.I&/....."..9..&.F#...Gjf..m.....J..A..Eo.....B~~z.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\749a220922933abd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	589
Entropy (8bit):	5.807557673293195
Encrypted:	false
SSDEEP:	12:OKE31zIA/1PGnux2pHgyye3CMxyHoqMGxa1DECh0T:OKElz91CuyAyyeS5Iqza1DEChE
MD5:	77B58864DEC2634B713353C47479D5AF
SHA1:	EB66BC7EF961E68508B7CA5A03306A86F8A194CC
SHA-256:	D4CFD912103A0B00A7814C40C8B9A50F8E2399B0AF4D0A6CF6EC33076E307091
SHA-512:	6CF5431B9BFF702FCC3C1751D94D46079E99467D9592C8994D26237DB3C8B1C55B0DCA6E78356775813CE54C0DC46D76A40D7E81030A384553154BA8A8EFB76
Malicious:	false
Reputation:	low
Preview:	0\r..m.....?....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/617640813/?random=1626947601282&cv=9&fst=1626947601282&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=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2wg7j0&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fclickup.com%2F&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/..&.I&/.....z_.....(.;.s.W..ND...v.....p.n..<...${..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7ab419a08f43bbb9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	94200
Entropy (8bit):	5.771076069995835
Encrypted:	false
SSDEEP:	1536:9IGi8endqgq433b1kojyHK1zvgTjbGkQEbs5qu4Wax3h5EYWZrDeNZ9G1qvSPq:45qF4yxHKZ/kdbsXni3h5DWZOw1q9
MD5:	DE75D6DF1D4F7FB2FE487E02B0822193

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7ab419a08f43bbb9_0	
SHA1:	28D74625CA119908136167EC5AC2C022E0A47E24
SHA-256:	1B66662CE6A722F9567347A761349A85EE75F65BC037D106A8A01A4D707F03D8
SHA-512:	07105373F235585D9DABB4915CF0B30A7B624980A1AE149BE34B5BA346C93C3CC462BCF531B3199D276715B6B09E46C31B7F861016FCDC6F2DC71422CA58F58
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...o.....E81DF66ADB400B31D2C527DEF23561CE08F3557798B721BFDDC438A3EEE2A49E.....'.JN....O ....n..Q.R@.....!..... .....(S.H..`L.....L`.....(S.p.`.....L`.....0Rc.....O.`....I`....Da....*.....Q.@..Qo....module....Q.@.....exports...Qc..O... ..document.(S.....5.a.....a.....a.....a.....a.....Pc.....exportsa.....I.....@.-....LP.!.....@...https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/j query.min.jsa.....D`....D`....D`.....`z...&...&..!.&....&.(S....I..`.C.....q.L`.....Rc@.....M.....Qb..gP....d.....Qb.....e.....Qbrz.....f.....QbN_S"....h.....S...Qb.3|.....j.....Q b..6....k.....Qbv.e.....l.....Qb.w.....n.....QbZ..U....o.....Qb.S.....p.....Qb>.....q.....Qb.<".....r.....Qbb.q8....s.....R....Qb.._....v.....Qb*V.....w.....Qb.%.....x.....Qb.2(.....y....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7bb6e79a05d24274_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	209
Entropy (8bit):	5.496796378665317
Encrypted:	false
SSDEEP:	6:meSYlNYpSVkL7LG8jFgTcklYeZh4j/ZK6t:apSVy+Csli
MD5:	2EC9F0A441FBF41EF74086057EC34CA6
SHA1:	F9DE4DC18AA85434A227714852184B2E1B368C3D
SHA-256:	88DADDE287AF5A7B5AC707579F6C85D0B5228EB9F0F9AF4FBB074DB001D8A297
SHA-512:	6828CC6ACC2691B0B760CF10D1B255DB6C627B179D2B1E7B964C25B9AB9778BBEBB60E9B11DC078F8BFBBEE3DC6431B35DD69839C4BE583983CCDE6340AF9 63D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....M.../.\Z...._keyhttps://kit.fontawesome.com/585b051251.js .https://mega-sharedrives.club/....I&/.....uPF..i,...{w>.p..k.]..W\e.Z...".A..Eo.....A..Eo .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7ebb96a0f70a6e4d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	416
Entropy (8bit):	5.574116665668942
Encrypted:	false
SSDEEP:	6:mYXVYGKxWWdsG6gibRPRHgSklvoOecwsqbK6tWYXVYGKxWWdsG6gibRPegVoOecY:X1l9jgibV0lCBfNJ1l9jgibVOB/
MD5:	FDC40ED46AD9E948A77BEB16B147007B
SHA1:	384D6FB774B552EEB2E966A27A3EDDC91041BAFA
SHA-256:	5F7A0678549A85C9DCF22BC1B17CE273F8B9F275DC1CBCA1E1C39F609CD4DC2A
SHA-512:	133F8EBDDE8DDCCCA20551541CA9579BB1F1B241317550F461A78FCBD5BE06C0E8C9092D1BD30243E6DC8D619A4145A2A37613EE57BD83A328113D9ED0F022 6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....L...JYf@...._keyhttps://ws.zoominfo.com/pixel/xHmqLhll6GszCuhf3oq6 .https://clickup.com/o7..I&/.....(...}....~.n..u.B.....A..Eo.....g.....A..Eo..... .....0\r..m.....L...JYf@...._keyhttps://ws.zoominfo.com/pixel/xHmqLhll6GszCuhf3oq6 .https://clickup.com/R...I&/.....1[.....(...}....~.n..u.B.....A..Eo.....Ej..... ...A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\80df7f2f865f475d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	364
Entropy (8bit):	5.922049000322541
Encrypted:	false
SSDEEP:	6:m2YXXYSHT8NWQAlKPUQyh7LGxHgf1PerBhpGvP4fAK6thAv/GLrwJNXDerBhpGve:61z8NWQCUU3+vrkCiQv+H6X6rkm
MD5:	FFEA978F0A01DACC227560A2923F8D78
SHA1:	931964886FEDFB2FFA69C00819EB5F8C60D641EB
SHA-256:	27E59C56022C04EFE9A5AC88CE3CEEBE71E005CF0A08D189D82A8722BEB244BB
SHA-512:	5FDF0166A1D77D65057A2B767C28CA08169E6AA5CAFE0897E5ABDD94D954AB200049C69E29C4A381BF20F169231F484439B685F015C13FA180BBB7733EB0C07
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d...U.O9...._keyhttps://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js .https://mega-sharedrives.club/>N..I&/.....Dl...4..m..~Y.D.k.7e.H..Y... ..A..Eo.....A..Eo.....>N..I&/.Po..E81DF66ADB400B31D2C527DEF23561CE08F3557798B721BFDDC438A3EEE2A49E.Dl...4..m..~Y.D.k.7e.H..Y.....A..E o.....I5..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\82781dd014573594_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	712
Entropy (8bit):	5.7970396624745275
Encrypted:	false
SSDEEP:	12:4E31zIA3KJHD/ux2pHgyye3CMxuIJcZJwloqMGxa1DEChkSz/:4Elz9aJHLuyAyyeSHIyZxqza1DEChb
MD5:	8635B5D6DE519EF9902D7E9E1F5E7E22
SHA1:	4E167258ED9502DF0E27A728269F3FE7967657F3
SHA-256:	AC51C01E3CA88789AE9F6FEBDF698F015A9F44C56D372337A8C33D5E3C305ACB
SHA-512:	3EBAE2D1FF2CEF705DF959CA9361A530791E3FA310A21068EFE53116FF44B6E0AC050A25CEF9931F112BB4CA89A718722F1760B975A52C3E2820F90D33ECA8E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....D...I..Y...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/617640813/?random=1626947602080&cv=9&fst=1626947602080&num=1&value=0&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=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa7j0&sendb=1&ig=1&data=event%3DInvalid_Users%3Bevent_category%3DCHEQ%3Bevent_label%3DInvalid_Users%3BnonInteraction%3Dtrue&frm=0&url=https%3A%2F%2Fclickup.com%2F&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/.33.I&/.....vc.....!...*F..D....).B.(..~.2.Z....A..Eo.....Ya(.....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):	390
Entropy (8bit):	5.4522616730421785
Encrypted:	false
SSDEEP:	6:mcdnYk+OVFugvtryIlyA8DK6tWcdnYk+OVfyg97yIlyAK/hK6t:FdD+OV5m7/jdD+OV3275
MD5:	4E07BD754E2611F9A1492F95F1FE943A
SHA1:	7A5D471037917C0AA5BFFEBFE3B3C1BB684C1DDB
SHA-256:	E9AF690DAB04F0D19E775131B28574B231EE5405E54CA50B4DFECCC932EAFCE7
SHA-512:	C2A33CF781F8B58315FEF5C3EFE43E2C4AA2C76237D53786DF68584FB410C9673C2C08EEC29300EEA8E0C347F86CB383839EE3A1B49F5491E2FEDBFCC8B6660
Malicious:	false
Reputation:	low
Preview:	0\r..m.....?....;....._keyhttps://static.ads-twitter.com/uwt.js .https://clickup.com/._..I&/.....,~...".W.W.!.....>.....'|.A..Eo.....q+=.....A..Eo.....0\r..m.....?....;....._keyhttps://static.ads-twitter.com/uwt.js .https://clickup.com/6...I&/.....3].....,~...".W.W.!.....>.....'|.A..Eo.....U.m.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8aea18e4f4e904e8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	589
Entropy (8bit):	5.827217281310606
Encrypted:	false
SSDEEP:	12:O+E3YmRRdyRAOux2pHgyye3CMxyHoqMGxa1DEChBEuU:O+EImRRdyRAOuyAyyeS5Iqza1DECh2uU
MD5:	8C6E56A4A3DD81A2249B6038D68A2B24
SHA1:	76376522E81A5E8DF3C2BF334F716D0ACCBFE67E
SHA-256:	42D5E87FB2A737CB92CBFA36BC1802CA1EEDD11FC44A3067326EC72D3A555FDF
SHA-512:	DF75B5503EE794D374189D994D3C2BA3BF469365E57707BF7ED8B1D3747EB41D2AF1793E660A2F8E8CDE9BC2D60A27D2A9DB0D5851C423E19CD9745739A114AE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/867030291/?random=1626947601264&cv=9&fst=1626947601264&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=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2wg7j0&sendb=1&ig=1&frm=0&url=https%3A%2F%2Fclickup.com%2F&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/..&.I&/.....x_.....u..~.LDJH..E.,.st...#..Q.+.`.. .A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8cc58348a8fa4cb8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.487218496630977
Encrypted:	false
SSDEEP:	6:maTiPYOXdT04+pmlKvtgOljAnaf9kAP8nK6t:rsXmpN4uZ0

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8cc58348a8fa4cb8_0	
MD5:	C49BCAFA69680ABC5C6990C727FBF5D7
SHA1:	13D25BBE2522871F8EB0788309DFB53A960470A4
SHA-256:	0156E647162823C30619B1778C433586D4FABCED234012B4315AB0E49E5A2D4C
SHA-512:	80D7B5FB8FFDBB871900DEA05D4D93B2A6814F414E575420F496B685E3A7EA96ADBEC4586E5D37AECC5FE64571D0003B8BFF4DB4D4F8663F13E204DD84600E2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K...K/....._keyhttps://js.intercomcdn.com/app-modern.b3a36376.js .https://clickup.com/..4.I&/....."".....U..&..^d.r9e'...y.`oC.....7z.A..Eo.....F..%.....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):	468
Entropy (8bit):	5.615042545617755
Encrypted:	false
SSDEEP:	6:mQ/YMdqdaX2shRd7Me0gHQuxknRK6tWQ/YMdqdaX2shRd7MouLHgmXeuxkn/+DK+:bk22shROe/QFhk22shROouER+1
MD5:	0542D91FC9DC13B5998CDDD4B8E2563E
SHA1:	278EADD16A85F44BA3C838C2042FFE6FA22DEE9E
SHA-256:	ED91EDF0C34E15C3C1FC370CF3248FF0DCB91C4C3ECC5D7D81DDD9EC00F8B3F9
SHA-512:	46BC82441FB4C9B6C09437A32E4BD6D21DB66AB8C20C3E6F65CAD2E982CB641F3EB1EB470121F16210F3FA683577F7941AD9B4CF417B89AAAD11FF9446A52A3F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....f....)....._keyhttps://client-registry.mutinycdn.com/personalize/client/e970333877260fa7.js .https://clickup.com/6A.I&/.....`.,...-F.Sy..C].Z.t...c..D..A..Eo.....A..Eo.....0\r..m.....f....)....._keyhttps://client-registry.mutinycdn.com/personalize/client/e970333877260fa7.js .https://clickup.com/I`..I&/.....S.....`.,...-F.Sy..C].Z.t...c..D..A..Eo.....7.....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
Size (bytes):	2233
Entropy (8bit):	5.60602730467417
Encrypted:	false
SSDEEP:	48:+sLApfr5WrcaLXGcPEtZw/c35QdgUywTgRQgBd:+sEpT5kcabGcPc/xUywYvd
MD5:	96D89E07A896DFBD09AAC599C0A022E6
SHA1:	98E98A1D891415F4692AB5147654C15D2312306B
SHA-256:	3F4527A169A471E9B2EF70EA9DA9771C1A652562AA3D9820D322383FA8C8AB1F
SHA-512:	72C65CB0A43EC75A22AFE1CEDE9CB5D7928F0CB88E2DFE6AC07C9674B1B4620BA4E987BC0909C5B3F01C945DB0736827E732C434DB32F6B38A79110B04A3191
Malicious:	false
Reputation:	low
Preview:	0\r..m.....I....._keyhttps://clickup.com/landing/js/cssrelpreload.js .https://clickup.com/..I&/.....|.....(..U...#.<.I..n.....C...DL....A..Eo.....b'.....A..Eo.....I&/.....'.(.....O....h...}.J.....(S.@..`<.....L`.....(S.)..`.....PL`$....@Rc.....Qb..)g....w.....Qb.Y.)....rp....Qb.".9....run.b$.....I`....DaV.....Q.@j.....loadCSS..(S.....Pd.....w.loadCSS...a]...a...I..q..@.-....<P...../...https://clickup.com/landing/js/cssrelpreload.js.a.....D`....D`....D`.....4...`....&...&....&....&.(S.|.`.....,L`.....4Rc.....Qb.C.....ret.`....I`....Da(...&.....Qcn..F....document..Qe...+....createElement.....QbB.....link..Qc.ZQ....relList...Qc..DT....supports..Q.@...-....preload.. Rc....J.....Qb..s....e...`.....(S.(..`....]..K`....Dd.....,Rc.....I`....Da....$.....d.....@..@.....Kd .....<.....Dy0.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9135788bb4afad70_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	340
Entropy (8bit):	5.9285623231203335
Encrypted:	false
SSDEEP:	6:mZYMK1ME/JmUSLgyjkez5spYK6tWDSNiVBRFUccbNWakez5sp:gREh/MjDNEOuSbNWaD
MD5:	F8F24A263BE5C52F949557F86A677691
SHA1:	C8758C307429E92BB3A931C206BDFFC2B75450AC
SHA-256:	02F34C609A3E499839080195DDF09A234EC53025D071D786CEFB8A3FE30D2E39
SHA-512:	952316A6897DDAAE2518F11E0A5C7AEF194BF5D7014D750EDA591CEAA37040F7A22E6B0F525695BB715CFAFBF9DFFC559CAC144438DDC2E7F27BEFD13D84136F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9135788bb4afad70_0	
Preview:	0\r..m.....L....lh...._keyhttps://clickup.com/landing/js/app.min.ed0eecfe.js .https://clickup.com/&..I&/.....{.....;..ga.....|.....v....A..Eo.....$.W.....A..Eo.....&..I&/.X...9B0892A7C0BE3EEE7EF211B7A770CB217F33B4F90A1F999DA85BDF4804C4562D;..ga.....|.....v....A..Eo.....i..VL.....

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):	5.47180956471078
Encrypted:	false
SSDEEP:	6:mw4YGL+MIwJJyQTgvBtlB/SD/5lhK6tWw4YGL+MIwJJy2lHgctZ/SD/9nK6t:dwlwvyDxqTnwlwvyC3HqD
MD5:	EBA8C01F11E750DF07B18075951FE6AF
SHA1:	FADBFEE6E22C5175FB7A29802B1B5D7DEE2929D7
SHA-256:	AF1DBC024B1EC7F241C5357B694560867ADD5A3F26AB5AA42D6DED9BF4DCD0F9
SHA-512:	5688C5281247D8616A24069673533AE8A48C39852875CDDFF9A3859459A63A1B759E7A49FAB52E2D36FEDCC60D61B2B02BF184BE79FD8E1FE5E9CE0235866AA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G...O....._keyhttps://www.google-analytics.com/analytics.js .https://clickup.com/j...I&/.....g...3..$<-,.s...].....KU...D.A..Eo.....e.Q.....A..Eo..... 0\r..m.....G...O....._keyhttps://www.google-analytics.com/analytics.js .https://clickup.com/*2..I&/.....S^.....g...3..$<-,.s...].....KU...D.A..Eo.....K.....A..Eo..... .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\96f2ac4fdcea48f7_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	556
Entropy (8bit):	5.8054025889159036
Encrypted:	false
SSDEEP:	12:m7wE3YmnKSoux2pHgyye3CMxuDwvChB94ri:mkEImKbuyAyyeSHDsChB9H
MD5:	102F9225389FD722C6A751E20AC455C1
SHA1:	44B0E86CB75D64A2FCEBA58759D8E839C217D29A
SHA-256:	F3C909F1AC66D65F9F939C3799394D80ECA84FCBFBAE1B8F1F93287210DD5FFB
SHA-512:	76AC7E9A424936C44FBA73D59092250B45BE4B4FFAE0D89CDB845804C17DEF089905C5FC3D37851AD794A214080CC8CF7B94C28D7005D17CF41881EC6B9DDA 6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....%...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/867030291/?random=1626947602800&cv=9&fst=1626947602800&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=-420&u_java=false&u_nplug=1& u_nmime=2&gtm=2oa7j0&sendb=1&ig=1&data=event%3Dgtag.config&frm=1&url=https%3A%2F%2Fclickup.com%2F&hn=www.googleadservices.com&async=1&rfmt=3 &fmt=4 .https://clickup.com/.;>.I&/.....e...../.B.....I.<.e.9...AQlh4"..<!...A..Eo....._.`J.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9dd354eb0f4a9237_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1118
Entropy (8bit):	5.384435933553892
Encrypted:	false
SSDEEP:	24:BYaOdIYNbza1DHPZFGOen44aVza1FUfYk3LKV3YXPkYX7XZvBfMSLE6Ta2Qpmw:362Z8744awUfYkb23kPkk7XZvBfMS4Uw
MD5:	A86265D0DF07A20C5D2CF7D9B6031620
SHA1:	7F2F06E8546547D932E461C2D9AB9BD48074EEB6
SHA-256:	96310D39B6E9D2A2E79ED619FF7005C209D0438E95677B4E74DD3FA18E765A3B
SHA-512:	80A3389DD0DA114FDF8E5D9E6F881FB48958C592FE1EF4F5038FF3425492856650D808192E153924442247326077A78B41B7F73F58927D6E64664F9860A80761
Malicious:	false
Reputation:	low
Preview:	0\r..m.....l|...._keyhttps://px.steelhousemedia.com/st?ga_tracking_id=UA-87708648-1&ga_client_id=468527249.1626947568&shpt=ClickUp%E2%84%A2%20%7 C%20One%20app%20to%20replace%20them%20all&ga_info=%7B%22status%22%3A%22OK%22%2C%22ga_tracking_id%22%3A%22UA-87708648-1%2 2%2C%22ga_client_id%22%3A%22468527249.1626947568%22%2C%22shpt%22%3A%22ClickUp%E2%84%A2%20%7C%20One%20app%20to%20replace% 20them%20all%22%2C%22dcm_cid%22%3A%22468527249.1626947568%22%2C%22dcm_gid%22%3A%221227578407.1626947568%22%2C%22execution_workflow %22%3A%7B%22iteration%22%3A1%2C%22getTrackingIdByGA%22%3A%22FAILED%22%2C%22getTrackingIdByOther1%22%3A%22FAILED%22%2C%22 getTrackingIdByOther2%22%3A%22OK%22%2C%22getClientIdByGA%22%3A%22OK%22%2C%22shpt%22%3A%22OK%22%2C%22dcm_gid%22%3A%22OK%2 2%7D%7D&dcm_cid=468527249.1626947568&dcm_gid=1227578407.1626947568&dxver=4.0.0&shaid=31571&plh=https%3A%2F%2Fclickup.com%2F&cb=178 93855213757682term%3Dvalue&shadditional=googletagmanager%3Dtrue%2C%2Chttps%3A%2F%2Fclickup.com%2F .https://cl

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9e928a5baed4ebb2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9e928a5baed4ebb2_0	
File Type:	data
Category:	dropped
Size (bytes):	20520
Entropy (8bit):	5.685574579056097
Encrypted:	false
SSDEEP:	384:B1l3uuHrZiZLsfBNRIfT06hKafP92XqfWC/GKv5xA4TGfwiNhfca:t3mCBNRIhhP+S5xqwiN
MD5:	E353E48656558CA75ADBDDC1843E2A3F
SHA1:	23BB5DAB928813756CDCC388D55587A26CC5339F
SHA-256:	77AB45F4917F0FD162DE3CEC4E99659FBA65036B910F73DA11289FF032F6BC0A
SHA-512:	229020B182456430156CEA31B7E667376345E2E502B7B07226A4A60E0F9EBA6A1B55E437ECBFBF6CDA6ED7E7D271B914AB5EFF50CF0472321A093593CD1AE7D7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....B....._keyhttps://acdn.adnxs.com/dmp/up/pixie.js .https://clickup.com/WZ .I&/.....g.....A..TL..K.....S.u-.....A..Eo.....;^.u.....A..Eo.....'..#....O.....N....@.....X.....(S....`.....0L`.....(S...`.....LL`"....@Rc.....Qb..s....e.....Qb~..u....t.....Qb:.:.....n...b$.....I`....Da...."....(S...`.....L`.....Q.@.(.....exports..$..a.....S.C..Qb.7d.....I...H..!....a.....Qb...0....call.....K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&....&.'.W.....-...(.....,Rc.....`....Da@...8....!....e..... P.....@....@.-....4P.....&...https://acdn.adnxs.com/dmp/up/pixie.js..a.....D`....D`....D`.....M....`....&...&....&....&.(S.....Pb.....n.d.a.....I.....d.....&.(S.....Pb.....n.r.a.....I..!..d.....&.(S.....Pb.....n.t.a.....

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):	474
Entropy (8bit):	5.623683882082883
Encrypted:	false
SSDEEP:	12:2Xg4KyaKC/nE8fSrIXg4KyysialxE88T:2XsyeRfSrIXsyysik8T
MD5:	87ACE2389BC836520137E92D97CC3834
SHA1:	9F79ABA8498B5CEC07B4573DB34330C566ADD9D0
SHA-256:	57DD6D898BA0C3173A933A090A9A39E20AE42DDBEAE062C4A56A1294B4F6A386
SHA-512:	190CF9C6526BAEB2FCEC8BA03805EF45A2BD3FCECB073DC6991BF3DF2950330AF8E77B42AE1A512AAB3320AC4BE6ADACA1B9EFDF537F2150AD569C426A3B9EBC
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i..../.g...._keyhttps://x.clearbitjs.com/v1/pk_77a36b09108b9b80c547cddad434b648/clearbit.min.js .https://clickup.com/?k..I&/.....u.W.I.....Fl...JJ..y...A..Eo.....A..Eo.....0\r..m.....i..../.g...._keyhttps://x.clearbitjs.com/v1/pk_77a36b09108b9b80c547cddad434b648/clearbit.min.js .https://clickup.com/.m..I&/.....[.....u.W.I.....Fl...JJ..y...A..Eo.....``.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a5e19f85d998c415_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	3748
Entropy (8bit):	5.7949047297991685
Encrypted:	false
SSDEEP:	48:pPDh6rgwqMlhmGkSJlwIEsMylElOkFaWww12kOOtsIOCQbsszR2Uw:h96swJmfcjNtlElNaWTxtsrtWU
MD5:	AA614FAA3DC87CB2CCD4B4ECE5301FA2
SHA1:	213F6ED9E470D18768B94E5D093F93ACFFE172C4
SHA-256:	EC21FF69A9601B2BFDA6DB00727CC58FDBE81D2239A61BDFB77713D505C16573
SHA-512:	E8519CF90002F7E5A4A27B9E4D505B82FD4E964A964E45B653E47ACD73F8FC50D531588F2E41CFB189D5A255B0A26E699AF9459410EA522CBEF3AE002F498A92
Malicious:	false
Reputation:	low
Preview:	0\r..m..... ...d.1....._keyhttps://obs.cheqzone.com/ct?id=3839&url=https%3A%2F%2Fclickup.com%2F%3Futm_source%3Dclickup%26utm_medium%3Ddoc%26utm_campaign%3D12600861&sf=0&tpi=&ch=cheq4ppc&tsf=0&tsfmi=&tsfu=&cb=1626947568561&hl=1&op=0&ag=3098761112&rand=048970501731209870002868051659052002968510072105212015162680155671 12&fs=1280x869&fst=1280x869&np=win32&nv=google%20inc.&ref=&ss=1280x1024&nc=0&at=&di=W1siZWYiLDk1MzldLFsiY2IiLCIwLDAsMCwwLDMsMCwwLDAsMCwxMiwxLDAsMCwzLDEsMCwwLDAsMCwwLDAsMCwwLDAsMCwxLDAsMCwwLDAsMSwwLDAsMCwwLDAsMCwwLDEsMCwwLDAsMywwLDAsMCw1LDAsMCwwLDAsMCwwLDAsMSwwLDAsMCwwLDEsMCwwll0sWy0xLCItIl0sWy0yLCIyMyx2MElrMkt2VmZBaG1JM1dHS2lzVVFUbzhhYUdHdlVUeE9OK2hrVGpZbkdpaTJXb0lsSzFLalJHTVVTQlFzZ1JRU0JwU3hzblpsenpsdi82emt6WjNkWVFmMzhsMnV2bVowdDdKIl0sWy0zLCJbXCJpbnRlcm5hbC1uYWNsLXBsdWdpblwiXSJdLFstNCwiLSJdLFstNSwiLSJdLFstNiwie1wid1wiOltcImRhdGFMYXllclwiLFwibG9hZENTU1wiLFwiaGppZFwiLFwiaGpcIixcIl9oalNldHRpbmdzXCIsXCJndGFnXCIsXCJnb29nbGVfdGFnX21hbmFnZXJcIixcImdvb2dsZV9vcHRpbW	

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):	384

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a81f1b4d5a99dd1d_0	
Entropy (8bit):	5.3428018671291655
Encrypted:	false
SSDEEP:	6:mGYHWd+LMbFgZykl/lCIST4jBK6tWGYHWd+LMCiHgEll6IST4FnK6t:rQ4bKyktxTb5Q4CqVp
MD5:	1EFED7A523642362BF538882F5C0172D
SHA1:	2F9A43A46B6FDEAEBACF5BF671AD6231488458B5
SHA-256:	624D075B7FC95294BD4BFCCE4175A7F5F395FFCAA416133126CFB99C09C2224D
SHA-512:	3C9B780B129634432E8780FF2F380D8AF2B0915B9E13CF14585E978F0562AD7FBC84ADA1A4589D8149B109D9E050E7BD582BF00EB2E27800B536D066C1A68F3A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<...|....._keyhttps://edge.fullstory.com/s/fs.js .https://clickup.com/.u.I&/.....<.....>..Lwc.....J..?..7....D...7....A..Eo.....7.....A..Eo.....0\r..m.....<...|.....keyhttps://edge.fullstory.com/s/fs.js .https://clickup.com/.L..I&/.....;X.....>..Lwc.....J..?..7....D...7....A..Eo.....9.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ab1ff0972b4447a6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	386
Entropy (8bit):	5.5100823402267025
Encrypted:	false
SSDEEP:	6:mqYcW3nVDLgEscf0RK6tWqYcW3nVfFgVcfUK6t:wFDvsccr+FGc+
MD5:	D70C2DC69BEE764C0FF8A7C69410F15F
SHA1:	357600456B3484713C5042DC26F1877DA3732512
SHA-256:	448C44EA555BF542F302AFC92EC9CA01D42EFC0E86BDABF36411C5C105F12C8A
SHA-512:	4841709E65918DA7C75C8F4A326A14AAAF9D1ED79ED35356FFF3800B2C16F4D14316529FC74BF15CFFD025A651463ED2E75242A1F47A9146FDE0FDBED84B790
Malicious:	false
Reputation:	low
Preview:	0\r..m.....=.....(_...._keyhttps://js.hs-banner.com/6613321.js .https://clickup.com/6V..I&/.....T.....-u7....>....Y..W$F...v@.A..Eo.....S.+.....A..Eo.....0\r..m.....=.....(_...._keyhttps://js.hs-banner.com/6613321.js .https://clickup.com/....I&/.....5^.....-u7....>....Y..W$F...v@.A..Eo.....i^.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ae1b8af4ec83ef34_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1487
Entropy (8bit):	5.338174662057501
Encrypted:	false
SSDEEP:	24:sWaOdIYNbza1DHPZFGOen44aVza1FUfYk3LKjYXPkYX7XZv+iYX2kYXnvYXBzfpy:sX62Z8744awUfYkbakPkk7XZvJk2kkvB
MD5:	EC8D838EADFBEF1B325C52E9434F66DA
SHA1:	2076BF78D7BF6799DB211F99D7A4B254A8241746
SHA-256:	FCFA76033B05CF3B4016F63D460658AEEED5A99C4892BE3CFA50979212338F48
SHA-512:	4217C9A0C1557AF8C0E6867D8FECEC7C3F8E662858D7C827B38098B12C7A19923C8DC55B1FF3B0A401DA13BAD9DF9E04D0616C9210B3B59944AE4066D55B9C5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K...w>.3...._keyhttps://px.steelhousemedia.com/st?ga_tracking_id=UA-87708648-1&ga_client_id=468527249.1626947568&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%22468527249.1626947568%22%2C%22shpt%22%3A%22ClickUp%E2%84%A2%20%7C%20One%20app%20to%20replace%20them%20all%22%2C%22dcm_cid%22%3A%22468527249.1626947568%22%2C%22dcm_gid%22%3A%221227578407.1626947568%22%2C%22execution_workflow%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%22getClientIdByGAData%22%3A%22FAILED%22%2C%22getClientIdByCookie%22%3A%22FAILED%22%2C%22shpt%22%3A%22OK%22%2C%22dcm_cid%22%3A%22OK%22%2C%22dcm_gid%22%3A%22OK%22%7D%2C%22message%22%3A%7B%7D%7D&dcm_cid=468527249.1626947568&dcm_gid=1227578407.1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\af4a34b63c1fb86d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	241
Entropy (8bit):	5.693476967486687
Encrypted:	false
SSDEEP:	6:mf8PYKf4udpYS4iyCGbFgPzjLiWfIhHqDK6t:VK8pYkGb2zjLH
MD5:	497B4C1EA9AB7E5A99C7E5642700DCCB
SHA1:	D142EAD98A09EE299CC4FAE35DA661D274F2BCF5
SHA-256:	24C3A72F2F05596E506AF977F53DABBE4D15C88F3CE0376B4D5C9DD47FB4CF7E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\af4a34b63c1fb86d_0	
SHA-512:	9E999917926D8D5D48B534EBFAB8D69B78D2F20E70D0416A83A8DF39CA50D23DAB78FE2AED56551BA6124F7AC4841FA18686726C73366AFA66D294955DCB7D2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m....._keyhttps://doc-cdn.clickup.com/intl-getcanonicallocales-es2015.53fe707c6dd6a6bf6bb4.js .https://clickup.com/.*.I&/.....O..a..WHV..C#._.[..{ ....w...A..Eo.....`.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b563799a9ea12818_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	342
Entropy (8bit):	5.8680027378867265
Encrypted:	false
SSDEEP:	6:mGnYM++E/yO3Xt4sZtgyNJGq9USoS4DK6tHGiVYjhUEQHGnwGq9USoS4:z+z8mvNJx+V0iVxGnwx+
MD5:	5D9BCB6E8F5DBF8D70932CB487291BAA
SHA1:	81AB7F5576E928AF39D24CC2E4D5098C7D369E2B
SHA-256:	6485DC0ABCB93F99E88CEEEBB3F4E78AAE9FAFE2F9119FEC270088F00D6BBC56
SHA-512:	6FAD4F5559E1F2FC4CBC26EE2AF56B7F6FD2BE8250AC7F5E06A25E0F7C2516DB9600908E43C9BBCCD4B1F587CA1215990FBDEADBB7EE6EC26524356EDE904 3B7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N....l....._keyhttps://scripts.attributionapp.com/v2/attribution.js .https://clickup.com/IA.I&/.....4.c.....U.1Lu.VM^.A..Eo.....`.....A..Eo..... .....IA.I&/.@'..29158285F9321495A98C3E8F1351323E8745F2D60B24F8CC1F132D5F81EA1D5B...4.c.....U.1Lu.VM^.A..Eo.....q2..L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b9b2c7c1ed677a45_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	516
Entropy (8bit):	5.864380793862653
Encrypted:	false
SSDEEP:	6:mC/gEYGL+MORm/b8fKgCejVVCugeYAtTVbK6tWC/gEYGL+MORm/b8fKgCejVVlgp:tIspQSgbVVAIXzIspQSgbVVxIm
MD5:	4DBA0D39517AD098227C92D736F38000
SHA1:	FEA76F90A2544283EA19221FB9EDA4E2C4D1F274
SHA-256:	6CC040FD56C7D9CA410536934A004556CF92634E89C0524C61CA1504EC63CFD6
SHA-512:	F3B709A6308CAD37207DB6C367A8A198D02FE3388713F61ABDB21A977539AC9D8EAE0FAAA6A2AAEB968A3A5B575DE8F577B3FDF09F26D38525DDB89C99708D A2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....~....._keyhttps://www.google-analytics.com/gtm/js?id=GTM-PBLF7VJ&t=gtag_UA_87708648_1&cid=468527249.1626947568 .https://clickup.com/D$*.I&/..... .....~..... .....2.%.\G.o..I..3....w.E..*..A..Eo.....A..Eo.....0\r..m.....~....._keyhttps://www.google-analytics.com/gtm/js?id=GTM-PBLF7VJ&t=gt ag_UA_87708648_1&cid=468527249.1626947568 .https://clickup.com/.b&.I&/....._..... .....2.%.\G.o..I..3....w.E..*..A..Eo.....aA.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bb72bde58bf332c1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	200448
Entropy (8bit):	6.0439697422213925
Encrypted:	false
SSDEEP:	3072:9g0l1WG0lfDi/7OswJuBFUVl6Ckth2tb2SMC8ec/CuQd:luNfDvqiotqb2UHc/Cvd
MD5:	F0B5B617F4E5B4D3FDF29BB7F69D2881
SHA1:	B180EDB5F4FC82C22073DA3268D81702EF4306E1
SHA-256:	0386C96B2419E21467D63A3A0AEF15E279D5410338F0F1419CC038B09D127F80
SHA-512:	99A26439E7C08720CA8AC13D0C8B48B5F5B5407E99D804BD969CFDE3A8C41FB7699778FB6E0B15D2AC8A1270DC5C05A8C46F131A599B8DF051DB5500258E312
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....9B0892A7C0BE3EEE7EF211B7A770CB217F33B4F90A1F999DA85BDF4804C4562D.....'..?....O>...8.....&.....(.....(...@%.....`.... .....L.....@...,.....l.....4.....(S.....`d].....5.L`.....L`.....Qc.....planType .]...Qd.d.....stored_promo..Qd..l.....translations..Qd...Y....form_label....Qd..P.....country_code..Qe*.....country_currency..Qe.....currency_rate.....Qe..`.....COU NTRY_CODES....(S.....IaXv...v....Qe.DIC....removeHashtags..E.@.-....@P.....2...https://clickup.com/landing/js/app.min.ed0eecfe.js..a.....D`....D`>...D`.....`....&...&... (S.p.`.....L`.....0Rc.....Qb~..u....t...`....I`....Da.....Q.@.A.....module....Q.@.(.....exports...Qcn..F....document.(S.....5.a.....a.....a.....!....a.....a. .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bc87eb11ecaab1b5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.470360325724911
Encrypted:	false
SSDEEP:	6:mPY68E9xEEUgLEri7LGHmapvtgauFVR9mMM/kK6t:GYg9+GWw5MMD
MD5:	E7AF94002B527F178E3EBCF529FB44A8
SHA1:	1ADE7E474EC709DD533A639D69A01FD126997030
SHA-256:	613A34679CFAFA60C5565617D72D459C693926281480F7D42E8DC8D675E0B8E1
SHA-512:	32A82EF4D8EADAC5ACB882901ED892C609D5F3FBE239FBC1F9692C540A650545FF9F31D522E7B63D57E045DBCCAEA343595205B9BD14704A5F8B2DD7FE59DE 29
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g....J*....._keyhttps://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/js/bootstrap.min.js .https://mega-sharedrives.club/.C..I&/.....3...../..1W.pp+[.....e.{.... H..L./..A..Eo.....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):	414
Entropy (8bit):	5.418536037421464
Encrypted:	false
SSDEEP:	6:mTnYk+z6pFDaKl1tggk6S14SRK6tWTnYk+z6pFDhyg3/S6S1421K6t:G+oaKM6S1Frs+or66S1VP
MD5:	2D95B86ACDC282597B4E00DAE6BC1EE6
SHA1:	9491FE185E4D12E4A24CF3E111EFD293FE67563C
SHA-256:	B5F91C5949BF549A99E44A09D1D2684EA1F10D04820FF133C947491E8A65669D
SHA-512:	A79B01DF7AC45E479C4961D52D02EA2F6B75904B3BB193434F11B897BD05D4D3A891566E1619E075ED0331A85214D484AC7680C926461A0EFAE84F31F77D9835
Malicious:	false
Reputation:	low
Preview:	0\r..m.....K....d....._keyhttps://static.hotjar.com/c/hotjar-779854.js?sv=6 .https://clickup.com/a..I&/.....-t.S.....+[..../..j.....w.'.'.A..Eo.....e.....A..Eo..... .....0\r..m.....K....d....._keyhttps://static.hotjar.com/c/hotjar-779854.js?sv=6 .https://clickup.com/<...I&/.....W.....-t.S.....+[..../..j.....w.'.'.A..Eo.....,P.....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):	199548
Entropy (8bit):	6.142826723048978
Encrypted:	false
SSDEEP:	3072:xjVcwYuVDd1eRSqVr3YbVspCcFs1sVLtXVjr+rAlbVSmWVr7dhFZc:M9GmdIBYhtle2muzs
MD5:	FCDB6C7623967D101E0597116AA7AB61
SHA1:	C34C43E6B0DDBE6BB561C40B27FCF2184ED29BDE
SHA-256:	F3B046F97D067905619EA3D9727118BCFC7D161E3F2CEE38B53342388323FCE2
SHA-512:	08379147E1420CB1B1EC9D77A950C66C600D810A1EF23D232BAF693F95DF129A6F7E3D4ED9E59460B6F066FB2E457E03A3D2CF5162F6F7E6F631E58ED218134
Malicious:	false
Reputation:	low
Preview:	0\r..m.....U....._keyhttps://www.googleadservices.com/pagead/conversion_async.js .https://clickup.com/:...I&/.....0.....~^.xY_..{....a2.9V;...K.H.....A..Eo.....k..... ...A..Eo.....'.....O.....^.....P.....h.....(S.<..`2....L`.....(S...`.....E.L`.....Rc.....f.....Qb.P.....aa....Qb>w E.....l.....Qb...w....ca....Qb.. .....da....QbV<.....t.....Qb.....v.....Qb.....x.....Qb...+....ea....Qb..G.....fa....Qb*..+....B.....QbZnd.....ha....Qb.)]....ia....Qb>..x....ka....Qb.n.&....ja.. ..Qbzk.'....la....Qb.z.1....ma....Qb2.....D.....QbV.....na....Qb.y.....oa....QbZ.....pa....QbZ..g....qa....Qb2. Q....xa....Qb.....za....Qb2Cl.....Aa....Qb.S.....Ba....Qbb}.'....Ca.. ..Qb..P....Da....Qb..|.....Ea....QbJ7c.....Fa....QbZ.....Ga....QbF|.....F.....QbZ\i.....Ha....Qb...3....Ia....Qb.}.....Ka....Qb..v....La....Qbn.pf....Ja....Qb.ws.....Ma....Qb.7B

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):	384
Entropy (8bit):	5.491140120491149
Encrypted:	false
SSDEEP:	6:m5llIVY0IX1qPWnVoQtgJYdmLU6grY4K6tW5llIVY0IX1qPWnV4ugglljmLU6grL:ElllIX10WVoQiYdmdaullIX10WVZN
MD5:	60EC6E9A0462C47BC125FCE6AE53D6BC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\be4f8f8a4aeaa100_0	
SHA1:	EE83A9E79066FAF19D723BC4FD93F73B931B7C84
SHA-256:	F27DDAB37BD427C4803DE25F28B14A253D7CA7B6429E34631717384F77D1EEDE
SHA-512:	AB105AD433A63BCBA87E8E1754579565375075F1967AC14387ED6F2D8FD993A2A2243CF9AA3FC6187622B074064F686EA56BFF3D0E8751FFBB2594B3F2367867
Malicious:	false
Reputation:	low
Preview:	0\r..m.....<...0.g....._keyhttps://tag.getdrip.com/4818331.js .https://clickup.com/...I&/.....).,(....a.....s.5.m..Y.q...A..Eo.....M".....A..Eo.....0\r..m.....<...0.g....._keyhttps://tag.getdrip.com/4818331.js .https://clickup.com/....I&/.....X.....).,(....a.....s.5.m..Y.q...A..Eo.....B.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\bf924b09c5cf1dc4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.6321405877901425
Encrypted:	false
SSDEEP:	3:m+lAds8RzYKfG9HuVLAIvEnAWIUSE2rzFc27P9LVeWt/lHCL/l/lLhv5MHbN9hyS:ml9YKf4WTwSFDFgDtlFqh+4bthK6t
MD5:	9FE3591E092D483E7838105BC1FF2ED7
SHA1:	E9FF3B3EBC942645B911C8D0B823795ADD051B4F
SHA-256:	F723602ADD8A5CF2F3D5A2415BC8D030781C1AEA658387BF6BE681ED077ECC24
SHA-512:	0D839CC6420BEAEAAB19778D9D1130CCD5316F8A9159FBA89FF5244BF37DA30DCED286A454C2D66FE00B25BB9046E9992D3B688A7DAB5FBAA4050549F5526C6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`...M....._keyhttps://doc-cdn.clickup.com/intl-locale-es2015.29178cde0d30fc24e3f9.js .https://clickup.com/V..I&/.....}.....Nhj..4K...".. .).....R.R.A..Eo.....<.....A..Eo.....

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):	693
Entropy (8bit):	5.717073841045296
Encrypted:	false
SSDEEP:	12:2HMMpDV/jPoqMNoHMMpDVWlUPoq+86roHMMpDVPPoqfT:WlDVkqMNElDVWDq+86rElDVIqL
MD5:	57ED1E844C33744E09312DC08F49A8C9
SHA1:	1A4BE2EDBF9D7E72CA5B1751AB20BD654A9962DA
SHA-256:	9F738714035EB86B1F8BC698B623E978646284A4CD4AFD765864EF3ABF928DDD
SHA-512:	2493598E3E2CCBAE50DBC51FCECE928350196B586C439299A53C6D5BE31AD326F9BC14ABECD06FB0AE5A9D4315F62F9F18C2EB760A0C2F54EA50AE3174DF5BBC
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/....I&/.....^.....z....J....<Y...O...^.i...My..A..Eo.....e.....A..Eo.....0\r..m.....c.....I...._keyhttps://www.googletagmanager.com/gtag/js?id=AW-617640813&l=dataLayer&cx=c .https://clickup.com/.7..I&/.....^.....z....J....<Y...O...^.i...My..A..Eo.....,.....A..Eo.....0\r..m.....c.....I...._keyhttps://www.googletagmanager.com/gtag/js?id=AW-617640813&l=dataLayer&cx=c .https://clickup.com/.y;.I&/.....d.....z....J....<Y...O...^.i...My..A..Eo.....G+.`.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\c4ae7226ec263bdd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	328576
Entropy (8bit):	5.91825968550436
Encrypted:	false
SSDEEP:	6144:MjiIRO7s42DkgDC0gFKvbMvsQ8iA+uHxm:MjL+2YgDChF0bMVnA+uHU
MD5:	3BA5E39E2FF0D5B01C040B6E77F2EA8D
SHA1:	521A545E03F0D9279878C8A19F7058F9A23BE70C
SHA-256:	A59911227052D943E38709E9ABA49BF397217AAED5BDB2492C0690A8D50F527A
SHA-512:	744B4F1A66529AD62C64B0273C75BFB3373B90BD10DEEB0B0F415E905352296A4968E5B0E887C97A61B16A308FF03D73ADB601DDC88C47F30F7261FCD9CAD11
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@.....S.....0FD77AA65AA6586DB5AB54456C6A0F3028FDE8F355F5A8FF8273C9D8BBFF91D3.....'.....Od... ....Q.\.....%.....`.....%.....0.....X.....8.....t.....p.....(S.m...`.....L`.....(S.A..`8.....L`<....`Rc,.....Qb..s....e.....Qb:.:.....n.....QbB. .....r.....S...Qb..|.....s.....Qb...q....o.....Qb.....d...f$.....I`....Da.....(S.M..`P....(L`.....M.....Qe...a....hasOwnProperty....Qb...0....call..Qbj..U....push..Qcn.+.....shift.....K`....D...x.....*..&...*..&...*..&..&.|.&.(...i...e%.*..&...&.(...&.(...&...&.Z.....)..&.%.*....(...&...&.%.*..&..*..&.Y.....&..0..

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 02:52:24.736521959 CEST	192.168.2.3	8.8.8.8	0xf513	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:24.738019943 CEST	192.168.2.3	8.8.8.8	0xe658	Standard query (0)	doc.clickup.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:24.740189075 CEST	192.168.2.3	8.8.8.8	0x92d	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:25.856057882 CEST	192.168.2.3	8.8.8.8	0xa045	Standard query (0)	doc-cdn.clickup.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:25.856142998 CEST	192.168.2.3	8.8.8.8	0x827d	Standard query (0)	scripts.attributionapp.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:27.554162025 CEST	192.168.2.3	8.8.8.8	0x752a	Standard query (0)	app.clickup.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:28.103234053 CEST	192.168.2.3	8.8.8.8	0xe019	Standard query (0)	t12600861.p.clickup-attachments.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:29.343975067 CEST	192.168.2.3	8.8.8.8	0xc4e9	Standard query (0)	usage.tracjs.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:29.344491005 CEST	192.168.2.3	8.8.8.8	0x7858	Standard query (0)	app-cdn.clickup.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:30.379179001 CEST	192.168.2.3	8.8.8.8	0xa765	Standard query (0)	app-cdn.clickup.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:30.521873951 CEST	192.168.2.3	8.8.8.8	0xcca7	Standard query (0)	doc-cdn.clickup.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:30.526772976 CEST	192.168.2.3	8.8.8.8	0x6105	Standard query (0)	t12600861.p.clickup-attachments.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:38.276609898 CEST	192.168.2.3	8.8.8.8	0x7e30	Standard query (0)	mega-sharedrives.club	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:39.492830992 CEST	192.168.2.3	8.8.8.8	0x7afa	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:39.665647030 CEST	192.168.2.3	8.8.8.8	0x4b05	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:39.667799950 CEST	192.168.2.3	8.8.8.8	0xa47f	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:39.671384096 CEST	192.168.2.3	8.8.8.8	0x450	Standard query (0)	kit.fontawesome.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:40.051433086 CEST	192.168.2.3	8.8.8.8	0xc525	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:40.100414038 CEST	192.168.2.3	8.8.8.8	0xe2c3	Standard query (0)	ka-f.fontawesome.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:42.481780052 CEST	192.168.2.3	8.8.8.8	0xe75a	Standard query (0)	mega-sharedrives.club	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:43.913286924 CEST	192.168.2.3	8.8.8.8	0x6fb4	Standard query (0)	clickup.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.231081009 CEST	192.168.2.3	8.8.8.8	0xa0e5	Standard query (0)	calendly.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.231604099 CEST	192.168.2.3	8.8.8.8	0x4965	Standard query (0)	www.googleoptimize.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 02:52:44.233110905 CEST	192.168.2.3	8.8.8.8	0x994c	Standard query (0)	client-registry.mutinycdn.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.736197948 CEST	192.168.2.3	8.8.8.8	0xc787	Standard query (0)	user-data.mutinycdn.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.758519888 CEST	192.168.2.3	8.8.8.8	0x338c	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.761961937 CEST	192.168.2.3	8.8.8.8	0x49fa	Standard query (0)	static.hotjar.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.763358116 CEST	192.168.2.3	8.8.8.8	0xff7e	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.765217066 CEST	192.168.2.3	8.8.8.8	0xb228	Standard query (0)	tag.getdrip.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.765564919 CEST	192.168.2.3	8.8.8.8	0xe51	Standard query (0)	js.hs-scripts.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.816874027 CEST	192.168.2.3	8.8.8.8	0x72a0	Standard query (0)	a.quora.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.841640949 CEST	192.168.2.3	8.8.8.8	0x5c07	Standard query (0)	snap.licdn.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.841814995 CEST	192.168.2.3	8.8.8.8	0x18c5	Standard query (0)	cdn.firstpromoter.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.859864950 CEST	192.168.2.3	8.8.8.8	0x77a8	Standard query (0)	tracking.g2crowd.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:45.114248037 CEST	192.168.2.3	8.8.8.8	0x48fd	Standard query (0)	x.clearbitjs.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:45.124650955 CEST	192.168.2.3	8.8.8.8	0x449a	Standard query (0)	ws.zoominfo.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:45.124834061 CEST	192.168.2.3	8.8.8.8	0xb7be	Standard query (0)	edge.fullstory.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:46.347609997 CEST	192.168.2.3	8.8.8.8	0xe2c1	Standard query (0)	api.clickup.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:46.394853115 CEST	192.168.2.3	8.8.8.8	0xe80d	Standard query (0)	static.ads-twitter.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:46.401948929 CEST	192.168.2.3	8.8.8.8	0x35ea	Standard query (0)	dx.steelhousemedia.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.449973106 CEST	192.168.2.3	8.8.8.8	0x46ae	Standard query (0)	track.attributionapp.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.491347075 CEST	192.168.2.3	8.8.8.8	0xeb32	Standard query (0)	script.hotjar.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.530728102 CEST	192.168.2.3	8.8.8.8	0x8984	Standard query (0)	q.quora.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.531434059 CEST	192.168.2.3	8.8.8.8	0xc37a	Standard query (0)	js.hs-analytics.net	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.532463074 CEST	192.168.2.3	8.8.8.8	0xd38f	Standard query (0)	js.hs-banner.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.533093929 CEST	192.168.2.3	8.8.8.8	0xee2a	Standard query (0)	api.getdrip.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.546376944 CEST	192.168.2.3	8.8.8.8	0x11ba	Standard query (0)	js.hscollectedforms.net	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.789926052 CEST	192.168.2.3	8.8.8.8	0x63b1	Standard query (0)	x.clearbit.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.790225983 CEST	192.168.2.3	8.8.8.8	0x3769	Standard query (0)	rs.fullstory.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.793975115 CEST	192.168.2.3	8.8.8.8	0x92ff	Standard query (0)	api.exchangeratesapi.io	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.843928099 CEST	192.168.2.3	8.8.8.8	0xb96b	Standard query (0)	ob.cheqzone.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.871325016 CEST	192.168.2.3	8.8.8.8	0x9603	Standard query (0)	www.redditstatic.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.902403116 CEST	192.168.2.3	8.8.8.8	0x29dc	Standard query (0)	m.servedby-buysellads.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.904057980 CEST	192.168.2.3	8.8.8.8	0x5e44	Standard query (0)	cdn.pdst.fm	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.068737984 CEST	192.168.2.3	8.8.8.8	0xcfe	Standard query (0)	acdn.adnxs.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.242283106 CEST	192.168.2.3	8.8.8.8	0xca10	Standard query (0)	vars.hotjar.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.247606993 CEST	192.168.2.3	8.8.8.8	0x4c6f	Standard query (0)	client.mutinycdn.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.369276047 CEST	192.168.2.3	8.8.8.8	0x94d3	Standard query (0)	api-v2.mutinyhq.io	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.538425922 CEST	192.168.2.3	8.8.8.8	0x5448	Standard query (0)	t.co	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.595423937 CEST	192.168.2.3	8.8.8.8	0x5a92	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 02:52:48.859498978 CEST	192.168.2.3	8.8.8.8	0x484b	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.896673918 CEST	192.168.2.3	8.8.8.8	0x8f97	Standard query (0)	alb.reddit.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.945255995 CEST	192.168.2.3	8.8.8.8	0xdc70	Standard query (0)	ib.adnxs.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.956944942 CEST	192.168.2.3	8.8.8.8	0x9b3	Standard query (0)	forms.hubspot.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.998486042 CEST	192.168.2.3	8.8.8.8	0x1c59	Standard query (0)	us-central1-adaptive-growth.cloudfunctions.net	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:49.963252068 CEST	192.168.2.3	8.8.8.8	0x5f4	Standard query (0)	obs.cheqzone.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:49.965784073 CEST	192.168.2.3	8.8.8.8	0xc9b3	Standard query (0)	px.steelhousemedia.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.138766050 CEST	192.168.2.3	8.8.8.8	0xcf5d	Standard query (0)	forms.hsforms.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.410810947 CEST	192.168.2.3	8.8.8.8	0x4ded	Standard query (0)	stats.g.doubleclick.net	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.427761078 CEST	192.168.2.3	8.8.8.8	0x48cf	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.430520058 CEST	192.168.2.3	8.8.8.8	0xd8e4	Standard query (0)	www.google.de	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:54.311707020 CEST	192.168.2.3	8.8.8.8	0x80c6	Standard query (0)	ww.steelhousemedia.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:55.755774975 CEST	192.168.2.3	8.8.8.8	0x82d9	Standard query (0)	in.hotjar.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:56.038944960 CEST	192.168.2.3	8.8.8.8	0x8458	Standard query (0)	match.adsrvr.org	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:56.042747974 CEST	192.168.2.3	8.8.8.8	0xe2bb	Standard query (0)	insight.adsrvr.org	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:56.054312944 CEST	192.168.2.3	8.8.8.8	0x400f	Standard query (0)	clickup.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:57.400614977 CEST	192.168.2.3	8.8.8.8	0x1897	Standard query (0)	widget.intercom.io	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:57.481733084 CEST	192.168.2.3	8.8.8.8	0x6379	Standard query (0)	analytics.twitter.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:57.511550903 CEST	192.168.2.3	8.8.8.8	0xbfc5	Standard query (0)	track.hubspot.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:57.712742090 CEST	192.168.2.3	8.8.8.8	0x1bb9	Standard query (0)	js.intercomcdn.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:59.216038942 CEST	192.168.2.3	8.8.8.8	0x4b3e	Standard query (0)	api-iam.intercom.io	A (IP address)	IN (0x0001)
Jul 22, 2021 02:53:00.262403011 CEST	192.168.2.3	8.8.8.8	0x1381	Standard query (0)	nexus-websocket-a.intercom.io	A (IP address)	IN (0x0001)
Jul 22, 2021 02:53:00.778495073 CEST	192.168.2.3	8.8.8.8	0x2314	Standard query (0)	clockify.me	A (IP address)	IN (0x0001)
Jul 22, 2021 02:53:03.573575974 CEST	192.168.2.3	8.8.8.8	0x1966	Standard query (0)	px.ads.linkedin.com	A (IP address)	IN (0x0001)
Jul 22, 2021 02:53:32.393996000 CEST	192.168.2.3	8.8.8.8	0xc7e0	Standard query (0)	insight.adsrvr.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 02:52:24.786839008 CEST	8.8.8.8	192.168.2.3	0xf513	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:24.786839008 CEST	8.8.8.8	192.168.2.3	0xf513	No error (0)	clients.l.google.com		142.250.185.142	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:24.801865101 CEST	8.8.8.8	192.168.2.3	0xe658	No error (0)	doc.clickup.com	app.clickup.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:24.801865101 CEST	8.8.8.8	192.168.2.3	0xe658	No error (0)	app.clickup.com		3.125.16.43	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:24.801865101 CEST	8.8.8.8	192.168.2.3	0xe658	No error (0)	app.clickup.com		3.67.223.105	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:24.801865101 CEST	8.8.8.8	192.168.2.3	0xe658	No error (0)	app.clickup.com		18.184.109.158	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 02:52:24.809571028 CEST	8.8.8.8	192.168.2.3	0x92d	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:25.914194107 CEST	8.8.8.8	192.168.2.3	0xee25	No error (0)	www-google tagmanager.l.google.com		172.217.168.8	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:25.917814970 CEST	8.8.8.8	192.168.2.3	0xa045	No error (0)	doc-cdn.clickup.com		13.224.99.46	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:25.917814970 CEST	8.8.8.8	192.168.2.3	0xa045	No error (0)	doc-cdn.clickup.com		13.224.99.4	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:25.917814970 CEST	8.8.8.8	192.168.2.3	0xa045	No error (0)	doc-cdn.clickup.com		13.224.99.112	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:25.917814970 CEST	8.8.8.8	192.168.2.3	0xa045	No error (0)	doc-cdn.clickup.com		13.224.99.69	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:25.937357903 CEST	8.8.8.8	192.168.2.3	0x827d	No error (0)	scripts.attributionapp.com	d279x8308vq8mj.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:25.937357903 CEST	8.8.8.8	192.168.2.3	0x827d	No error (0)	d279x8308vq8mj.cloudfront.net		13.224.99.54	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:25.937357903 CEST	8.8.8.8	192.168.2.3	0x827d	No error (0)	d279x8308vq8mj.cloudfront.net		13.224.99.118	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:25.937357903 CEST	8.8.8.8	192.168.2.3	0x827d	No error (0)	d279x8308vq8mj.cloudfront.net		13.224.99.81	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:25.937357903 CEST	8.8.8.8	192.168.2.3	0x827d	No error (0)	d279x8308vq8mj.cloudfront.net		13.224.99.4	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:26.379538059 CEST	8.8.8.8	192.168.2.3	0xae67	No error (0)	www-google-analytics.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:27.613302946 CEST	8.8.8.8	192.168.2.3	0x752a	No error (0)	app.clickup.com		18.184.109.158	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:27.613302946 CEST	8.8.8.8	192.168.2.3	0x752a	No error (0)	app.clickup.com		3.125.16.43	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:27.613302946 CEST	8.8.8.8	192.168.2.3	0x752a	No error (0)	app.clickup.com		3.67.223.105	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:28.164086103 CEST	8.8.8.8	192.168.2.3	0xe019	No error (0)	t12600861.p.clickup-attachments.com		13.224.99.60	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:28.164086103 CEST	8.8.8.8	192.168.2.3	0xe019	No error (0)	t12600861.p.clickup-attachments.com		13.224.99.64	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:28.164086103 CEST	8.8.8.8	192.168.2.3	0xe019	No error (0)	t12600861.p.clickup-attachments.com		13.224.99.37	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:28.164086103 CEST	8.8.8.8	192.168.2.3	0xe019	No error (0)	t12600861.p.clickup-attachments.com		13.224.99.102	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:29.402128935 CEST	8.8.8.8	192.168.2.3	0xc4e9	No error (0)	usage.trackjs.com		158.69.52.117	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:29.402128935 CEST	8.8.8.8	192.168.2.3	0xc4e9	No error (0)	usage.trackjs.com		138.197.155.84	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:29.402128935 CEST	8.8.8.8	192.168.2.3	0xc4e9	No error (0)	usage.trackjs.com		167.114.119.127	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:29.402128935 CEST	8.8.8.8	192.168.2.3	0xc4e9	No error (0)	usage.trackjs.com		51.89.217.92	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:29.415380001 CEST	8.8.8.8	192.168.2.3	0x7858	No error (0)	app-cdn.clickup.com	d5txjkmyderx.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:29.415380001 CEST	8.8.8.8	192.168.2.3	0x7858	No error (0)	d5txjkmyderx.cloudfront.net		13.224.99.77	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 02:52:29.415380001 CEST	8.8.8.8	192.168.2.3	0x7858	No error (0)	d5txjkmyderx.cloudfront.net		13.224.99.63	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:29.415380001 CEST	8.8.8.8	192.168.2.3	0x7858	No error (0)	d5txjkmyderx.cloudfront.net		13.224.99.102	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:29.415380001 CEST	8.8.8.8	192.168.2.3	0x7858	No error (0)	d5txjkmyderx.cloudfront.net		13.224.99.5	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:30.443172932 CEST	8.8.8.8	192.168.2.3	0xa765	No error (0)	app-cdn.clickup.com	d5txjkmyderx.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:30.443172932 CEST	8.8.8.8	192.168.2.3	0xa765	No error (0)	d5txjkmyderx.cloudfront.net		13.224.99.77	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:30.443172932 CEST	8.8.8.8	192.168.2.3	0xa765	No error (0)	d5txjkmyderx.cloudfront.net		13.224.99.63	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:30.443172932 CEST	8.8.8.8	192.168.2.3	0xa765	No error (0)	d5txjkmyderx.cloudfront.net		13.224.99.5	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:30.443172932 CEST	8.8.8.8	192.168.2.3	0xa765	No error (0)	d5txjkmyderx.cloudfront.net		13.224.99.102	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:30.586112022 CEST	8.8.8.8	192.168.2.3	0xcca7	No error (0)	doc-cdn.clickup.com		13.224.99.69	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:30.586112022 CEST	8.8.8.8	192.168.2.3	0xcca7	No error (0)	doc-cdn.clickup.com		13.224.99.112	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:30.586112022 CEST	8.8.8.8	192.168.2.3	0xcca7	No error (0)	doc-cdn.clickup.com		13.224.99.46	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:30.586112022 CEST	8.8.8.8	192.168.2.3	0xcca7	No error (0)	doc-cdn.clickup.com		13.224.99.4	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:30.588659048 CEST	8.8.8.8	192.168.2.3	0x6105	No error (0)	t12600861.p.clickup-attachments.com		13.224.99.60	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:30.588659048 CEST	8.8.8.8	192.168.2.3	0x6105	No error (0)	t12600861.p.clickup-attachments.com		13.224.99.64	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:30.588659048 CEST	8.8.8.8	192.168.2.3	0x6105	No error (0)	t12600861.p.clickup-attachments.com		13.224.99.37	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:30.588659048 CEST	8.8.8.8	192.168.2.3	0x6105	No error (0)	t12600861.p.clickup-attachments.com		13.224.99.102	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:38.343755960 CEST	8.8.8.8	192.168.2.3	0x7e30	No error (0)	mega-sharedrives.club		66.29.132.95	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:39.576862097 CEST	8.8.8.8	192.168.2.3	0x7afa	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:39.576862097 CEST	8.8.8.8	192.168.2.3	0x7afa	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:39.715790033 CEST	8.8.8.8	192.168.2.3	0x4b05	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:39.724821091 CEST	8.8.8.8	192.168.2.3	0xa47f	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:39.724821091 CEST	8.8.8.8	192.168.2.3	0xa47f	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:39.732553959 CEST	8.8.8.8	192.168.2.3	0x450	No error (0)	kit.fontawesome.com	kit.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:40.035425901 CEST	8.8.8.8	192.168.2.3	0xff29	No error (0)	gstaticadssl.l.google.com		172.217.168.3	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 02:52:40.108501911 CEST	8.8.8.8	192.168.2.3	0xc525	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:40.108501911 CEST	8.8.8.8	192.168.2.3	0xc525	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:40.162748098 CEST	8.8.8.8	192.168.2.3	0xe2c3	No error (0)	ka-f.fontawesome.com	ka-f.fontawesome.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:42.540098906 CEST	8.8.8.8	192.168.2.3	0xe75a	No error (0)	mega-sharedrives.club		66.29.132.95	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:43.975394011 CEST	8.8.8.8	192.168.2.3	0x6fb4	No error (0)	clickup.com		13.224.99.47	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:43.975394011 CEST	8.8.8.8	192.168.2.3	0x6fb4	No error (0)	clickup.com		13.224.99.125	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:43.975394011 CEST	8.8.8.8	192.168.2.3	0x6fb4	No error (0)	clickup.com		13.224.99.13	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:43.975394011 CEST	8.8.8.8	192.168.2.3	0x6fb4	No error (0)	clickup.com		13.224.99.46	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.296709061 CEST	8.8.8.8	192.168.2.3	0xa0e5	No error (0)	calendly.com		104.20.247.116	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.296709061 CEST	8.8.8.8	192.168.2.3	0xa0e5	No error (0)	calendly.com		104.20.248.116	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.299331903 CEST	8.8.8.8	192.168.2.3	0x994c	No error (0)	client-registry.mutinycdn.com	c3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:44.313359022 CEST	8.8.8.8	192.168.2.3	0x4965	No error (0)	www.googleoptimize.com		142.250.203.110	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.798451900 CEST	8.8.8.8	192.168.2.3	0xc787	No error (0)	user-data.mutinycdn.com	c3.shared.global.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:44.823591948 CEST	8.8.8.8	192.168.2.3	0xff7e	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:44.823591948 CEST	8.8.8.8	192.168.2.3	0xff7e	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.823791981 CEST	8.8.8.8	192.168.2.3	0x49fa	No error (0)	static.hotjar.com	static-cdn.hotjar.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:44.823791981 CEST	8.8.8.8	192.168.2.3	0x49fa	No error (0)	static-cdn.hotjar.com		13.224.99.122	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.823791981 CEST	8.8.8.8	192.168.2.3	0x49fa	No error (0)	static-cdn.hotjar.com		13.224.99.100	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.823791981 CEST	8.8.8.8	192.168.2.3	0x49fa	No error (0)	static-cdn.hotjar.com		13.224.99.58	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.823791981 CEST	8.8.8.8	192.168.2.3	0x49fa	No error (0)	static-cdn.hotjar.com		13.224.99.50	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.827270985 CEST	8.8.8.8	192.168.2.3	0xe51	No error (0)	js.hs-scripts.com		104.17.212.204	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.827270985 CEST	8.8.8.8	192.168.2.3	0xe51	No error (0)	js.hs-scripts.com		104.17.213.204	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.827270985 CEST	8.8.8.8	192.168.2.3	0xe51	No error (0)	js.hs-scripts.com		104.17.214.204	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.827270985 CEST	8.8.8.8	192.168.2.3	0xe51	No error (0)	js.hs-scripts.com		104.17.210.204	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.827270985 CEST	8.8.8.8	192.168.2.3	0xe51	No error (0)	js.hs-scripts.com		104.17.211.204	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.828468084 CEST	8.8.8.8	192.168.2.3	0x338c	No error (0)	px.ads.linkedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 02:52:44.828468084 CEST	8.8.8.8	192.168.2.3	0x338c	No error (0)	mix.linkedin.com	glb-na.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:44.828468084 CEST	8.8.8.8	192.168.2.3	0x338c	No error (0)	glb-na.mix.linkedin.com	pop-edc2.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:44.828468084 CEST	8.8.8.8	192.168.2.3	0x338c	No error (0)	pop-edc2.mix.linkedin.com		108.174.11.85	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.831418991 CEST	8.8.8.8	192.168.2.3	0xb228	No error (0)	tag.getdrip.com	d10w4ikcrdu13z.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:44.831418991 CEST	8.8.8.8	192.168.2.3	0xb228	No error (0)	d10w4ikcrdu13z.cloudfront.net		13.224.99.21	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.831418991 CEST	8.8.8.8	192.168.2.3	0xb228	No error (0)	d10w4ikcrdu13z.cloudfront.net		13.224.99.34	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.831418991 CEST	8.8.8.8	192.168.2.3	0xb228	No error (0)	d10w4ikcrdu13z.cloudfront.net		13.224.99.111	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.831418991 CEST	8.8.8.8	192.168.2.3	0xb228	No error (0)	d10w4ikcrdu13z.cloudfront.net		13.224.99.66	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.877832890 CEST	8.8.8.8	192.168.2.3	0x72a0	No error (0)	a.quora.com	quora.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:44.877832890 CEST	8.8.8.8	192.168.2.3	0x72a0	No error (0)	quora.map.fastly.net		151.101.1.2	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.877832890 CEST	8.8.8.8	192.168.2.3	0x72a0	No error (0)	quora.map.fastly.net		151.101.65.2	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.877832890 CEST	8.8.8.8	192.168.2.3	0x72a0	No error (0)	quora.map.fastly.net		151.101.129.2	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.877832890 CEST	8.8.8.8	192.168.2.3	0x72a0	No error (0)	quora.map.fastly.net		151.101.193.2	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.899753094 CEST	8.8.8.8	192.168.2.3	0x5c07	No error (0)	snap.licdn.com	wildcard.licdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:44.905782938 CEST	8.8.8.8	192.168.2.3	0x18c5	No error (0)	cdn.firstpromoter.com	d2ycxbs0cq3yaz.cloudfront.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:44.905782938 CEST	8.8.8.8	192.168.2.3	0x18c5	No error (0)	d2ycxbs0cq3yaz.cloudfront.net		13.224.99.29	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.905782938 CEST	8.8.8.8	192.168.2.3	0x18c5	No error (0)	d2ycxbs0cq3yaz.cloudfront.net		13.224.99.55	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.905782938 CEST	8.8.8.8	192.168.2.3	0x18c5	No error (0)	d2ycxbs0cq3yaz.cloudfront.net		13.224.99.26	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.905782938 CEST	8.8.8.8	192.168.2.3	0x18c5	No error (0)	d2ycxbs0cq3yaz.cloudfront.net		13.224.99.12	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.920770884 CEST	8.8.8.8	192.168.2.3	0x77a8	No error (0)	tracking.g2crowd.com		104.18.27.190	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:44.920770884 CEST	8.8.8.8	192.168.2.3	0x77a8	No error (0)	tracking.g2crowd.com		104.18.26.190	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:45.177009106 CEST	8.8.8.8	192.168.2.3	0xb7be	No error (0)	edge.fullstory.com		35.201.112.186	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:45.185930967 CEST	8.8.8.8	192.168.2.3	0x449a	No error (0)	ws.zoominfo.com		104.16.168.82	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:45.185930967 CEST	8.8.8.8	192.168.2.3	0x449a	No error (0)	ws.zoominfo.com		104.16.101.12	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:45.187757969 CEST	8.8.8.8	192.168.2.3	0x48fd	No error (0)	x.clearbitjs.com	global-v2.clearbit.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:45.187757969 CEST	8.8.8.8	192.168.2.3	0x48fd	No error (0)	global-v2.clearbit.com		18.168.223.221	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 02:52:45.187757969 CEST	8.8.8.8	192.168.2.3	0x48fd	No error (0)	global-v2.clearbit.com		18.134.49.160	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:46.406661034 CEST	8.8.8.8	192.168.2.3	0xe2c1	No error (0)	api.clickup.com		3.124.156.213	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:46.406661034 CEST	8.8.8.8	192.168.2.3	0xe2c1	No error (0)	api.clickup.com		3.123.224.68	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:46.406661034 CEST	8.8.8.8	192.168.2.3	0xe2c1	No error (0)	api.clickup.com		3.65.4.135	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:46.454483986 CEST	8.8.8.8	192.168.2.3	0xe80d	No error (0)	static.ads-twitter.com	platform.twitter.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:46.454483986 CEST	8.8.8.8	192.168.2.3	0xe80d	No error (0)	platform.twitter.map.fastly.net		199.232.136.157	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:46.462276936 CEST	8.8.8.8	192.168.2.3	0x35ea	No error (0)	dx.steelhousemedia.com		52.11.37.91	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:46.462276936 CEST	8.8.8.8	192.168.2.3	0x35ea	No error (0)	dx.steelhousemedia.com		44.241.10.203	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:46.462276936 CEST	8.8.8.8	192.168.2.3	0x35ea	No error (0)	dx.steelhousemedia.com		44.236.162.197	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:46.462276936 CEST	8.8.8.8	192.168.2.3	0x35ea	No error (0)	dx.steelhousemedia.com		54.69.84.146	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.519370079 CEST	8.8.8.8	192.168.2.3	0x46ae	No error (0)	track.attributionapp.com	fluffy-alpaca-j1w7zdv61tmqz86b33z4c6tl.herokudns.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:47.519370079 CEST	8.8.8.8	192.168.2.3	0x46ae	No error (0)	fluffy-alpaca-j1w7zdv61tmqz86b33z4c6tl.herokudns.com		52.45.121.249	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.519370079 CEST	8.8.8.8	192.168.2.3	0x46ae	No error (0)	fluffy-alpaca-j1w7zdv61tmqz86b33z4c6tl.herokudns.com		52.44.24.39	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.519370079 CEST	8.8.8.8	192.168.2.3	0x46ae	No error (0)	fluffy-alpaca-j1w7zdv61tmqz86b33z4c6tl.herokudns.com		3.223.240.69	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.519370079 CEST	8.8.8.8	192.168.2.3	0x46ae	No error (0)	fluffy-alpaca-j1w7zdv61tmqz86b33z4c6tl.herokudns.com		52.45.185.230	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.519370079 CEST	8.8.8.8	192.168.2.3	0x46ae	No error (0)	fluffy-alpaca-j1w7zdv61tmqz86b33z4c6tl.herokudns.com		52.45.37.112	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.519370079 CEST	8.8.8.8	192.168.2.3	0x46ae	No error (0)	fluffy-alpaca-j1w7zdv61tmqz86b33z4c6tl.herokudns.com		52.4.65.107	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.519370079 CEST	8.8.8.8	192.168.2.3	0x46ae	No error (0)	fluffy-alpaca-j1w7zdv61tmqz86b33z4c6tl.herokudns.com		52.45.2.162	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.519370079 CEST	8.8.8.8	192.168.2.3	0x46ae	No error (0)	fluffy-alpaca-j1w7zdv61tmqz86b33z4c6tl.herokudns.com		35.169.250.74	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.554191113 CEST	8.8.8.8	192.168.2.3	0xeb32	No error (0)	script.hotjar.com		13.224.99.26	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.554191113 CEST	8.8.8.8	192.168.2.3	0xeb32	No error (0)	script.hotjar.com		13.224.99.33	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 02:52:47.554191113 CEST	8.8.8.8	192.168.2.3	0xeb32	No error (0)	script.hotjar.com		13.224.99.44	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.554191113 CEST	8.8.8.8	192.168.2.3	0xeb32	No error (0)	script.hotjar.com		13.224.99.19	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.587615967 CEST	8.8.8.8	192.168.2.3	0x8984	No error (0)	q.quora.com		3.224.194.150	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.587615967 CEST	8.8.8.8	192.168.2.3	0x8984	No error (0)	q.quora.com		18.205.51.212	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.587615967 CEST	8.8.8.8	192.168.2.3	0x8984	No error (0)	q.quora.com		3.230.50.184	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.587615967 CEST	8.8.8.8	192.168.2.3	0x8984	No error (0)	q.quora.com		18.215.205.165	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.587615967 CEST	8.8.8.8	192.168.2.3	0x8984	No error (0)	q.quora.com		52.71.230.189	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.587615967 CEST	8.8.8.8	192.168.2.3	0x8984	No error (0)	q.quora.com		3.225.115.141	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.591324091 CEST	8.8.8.8	192.168.2.3	0xc37a	No error (0)	js.hs-analytics.net		104.17.70.176	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.591324091 CEST	8.8.8.8	192.168.2.3	0xc37a	No error (0)	js.hs-analytics.net		104.17.71.176	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.591324091 CEST	8.8.8.8	192.168.2.3	0xc37a	No error (0)	js.hs-analytics.net		104.17.68.176	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.591324091 CEST	8.8.8.8	192.168.2.3	0xc37a	No error (0)	js.hs-analytics.net		104.17.67.176	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.591324091 CEST	8.8.8.8	192.168.2.3	0xc37a	No error (0)	js.hs-analytics.net		104.17.69.176	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.591975927 CEST	8.8.8.8	192.168.2.3	0xd38f	No error (0)	js.hs-banner.com		104.18.20.191	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.591975927 CEST	8.8.8.8	192.168.2.3	0xd38f	No error (0)	js.hs-banner.com		104.18.21.191	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.605622053 CEST	8.8.8.8	192.168.2.3	0x11ba	No error (0)	js.hscollectedforms.net		104.17.129.171	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.605622053 CEST	8.8.8.8	192.168.2.3	0x11ba	No error (0)	js.hscollectedforms.net		104.17.127.171	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.605622053 CEST	8.8.8.8	192.168.2.3	0x11ba	No error (0)	js.hscollectedforms.net		104.17.131.171	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.605622053 CEST	8.8.8.8	192.168.2.3	0x11ba	No error (0)	js.hscollectedforms.net		104.17.130.171	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.605622053 CEST	8.8.8.8	192.168.2.3	0x11ba	No error (0)	js.hscollectedforms.net		104.17.128.171	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.625277042 CEST	8.8.8.8	192.168.2.3	0xee2a	No error (0)	api.getdrip.com		13.224.99.3	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.625277042 CEST	8.8.8.8	192.168.2.3	0xee2a	No error (0)	api.getdrip.com		13.224.99.13	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.625277042 CEST	8.8.8.8	192.168.2.3	0xee2a	No error (0)	api.getdrip.com		13.224.99.49	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.625277042 CEST	8.8.8.8	192.168.2.3	0xee2a	No error (0)	api.getdrip.com		13.224.99.82	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.852085114 CEST	8.8.8.8	192.168.2.3	0x63b1	No error (0)	x.clearbit.com		18.134.49.160	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.852085114 CEST	8.8.8.8	192.168.2.3	0x63b1	No error (0)	x.clearbit.com		18.168.223.221	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 02:52:47.854733944 CEST	8.8.8.8	192.168.2.3	0x92ff	No error (0)	api.exchangeratesapi.io		104.26.8.91	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.854733944 CEST	8.8.8.8	192.168.2.3	0x92ff	No error (0)	api.exchangeratesapi.io		172.67.74.213	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.854733944 CEST	8.8.8.8	192.168.2.3	0x92ff	No error (0)	api.exchangeratesapi.io		104.26.9.91	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.856849909 CEST	8.8.8.8	192.168.2.3	0x3769	No error (0)	rs.fullstory.com		35.186.194.58	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.903727055 CEST	8.8.8.8	192.168.2.3	0xb96b	No error (0)	ob.cheqzone.com		13.224.99.100	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.903727055 CEST	8.8.8.8	192.168.2.3	0xb96b	No error (0)	ob.cheqzone.com		13.224.99.93	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.903727055 CEST	8.8.8.8	192.168.2.3	0xb96b	No error (0)	ob.cheqzone.com		13.224.99.27	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.903727055 CEST	8.8.8.8	192.168.2.3	0xb96b	No error (0)	ob.cheqzone.com		13.224.99.105	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.940283060 CEST	8.8.8.8	192.168.2.3	0x9603	No error (0)	www.redditstatic.com	reddit.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:47.940283060 CEST	8.8.8.8	192.168.2.3	0x9603	No error (0)	reddit.map.fastly.net		151.101.1.140	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.940283060 CEST	8.8.8.8	192.168.2.3	0x9603	No error (0)	reddit.map.fastly.net		151.101.65.140	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.940283060 CEST	8.8.8.8	192.168.2.3	0x9603	No error (0)	reddit.map.fastly.net		151.101.129.140	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.940283060 CEST	8.8.8.8	192.168.2.3	0x9603	No error (0)	reddit.map.fastly.net		151.101.193.140	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.959450960 CEST	8.8.8.8	192.168.2.3	0x29dc	No error (0)	m.servedby-buysellads.com	monetization-framework.bsa.netdna-cdn.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:47.959450960 CEST	8.8.8.8	192.168.2.3	0x29dc	No error (0)	monetization-framework.bsa.netdna-cdn.com		108.161.189.78	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:47.963596106 CEST	8.8.8.8	192.168.2.3	0x5e44	No error (0)	cdn.pdst.fm		35.244.142.80	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.125464916 CEST	8.8.8.8	192.168.2.3	0xcfe	No error (0)	acdn.adnxs.com	prod.appnexus.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:48.125464916 CEST	8.8.8.8	192.168.2.3	0xcfe	No error (0)	prod.appnexus.map.fastly.net		151.101.1.108	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.125464916 CEST	8.8.8.8	192.168.2.3	0xcfe	No error (0)	prod.appnexus.map.fastly.net		151.101.65.108	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.125464916 CEST	8.8.8.8	192.168.2.3	0xcfe	No error (0)	prod.appnexus.map.fastly.net		151.101.129.108	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.125464916 CEST	8.8.8.8	192.168.2.3	0xcfe	No error (0)	prod.appnexus.map.fastly.net		151.101.193.108	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.317331076 CEST	8.8.8.8	192.168.2.3	0x4c6f	No error (0)	client.mutinycdn.com		13.224.99.6	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.317331076 CEST	8.8.8.8	192.168.2.3	0x4c6f	No error (0)	client.mutinycdn.com		13.224.99.113	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.317331076 CEST	8.8.8.8	192.168.2.3	0x4c6f	No error (0)	client.mutinycdn.com		13.224.99.18	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.317331076 CEST	8.8.8.8	192.168.2.3	0x4c6f	No error (0)	client.mutinycdn.com		13.224.99.108	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.334353924 CEST	8.8.8.8	192.168.2.3	0xca10	No error (0)	vars.hotjar.com		13.224.99.33	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 02:52:48.334353924 CEST	8.8.8.8	192.168.2.3	0xca10	No error (0)	vars.hotjar.com		13.224.99.30	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.334353924 CEST	8.8.8.8	192.168.2.3	0xca10	No error (0)	vars.hotjar.com		13.224.99.109	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.334353924 CEST	8.8.8.8	192.168.2.3	0xca10	No error (0)	vars.hotjar.com		13.224.99.12	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.430783033 CEST	8.8.8.8	192.168.2.3	0x94d3	No error (0)	api-v2.mutinyhq.io	gentle-meadow-3800.shrouded-lake-4691.herokuspace.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:48.430783033 CEST	8.8.8.8	192.168.2.3	0x94d3	No error (0)	gentle-meadow-3800.shrouded-lake-4691.herokuspace.com		50.112.148.251	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.430783033 CEST	8.8.8.8	192.168.2.3	0x94d3	No error (0)	gentle-meadow-3800.shrouded-lake-4691.herokuspace.com		34.210.130.159	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.587496996 CEST	8.8.8.8	192.168.2.3	0x5448	No error (0)	t.co		104.244.42.133	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.587496996 CEST	8.8.8.8	192.168.2.3	0x5448	No error (0)	t.co		104.244.42.197	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.587496996 CEST	8.8.8.8	192.168.2.3	0x5448	No error (0)	t.co		104.244.42.5	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.587496996 CEST	8.8.8.8	192.168.2.3	0x5448	No error (0)	t.co		104.244.42.69	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.653606892 CEST	8.8.8.8	192.168.2.3	0x5a92	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:48.653606892 CEST	8.8.8.8	192.168.2.3	0x5a92	No error (0)	star-mini.c10r.facebook.com		157.240.17.35	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.927558899 CEST	8.8.8.8	192.168.2.3	0x484b	No error (0)	googleads.g.doubleclick.net		172.217.168.2	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.954720974 CEST	8.8.8.8	192.168.2.3	0x8f97	No error (0)	alb.reddit.com	reddit.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:48.954720974 CEST	8.8.8.8	192.168.2.3	0x8f97	No error (0)	reddit.map.fastly.net		151.101.1.140	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.954720974 CEST	8.8.8.8	192.168.2.3	0x8f97	No error (0)	reddit.map.fastly.net		151.101.65.140	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.954720974 CEST	8.8.8.8	192.168.2.3	0x8f97	No error (0)	reddit.map.fastly.net		151.101.129.140	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.954720974 CEST	8.8.8.8	192.168.2.3	0x8f97	No error (0)	reddit.map.fastly.net		151.101.193.140	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.997229099 CEST	8.8.8.8	192.168.2.3	0xdc70	No error (0)	ib.adnxs.com	g.geogslb.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:48.997229099 CEST	8.8.8.8	192.168.2.3	0xdc70	No error (0)	g.geogslb.com	ib.anycast.adnxs.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:48.997229099 CEST	8.8.8.8	192.168.2.3	0xdc70	No error (0)	ib.anycast.adnxs.com		185.33.220.244	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.997229099 CEST	8.8.8.8	192.168.2.3	0xdc70	No error (0)	ib.anycast.adnxs.com		185.33.220.240	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.997229099 CEST	8.8.8.8	192.168.2.3	0xdc70	No error (0)	ib.anycast.adnxs.com		185.33.221.50	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.997229099 CEST	8.8.8.8	192.168.2.3	0xdc70	No error (0)	ib.anycast.adnxs.com		185.33.221.87	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.997229099 CEST	8.8.8.8	192.168.2.3	0xdc70	No error (0)	ib.anycast.adnxs.com		185.33.221.90	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 02:52:48.997229099 CEST	8.8.8.8	192.168.2.3	0xdc70	No error (0)	ib.anycast .adnxs.com		185.33.220.242	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.997229099 CEST	8.8.8.8	192.168.2.3	0xdc70	No error (0)	ib.anycast .adnxs.com		185.33.220.241	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:48.997229099 CEST	8.8.8.8	192.168.2.3	0xdc70	No error (0)	ib.anycast .adnxs.com		185.33.221.91	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:49.016273975 CEST	8.8.8.8	192.168.2.3	0x9b3	No error (0)	forms.hubs pot.com		104.19.155.83	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:49.016273975 CEST	8.8.8.8	192.168.2.3	0x9b3	No error (0)	forms.hubs pot.com		104.19.154.83	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:49.063577890 CEST	8.8.8.8	192.168.2.3	0x1c59	No error (0)	us-central1-adaptive-growth.cl oudfunctions.net		216.239.36.54	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.023077011 CEST	8.8.8.8	192.168.2.3	0x5f4	No error (0)	obs.cheqzo ne.com		3.227.190.204	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.023077011 CEST	8.8.8.8	192.168.2.3	0x5f4	No error (0)	obs.cheqzo ne.com		52.45.196.192	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.023077011 CEST	8.8.8.8	192.168.2.3	0x5f4	No error (0)	obs.cheqzo ne.com		50.16.211.97	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.023077011 CEST	8.8.8.8	192.168.2.3	0x5f4	No error (0)	obs.cheqzo ne.com		34.199.234.25	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.023077011 CEST	8.8.8.8	192.168.2.3	0x5f4	No error (0)	obs.cheqzo ne.com		54.83.110.109	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.023077011 CEST	8.8.8.8	192.168.2.3	0x5f4	No error (0)	obs.cheqzo ne.com		35.172.245.152	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.028353930 CEST	8.8.8.8	192.168.2.3	0xc9b3	No error (0)	px.steelho usemedia.com		52.10.121.135	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.028353930 CEST	8.8.8.8	192.168.2.3	0xc9b3	No error (0)	px.steelho usemedia.com		44.237.157.168	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.028353930 CEST	8.8.8.8	192.168.2.3	0xc9b3	No error (0)	px.steelho usemedia.com		54.245.46.233	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.028353930 CEST	8.8.8.8	192.168.2.3	0xc9b3	No error (0)	px.steelho usemedia.com		44.225.29.129	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.028353930 CEST	8.8.8.8	192.168.2.3	0xc9b3	No error (0)	px.steelho usemedia.com		54.244.159.189	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.201508045 CEST	8.8.8.8	192.168.2.3	0xcf5d	No error (0)	forms.hsfo rms.com		104.16.86.5	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.201508045 CEST	8.8.8.8	192.168.2.3	0xcf5d	No error (0)	forms.hsfo rms.com		104.16.85.5	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.201508045 CEST	8.8.8.8	192.168.2.3	0xcf5d	No error (0)	forms.hsfo rms.com		104.16.87.5	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.201508045 CEST	8.8.8.8	192.168.2.3	0xcf5d	No error (0)	forms.hsfo rms.com		104.16.88.5	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.201508045 CEST	8.8.8.8	192.168.2.3	0xcf5d	No error (0)	forms.hsfo rms.com		104.16.89.5	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.478393078 CEST	8.8.8.8	192.168.2.3	0x4ded	No error (0)	stats.g.do ubleclick.net	stats.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:50.478393078 CEST	8.8.8.8	192.168.2.3	0x4ded	No error (0)	stats.l.do ubleclick.net		108.177.126.156	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.478393078 CEST	8.8.8.8	192.168.2.3	0x4ded	No error (0)	stats.l.do ubleclick.net		108.177.126.157	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.478393078 CEST	8.8.8.8	192.168.2.3	0x4ded	No error (0)	stats.l.do ubleclick.net		108.177.126.155	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 02:52:50.478393078 CEST	8.8.8.8	192.168.2.3	0x4ded	No error (0)	stats.l.doubleclick.net		108.177.126.154	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.490376949 CEST	8.8.8.8	192.168.2.3	0x48cf	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:50.496829033 CEST	8.8.8.8	192.168.2.3	0xd8e4	No error (0)	www.google.de		172.217.168.3	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:54.374402046 CEST	8.8.8.8	192.168.2.3	0x80c6	No error (0)	ww.steelhousemedia.com		44.238.216.23	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:54.374402046 CEST	8.8.8.8	192.168.2.3	0x80c6	No error (0)	ww.steelhousemedia.com		44.238.130.186	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:55.807744026 CEST	8.8.8.8	192.168.2.3	0x82d9	No error (0)	in.hotjar.com	in-live.live.eks.hotjar.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:55.807744026 CEST	8.8.8.8	192.168.2.3	0x82d9	No error (0)	in-live.live.eks.hotjar.com		63.32.233.146	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:55.807744026 CEST	8.8.8.8	192.168.2.3	0x82d9	No error (0)	in-live.live.eks.hotjar.com		54.78.108.238	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:55.807744026 CEST	8.8.8.8	192.168.2.3	0x82d9	No error (0)	in-live.live.eks.hotjar.com		54.77.167.46	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:55.807744026 CEST	8.8.8.8	192.168.2.3	0x82d9	No error (0)	in-live.live.eks.hotjar.com		99.81.27.250	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:55.807744026 CEST	8.8.8.8	192.168.2.3	0x82d9	No error (0)	in-live.live.eks.hotjar.com		99.81.42.58	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:55.807744026 CEST	8.8.8.8	192.168.2.3	0x82d9	No error (0)	in-live.live.eks.hotjar.com		54.75.159.38	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:55.807744026 CEST	8.8.8.8	192.168.2.3	0x82d9	No error (0)	in-live.live.eks.hotjar.com		52.49.237.17	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:55.807744026 CEST	8.8.8.8	192.168.2.3	0x82d9	No error (0)	in-live.live.eks.hotjar.com		52.213.131.161	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:56.102420092 CEST	8.8.8.8	192.168.2.3	0xe2bb	No error (0)	insight.adsrvr.org	insight-566961044.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:56.102420092 CEST	8.8.8.8	192.168.2.3	0xe2bb	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		52.50.64.214	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:56.102420092 CEST	8.8.8.8	192.168.2.3	0xe2bb	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		99.80.189.193	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:56.102420092 CEST	8.8.8.8	192.168.2.3	0xe2bb	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		34.254.108.170	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:56.102420092 CEST	8.8.8.8	192.168.2.3	0xe2bb	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		34.254.127.126	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:56.102420092 CEST	8.8.8.8	192.168.2.3	0xe2bb	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		52.31.175.99	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:56.102420092 CEST	8.8.8.8	192.168.2.3	0xe2bb	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		54.77.48.133	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:56.102420092 CEST	8.8.8.8	192.168.2.3	0xe2bb	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		34.255.138.57	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 02:52:56.102420092 CEST	8.8.8.8	192.168.2.3	0xe2bb	No error (0)	insight-56 6961044.eu-west-1.el b.amazonaw s.com		52.213.189.245	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:56.108792067 CEST	8.8.8.8	192.168.2.3	0x8458	No error (0)	match.adsrvr.org	match-aga.adsrvr.org		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:56.108792067 CEST	8.8.8.8	192.168.2.3	0x8458	No error (0)	match-aga. adsrvr.org	a97adde81b00f2ca4.awsg lobalaccelerator.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:56.108792067 CEST	8.8.8.8	192.168.2.3	0x8458	No error (0)	a97adde81b 00f2ca4.aw sglobalacc elerator.com		13.248.242.197	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:56.108792067 CEST	8.8.8.8	192.168.2.3	0x8458	No error (0)	a97adde81b 00f2ca4.aw sglobalacc elerator.com		76.223.111.131	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:56.115195990 CEST	8.8.8.8	192.168.2.3	0x400f	No error (0)	clickup.com		13.224.99.47	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:56.115195990 CEST	8.8.8.8	192.168.2.3	0x400f	No error (0)	clickup.com		13.224.99.125	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:56.115195990 CEST	8.8.8.8	192.168.2.3	0x400f	No error (0)	clickup.com		13.224.99.13	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:56.115195990 CEST	8.8.8.8	192.168.2.3	0x400f	No error (0)	clickup.com		13.224.99.46	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:57.462811947 CEST	8.8.8.8	192.168.2.3	0x1897	No error (0)	widget.int ercom.io		13.224.99.107	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:57.462811947 CEST	8.8.8.8	192.168.2.3	0x1897	No error (0)	widget.int ercom.io		13.224.99.33	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:57.462811947 CEST	8.8.8.8	192.168.2.3	0x1897	No error (0)	widget.int ercom.io		13.224.99.10	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:57.462811947 CEST	8.8.8.8	192.168.2.3	0x1897	No error (0)	widget.int ercom.io		13.224.99.109	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:57.533782959 CEST	8.8.8.8	192.168.2.3	0x6379	No error (0)	analytics. twitter.com	ads.twitter.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:57.533782959 CEST	8.8.8.8	192.168.2.3	0x6379	No error (0)	ads.twitter.com	s.twitter.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:52:57.533782959 CEST	8.8.8.8	192.168.2.3	0x6379	No error (0)	s.twitter.com		104.244.42.67	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:57.533782959 CEST	8.8.8.8	192.168.2.3	0x6379	No error (0)	s.twitter.com		104.244.42.3	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:57.533782959 CEST	8.8.8.8	192.168.2.3	0x6379	No error (0)	s.twitter.com		104.244.42.131	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:57.533782959 CEST	8.8.8.8	192.168.2.3	0x6379	No error (0)	s.twitter.com		104.244.42.195	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:57.574112892 CEST	8.8.8.8	192.168.2.3	0xbfc5	No error (0)	track.hubs pot.com		104.19.154.83	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:57.574112892 CEST	8.8.8.8	192.168.2.3	0xbfc5	No error (0)	track.hubs pot.com		104.19.155.83	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:57.773173094 CEST	8.8.8.8	192.168.2.3	0x1bb9	No error (0)	js.interco mcdn.com		13.224.99.12	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:57.773173094 CEST	8.8.8.8	192.168.2.3	0x1bb9	No error (0)	js.interco mcdn.com		13.224.99.116	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:57.773173094 CEST	8.8.8.8	192.168.2.3	0x1bb9	No error (0)	js.interco mcdn.com		13.224.99.75	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:57.773173094 CEST	8.8.8.8	192.168.2.3	0x1bb9	No error (0)	js.interco mcdn.com		13.224.99.60	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 02:52:59.273031950 CEST	8.8.8.8	192.168.2.3	0x4b3e	No error (0)	api-iam.intercom.io		99.83.219.81	A (IP address)	IN (0x0001)
Jul 22, 2021 02:52:59.273031950 CEST	8.8.8.8	192.168.2.3	0x4b3e	No error (0)	api-iam.intercom.io		75.2.88.188	A (IP address)	IN (0x0001)
Jul 22, 2021 02:53:00.311500072 CEST	8.8.8.8	192.168.2.3	0x1381	No error (0)	nexus-websocket-a.intercom.io		35.170.0.145	A (IP address)	IN (0x0001)
Jul 22, 2021 02:53:00.311500072 CEST	8.8.8.8	192.168.2.3	0x1381	No error (0)	nexus-websocket-a.intercom.io		35.174.127.31	A (IP address)	IN (0x0001)
Jul 22, 2021 02:53:00.311500072 CEST	8.8.8.8	192.168.2.3	0x1381	No error (0)	nexus-websocket-a.intercom.io		34.237.73.95	A (IP address)	IN (0x0001)
Jul 22, 2021 02:53:00.839313984 CEST	8.8.8.8	192.168.2.3	0x2314	No error (0)	clockify.me		13.224.99.4	A (IP address)	IN (0x0001)
Jul 22, 2021 02:53:00.839313984 CEST	8.8.8.8	192.168.2.3	0x2314	No error (0)	clockify.me		13.224.99.77	A (IP address)	IN (0x0001)
Jul 22, 2021 02:53:00.839313984 CEST	8.8.8.8	192.168.2.3	0x2314	No error (0)	clockify.me		13.224.99.23	A (IP address)	IN (0x0001)
Jul 22, 2021 02:53:00.839313984 CEST	8.8.8.8	192.168.2.3	0x2314	No error (0)	clockify.me		13.224.99.108	A (IP address)	IN (0x0001)
Jul 22, 2021 02:53:03.633775949 CEST	8.8.8.8	192.168.2.3	0x1966	No error (0)	px.ads.linkedin.com	mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:53:03.633775949 CEST	8.8.8.8	192.168.2.3	0x1966	No error (0)	mix.linkedin.com	glb-na.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:53:03.633775949 CEST	8.8.8.8	192.168.2.3	0x1966	No error (0)	glb-na.mix.linkedin.com	pop-edc2.mix.linkedin.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:53:03.633775949 CEST	8.8.8.8	192.168.2.3	0x1966	No error (0)	pop-edc2.mix.linkedin.com		108.174.11.85	A (IP address)	IN (0x0001)
Jul 22, 2021 02:53:11.518222094 CEST	8.8.8.8	192.168.2.3	0x304d	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:53:32.453568935 CEST	8.8.8.8	192.168.2.3	0xc7e0	No error (0)	insight.adsrvr.org	insight-566961044.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 02:53:32.453568935 CEST	8.8.8.8	192.168.2.3	0xc7e0	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		34.255.138.57	A (IP address)	IN (0x0001)
Jul 22, 2021 02:53:32.453568935 CEST	8.8.8.8	192.168.2.3	0xc7e0	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		52.31.175.99	A (IP address)	IN (0x0001)
Jul 22, 2021 02:53:32.453568935 CEST	8.8.8.8	192.168.2.3	0xc7e0	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		99.80.189.193	A (IP address)	IN (0x0001)
Jul 22, 2021 02:53:32.453568935 CEST	8.8.8.8	192.168.2.3	0xc7e0	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		34.254.108.170	A (IP address)	IN (0x0001)
Jul 22, 2021 02:53:32.453568935 CEST	8.8.8.8	192.168.2.3	0xc7e0	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		34.254.127.126	A (IP address)	IN (0x0001)
Jul 22, 2021 02:53:32.453568935 CEST	8.8.8.8	192.168.2.3	0xc7e0	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		52.50.64.214	A (IP address)	IN (0x0001)
Jul 22, 2021 02:53:32.453568935 CEST	8.8.8.8	192.168.2.3	0xc7e0	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		52.30.148.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 02:53:32.453568935 CEST	8.8.8.8	192.168.2.3	0xc7e0	No error (0)	insight-566961044.eu-west-1.elb.amazonaws.com		52.213.189.245	A (IP address)	IN (0x0001)

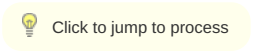
HTTP Request Dependency Graph

- mega-sharedrives.club

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 5712 Parent PID: 2844

General

Start time:	02:52:18
Start date:	22/07/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://doc.clickup.com/p/h/c0hgx-46/b302180a8f685f8'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 3484 Parent PID: 5712

General

Start time:	02:52:19
Start date:	22/07/2021

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=1576,9348279836173803146,15535106751469244526,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1700 /prefetch:8
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Disassembly